Helmut Seidl, Christin Seifert (editors)

Proceedings of the 2023 Joint Workshop of the German Research Training Groups in Computer Science

June 4–June 7, 2023

DFG Deutsche Forschungsgemeinschaft

Publishing institution:
Universität Duisburg-Essen
Universitätsbibliothek, DuEPublico
Universitätsstraße 9-11
45141 Essen
https://duepublico2.uni-due.de

Bibliographic Data:

Christin Seifert, Helmut Seidl (eds.): Proceedings of the 2023 Joint Workshop German Research Training Groups in Computer Science. 2023. DOI: 10.17185/duepublico/78280

Preface

For the 27th year, the annual Joint meeting Of the German Research Training Groups funded by the Deutsche Forschungsgemeinschaft (DFG) in the field of computer science took place at Schloss Dagstuhl – Leibniz Center for Informatics. Schloss Dagstuhl is one of the world's premier venues for computer science-related seminars.

The aim of the meeting is to interactively exchange research results, ideas, and experiences in order to strengthen the German computer science community, also across different levels of seniority. This volume documents the abstracts of the research topics of funded researchers in the participating RTGs.

The event was jointly organized by RTG 2428 (ConVeY — Continuous Verification of Cyber-Physical Systems) and RTG 2535 (WisPerMed – Wissens- und datenbasierte Personalisierung von Medizin am Point of Care). It took place from Sunday, June 4 to Wednesday, June 7, 2023 (Dagstuhl event number 23233). The meeting consisted of a balanced mixed of research presentations, a project ideation workshop, a poster session and session where junior research could ask senior researchers "anything you always wanted to know about research and a research career". Additionally, two keynotes on current important topics in computer science were organised: Prof. Thomas Huckle showcased *Software Desasters* and their prevention, and Johannes Köster advocated for *Reproducibility* in Research.

The organisers would like to thank all participants for their contribution to a successful and insightful event in an open and welcoming atmosphere.

München/Essen/Marburg, May 4, 2023 Helmut Seidl and Christin Seifert

Contents

GRK 2050: Privacy and Trust for Mobile Users

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

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

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

Privacy and trust are not yet commonly perceived as paired, i.e., tightly interwoven necessities for making the Internet (and networks in general) a liveable digital habitat. This is in part due to a somewhat misleading use of the term trust in cybersecurity research: fields like trusted computing, trustworthy ICT, and trust management refer to issues of reliability-plus-security, tamper-free hard- and software, and digital identities, respectively – all quite remote from the primary meaning of the term trust. Our RTG fosters research into trust in its primary meaning: justified readiness to engage in a risky engagement, with risks including privacy violations and other negative experience with service provision. An important area of our trust research is *computational trust*, where trust is formalized as the probability of a trustee acting as expected; expectations in turn are justified from two categories of evidence: experience (own prior experience, reputation) and indicators (certified audit results, attestations, etc.). Since trust assessment relies on evidence, i.e., information about the trustee, there is a potential conflict: trust aims at revealing what privacy aims at concealing: information about an entity. This is relevant if trusters and trustees do not form two distinct sets (cf. social network participants and agents in peer-to-peer economies). In the RTG, privacy related research is (at least) as prominent as research on trust. Due to their interweaving, we are addressing both aspects jointly in our research areas, structuring our RTG according to the above-mentioned network categories: (social) collectives, service networks, and sensor networks in form of the 'IoT' – with an additional focus area emphasizing novel mobile user support.

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

Scalable Application of Secure Multi-Party Computation

Andreas Brüggemann (brueggemann@encrypto.cs.tu-darmstadt.de)
Supervisor: Prof. Dr.-Ing. Thomas Schneider

Data collection has risen to unprecedented levels. Especially mobile devices enable to gather large quantities of user data which can be of interest, e.g., for training machine learning (ML) models in the health, finance or insurance sector. Simultaneously, users are becoming more aware and concerned about collection and use of their private data, and legislation like the General Data Protection Regulation (GDPR) restricts which and how personal data can be used. Thus, new mechanisms become necessary that allow to profit from access to a wide collection of data while also protecting the users from undue data usage, providing transparency on how their data is used and satisfying statutory provisions.

Secure multi-party computation (MPC) is a cryptographic technique that allows multiple parties to compute some fixed function on their private input data without requiring any party to disclose any of its private information. Thus, MPC can be used to process data from different users while keeping everything but the result of the publicly known function private. Such privacy guarantee does not come for free. Instead, the used cryptographic primitives often drastically decrease overall scalability rendering the processing of large data sets difficult or even unfeasible.

We identify use cases that strongly benefit from using large sets of sensitive data from different users and then build according MPC solutions tailored to maximise efficiency and scalability. In addition, we identify wider fields and work on the development of more generic building blocks which simplify the later construction of more specific protocols which also increases the general applicability of MPC. We focus on two general directions. First, we work on increasing the scalability of MPC solutions for machine learning tasks. These have received large interest for a multitude of use cases while the current scalability of such approaches remains limited. Second, revisiting graph problems while keeping privacy in mind yields multiple opportunities for MPC protocols as has been demonstrated, e.g., for contact tracing.[1] We have already proposed a novel graph-based protocol that can match users for, e.g., multi-party bartering or online dating, in a privacy-preserving manner[2] as well as an optimized shuffling mechanism[3] which improves the prior state-of-the-art graph analysis approach[1].

[1] T. Araki, J. Furukawa, K. Ohara, B. Pinkas, H. Rosemarin, and H. Tsuchida, "Secure Graph Analysis at Scale," Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS'21), p. 610–629, 2021

[2] A. Brüggemann, M. Breuer, A. Klinger, T. Schneider, and U. Meyer, "Secure Maximum Weight Matching Approximation on General Graphs," Proceedings of the 21st Workshop on Privacy in the Electronic Society, p. 83–87, 2022

[3] A. Brüggemann, T. Schneider, A. Suresh, and H. Yalame, "Poster: Efficient Three-Party Shuffling Using Precomputation," CCS'22, p. 3331–3333, 2022

Paving the Way Towards the Adoption of Artificial Intelligence - A Trust Perspective

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

Recent advances in digitization and the availability of high volume of data have led to higher interest and usage of artificial intelligence (AI). The enormous potential of AI performing tasks previously preserved for humans and its ability to be applicable in a variety of contexts have made it one of the most important general-purpose technologies of our time. Thus, AI and especially machine learning methods are increasingly influencing and improving many areas of our lives (e.g. medical diagnosis, autonomous driving, digital voice assistants). However, the complexity of AI, its non-deterministic behavior and inscrutability have also raised concerns. AI-based systems are often perceived as black boxes whose inner logic cannot be explained, thus making it difficult to predict the outcome of these systems. This is particularly critical with regard to automated decision processes, where decisions are delegated completely or partially to a machine or system. Thus, even AI-based applications may be outstanding in their performance, distrust towards AI persists.

Trust is a multi-faced concept that has been examined in various disciplines. It helps to overcome perceived uncertainties and risks, especially in unfamiliar situations. Trust has been identified as a decisive factor influencing the adoption and continuous usage of technologies including AI.

This project investigates relevant factors for the organizational adoption and usage of AI-based technologies as well as relevant concepts and dimensions of trust for the initial adoption and continuous usage of AI-based systems.

Procedural Requirements in the General Data Protection Regulation

Loïc Reissner (reissner@jur.uni-frankfurt.de)
Supervisor: Prof. Dr. Indra Spiecker gen. Döhmann

The GDPR forms the law framework for data processing. It contains the approach "procedure against content" for example to enable the processing of data of special categories, like health data. So when we take back the "Content-rule", for example a total ban of processing, there still has to be "enough" data protection. And this should be guaranteed through rules of procedure. Those procedural rules must be implementable for processors. Therefor we need generalized standards so that this can result in cost-effective data-protection.

Procedural law is considered to be the counterpart to substantive law.[1] But how do these two counterparts interact with each other? How far is it possible to ensure material legal requirements through rules of procedure? These general questions are particularly important in view of the GDPR. Namely, the GDPR contains several rules that enable the compensation of substantive law through "technical and organizational measures", e.g., in Art. 5 para. 1 lit. e), Art. 24 para. 1, 25 para. 1, 2 GDPR. Moreover, opening clauses grant a margin in implementation for the member states. Objective of the thesis in Research Area A.4 is an examination of the procedural requirements for the protection of personal data and whether there are standards for rules of procedure to ensure material requirements. For companies as data processors, the findings may provide leeway for the development of new technologies or risky data processing instead of a complete ban of such procedures.

The examination is particularly important seen the uprising role of private companies as processors. Earlier, it was the state who was the biggest processor. Nowadays, a focus has to be added on the private processors. The risk-based approach in the GDPR not may provide leeway; nevertheless, data subjects have to be protected. A critical examination has to take place, whether this can be achieved by the current approach of "regulated self-regulation"[2] of the GDPR. In this context, also the role of the data protection authorities is of particular importance. Examples from the practice show, that this might lead to other – structural – problems within the European supervisory-mechanism.

A focus is set on getting an overview of the different data protection rules dealing with procedural requirements. Thus, different norms of the GDPR were examined. A focus was then laid on the data protection impact assessment (Art. 34 GDPR), but also on the general Art. 6 para. 1 lit. f) GDPR, being a key-norm for the risk-based approach in the GDPR. Also the Data Protection Officer should be subject of the examination as this position is highly relevant for many processors.

Another focus is to examine, whether it is possible to draw values directly from the GDPR. The examination showed, that there are nearly no concrete clues within the GDPR that can be used for that.

Another point is the examination about the core of the fundamental right of data protection in Art. 7, 8 GRC, Art. 8 EMRK and Art. 16 AEUV. That followed an examination of elements

[1] Reimer, Verfahrenstheorie, p. 68.

[2] To other instruments of the "regulated self-regulation" see Stürmer, Regulierte Selbstregulierung im europäischen Datenschutzrecht.

that influence the depth of an intervention in the fundamental right of data protection. Here, a clear distinction has to be made between risks resulting through a huge number of data subjects concerned and a high risk resulting of, e.g., the sensitivity of the data collected from only one data subject.

The current work will be pursued to develop standards for rules of procedure. Therefore, much effort has to be put in the analysis of procedural rules. It has to be examined, which concrete effect, e.g., organizational measures do have in practice on the processing and like that, what this means for the rights of the data subject.

Trust is Good, Algorithms are Better? Social Media and the Modelling of Functional Platform Ecosystems

Florian Müller (florian.mueller@uni-kassel.de)
Supervisor: Prof. Dr. Jörn Lamla

In the course of the last 20 years, social media platforms have become enmeshed in virtually all aspects of social life. Thereby, platforms are not just neutral mediators or intermediaries, but rather economically driven companies, who increasingly decide, organize and structure under what conditions we act, communicate, conduct relationships, consume content and make transactions. This makes platform companies very central and powerful actors in the orchestration and regulation of sociality and at the same time raises questions and debates about the regulation, governance and trustworthiness of these platforms.

With regard to non-transparent structures, data scandals, manipulation and the like, the trustworthiness of social media platforms or platform companies is repeatedly called into question. At the same time, it is very important for social media platforms to secure the trust of users and other actor groups, that is necessary for the use and functionality of the platform. Trust thus becomes in various respects a very central yardstick for the negotiation of digital transformation processes and presents a crucial condition for the success of platform companies, a central 'problem area', which they try to deal with and solve through various (platform-specific) coordination and regulation arrangements.

This is particularly evident - as I will be elaborating on in my thesis - in algorithmic procedures on social media platforms. More and more processes on social media platforms are coordinated and regulated by complex networks of algorithms, and more and more decisions are made and legitimized by and within the framework of algorithmic processes. On the one hand, platform algorithms thus deal with and solve various trust problems, for example by assisting platform users in assessing trustworthiness or by performing various regulating and controlling functions related to the fulfillment of certain normative trust expectations. On the other hand, with regard to non-transparent calculation processes, bias, manipulation and discrimination, they are themselves sources of trust problems.

In order to capture and examine this ambiguity of platform algorithms, the main goal of my PhD thesis is to examine the role of algorithms in generating and substituting trust for securing the functionality of social media platform companies' services. For this purpose, the thesis is structured into three main sections, in which theoretical and empirical aspects are continuously interlinked to address specific dimensions of the objective.

From an empirical point of view, the focus is primarily on the social media platform "YouTube". Like other 'big' social media platforms, YouTube's history does not only appear as a one of success and increasing influence, but also as a story in which the platform company has been confronted with many different challenges and trust problems. In this context, YouTube is interpreted as both a typical and a special social media platform and thus serves as a case which is compared and contrasted with other social media platforms and in relation to which various theories and arguments are discussed and developed in the three sections.

The central issue of the first section is the development of the so-called heuristic of the trust problem. In conjunction with the primarily social science research landscape on the trust phenomenon, a perspective is developed, that frames trust as a type of problem that needs to be addressed by designers of social order to activate diverse functions attributed to trust. With respect to social media platform ecosystems, this perspective thus serves to highlight structural

conditions of the functionality of these ecosystems, to reinterpret them as specific trust problems, and to elaborate on them in terms of their significance for the algorithmic.

Subsequently, the following two sections will deal with the question of how social media platform companies deal with trust problems by generating and substituting trust. For this purpose, the so-called trust problem is first interpreted as a legitimation problem (section 2) and then as a coordination and governance problem (section 3), whereby both theoretically and empirically the question is addressed as to how trust and legitimation, or trust and governance, are interrelated and what role the algorithmic plays here in each case.

Thus, even though the epistemological interest is essentially focused on the algorithmic, this work is about much more than isolated technical problem-solving procedures. It is about ecosystems, about business models, about actors and groups of actors, about delegated and disappointed expectations, about patterns of legitimation and justification, and about sociotechnical constellations. It is about the algorithmic as a structurally embedded entity that unfolds in many ways and, in the course of embedding and unfolding, emerges both as a solution and as a source of trust problems.

User Empowerment Through Technical Transparency

Simon Althaus (althaus@tk.tu-darmstadt.de)
Supervisor: Prof. Dr. Max Mühlhäuser

Platform providers of large Internet services such as online social networks are known to collect large amounts of data on their users that is monetized and used to provide targeted advertising for example. The data collection of such platforms is often neither in the best interest of the users nor are users aware of the extent and impact of this data collection.

A user could exercise his right of access according to the GDPR in order to request the data that a provider has on the user. This would yield a first insight into the user data stored at providers, however it is not guaranteed to be complete. Related work proposed transparency enhancing tools (TETs) that try to make the user aware of this data collection on mobile devices. On the one hand, this previous work mainly focused on the network view of data collection instead of directly looking at what's happening on the device level. Some work also looked at discrepancies between this network data collection and privacy policy statements. On the other hand, previous work considered the potential data collection as identified by the granted and accessed permission of applications. However, this only reveals what data apps could have accessed in the worst case, not what was actually collected and is subsequently used by platform providers.

As such, current approaches like TETs are still lacking in the completeness of information gathered and in illustrating implications of what platform providers can do with such information. Thus, this subproject B.2 of the Research Training Group (RTG) 2050 focuses on empowering users by increasing the transparency of this data collection by platform providers on mobile devices. Among the expected benefits of this approach in comparison to previous work are a more complete view of the gathered information on users and the potential to provide explanations on observations how derived data is used, e.g., for targeted advertising. Also, the support for more recent versions of smartphone operating systems is achieved.

For this, a TET is proposed that utilizes information from different scopes: First, by adopting an approach from the insider detection domain, we discover what data is collected on a low-level of the operating system, whether this data collection is (ab)normal and with whom this information is potentially shared. Second, on the application level, shadow profiles are created that depict what information a service provider has collected from a user. Third, the user perspective is considered to empower users by making them aware about the observed data collection of their own data. Finally, the information of different users is combined in order to simulate the platform provider's view and derive what additional information can be induced that was not apparent beforehand.

Transparency mechanisms in algorithmic contexts

Rebecca Heigl (rmheigl@wiwi.uni-frankfurt.de)
Supervisor: Prof. Dr. Oliver Hinz

Ubiquitous application of algorithmic recommendation systems facilitated worldwide policy advances. In this context, it is important to examine in more detail how privacy is functionalized for the formation of trust by means of these very procedures or, conversely, how algorithmically secured platform trust changes the parameters of private lifestyles.

The goal is to explore how privacy and trust in hybrid constellations and in the confrontation between machine and human intelligence are variously set in relation to each other and thereby mutually stabilize and modify each other. One parameter that has not been researched is the influence of reciprocal relationships: Content and algorithms continuously adapt to their users by observing and recording their behaviour and using it as training data.

The goal of my project is threefold: First, I would like to explore the mental models of users while being in this recursive relationship with algorithmic systems. Are users aware of the connection between algorithmic accuracy and trust and are they willing to disclose more data to improve the accuracy of the algorithm? Is this a conscious and unconscious mechanism? What are the underlying mechanisms for the information processing in algorithmic contexts?

Second, I want to shed light on transparency mechanisms that enhance both trust and privacy in those contexts. What tools and training can be provided? What can platform owners do to increase trust?

Third, I plan to write a cumulative thesis where the above-mentioned questions are brought together and will be related to each other in a holistic way.

My current work concentrates on transparency mechanisms in algorithmic contexts. Recent literature explores the interaction between AI predictions and users' decision-making. However, little is known about the influence of the AI developer's identity on the acceptance or rejection of algorithmically generated predictions by users. My current study aims to fill this gap. Drawing on social identity theory to analyze how disclosing the developer identity to users impacts users' demand for and processing of algorithmic advice. A novel experimental design was developed where the developer identity was disclosed to participants in an online experiment which included 800 participants. The two popular constructs of willingness to pay (WTP) and weight on advice (WOA) operationalized information demand and processing, respectively. Moreover, the goal is to disentangle the effect attributable to expected accuracy from social identity effects. The findings of this study contribute to the literature on advice taking, algorithm aversion as well as social identity and may provide practical guidance to organizations for defining strategies that aid in the successful adoption and value creation of algorithmic applications.

One part of my work concentrates on another aspect of transparency in algorithmic contexts: Revealing discriminatory practices and offering counter measures. Machine-learning (ML) models support human decision-making in a wide range of domains. By influencing decisions, ML models often endogenously shape the data available for future model updating that aims to improve or maintain prediction accuracy. For example, a low-performance prediction entailing the rejection of a job applicant prevents a company from learning this person's actual job performance, so this data point is unavailable for future updates. Therefore, I explored the relationship between

the continuous updating of ML models and algorithmic discrimination in environments where predictions endogenously shape the creation of additional training data. Examining the dynamic evolution of a ML model's fairness and technical performance in a strategic setting that simulates sequential interactions, such as hiring and loan decisions. The results show that continuous updating can lead to a feedback loop that helps improve the performance and reduce discrimination of ML models over time. However, the results indicate that the human decision-makers, who can override ML predictions, may obstruct the process of correcting discriminatory models, and even cause initially unbiased models to become discriminatory over time. These findings emphasize the complex, socio-technological nature of algorithmic discrimination and the pivotal role that humans in the loop play in addressing it when ML models undergo repeated updating.

Finally, I have worked on one paper that revolves around the influence of information systems on the perception of stress. Many companies have introduced information and communication software to replicate on-site teamwork as closely as possible that keeps employees in close contact with the team, such as Microsoft Teams. Studies confirm that the use of technology, and thus software, is related to the perception of stress, known as technostress. So far, research has predominantly focused on the negative concept of stress, namely distress. To examine the effects of technostress creators on perceived eustress, data of 207 employees using regularly Microsoft Teams during the pandemic were collected with an online survey. The analysis reveals that the classic technostress creators are generally negatively associated with perceived eustress. However, this study shows that techno-insecurity particularly induces positive stress. Furthermore, the analysis reveals that work-home conflict and job satisfaction moderate the effects of technostress creators on perceived eustress. This work gives insights about the users' perspective, which can be valuable in further examining the mental models of information processing in recursive contexts.

ICT Use and Privacy in Low-Trust- And Safety-Critical Environments

Enno Steinbrink (steinbrink@peasec.tu-darmstadt.de)
Supervisor: Prof. Dr.Ḋr. Christian Reuter

In times of crisis or uncertainty, modern information and communication technology can be an instrument to support public or personal safety. But due to the circumstances, users can change their behavior or adapt their risk-benefit-evaluation, which can in some cases expose them to additional risks or prevent the unlocking of the full technological potential.

This PhD project addresses the question how ICT use and privacy behavior is affected in low-trust-environments (for example during crises when political, institutional or social trust can be damaged) or in safety-critical environments in which trust is of higher importance than usual (e.g., in political contexts or in the context of critical infrastructure). Often technology is designed for everyday life user contexts and similarly much of the research is dedicated to study privacy behavior in these contexts. In the past, privacy behavior was often linked to trust of the users in technology or interaction partners. Within this project, specific contexts will be studied in which this trust might be changed. In several studies different aspects of this subject will be covered:

First, I consider the smartphone use and privacy behavior in the context of flight from (civil) war, political persecution or political instability, to see how these behaviors change when refugees or asylum seekers are confronted with an immediate safety threat which can result from smartphone use. [1] Secondly, I consider how missing trust can be a hindrance for digital crisis measures and affect the adoption of crisis response apps within the civil population, using the example of contact tracing apps during the COVID-19 pandemic. Related to this, I look upon how decentralized and transparent applications can be used in crisis or critical infrastructure to exchange information and encourage collaboration. For this, prototypes are evaluated, exploring how transparent data-sharing applications should look like, for example in the context of agriculture. [2] Lastly, while researching how a more reliable privacy persona inventory could be developed, this resulted in a methodological paper, discussing the lessons learned of trying to apply a modern test construction approach, which could help to develop more reliable tests for research in the future. [3]

[1] Steinbrink, Reichert, Mende and Reuter, "Digital Privacy Perceptions of Asylum Seekers in Germany – An Empirical Study about Smartphone Usage during the Flight" Proceedings of the ACM: Human Computer Interaction (PACM): Computer-Supported Cooperative Work and Social Computing, vol. 5(CSCW2), 1–24, 2021

[2] Linsner, Steinbrink, Kuntke, Franken and Reuter, "Supporting Users in Data Disclosure Scenarios in Agriculture through Transparency" Behaviour and Information Technology (BIT), vol. 41(10), 2137–2159, 2022

[3] Biselli, Steinbrink, Herbert, Schmidbauer-Wolf and Reuter, "On the Challenges of Developing a Concise Questionnaire to Identify Privacy Personas" Proceedings on Privacy Enhancing Technologies (PoPETs), vol. 2022(4), 645–669, 2022

Privacy Risks of Human-Centric Sensor Data

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

In our world of increasingly complex computing systems it becomes more and more difficult to stay in control of the information gathered by sensors of everyday devices. An increasing number of more accurate sensors create opportunities but also possibilities to violate the privacy of users in ways they are often unaware of. In my current work I am focusing on analysing data from human-centric sensors, working on *human-targeted keylogging side-channel attacks* and *risks of user identification*.

Wearables with human-centric sensors like accelerometers or gyroscopes, but also with emerging sensors like electromyographic sensors, can be exploited to infer human actions like typing on a keyboard. In the first part of my work, I am studying the effectiveness of such side-channel attacks when using different sensor modalities in varying settings on different persons.

To study this, we collected a data corpus containing about 310000 keystrokes from 37 participants typing predefined texts and passwords. Using end-to-end machine learning we show that we are able to detect keystrokes, as well as reduce the search space for passwords[1]. To foster further research, we made the dataset, as well as the source code openly accessible.

Similarly, sensor data from wearables can also be used to derive attributes from their owners, potentially allowing the user to be identified. As part of my second research aspect, we are investigating photoplethysmogram (PPG) based inter-sensor impersonation attack on off-the-person electrocardiogram (ECG) based authentication system. Using conditional generative adversarial networks (cGAN), we transform PPG samples into impostor ECG samples in order to fool an ECG identification system. For evaluating the attack on an authentication system we are currently in the process of extending our data corpus of synchronized ECG/PPG samples.

In the future, I will continue to expand my view on both topics by stuying such side-channels under varying conditions. With this, I am pursuing the goal of making the privacy risks of using human-centric sensors more tangible and open the way for deriving defenses.

[1] "My(o) Armband Leaks Passwords: An EMG and IMU Based Keylogging Side-Channel Attack" by Matthias Gazzari, Annemarie Mattmann, Max Maass and Matthias Hollick in Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, vol. 5, Issue 4, 2021.

The compatibility of data processing by sensor-based devices in the Internet of Things with the transparency requirements of (data protection) law

Linda Seyda (linda.seyda@uni-kassel.de)
Supervisor: Prof. Dr. Gerrit Hornung, LL.M.

IoT environments like smart cities or smart cars are increasingly using more sensors that often cannot be seen with the bare eye. By now, sensors have been designed so intelligently that their capabilities sometimes exceed those of human perception. For example, the laser sensor technology of autonomous vehicles can identify parking spaces as they drive past.

The great potential of sensors is also evident in their interaction with humans: Acceleration sensors on smartphones can provide information about the driving behavior of users , so that even car drivers can be recognized by their specific driving behavior (driver fingerprinting) . Finally, even the heart function of the driver can be detected . Moreover, acceleration sensors can be used to derive extensive information about a person's location, activities, body characteristics, gender, age, personality traits and emotional state. The potential of acceleration sensors, previously considered harmless to privacy, even extends to the point where they can be used to unambiguously reconstruct sequences of text entered into a device, including passwords.

These smart sensors and the resulting intelligent data analysis open up great opportunities, but at the same time also significant risks and challenges for privacy, especially regarding data protection principles such as transparency. Therefore, a clear and universally applicable solution for user privacy is needed (legally and technically). Such a solution could be found in the development of new normative approaches and regulatory mechanisms regarding transparency. Intransparency is a problem that has been criticized since the beginning of the implementation of the IoT, and for which there is still no all-encompassing solution.
The principle of transparency (originally set up with the Census Judgment of the federal constitutional court (BVerfG) in 1983 , now fixed in Art. 5 (1) lit. a GDPR, mainly realized through the data subject's rights in Art. 12- 23 GDPR) has to be analyzed with regard to the end-user. In that context, the principle is an expression and requirement of the fundamental right to informational self-determination. Parallelly, the great amount of information in the form of privacy-policies in web-applications leads to the paradox result of over-information and fatigue of the data subject as end-user, resulting in an information-overload, what is equal to intransparency. Clearly, the situation of intransparency will be intensified if interaction between the user and the data-processing object, such as occurs with websites and mobile applications, is completely absent due to the lack of physical perceptibility of sensors, what leads to an information-gap in sensor-based-environments.

When considering the information requirements, alternative presentation options shall be developed, such as the standardized image symbols provided for in Art. 12 (7) GDPR. Since some information must be removed in order to maintain clarity, it must be assessed whether quantitatively less information can lead to a qualitative increase in transparency. Not in a way to make existing transparency regulations even stricter, but to find solutions for implementing and enforcing them legally and in fact, and to propose changes if necessary when (technical) feasibility fails.

To this end, after presenting the technical problems and the legal situation, a proposal for a Commission Regulation pursuant to Article 12 (8) of the GDPR is to be developed, which provides for the use of standardized icons for the overview-like information of the data subject. The result is a standardized data protection information document (DPID), oriented to the insurance law "insurance product information document" (IPID), based on the European IPID Regulation (COMMISSION IMPLEMENTING REGULATION (EU) 2017/1469 of 11 August 2017, Official Journal of the European Union L 209/19). Finally, it is necessary to develop how the DPID can also be implemented in sensor-based environments to provide more information to end users. In this context, it will be examined to what extent personal information management systems (PIMS), which were made possible by §§ 25 and 26 of the new Telekommunkations- und Telemedien-Datenschutz-Gesetz (TTDSG), offer a technically and practically manageable solution to facilitate the information of the data subject and thereby increase the level of transparency. It has to be elaborated, if these regulations or their underlying ideas are applicable to sensor-based IoT devices.

Privacy and Trust Enhancing Techniques for Internet-based Federation Infrastructures

Carsten Schmidt (carsten.schmidt@sit.tu-darmstadt.de)
Supervisor: Prof. Dr. Michael Waidner

Secure and private communication via the Internet has some requirements to the communication partners as well as to the Internet services and protocols. Furthermore, as attackers are also advancing, these requirements should be looked at regularly.

On the end user side, mass produced devices tend to get smaller and lose core functionality. This happens because manufacturers tend to minimalize the internal layout due to a lower production cost, but still want their product to be "smart" - controllable via the smartphone or the Internet. This leads to weak cryptography and inevitably to a loss of privacy and trust. Therefore we want to identify the bare minimum of requirements to the user devices to securely participate in the Internet. If possible, we want to suggest alternatives to standard methods if the requirements are too high or could be lifted with new approaches.

On the Internet services side, we see that some of the core infrastructures (e.g. BGP, DNS) are quite old and are unsecure already at this time. Furthermore, the deployment of new, secure services is usually slow, as the service providers don't want to exclude customers or old hardware. As a result, even security extensions to mitigate some of these problems often support the old unsecure method, which can be a problem in itself. We want to have a closer look at these core infrastructure and especially how to ensure privacy and trust while using them. Our suggestions will be in a way that new technology on either the attacker side or the end user side can be used or developed without affecting the trust model. As an example, the availability of quantum computers to the broad public, which breaks current cryptography, shouldn't be a problem to our suggestions.

As a result we'll modernize the way of communicating via the Internet to a recent technological level and also adapt to new advancements in technology.

AlterEgo as Trustworthy Device Collective

Dr. Ephraim Zimmer (zimmer@privacy-trust.tu-darmstadt.de)
Supervisor: Prof. Dr. Max Mühlhäuser

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

To achieve this goal, this subproject D.4 of our Research Training Group (RTG) follows a multi-layered approach: (1) deep and collaborative activity monitoring architecture, (2) distributed AlterEgo architecture, (3) proactive user assistance, and (4) mechanisms to protect privacy and assess trust according to dynamic constraints.

At the lowest layer 1, the lack of possibilities to assess the trust in a personal device is addressed. No matter what functionality, data, and even security or privacy mechanisms are deployed on the devices of users, if the hardware and software of those devices cannot be trusted, than the personal data is at stake. Mechanisms for deep as well as inter-device collaborative monitoring are able to assess the nature of ongoing device and network activities. As a result, among others, hidden functionalities in hardware and software can be identified and a level of trustworthiness can be established.

On layer 2 the privacy interests and rights of a user are provided and enforced accross different devices by the functionality of an AlterEgo, which acts in a distributed manner. Either agent-based or by means of an even stronger inter-connection of lower device levels than it is known nowadays, the AlterEgo is providing access to private data for third parties but at the same time keeps the control over this private data fully in the hands of the respective owner.

Layer 3 extends AlterEgo with device-local proactive assistance functionality. This functionality intends to increase the users' understanding of their actions' implications on privacy and trust and even aims at interacting on the users' behalf.

Layer 4 links this research project to the other research areas of our RTG 2050 by combining their research into a holistic AlterEgo with additional measures to flexibly assess privacy and trust, and enabling respective enforcement measurements.

GRK 2193: Adaptation Intelligence of Factories in a Dynamic and Complex Environment

Prof. Dr. Jakob Rehof
Email: sevda.tarkun@tu-dortmund.de
Internet: https://www.grk2193.tu-dortmund.de/

The Research Training Group (RTG) "Adaptation Intelligence of Factories in a Dynamic and Complex Environment" enables particularly qualified doctoral candidates from different disciplines to work on their dissertations in the field of adaptation planning of factory systems. The central research topic of RTG 2193 lies in the systematic, interdisciplinary and end-to-end support of factory system adaptation. The process of factory adaptations, which has gained in importance in the course of the dynamization of the corporate environment in recent years, comprises a multitude of tasks and complex decision-making processes, the appropriate execution of which can only be ensured by involving experts from different disciplines.

Efficient Industry Sales Forecasting

Alina Timmermann (alina.timmermann@tu-dortmund.de)
Supervisor: Prof. Dr. Peter Buchholz

Successful demand planning in industrial companies is still a challenge. Especially in today's time of many crises and uncertainty, estimation is difficult. Demand planning is supported by successful demand forecasting. This can be done on the basis of expert opinions or increasingly by support software [1]. Forecasting software should, on the one hand, provide forecasts of the highest possible quality. On the other hand, forecasting software must be trustworthy for the user in order to successfully replace expert opinions as the standard. In order to meet the requirements of crisis robustness and trustworthiness, our forecasting model consists of the following steps:

1. Article grouping
2. Model training
3. Article Forecast

In step 1 of article grouping, products are grouped based on their risk sensitivity and statistical properties. This is to be done automatically, for example using hierarchical clustering. In step 2, a forecast model is trained for each group. This model receives as input forecast results of the group with different common forecast methods and generates as output the forecast validation. The purpose is to find the most suitable forecast methods for each group and to predict the result validation. This increases the quality of the forecast on the one hand and the trustworthiness on the other hand. Step 3 involves the actual prediction of the user. Here, based on the group (step 1) and the optimal method and validity (step 2), a prediction for the product is performed. The implementation of the project is done in Python. The forecasting methods used are Holt-Winters, ARIMA [2][3], Linear Regression, Support Vector Regression, Random Forest Regression, Artificial Neural Networks and Convolutional Neural Networks[4].

[1] Chang, Pei-Chann, and Yen-Wen Wang. "Fuzzy Delphi and backpropagation model for sales forecasting in PCB industry." Expert systems with applications 30.4 (2006): 715-726.

[2] Xia, Min, and Wai Keung Wong. "A seasonal discrete grey forecasting model for fashion retailing." Knowledge-Based Systems 57 (2014): 119- 126.

[3] Gilbert, Kenneth. "An ARIMA supply chain model." Management Science 51.2 (2005): 305-310.

[4] Chu, Ching-Wu, and Guoqiang Peter Zhang. "A comparative study of linear and nonlinear models for aggregate retail sales forecasting." International Journal of production economics 86.3 (2003): 217-231.

Analysis of Existing Methods for Pipeline Structure Creation in AutoML Frameworks

Hadi Kutabi (hadi.kutabi@tu-dortmund.de)
Supervisor: Prof. Dr. Anne Meyer

Automated machine learning aims to automate the construction and hyperparameter optimization for ML pipelines. In this context, a number of pre-processors, an estimator and their hyperparameters (HPs) must be selected with respect to a loss. AutoML frameworks must choose one of the approaches for generating pipeline structures [1]:

1. Fixed-structure approach: The components of the pipeline are pre-selected; only their HPs of are optimized.

2. Template-based approach: A pre-defined structure is maintained, while optimizing the selection of the components and HPs.

3. Flexible shape approach: The structure of the pipeline, selected components and their HPs values are tailored to the problem instance during optimization.

Many AutoML Frameworks follow the fixed-structure or the template-based approach to reduce the complexity of the task. Yet, it is claimed that such structures may not be sufficient when presented with complex datasets[2], as ML pipelines in production are highly specialized to a specific problem instance.

Auto-Sklearn constructs template-based pipelines by using Bayesian Optimization to optimize component selection and their HPs[3]. DSWIZARD guides an MCTS by two random forests to construct template-based pipelines[4]. Alphad3m constructs template-based pipelines by combining MCTS with a neural network that predicts action probabilities for pipeline states[5]. Finally, TPOT uses a genetic programming to construct flexible-shaped pipelines and optimizes their HPs[6].

[1] Zöller, Marc-André, et al., "XAutoML: A Visual Analytics Tool for Establishing Trust in Automated Machine Learning., " arXiv preprint, arXiv:2202.11954, 2022

[2] Zöller, M. A., and Huber, M. F, "Benchmark and survey of automated machine learning frameworks, " Journal of artificial intelligence research, vol 70, pp. 409-472, 2021

[3] Feurer, Matthias, et al., "Efficient and robust automated machine learning., "Advances in neural information processing systems, 28, 2015

[4] Zöller, Marc-André, Tien-Dung Nguyen, and Marco F. Huber. "Incremental search space construction for machine learning pipeline synthesis." In Advances in Intelligent Data Analysis XIX: 19th International Symposium on Intelligent Data Analysis, IDA 2021, Porto, Portugal, April 26–28, 2021, Proceedings 19, pp. 103-115. Springer International Publishing, 2021.

[5] Drori, I., Krishnamurthy, Y., Rampin, R., Lourenco, R. d. P., Ono, J. P., Cho, K., Silva, C., and Freire, J., "AlphaD3M : Machine Learning Pipeline Synthesis, " International Conference on Machine Learning AutoML Workshop, 2018

[6] Olson, Randal S., and Jason H. Moore. "TPOT: A tree-based pipeline optimization tool for automating machine learning." In Workshop on automatic machine learning, pp. 66-74. PMLR, 2016.

GRK 2236: UNcertainty and Randomness in Algorithms, VErification, and Logic

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

Uncertainty is nowadays more and more pervasive in computer science. It is important both in big data and at the level of events and control. Applications have to treat large amounts of data, often from unreliable sources such as noisy sensors and untrusted web pages. Data may also be subject to continuous changes, may come in different formats, and is often incomplete. Robots, trains, and production machines have to deal with unpredictable environments. The growing use of machine-learning components — often providing weak guarantees — forms an additional factor of uncertainty. Probabilistic modelling and randomisation are key techniques for dealing with uncertainty.

Many trends witness this. Probabilistic programming exceeds the capabilities of probabilistic graphical models and automates statistical inference. Probabilistic databases deal with noisy data by associating probabilities to the possible worlds. Probabilistic model checking emerged as a key systems verification technique allowing to integrate correctness checking and performance analysis. Similar developments take place in automata, logic, and game theory.

The pervasiveness of uncertainty urges to make substantial enhancements in probabilistic modelling and reasoning so as to get deeper insight into, reason about, and master uncertainty. The aim of this RTG is and was to significantly advance various theoretical concepts (in algorithms, logic, verification) as well as their connection to deal with uncertainty and randomness, and to tailor and apply these techniques to problems in application areas such as railway engineering, network dynamics, and cyber-physical systems. This challenge is faced by a unique mixture of scientists from theoretical and applied computer science, management science, mechanical engineering, and railway engineering.

The qualification and supervision concept aims at offering the Ph.D. students an optimal environment to carry out their research. Every Ph.D. student has two supervisors; the rights and duties of the supervisors and students are laid down in a written supervision agreement. Progress and quality control is realised through regular individual meetings with the supervisors and regular talks at the RTG events. The curriculum consists of bi-weekly research seminars, soft-skill courses, reading groups, workshops (twice per year), a summer school in the first Ph.D. year, and (various new) advanced lectures.

Robust Appointment Scheduling in Hospitals

Mariia Anapolska (anapolska@math2.rwth-aachen.de)
Supervisor: Prof. Dr. Christina Büsing

Introduction. As the demand for health care services increases each year, the need for efficient management of health care systems becomes more and more apparent. One of the most important health care providers are hospitals. Hospitals are under tremendous cost pressure and must achieve a balance between economic efficiency and a treatment that focuses on the patient. To improve clinical operations and patient safety, my research considers the appointment scheduling problem within a hospital.

Problem description. The problem aims to maximize the utilization of the hospital resources while minimizing the patients' inconveniences such as waiting time. Typically, an arriving patient needs to undergo several types of treatment. This means that several hospital resources will be needed either simultaneously or sequentially in a short time period. The treatments must be scheduled so that they satisfy the resource capacity restrictions. The hospital environment is very dynamic: The length of patients' treatments varies and arriving patients represent an uncertain demand for resources. The presence of emergency patients requires the schedule to be highly adaptable, i. e., robust and stable solutions are needed.

Envisioned work. Solutions of robust optimization problems depend on the uncertainty sets constituting the problem's input. In robust optimization, researchers assume these sets to be given by experts. However, experts often do not understand the dynamics within robust optimization, e.g., that integrating scenarios with high fluctuations leads to unpredictably high costs. Furthermore, especially in the hospital context, even for experts it is quite difficult to measure and obtain all data needed for presenting a scenario. To overcome this obstacle, we will use agent-based simulation to obtain all important parameters. To that end, the simulation framework "SiM-Care" [1] developed by Martin Comis needs to be extended and adapted. This agent-based simulation models interactions between the population and the physicians in a primary care system. It evaluates the input health care system by computing performance indicators that characterize the system's efficiency both from patients' and physicians' points of view. Moreover, the simulation allows us to assess the impact of changes in the system, such as changes in the patient-to-physician ratio or novel management strategies of physicians.

In order to obtain realistic input scenarios for the appointment scheduling problem, we plan to extend the model of `SiM-Care` further in order to integrate emergency and elective patients requiring hospital treatment. Since `SiM-Care` produces scenarios based on parameterized probability distributions, we will investigate the influence of the uncertainty sets for demands generated by `SiM-Care` on the resulting solutions for the robust appointment scheduling problem.

[1] Martin Comis, Catherine Cleophas, Christina Büsing, "Patients, Primary Care, and Policy: Simulation Modeling for Health Care Decision Support," arXiv.org (2019), no. 1910.11027, `https://arxiv.org/abs/1910.11027`

Automated Verification of Partially Observable Stochastic Models

Alexander Bork (alexander.bork@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Joost-Pieter Katoen

Stochastic models like Markov decision processes (MDPs) and stochastic games are formalisms used in a wide array of domains to model systems where uncertainty and non-determinism are present. They assume perfect information about the state of the system at any time. Thus, these models often optimistically overestimate the amount of information available to a decision procedure to determine an optimal course of action for a given objective. In reality, a system's complete state is often hidden. *Partially observable* probabilistic systems extend the commonly used models with the notion that only *part* of the system's state is observable and decisions must be made based only on the observable information. These systems find application in fields like artificial intelligence, robotics and economics. Their analysis is significantly more involved compared to the fully observable case. Intuitively, this is due to the significantly increased dependence on the information history for making optimal decisions.

The research project focuses on the analysis and computer-aided verification of *partially observable MDPs (POMDPs)*. As perfect state information is not available, an optimal choice of action to satisfy a property is based on an estimate of the probabilities to be in states of the POMDP given the history of observations. These estimates are known as *beliefs*. These beliefs can be used to construct a fully observable, but typically infinite, *belief MDP* that captures the semantics of the POMDP.

Fully observable MDPs are well-studied in theory and many forms of analysis are tractable in practice, in particular for finite-state MDPs. However, even fundamental problems like the reachability problem (the question if a state of the system can be reached with a given probability at some point in time) are generally undecidable for finite-state POMDPs. As a consequence, related work typically restricts the considered properties to be bounded in time steps (*finite horizon*) or applies discounting in the computation to guarantee convergence. This, however, can severely distort results if a thorough analysis is desired.

The goal of the project is to develop novel, practically applicable verification methods for POMDPs in the *infinite horizon without discounting*. As such, finite abstractions of the belief MDP for a given POMDP are used to provide both upper[1] and lower bounds on the optimal value. These approximation algorithms leverage the existing knowledge in model checking finite MDPs to reason about POMDPs. An implementation of the approach as an extension of the probabilistic model checker Storm[2] shows its practical applicability.

Possible future directions include exploring compositional approaches to POMDP analysis, necessitating the definition of a compositional POMDP semantics and the development of model checking approaches for *partially observable stochastic games*.

[1] Bork, A., Junges, S., Katoen, J.-P., and Quatmann, T., "Verification of indefinite-horizon POMDPs", Automated Technology for Verification and Analysis. ATVA 2020. Lecture Notes in Computer Science, vol. 12302, pp. 288-304, 2020

[2] Hensel, C., Junges, S., Katoen, J.-P., Quatmann, T., and Volk, M., "The Probabilistic Model Checker Storm", STTT, 2021

Robust Hospital Management

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

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

1. the operational planning and utilization of hospital beds,
2. the patient appointment scheduling, and
3. the transportation from patients to their appointments.

In the next subsection we will give a rough overview of existing scientific work in the mentioned subproblems. Finally, we will describe our approach to these problems in detail.

In 2012, Hulshof et al. [14] published a detailed bibliography and taxonomic classification on methods from operations research applied to problems in health care. Uncertainties are part of most decision problems in planning and controlling in health care. Mainly methods from queuing theory, Markov processes, and stochastic programming are used to include them into the optimization process, e.g., [1,2,3,9,13]. Besides dealing with uncertainties, [14] identifies the challenge for researchers to develop integral models of different hierarchical planning levels and services in health care.

The location of beds and the assignment of patients to these beds in a hospital is studied in operations research at the strategical, tactical and operational level. To support strategic planning queuing techniques, simulation and models from mathematical programming are already used. Traditionally, these planning decisions are based on target occupancy levels. However, Green [36] points out that, due to high fluctuations, different measurements such as patient waiting time [5] or patient refusal rate [18] need to be integrated into the optimization process. In [17], Ma and Demeulemeester combine the allocation of beds with the appointment of elective patients. In order to integrate emergencies, they reserve a fixed capacity. The Patient-to-Bed Assignment Problem on an operational level has been formalized in 2010 by Demeester et al. [8]. They use a combination of a patient-bed-suitability rating, the number of inpatient transfers and the number of mixed-gender-occupied rooms as the objective function and propose a hybrid tabu search algorithm for this problem. Later, the problem is reformulated to patient-to-room assignment, as it is generally assumed that all beds, located in the same room, are equal. Also more practical variants and other exact and heuristic approaches for patient-to-room assignment have been published, e.g., [6,7,16].

Vehicle routing problems are well-studied in discrete optimization [10]. In the context of patient routing within the hospital, Hanne et al. [12] designed a computer-based planning system. Johnson et al. [15] introduced a simulation tool, and Beaudry et al. [4] a two-phase heuristic to solve the

dynamic problem. Schmid and Doerner [19] solved the combination of operating room scheduling and transportation with a hybrid metaheuristic.

So far, we concentrated on the operational patient-to-room assignment. Hospital beds are a special resource in a hospital. According to the number of beds the capacity of a hospital is measured and, thereby, the size of wards and clinics are given by this number and the corresponding budget on medical and nursing staff is determined by this number. Yet, the number of available beds fluctuates due to capacity changes in the nursing staff, patient demands and special needs of patients [11]. These fluctuations primarily affect the scheduling of elective patients and the daily allocation of emergency patients to different wards and rooms. In the case of a mismatch of available beds to admitted patients, a relocation of a bed or of a patient to a different clinic or ward, or the rejection of elective patients is possible. However, such means should only be used in extreme situations and not on a daily basis.

Contrary to all previously published work, we do not regard a weighted combination of the patient-bed-suitability rating, the number of inpatient transfers and the number mixed-gender-occupied rooms as the objective function. Choosing appropriate weights is very challenging and, also, no procedure has yet been proposed to check afterward if good weights have been chosen. Also, using a weighted combination prevents us from gaining better insights into how the different objectives influence each other. For this reason we keep the three different aspects separated and treat them as independent objective functions. We compare and develop exact and heuristic approaches to solve the multi-objective patient-to-room assignment problem with a focus on robust solutions.

References:

1. R. Akkerman and M. Knip. Reallocation of beds to reduce waiting time for cardiac surgery. Health Care Management Science, 7:119–126, 2004.
2. M. Asaduzzaman, T.J. Chaussalet, and N.J. Robertson. A loss network model with overflow for capacity planning of a neonatal unit. Annals of Operations Research, 178:67–76, 2010.
3. S. Batun, B.T. Denton, T.R. Huschka, and A.J. Schaefer. Operating room pooling and parallel surgery processing under uncertainty. INFORMS Journal on Computing, 23:220–237, 2011.
4. A. Beaudry, G. Laporte, T. Melo, and S. Nickel. Dynamic transportation of patients in hospitals. OR spectrum, 32:77–107, 2010.
5. P. Van Berkel and J. Blake. A comprehensive simulation for wait time reduction and capacity planning applied in general surgery. Health Care Management Science, 7:373–385, 2007.
6. S. Ceschia and A. Schaerf. Local search and lower bounds for the patient admission scheduling problem. Computers and Operations Research, 38(10):1452–1463, 2011
7. S. Ceschia and A. Schaerf. Modeling and solving the dynamic patient admission scheduling problem under uncertainty. Artificial Intelligence in Medicine, 56(3): 199–205, 2012.
8. P. Demeester, W. Souffriau, P. D. Causmaecker, and G. V. Berghe. A hybrid tabu search algorithm for automatically assigning patients to beds. Artificial Intelligence in Medicine, 48(1):61–70, 2010.
9. G. Dobson, H.H. Lee, and E. Pinker. A model of icu bumping. Operations Research, 58:1564–1576, 2010.
10. B.L. Golden, S. Raghavan, and E.A. Wasil, editors. The Vehicle Routing Problem: Latest Advances and New Challenges. Springer, 2008.
11. L.V. Green. Capacity planning and management in hospitals. In Operations Research and Health Care: A Handbook of Methods and Applications, pages 15–41. Kluwer Academic Publishers, Boston, 2004.
12. T. Hanne, T. Melo, and S. Nickel. Bringing robustness to patient flow management through optimized patient transports in hospitals. Interfaces, 39:241–255, 2009.
13. P.R. Harper, A.K. Shahani, J.E. Gallagher, and C. Bowie. Planning health services with explicit geographical considerations: a stochastic location-allocation approach. Omega, 33:141–152, 2005.
14. P. Hulshof, N. Kortbeek, R. Boucherie, E. Hans, and P. Bakker. Taxonomic classification of planning decisions in health care: a structured review of the state of the art in or/ms. Health Systems, 1:129–175, 2012.

15. K. Johnson, D. Kalowitz, J. Kellegrew, B. Kubic, J. Lim, J. Silberholz, A. Simpson, E. Sze, E. Taneja, and E. Tao. Emergency department efficiency in an academic hospital: A simulation study. Ph.D. Dissertation, Univ. of Maryland, 2010.

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

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

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

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

Design and Analysis of Algorithms for Combinatorial Optimization Problems under Uncertainties

Katharina Eickhoff (katharina.eickhoff@oms.rwth-aachen.de)
Supervisor: Prof. Dr. Britta Peis

Matching Markets

Matchings appear in many combinatorial optimization models of applications where assignments between two parties (sellers and buyers, students and courses, ...) have to be found. In these examples each player has preferences to which he would like to be matched. Often, prices might be used to regulate imbalances between supplies and demands.

A possible aim is to find assignments and prices such that everyone is happy, i.e., with these prices no one prefers to trade with someone else instead of the assigned person. These prices are called equilibrium prices. If furthermore as much as possible is sold we call the prices market-clearing. Prices which are competitive and market-clearing describing the set of Walrasian prices. One possibility to find Walrasian prices is by a price raising auction (see for example [1] [2] [3]). To find the set of objects whose prices should be raised is quite complicated in the general case. We could show that these sets could be found by a max-flow computation in case of linear valuations. Furthermore we could give sensitivity results for the prices if the demand or supply in the matching-market changes. In the future we like to generalize this results for matroid valuations.

There are many ways to expand this approach which we might consider in the future. One example are two-stage variants. In the first stage, agents decide on a strategy based on probability distributions of the agents' valuations. The agents are allowed to switch their strategies in a given neighborhood in the second stage when the true valuations are common knowledge. For example, the agents decide on a strategy based on guesses of the valuations and they can adapt their strategies in a given scope in the real scenario. The objective of an agent is to maximize the expected profit.

Furthermore, we like to consider the setting with risk-averse agents. They prefer a robust solution within all possible situations which means that the profit they receive in the worst-case scenario should be maximized. The strategies of the agents are in equilibrium if each strategy is the best robust response given the other strategies. We study the existence of equilibria in such markets. If equilibria exist, we like to analyze the complexity and design algorithms to compute or approximate them.

Stackelberg Network Pricing Games

Consider a game with to players. The leader can choose prices for some items of an underling network in the first stage. Afterwards, in the second stage, the follower chooses the items which yields a min cost solution of his optimization problem (e.g. matching, vertex cover, closure). Most of these problems are NP-hard in general, but if the underling network or the set of priceable items is restricted there might be a polynomial algorithm to solve it.

We consider the Stackelberg Bipartite Vertex Cover Problem, which is NP-hard [4]. It is known that the problem is polynomial solvable if the pricable vertices are on one side of the bipartition

[1] L.M. Ausubel, "An efficient dynamic auction for heterogeneous commodities," American Economic Review, vol. 96(3), p. 602–629, 2006

[2] G. Demange, D. Gale and M. Sotomayor, "Multi-item auctions," Journal of political economy, vol. 94.4, p. 863-872, 1986

[3] K. Murota, A. Shioura, Z. Yang, "omputing a walrasian equilibrium in iterative auctions with multiple differentiated items," International Symposium on Algorithms and Computation, p. 468–478, 2013

[5]. We like to show similar results for pricable vertices on both sides but if the underling graph has a special structure, e.g. if it is a path or a tree.

A Logic of Belief over Arbitrary Probability Distribution

Qihui Feng (qihui.feng@rwth-aachen.de)
Supervisor: Prof. Dr. Gerhard Lakemeyer

When it comes to robotic agents operating in an uncertain world, a major concern in knowledge representation is to better relate high-level logical accounts of beliefs and actions to the low-level probabilistic sensorimotor data. Perhaps the most general formalism for dealing with degrees of belief in formulas is the first-order logical account by Bacchus, Halpern, and Levesque. The main advantage of this logical account is that it allows a specification of beliefs that can be partial or incomplete, in keeping with whatever information is available about the domain, making it particularly attractive for general-purpose cognitive robotics. Recently, this model was extended to handle continuous distributions and joint distributions of discrete and continuous random variables. However, it is limited to finitely many nullary fluents and defines beliefs and integration axiomatically, the latter making semantic proofs about beliefs and meta-beliefs difficult.

In our recent work, we revisit the continuous model and cast it in a modal language. We will go beyond absolutely continuous distributions. Also, we allow fluents of arbitrary arity as is usual in the standard situation calculus. These necessitate a new and general treatment of probabilities on possible worlds, where we define measures on uncountably many worlds that interpret fluents of arbitrary arity. We then show how this leads to a fairly simple definition of knowing, degrees of belief, and also only-knowing. Properties thereof will also be analyzed.

Calculating the capacity of railway systems considering microscopic infrastructure constraints

Tamme Emunds (emunds@via.rwth-aachen.de)
Supervisor: Prof. Dr. Nils Nießen

With rising demand on public transportation due to political and environmental influences, railway transportation is subject to rising requirements on quality, quantity and efficiency of the used infrastructure. To fulfill those enhanced needs, infrastructure managers are required to identify bottlenecks in existing infrastructure and precisely estimate the capacity of newly constructed or extended infrastructure. In many cases the stations turn out to be the bottleneck in the railway network.

Developing methods for the analyzation of railway infrastructure capacity has therefore been one of the major suspects of interest to railway researchers. While sufficient methods for the estimation of railway lines have already been developed and heavily used for planning purposes, the capacity analysis of entire railway stations remains a challenging research question.

In this project, new methods for quantifying the capacity of railway stations will be developed and analyzed. The primary focus will be laid on the development of efficient algorithms to estimate the theoretical capacity of railway infrastructure in stations. Further, methodologies to quantify the influence of disturbances from multiple sources – in example technical failures, maintenance work or peaks in the transported traffic volume – to the infrastructure capacity will be developed and analyzed.

Optimization under Uncertainty

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

Many optimization algorithms make the assumption that the input to problem is completely known in advance. This is not always true in practice. In practice we often have to make decisions before all the data about the problem are known. A further problem is that we may not have complete information since the data we have to work with are not completely accurate. This is due to the way data is acquired which introduces uncertainty, for example, perhaps the sensor used only gives us an approximation of the actual value.

Nonetheless, we want to be able to make decisions in these cases. It is clear that we cannot hope to always find the optimal solution that fits the actual data but we want to find a solution that gives guarantees about objective value in comparison to the achievable value if the input is known.

In my work I study these kinds of robust optimization problems.

One way of approaching robust optimization problems is to consider a 2 player game. The first player (the algorithm) is presented with a (possibly infinite) set of possible inputs. The algorithm has to fix an output. Now, in a second stage, the second player (the adversary) picks one of those inputs from the set that causes the worst possible performance for the algorithm.

One of these 2-player problems is the Continuous Knapsack Problem (CKP). In the CKP, player 1, the leader, packs some items (or fractional parts of items) into their knapsack. In the second stage, player 2, the follower, chooses items (or fractions of items) from the set of items already chosen by player 1 to pack into their knapsack thereby trying to optimize their gain. The leader's objective is to minimize the follower's objective. In a recent paper it has been shown to be solvable in time $O(n^2)$ [1]. We were able to improve this running time in [2] to $O(n \log n)$.

One other robust optimization problem is the Recoverable Robust Assignment problem in which on a balanced bipartite graph with $2n$ vertices for given linear cost functions c_1 and c_2 the task is to find matchings M_1 and M_2 that have at least k edges in common while minimizing $c_1(M_1)+c_2(M_2)$. In joint work with Hartmann, Lendl, and Woeginger we were able to show W[1] hardness for parameter k and parameter $n-k$ even in very restricted special cases. We also showed that it is polynomial time solvable if the cost functions are restricted to being Monge and Anti-Monge. In the case where one of the matchings is fixed we showed that the Recoverable Robust Assignment problem is contained in RNC2 while being at least as hard as the well-known Exact Matching in Red-Blue Bipartite Graphs whose complexity is a long-standing open problem. These results are not published yet.

Another problem is the bilevel bottleneck assignment problem. In this problem a bipartite graph is given. The edges are split into a leader and follower set. The leader and follower have (different) cost functions for the edges. First the leader selects edges that form a matching from their leader set. Then the follower selects edges from the follower set to complete the leader matching to a perfect matching. The goal of the leader is to minimize the largest used edge according to the leader cost function. The goal for the follower is to minimize the largest used edge according to the follower's objective function. In joint work with Muluk and Woeginger we showed that this problem is NP complete.

[1] Margarida Carvalho, Andrea Lodi, PatriceMarcotte, "A polynomial algorithm for a continuous bilevel knapsack problem Oper," Res. Lett, vol. 46(2), p. 185–188, 2018

[2] Dennis Fischer, Gerhard J. Woeginger, "A faster algorithm for the continuous bilevel knapsack problem," Oper. Res. Lett., vol. 48(6), p. 784–786, 2020

Another project is joint work with the UnRAVeL members Tauer, Fuchs, Koch, and Ziegler in which we looked at complexity results in a train routing problem [3]. This train routing problem is a generalization of packet routing without buffers. We distinguished the case where the train depots are part of the network or not and showed various complexity results on different networks.

[3] Bjoern Tauer, Dennis Fischer, Janosch Fuchs, Laura Vargas Koch, Stephan Zieger, "Waiting for Trains: Complexity Results," CALDAM 2020, p. 282–303, 2020

Robust Infrastructure

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

The extended planning periods and the long life cycle of railway infrastructure require a lengthy planning horizon. Thus, bottlenecks in the infrastructure have to be recognized at an early stage to initiate adequate measures. At the present, the infrastructure is planned while only little about the intended operation is known. Hence, the timetable and the operation are adjusted to the infrastructure. Since space, time and money for extension measures of railway infrastructure are limited, each modification has to be done carefully and and in a long lasting manner. To meet the customers' future needs, infrastructural projects have to planned such that the infrastructure will be appropriate for future unknown demand.

For the long-term service life of the planned infrastructure, it makes sense to include timetable scenarios in the planning in order to be able to expand the railroad infrastructure, which is already reaching its capacity limits on some lines, in a targeted manner.

The aim of the project is to provide a procedure for timetable-based, robust infrastructure planning to complement the previous infrastructure-based timetable construction. In doing so, the idea of a long-term timetable and the infrastructure adaptation based on it will be precisely defined and further developed. For this purpose, infrastructure planning is modeled as a network design problem under uncertainties. Subsequently, a solution is to be found by means of robust optimization.

The term "robustness" is generally understood as the ability of a method to find a correct solution even under uncertain input data. In the context of this project, the timetables are not yet fixed until the end of the infrastructure's service life and are, thus, still uncertain at the time of infrastructure planning. For example, it is not a realistic scenario to run only one timetable throughout, but likewise infrastructure cannot be held in reserve for every scenario, no matter how unlikely, for both financial and spatial reasons. In the context of this project, both the various, potential timetable scenarios as well as the actual operational scenarios are to be included in the considerations.

For this purpose, the uncertain input data will be modeled in a first step. In the context of the project, it is first determined which criteria for a "similarity" of timetable scenarios have to be fulfilled to which extent.

Subsequently, infrastructure planning is modeled as a network design problem. Here, a solution has to be found for which new edges, i.e. track sections, are needed and for which edges the capacity should be increased. This solution should ensure the feasibility of all planned timetable scenarios at the lowest possible cost.

Probabilistic Hyperproperties

Carolina Gerlach (gerlach@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Erika Ábrahám

Model checking is traditionally concerned with analyzing whether a certain model satisfies a specific trace propertyd. A trace is a sequence of observable facts about the states visited along a system execution. A trace property, formally specified using temporal logics like LTL or CTL, can be viewed as a set of model traces, encoding requirements on the system executions.

However, many interesting requirements, such as information-flow security policies, cannot be expressed as trace properties. For example, the property of non-interference for a deterministic system requires that the values of secret input variables do not influence the observable values of public output variables. In order to check whether this property holds, we need to compare different program executions thar start in observationally equivalent initial configurations, i.e., with the same initial public variable values but possibly different secret inputs. Non-interference is satisfied if we can make the same observations along all executions with observationally equivalent initial
configurations, i.e., generating the same public variable values. Hence, non-interference cannot be expressed as a set of traces and is therefore not a trace property. Instead, security policies like noninterference are hyperproperties, which are sets of sets of traces.

Since established temporal logics can only capture sets of traces, but not sets of sets of traces, several temporal logics have been extended to hyperlogics. Clarkson et al. generalized LTL and CTL* to HyperLTL and HyperCTL*, respectively, by adding explicit quantification over multiple traces. Even though CTL* already permits quantification over traces, it does not allow quantifying over several traces at the same time, which HyperCTL* now does.

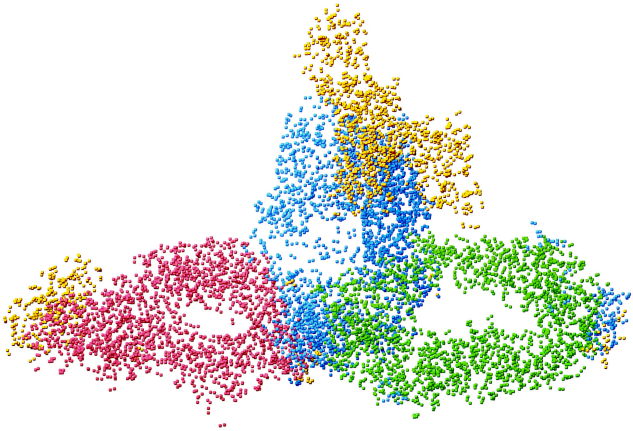
Probabilistic Hyperlogics. HyperPCTL was the first temporal logic for probabilistic hyperproperties. HyperPCTL extends PCTL by quantification over states to express probabilistic relations between several computation trees. Like PCTL, HyperPCTL formulas are evaluated over Markov chains. They can express information-flow security policies like probabilistic noninterference, which stipulates that, for all possible values of the public variables, the probability of observing these values should be the same for all program executions with observationally equivalent initial states.

HyperPCTL was lifted to Markov decision processes (MDPs) by additionally adding quantification over schedulers that resolve nondeterministic choices probabilistically. Model checking HyperPCTL for discrete-time Markov chains is decidable. For MDPs, the model checking problem becomes in general undecidable, but restricting scheduler quantification to deterministic memoryless schedulers makes it decidable again.

Research. We are currently working on an asynchronous extension of HyperPCTL, where the traces in different quantified computation trees do not have to evolve in lockstep anymore. This extension allows to capture the asynchronous nature of concurrent programs more accurately. One area of possible future research is to consider probabilistic hyperproperties in the context of stochastic games.

Randomness and Uncertainty in Signal Processing on Topological Spaces

Vincent Grande (grande@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Michael Schaub



Proteins are molecules that consist of long strings of amino acid residues. They play an integral role in almost every cellular process from metabolism, DNA replication, to intra-cell logistics. Their diverse functions are hugely influenced by their complex 3d geometry, which arises by folding the chains of amino acid residues. In the figure: Clustering of NALCN Channelosome, a channel membrane protein, data by Kschonsak et al., 2022. The topological structure influencing the function of the protein consists of three loops, which our methods are able to identify correctly.

Higher-order Information Encoded in Networks and Point Clouds

My research deals with the analysis of higher-order information in networks and point clouds. A central motive is to use a blend of techniques from algebra, topology, and homotopy theory to explore the relationship between small scale connectivity data and other localised information, and large-scale behaviour and global properties of data sets.

Over the last years, availability of large, complex data sets has increased dramatically with recent advances in collection, storage and processing techniques. Extracting human-interpretable information from these is a challenging task across application scenarios. Standard methods of data analysis include projecting the data set onto subspaces with the highest variance (PCA), clustering the data points using closeness- or density-based clustering algorithms (k-means, spectral clustering, DBSCAN, etc.), or fitting polynomials or other functions to the data points. However in many cases, the information encoded in the point cloud cannot be retrieved by these methods: The detection of loops, voids, and holes in the point cloud requires tools that consider more than just proximity of points or local density. For example, these features are relevant when trying to analyse complex proteins consisting of multiple loops, or trying to understand the

structure of a manifold in high-dimensional space from where the point cloud is sampled from.

From a different perspective, higher-order information are global features of the data-set. We cannot extract these from the **local** neighbourhood of a point of interest. However by combining all local information, higher-order **global** features arise. Because we are interested in information on the individual points, we finally need to find a way to **localise** these global features of the point cloud.

Combining Tools from Algebraic Topology and Network Science

Algebraic Topology is an area of Mathematics that was established trying to provide tools for capturing the "essence" of topological spaces. Topological features of a space are global and by design robust to local perturbations and noise, and are somewhat emergent properties of all the local connectivity data of the individual points. This is ideal for the setting of modern data analysis, where the goal is to extract information out of data sets where local perturbations are likely to occur because of noisy data collection. Current tools of topological data analysis provide a good way of generating these global invariants (Betti numbers, persistence landscapes, etc.) from local connectivity data of point clouds. However, there is considerably less work on relating back these global features to the local scale of the points with a real-world meaning. This is surprising, considering that extracting information like cluster assignments on a point level is highly useful in application scenarios and a key goal of many areas of data analysis. Network Science, and especially signal processing on networks, on the other hand, deals with similar problems trying to connect the local connectivity information on network nodes to the global behaviour of the network and dynamics on it, and then relating this back to the individual nodes.

The overarching theme of my research is to combine perspectives of algebraic topology, network science, signal processing and clasical data anlysis to develop tools from extracting higher order information from point clouds and networks.

Complexity and Algorithms in Optimization under Uncertainty

Christoph Grüne (gruene@algo.rwth-aachen.de)
Supervisor: Prof. Dr. Gerhard Woeginer

Introduction. Optimization under uncertainty is a field in which problems are optimized against some form of uncertainty. For this, finding measures of robustness to find solutions that deal with the given form of uncertainty is of interest. The project will focus on different measures of robustness and different complexity viewpoints to analyze certain forms of problems. Among those may be problems with one player against an adversary (the "nature"), two players against each other or multiple player settings playing against or with each other. That is, the uncertainty is modelled by an adversary player playing against the agent. The complexity analysis may be based on classical complexity classes as well as parameterized complexity.

The first project is on Recoverable Robustness with a Hamming-distance measure which shall encounter combinatorial uncertainty scenarios. In this setting, a solution S is given and for every possible scenario, which may occur in this setting, we can choose another solution, S', which differs in at most only k elements from solution S'. That is, we can recover from a harmful scenario by choosing a different solution, which is not too far away from the first solution.

The project surveys the complexity of k-Hamming-distance recoverable robust version of problems that are in NP for different types of scenarios among a constant number of arbitrary scenarios, Gamma-scenarios, and general scenarios for elements of the universe. The analysis is primarily based on classical complexity measures such as the polynomial hierarchy. There are already results that have to be formulated into a paper. The results contain a hardness proof for the recoverable robust version of the undirected s-t-path problem, which may extend to a variety of other problems. The aim is to provide a structural theorem that captures this very variety of combinatorial problems that have this hardness structure. The second project, which is currently planned, may inspect parameterized complexity counterparts to the classical complexity analysis of the first paper. Instead of NP problems, $W[t]$-problems and other problems in parameterized hierarchies are considered; they may have a similar or the same hardness structure.

References:

1. Christoph Grüne. Dial-a-Ride for Railway Traffic. Master Thesis, RWTH Aachen University 2019
2. Jörg Flum, Martin Grohe. Parameterized Complexity Theory, Springer, 1998.
3. G. Rodney Downey, M. R. Fellows. Parameterized Complexity, Springer, 1999.
4. Marek Cygan, Fedor V. Fomin, Lukasz Kowalik, Daniel Lokshtanov, Dániel Marx. Parameterized Algorithms, Springer, 2015.
5. Raymond Greenlaw, James Hoover, Walter L. Ruzzo. Limits to Parallel Computation: P-Completeness Theory, Oxford University Press, 1995.

Robust Execution of Abstract Task Plans on Mobile Robots

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

Introduction> Formalisms such as Golog [6] and PDDL [7] allow the specification of a robot's behavior in an abstract manner. Based on a logical model of the environment, the agent's actions are specified with preconditions and effects. This allows for determining the course of action by searching for an appropriate action sequence (PDDL), possibly intertwined with agent programs specified by the user (Golog). However, when deploying such a system on a real robot, one often faces additional challenges, such as the need to calibrate a robot arm before its usage. Those issues are intentionally ignored when specifying the abstract behavior, as it would impair the reasoner performance. This research project aims to close the gap between high-level reasoning and low-level robot platform [5]. Instead of specifying all the low-level details in the reasoning domain, we instead model the platform components separately as timed automata. Then, we specify constraints that connect a high-level program with the platform, e.g., by requiring that the arm needs to be calibrated five seconds before the robot picks up an object. We then need to transform the high-level program into a sequence of actions that satisfies all those constraints, resulting in a task specification that follows the high-level program while dealing with the low-level platform details.

A logic for specifying metric temporal constraints for Golog programs. In the first step, we extended ESG [3], a modal variant of the Situation Calculus that allows temporal constraints, with metric temporal constraints [4]. The resulting logic retains most of the properties of ESG and thus allows the specification of basic action theories and Golog programs extended with metric constraints.

Plan Transformation based on Timed Automata Reachability Analysis. In a first approach to solve the temporal platform constraints, we looked at timed automata reachability analysis. In a first step, we transform a high-level action sequence into a timed automaton such that each action is one location in the resulting automaton. This automaton is then combined with the platform model such that in the product automaton, all edges that violate a constraint are removed. Finally, we apply reachability analysis using the model checking tool UPPAAL [1]. The resulting path describes the transitions of the platform models such that all constraints are satisfied during the execution of the original plan. Despite the combinatorial blowup due to the automata product, this approach performs well and we were able to transform plans with 50 actions and several platform components in a few seconds.

Controller Synthesis for Golog Programs. The first approach, however, poses some limitations: For one, it only works on pre-determined plans. Thus, it cannot be used with any formalism that uses online sensing, as this would require online decision making. Also, it does not distinguish between controllable actions (e.g., starting to pick up an object) and actions that are controlled by the environment (e.g., the arm going into an error state, or even the end of an action). To tackle those limitations, we used a different approach based on MTL synthesis. Instead of applying reachability analysis, we build on top of results on controller synthesis for MTL specifications [1]. We first convert a given Golog program into a timed automaton, apply MTL controller synthesis on the automaton, the platform model, and the platform constraints, and then use the resulting controller to guide the Golog executor. We presented the theory of the approach in [8] and we are currently working on an implementation in cooperation with the former UnRAVeL researcher Stefan Schupp and UnRAVeL supervisor Erika Ábrahám. This cooperation, which allows us to combine expertise in robotics with expertise in hybrid systems, directly resulted from an UnRAVeL workshop in April 2020, where we presented preliminary results for the synthesis approach.

References:

1. Behrmann, G., David, A., and Larsen, K. G. A Tutorial on Uppaal. In: Formal Methods for the Design of Real-Time Systems: International School on Formal Methods for the Design of Computer, Communication, and Software Systems, Revised Lectures (pp. 200-–236). Springer, 2004.

2. Bouyer, P., Bozzelli, L., and Chevalier, F. Controller Synthesis for MTL Specifications. In Proceedings of the 17th International Conference on Concurrency Theory (CONCUR) (pp. 450—464). Springer, 2006.
3. Claßen, J. and Lakemeyer, G. A Logic for Non-Terminating Golog Programs. Proceedings of the 11th International Conference on Principles of Knowledge Representation and Reasoning (KR), 589—599, 2008.
4. Hofmann, T. and Lakemeyer, G. A logic for specifying metric temporal constraints for Golog programs. Proceedings of the 11th Cognitive Robotics Workshop (CogRob), 2018.
5. Hofmann, T., Mataré, V., Schiffer, S., Ferrein, A., and Lakemeyer, G. Constraint-based online transformation of abstract plans into executable robot actions. AAAI Spring Symposium: Integrating Representation, Reasoning, Learning, and Execution for Goal Directed Autonomy, 2018.
6. Levesque, H. J., Reiter, R., Lesperance, Y., Lin, F., and Scherl, R. B. GOLOG: a logic programming language for dynamic domains. Journal of Logic Programming, 31(1-3), 1997.
7. McDermott, D., Ghallab, M., Howe, A., Knoblock, C., Ram, A., Veloso, M., Weld, D., and Wilkins, D. PDDL - The Planning Domain Definition Language. The AIPS-98 Planning Competition Committee, 1998.
8. Hofmann, T. and Lakemeyer, G. Controller Synthesis for Golog Programs over Finite Domains with Metric Temporal Constraints. In: 17th International Conference on Principles of Knowledge Representation and Reasoning (Poster), 2020.

Safe Neural Network Controller for Agile Robots

Henrik Hose (henrik.hose@dsme.rwth-aachen.de)
Supervisor: Prof. Dr. Sebastian Trimpe

Fast feedback responses, stability, and constraint satisfaction are critical requirements for control in robotics to ensure safety. Model predictive control (MPC) achieves stability and constraint satisfaction, but is notoriously slow to evaluate. Approximation of such MPC controllers via (deep) neural networks (NNs) allows for fast online evaluation. However, the approximation introduces inaccuracies that can cause instabilities or constraint violations. In this project, novel methods for offline validation and safe online evaluation of approximations of MPC type controllers are developed. This work builds upon existing results in statistical offline validation, online safety certification in control, and explores the use of formal verification methods. Novel approximate MPC schemes with offline validation and safe online evaluation methods are evaluated in real-world problems from the robotics domain, such as the Wheelbot.

The Wheelbot, a small reaction wheel balancing robot, was originally developed at the DSME and MPI Stuttgart under the supervision of Prof. S. Trimpe. A video of the Wheelbot is available on Youtube ("The Wheelbot: A jumping reaction wheel unicycle"). The Wheelbot is a challenging robotics test bed for non-linear control when balancing, and even hybrid-systems with contact switches for stand-up maneuver. The next generation — the Mini Wheelbot — is engineered for production in small fleet quantities to serve as a hardware test bed at DSME.

Analyzing Termination and Expected Runtime Complexity for Probabilistic Term Rewriting

Jan-Christoph Kassing (kassing@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Jürgen Giesl

Using random actions or selections is a very useful ingredient for the development of algorithms. It is typically used to change deterministic algorithms with bad worst-case behavior into efficient random algorithms which produce correct results with a high probability. The Rabin-Miller primality test, Freivalds' matrix multiplication, and the random pivot selection in Hoare's quicksort algorithm are prime examples. These kinds of algorithms can be elegantly expressed as probabilistic programs. Determining runtime and termination in the probabilistic case is a difficult problem with often unintuitive results. In the probabilistic case there are multiple notions of termination. Two of the most important ones are Almost Sure Termination (AST), i.e., the program terminates with probability 1, and (Strong) Positive Almost Sure Termination (PAST), i.e., the program terminates within a finite number of expected steps. Whereas in the deterministic case a single diverging infinite run leads to non-termination and infinite runtime, this is not the case for either notion of termination in the probabilistic case. There are approaches amenable to automation, but most current techniques only focus on programs on numbers and disregard programs operating on data structures such as lists or trees. In contrast, in the non-probabilistic setting, many powerful and automatic approaches have been developed to analyze termination and complexity of these types of programs using an automatic analysis of term rewriting systems.
This project deals with the challenging question of how to automatically determine the respective properties of probabilistic programs dealing with data structures. The focus of the project is on analyzing probabilistic term rewriting systems (PTRSs). There are some results for PTRSs which use polynomial and matrix orders to determine PAST, but as with the non-probabilistic case, these techniques alone are not very powerful. The key idea for termination analysis in the classical case was the introduction of dependency pairs and the resulting possibility of a modular analysis of a term rewriting system. Therefore, one of the goals of this project is the adaption of this analysis technique to the probabilistic case, to develop a fully automated technique for the termination analysis of PTRSs. We have already created an adaption of the dependency pair framework to automatically analyze innermost AST, where we only consider rewrite sequences that follow an innermost evaluation strategy. Currently, we are investigating different ideas from the non-probabilistic framework on how to increase the effectiveness and applicability of our newly developed framework.

Privacy Preserving Online Algorithms

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

In secure multi-party computation a number of parties wants to compute a function over their inputs such that their inputs are kept private. The participating parties shall only learn their prescribed output without learning anything beyond that. The output can be either the same for all parties or each party obtains a different output. A trusted third party can be used to perform these computations. However, in some settings the parties want to keep their inputs private, e.g., if it is confidential or private information the parties are not willing to share with anyone. In order to keep the inputs private the parties avoid the trusted third party by computing the function in a distributed fashion, i.e., they jointly execute a secure protocol to simulate the trusted third party. In addition, such a protocol shall provide privacy and security in the presence of adversaries, i.e., a malicious party that wants to learn more than intended or deviates from the protocol specification arbitrarily.

For the most common secure multi-party computation settings it is assumed that everything is known prior to the protocol execution, i.e., the parties know their personal input and the set of parties participating in the protocol execution is somehow known. For such a determined setting there exist already a variety of protocols for different requirements. However, there are cases where the scenario is more uncertain and might change over time.

The aim of this dissertation project is to analyze these scenarios in more detail and provide a framework to define security and privacy in these settings. We will focus our research on online algorithms and develop protocols that can deal with different types of uncertainty.

Automated Complexity Analysis of Probabilistic Programs

Eleanore Meyer (eleanore.meyer@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Jürgen Giesl

In recent years, the study of probabilistic programs and methods to ensure their correctness has been an active field of research. Probabilistic programs are classical programs that are enriched with a notion of probabilistic choice. Such programs may then for instance branch on the outcome of a coin flip or assign a value that is sampled according to a probability distribution to a program variable.

One of the most important correctness properties of programs is their termination behaviour. When compared to classical programs the termination behaviour of their probabilistic counterparts is much more nuanced. One distinguishes between almost surely terminating (AST) programs, i.e., programs that terminate with probability 1 and positively almost surely terminating (PAST) programs that are characterised by the finiteness of their expected time to termination. In this project, we focus on the development of algorithms and techniques for the automated computation of (non-trivial) bounds on the expected time to termination. Such bounds can be interpreted as a measure of the efficiency of the analysed programs. Moreover, a finite bound guarantees the analysed program to satisfy PAST as well as AST (since PAST implies AST). Probabilistic ranking functions, a variant of ranking functions adapted for probabilistic programs based on the theory of ranking supermartingales[1] (RSM), present a natural way to obtain bounds on the expected time to termination.

In recently published work[2], we introduced the concept of expected sizes of program variables. Moreover, we presented a novel modular approach for the computation of (upper) bounds on the expected time to termination in a fully automated fashion by combining bounds on the expected time to termination for parts of the program with bounds on the expected variable sizes.

In ongoing work we are looking at possible improvements to the expressiveness of probabilistic ranking functions. While lexicographic variants already exist[3][4], there is, to the best of our knowledge, no equivalent of multiphase-linear ranking functions (MΦRFs)[5]. In the classical setting the nested version of MΦRFs leads to linear bounds on a program's runtime. If this does transfer to the probabilistic setting it will be particularly useful due to the linearity of the expected value operator.

For deterministic programs there are classes of non-trivial loops for which termination is known to be decidable[6][7]. In further ongoing work we investigate whether similar classes, which would allow the decidability of AST, exist in the case of probabilistic programs.

[1] L.M.F. Fioriti, Hermanns, H.: Probabilistic termination: Soundness, completeness, and compositionality. In: Proc. POPL '15. pp. 489–501 (2015)

[2] F. Meyer, M. Hark, J. Giesl: Inferring Expected Runtimes of Probabilistic Integer Programs Using Expected Sizes. In: Proc. TACAS (2021).

[3] S. Agrawal, K. Chatterjee, P. Novotný: Lexicographic ranking supermartingales: An efficient approach to termination of probabilistic programs. In: Proc. ACM Program. Lang. 2(POPL) (2017)

[4] K. Chatterjee, E.K. Goharshady, P. Novotný, J. Zárevúcky, D. Zikelic: On Lexicographic Proof Rules for Probabilistic Termination. In: Proc. Formal Methods (2021)

[5] A.M. Ben-Amram, S. Genaim: On multiphase-linear ranking functions. In: Proc. CAV '17 (2017)

[6] M. Hosseini, J. Ouaknine, J. Worrell: Termination Linear Loops over the Integers. In: Proc. ICALP 2019 (2019)

[7] M. Hark, F. Frohn, J. Giesl: Polynomial Loops: Beyond Termination. In: Proc. LPAR23 (2020)

Optimization under Adversarial Uncertainty

Komal Dilip Muluk (muluk@algo.rwth-aachen.de)
Supervisor: Prof. Dr. Britta Peis

An optimization problem under adversarial uncertainty can be essentially formulated as a game between a player and an adversary: The player partially constructs a feasible solution for a given scenario, and then the adversary completes this to a full feasible solution. The goal of the player is to optimize some objective function and the goal of the adversary is to make the player perform as bad as possible. There are various types of adversarial problems. The PhD thesis of Berit Johannes (2011)[1] develops a machinery for deriving hardness results for large classes of the optimization problems with adversarial uncertainty. The thesis only discusses the negative aspects (hardness results) of the area.

The goals of my doctoral project are twofold: On the one hand, the project will derive new negative results, perhaps by extending and generalizing the machinery of Johannes to other families of optimization problems, such as problems in robust optimization. This should lead to new families of hardness and completeness results for the first or the second level of the polynomial hierarchy or for one of the intermediate complexity classes. On the other hand, the goal of the project is to develop positive results for the considered optimization problems. Major emphasis will be put on the investigation of crucial problem parameters, which will be done by applying the tool kit of parameterized complexity. A further goal is the development of fast exact algorithms with decent running times. Finally, the project will identify tractable special cases, for instance by constraining the combinatorics of underlying graph structures, or by imposing additional conditions on underlying cost matrices.

[1] B. Johannes, "New Classes of Complete Problems for the Second Level of the Polynomial Hierarchy," Doctoral Thesis, TU Berlin, 2011

Algebraic Methods in SMT-Solving

Jasper Nalbach (Nalbach@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Erika Ábrahám

Introduction. Algorithms and tools for checking the satisfiability of quantifier-free first-order logic formulas over different theories have many applications in e.g. verification, planning and numerous other fields and enjoy increasing interest. The theory of non-linear real arithmetic (also called real algebra), whose formulas are Boolean combinations of (in)equalities between polynomial expressions evaluated over the real numbers, admits a high expressive power at the cost of high computational costs for satisfiability checking. A subset of this theory, linear arithmetic, where the polynomial expressions are all linear, can be solved more efficiently. In particular, these theories are expressive enough for encoding complex properties about uncertainties. These could be safety properties of systems with linear and non-linear behaviour such as neural networks, and more generally non-linear probability distributions This project is about the general problem of solving (non-)linear arithmetic rather than specific applications. For this, several algorithms are developed and extended, which are implemented and evaluated in our SMT solver `SMT-RAT` [1,2] which builds on top of our computer algebra library `CArL`.

Non-linear arithmetic. Although Tarski [3] proved in 1948 that non-linear arithmetic is decidable, the cylindrical algebraic decomposition (CAD) method published in 1975 by Collins [4] was the first complete decision procedure for its solution. Recently, several novel approaches have been developed; namely the model-constructing satisfiability calculus (MCSAT) [5], the one-cell construction method [6] and the cylindrical algebraic coverings method (CAlC) [7]. MCSAT and the one-cell construction can be used in a symbiotic way to solve existential real-arithmetic problems. This new approach is still based on the CAD idea, but instead of a full decomposition it uses the CAD idea to generalize a non-satisfying sample point to a non-satisfying region. The cylindrical algebraic covering methods generates a covering of unsatisfying regions using similar ideas. We developed and implemented a more flexible variant of the original one-cell construction algorithm. This work allows future improvements of both theoretical as well as heuristic nature.

Currently, a publication with a formal proof of the one-cell algorithm algorithm and its experimental evaluation is in progress. In the future, we will develop further improvements of this method and will re-implement the cylindrical algebraic coverings to benefit from these ideas as well.

Linear arithmetic. Linear arithmetic is of interest as it is not only a subset of non-linear arithmetic but also (incomplete) reductions from non-linear arithmetic to linear arithmetic exist. Thus, improving our linear arithmetic solver also benefits the non-linear solver.

The general Simplex algorithm [8] is the most common method for solving linear arithmetic in SMT solving. Despite its exponential running time in worst case, it is efficient in practical instances, heavily depending on chosen heuristics. We are working on improving our Simplex implementation using state-of-the-art heuristics.

Furthermore, we are developing a novel approach that could be promising in the SMT solving context based on the Fourier-Motzkin variable elimination [9] procedure. Extensions of this novel method for learning combinatorial properties of the problem as well as deeper interleaving with the Boolean structure of formulas are conceivable.

While working on these problems, we proved the extension of the Simplex method and others for strict inequalities, which is currently under review. Although a proof already exists, we think that our publication provides more insights into the nature of the problem.

`SMT-RAT` *and* `CArL`. For several reasons, we maintain our own library for arithmetic operations. We are currently evaluating our library against other libraries with regards to efficiency and examine possible extensions or integrations of our library.

References:

1. Kremer, Gereon, and Erika Ábrahám. Modular strategic SMT solving with SMT-RAT. Acta Universitatis Sapientiae, Informatica 10.1: 5-25, 2018.
2. Kremer, Gereon. Cylindrical Algebraic Decomposition for Nonlinear Arithmetic Problems. Dissertation RWTH Aachen, 2020.
3. Tarski, Alfred. A decision method for elementary algebra and geometry. Quantifier elimination and cylindrical algebraic decomposition. Springer, pages 24–84, 1998.
4. Collins, George E. Quantifier elimination for real closed fields by cylindrical algebraic decompostion. Automata Theory and Formal Languages, pages 134–183, Springer, 1975.
5. Jovanović, Dejan, and Leonardo De Moura. Solving non-linear arithmetic. International Joint Conference on Automated Reasoning. Springer, 2012.
6. Brown, Christopher W., and Marek Kosta. Constructing a single cell in cylindrical algebraic decomposition Journal of Symbolic Computation 70: 14–48, 2015.
7. Ábrahám, Erika, et al. Deciding the consistency of non-linear real arithmetic constraints with a conflict driven search using cylindrical algebraic coverings. Journal of Logical and Algebraic Methods in Programming 119: 100633, 2021.
8. Dutertre, Bruno, and Leonardo De Moura. A fast linear-arithmetic solver for DPLL (T). Proc. of CAV. Springer, 2006.
9. Fourier, Jean Baptiste Joseph. Solution d'une question particuliere du calcul des inégalités. Nouveau Bulletin des Sciences par la Société Philomatique de Paris 99: 100, 1826.

Analysis of the expressivity of Graph Neural Networks (GNNs) and similar deep learning architectures for graphs

Eran Rosenbluth (rosenbluth@oms.rwth-aachen.de)
Supervisor: Prof. Dr. Martin Grohe

Graph Neural Networks (GNNs) are a class of computation models for graph processing, used also in learning tasks on graphs. These may entail learning to classify graphs (or their nodes) or learning to regress unknown features of graphs (or their nodes). In any case, it is desired that the computational model of choice is both isomorphism-invariant and inherently scalable to arbitrary graph sizes. GNNs combine a Message-Passing computation scheme with Aggregation-and-Neural-Network computation blocks. The computation blocks are identical for every vertex, making GNNs isomorphism-invariant and inherently scalable algorithms. The use of neural networks makes GNNs deep learning algorithms, potentially benefiting from the power of that paradigm.
A key characteristic of any computational model used in learning is its expressivity. While there are significant results concerning the expressivity of GNNs, there are interesting and important questions yet to be answered. In my research I try to answer some of these questions e.g. how a certain property of a GNN's architecture affects its expressivity – whether a specific configuration subsumes others. While my work is mainly theoretical – formulating and proving theorems, it is augmented with developing experiments that test how the theoretical results come into play in practice.

Structural Network Analysis

Michael Scholkemper (scholkemper@cs.rwth-aachen.de)
Supervisor: Prof. Dr. Michael Schaub

Networks are a powerful abstraction to understand a range of complex systems such as

- protein interactions relating to drug efficacy,
- structural changes due to disease in respective tissue,
- the emergence of consensus or polarization through social interactions and epidemic spread, or
- the flow of traffic.

To comprehend such networks, we often seek patterns in their connections, e.g., densely interconnected communities or core-periphery structure, which facilitate a simpler or faster analysis of such systems. Communities are in this context typically envisioned as comparably tightly-knit nodes within a graph, though a range of different notions exists often defined in an algorithmic way, or by means of some cost function that is to be optimized. A complementary notion to „community“ is that of a role partition of the node. The concept of node roles – or node equivalences – originates in social network analysis, where a node‘s role – contrary to its community – is often related to symmetries or connectivity, rather than proximity. Both of these complementary approaches aim to simplify the network‘s complexity and provide a reduced view of the networks structure.

The intricacy of node role extraction derives from the lack of a clear definition of the role of a node in mathematical terms. Traditionally, exact equivalences such as automorphic or regular equivalence are considered. These approaches, while extremely expressive, yield a multitude of distinct roles that are incomparable to one another. More recently, node representation through embeddings aiming to capture these structural symmetries have been proposed. While these are clearly comparable by means of some distance measure in the vector space, the plethora of node embedding techniques yields no insight into what the role of a node is.

This research aims to derive a general definition of a node’s role and the resulting reduced view of the network’s structure. This, in turn, can then be applied to signal processing on graphs to provide a reduced view of a complex system of which only a process on the nodes but not the underlying network is observed. Apart from the structural analysis of a graph these node roles can also be used to obtain generative models that assert a certain global structure but are flexible locally. This is useful e.g. as a means of anonymization when sharing sensitive network data.

The Tournament Isomorphism Problem

Tim Frederik Seppelt (seppelt@informatik.rwth-aachen.de)
Supervisor: Prof. Dr. Martin Grohe

Introduction. The Graph Isomorphism Problem (GI), i.e. the computational problem of deciding whether two given graphs X and Y admit an isomorphism $X \leftrightarrow Y$, is of both theoretical and practical relevance in Computer Science and many adjacent fields [7]. For example, in chemistry it is desirable to determine whether two molecules encoded as graphs are structurally the same. The main interest from a theoretical viewpoint stems from the fact that despite intensive research efforts, the complexity of GI remains unknown. It is neither established that GI is NP-complete nor that it is in P. The best known algorithm, developed by Babai [2], runs in quasi-polynomial time in the number of vertices of the input graphs.

In order to resolve the complexity status of GI, restricted graph classes such as planar graphs and graphs with excluded minors have been considered in the past [6,8]. In each of these cases, researchers succeeded in showing that GI, when restricted to these classes, can be solved in polynomial time.

While the aforementioned graph classes have been eliminated as barriers for a potential polynomial time algorithm for GI, the class of tournaments persists in representing a bottleneck. Tournaments are directed graphs whose underlying undirected graphs are complete. The best known algorithm for the Tournament Isomorphism Problem (TI) from Babai and Luks [4].

Faster Algorithms for TI. Although decades-long research efforts have produced a variety of tools for variants of the GI, only a few methods tailored for the TI are known. TI fundamentally differs from other variants of GI in the sense that the automorphism group of a tournament is soluble which renders an efficient treatment of the occurring groups possible [9]. This in turn creates the need for refined combinatorial techniques. Subsequently, possible approaches for resolving the complexity status of TI are outlined.

Probabilistic Approaches. Probabilistic methods have been fruitfully used in the past in the context of TI. This includes randomized algorithms and reductions [11] but also probabilistic arguments used to derive structural insights into the involved combinatorial objects [1]. It is, therefore, desirable to further develop such probabilistic techniques in order to deepen the understanding of TI.

Exploiting Regularity. Whenever vertices of a graph can be distinguished, e.g. by their degrees, divide-and conquer techniques can be applied efficiently. These strategies fail if the graphs considered are regular. Looking at arcs instead of vertices gives rise to more powerful notions such as strong regularity. Especially in the realm of undirected graphs, the study of strongly regular graphs has led to a deep structural insights [5] and advanced algorithms [3,12]. This raises the question as to whether a structure theory for highly regular tournaments can be developed.

The Weisfeiler–Leman Algorithm. The Weisfeiler–Leman (WL) algorithm [13] is a ubiquitous tool in the context of the Graph Isomorphism Problem. Its k-dimensional version colors k-tuples of vertices according to their local structure. It is, hence, natural to identify levels of regularity with monochromaticity with respect to WL in certain dimensions. For example, graphs are strongly regular if and only if they are monochromatic with respect to 2-WL. Along these lines, the power of WL deserves further scrutiny. In [10], we studied the expressiveness of WL from a spectral perspective.

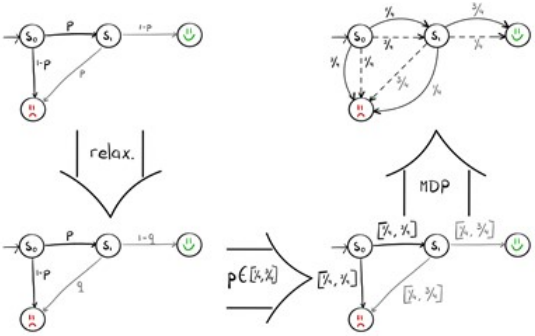
References:

1. László Babai. On the Order of Uniprimitive Permutation Groups. The Annals of Mathematics, 113(3):553, 1981.
2. László Babai. Graph Isomorphism in Quasipolynomial Time (Extended Abstract). In Proc. of STOC, pages 684—697, 2016.
3. László Babai, Xi Chen, Xiaorui Sun, Shang-Hua Teng, and John Wilmes. Faster Canonical Forms for Strongly Regular Graphs. I Proc. of FOCS, pages 157—166, 2013.
4. László Babai and Eugene M. Luks. Canonical labeling of graphs. Proc. of STOC, pages 171—183, 1983.
5. László Babai and John Wilmes. Asymptotic Delsarte cliques in distance-regular graphs. Journal of Algebraic Combinatorics, 43(4):771—782, 2016.
6. Martin Grohe and Dániel Marx. Structure Theorem and Isomorphism Test for Graphs with Excluded Topological Subgraphs. SIAM Journal on Computing, 44(1):114—159, 2015.
7. Martin Grohe and Pascal Schweitzer. The Graph Isomorphism Problem. Commun. ACM, 63(11):128–134, 2020.
8. Sandra Kiefer, Ilia Ponomarenko, and Pascal Schweitzer. The Weisfeiler-Leman dimension of planar graphs is at most 3. Proc. of LICS, pages 1—12, 2017
9. Eugene Luks. Permutation groups and polynomial-time computation. In Larray A. Finkelstein and William M. Kantor, editors, Groups and Computation, volume 11 of DIMACS Series in Discrete Mathematics and Theoretical Computer Science. American Mathematical Society, 1993.
10. Gaurav Rattan and Tim Seppelt. Weisfeiler–Leman, Graph Spectra, and Random Walks. 2021. Under Review for WG 2021.
11. Pascal Schweitzer. A polynomial-time randomized reduction from tournament isomorphism to tournament asymmetry. arXiv:1704.08529 2017.
12. Xiaorui Sun and John Wilmes. Faster Canonical Forms for Primitive Coherent Configurations: Extended Abstract. In Proc. of STOC, pages 693–-702, 2015.
13. Boris Weisfeiler. On Construction and Identification of Graphs, volume 558 of Lecture Notes in Mathematics. Springer, 1976.

Monotonicity in Parametric Markov Chains

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

In several kinds of systems probabilistic behaviour occurs. For instance unreliable or unpredictable behaviour in computer networks can be seen as probabilistic behaviour. Also, in a communication protocols, messages might not be received with a given probability, this yields a probabilistic state change.



Research has been done on formal methods for the specification and verification of probabilistic systems. Questions such as: “What is the probability that the file is transferred correctly if messages are lost with a probability 0.05?” could be analyzed through formal methods. One way to describe these probabilistic systems is through Markov chains. In a subset of these Markov chains all state changes are probabilistic and in discrete time.

However, the probabilities of these state changes are not always known in advance. Therefore, parametric Markov chains have been developed. They allow the use of parameters in the probabilities. For instance, in a biochemical reaction network, the rates of reactions might not be exactly known. In the past, they were then estimated. However, parametric Markov chains allow the analysis of them more precisely. Also in the case of transferring a file, the probability that a message is lost might not be known in advance. Instead of estimating this probability, we can now — based on the parametric Markov chain and a requirement, for instance “the probability that the file is transferred correctly should be at least 99%” — obtain parameter values for which the requirement holds.

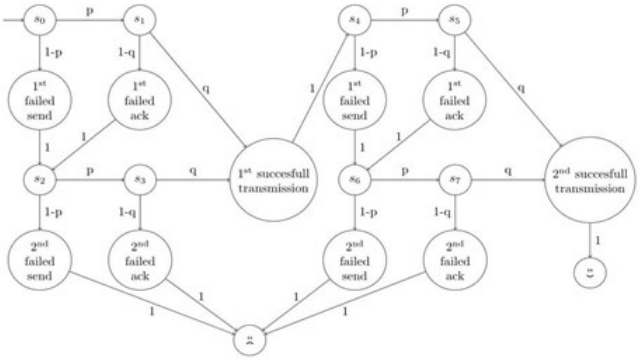


Figure 1: Parametric Markov chain

I want to investigate the effect of changing these parameter values on the probability that a requirement holds. In particular, parameters might have a monotone effect on the probability that a given system state is reached. I want to find this monotonicity in parameters and exploit this to improve the analysis on the behaviour of systems. During my Master's thesis I began work on this by providing a framework to determine monotonicity based on the probabilistic program describing a system.

My first two publications focus on finding monotonicity in parametric Markov chains and integrating this approach into existing techniques. The next goal is to extend the search for monotonicity to Markov decision processes, and possibly also to other Markov models. Furthermore, together with colleagues, I'm looking at other methods to improve the existing techniques.

Probabilites in Database Queries: Power and Complexity

Christoph Standke (standke@informatik.rwth-aachen.de)
Supervisor: Prof. Dr. Martin Grohe

Uncertainty plays a central role in modern database systems. It arises from many use cases, such as data integration, noisy data, data from unreliable sources or randomized processes. To obtain a quantitative framework to handle uncertainty, it is modelled via probability distributions.

Best studied in this area is the notion of finite *probabilistic databases (PDBs)*, which are finite probability spaces over database instances. For finite PDBs, the questions of representation and query evaluation under set semantics are well understood. We extend this knowledge in different directions:

Tuple-Independent Representations of Infinite Probabilistic Databases We systematically study the representability problem for infinite PDBs by means of tuple-independence and first-order views. Although first-order views over tuple-independent PDBs are not a complete representation system for infinite PDBs, they form a fairly robust class: Adding first-order constraints does not give them additional expressive power, and they cover many relevant special cases such as block-independent disjoint PDBs, and PDBs of bounded instance size. We identify criteria for representability (or non-representability) in this class and explore their limits.

Probabilistic Query Evaluation with Bag Semantics We study probabilistic query evaluation under *bag semantics* where tuples are allowed to be present with duplicates. Due to potentially unbounded multiplicities, the bag probabilistic databases we consider are no longer finite objects, which requires a treatment of representation mechanisms. Moreover, the answer to a Boolean query is a probability distribution over non-negative integers, rather than a probability distribution over $\{\mathsf{true}, \mathsf{false}\}$. Therefore, we explore two flavors of probabilistic query evaluation: computing expectations of answer tuple multiplicities, and computing the probability that a tuple is contained in the answer at most k times for some parameter k.

Furthermore, we also consider other sources of randomness than distributions over database instances:

The Importance of Parameter Values in Database Queries We propose and study a framework for quantifying the importance of the choices of parameter values to the result of a query over a database. These parameters occur as constants in logical queries such as conjunctive queries. This quantity is the SHAP score of the individual parameter values, as previously applied to feature values in machine-learning models. The application of the SHAP score requires two components in addition to the query and the database: (a) a probability distribution over the combination of parameter values, and (b) a utility function that measures the distance between the result for the original parameters and the result for hypothetical parameters. The main question we investigate is the complexity of calculating the SHAP score for different distributions and distances.

Programming and Verifying Uncertain Phenomena

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

In recent years, programming languages have been enhanced with probabilistic constructs, allowing programmers to write statements like "Flip a fair coin, if heads comes up then increment variable x by 1" or "If two processes A and B are in the same state, then process B crashes with probability 5%". It is important to understand that this extra randomness does not present a contradiction to the unambiguous nature of programming languages: Instead of yielding a predetermined output like classical programs, a probabilistic program typically results in a predetermined probability distribution over possible outputs. The following are a few of the most important use cases of probabilistic programs:

Randomized Algorithms are traditional algorithms extended with coin flips to increase performance or enable realizability of certain computational tasks. The latter is especially the case for computations distributed among several agents [1]. Such algorithms are meant to be actually implemented and run on a physical machine, often using a pseudo-random number generator.

Probabilistic Model Checking aims at verifying behavioural properties of processes involving randomness. The process under consideration is usually modelled by means of a probabilistic program. The purpose of the program is not to be actually executed but describe the process of interest in a precise mathematical manner. Application areas include verification of randomised—often distributed— algorithms (internal randomness), systems making decisions in an uncertain environment (external randomness), biological processes and many more. A distinguishing feature of model checking is that the program at hand is typically (but not always) finite-state. This enables exact algorithmic solvability (decidability) of almost all properties of interest by constructing a finite low-level model of the process such as a continuous- or discrete-time Markov chain, a Markov Decision Process, a stochastic game and others. See [2] for an overview of the field.

Probabilistic Programming (e.g. [3]) is a relatively new paradigm that aims to automate statistical inference. Similar to model checking, programs of the corresponding languages are not meant to be run directly but rather to describe a process in which unknown events may occur. The purpose of a Probabilistic Programming System is to automatically infer the likelihood of those events given observations about the outcome (or intermediate stages) of the process. It can, thus, be seen as an automated approach to Bayesian statistics, and it generalizes traditional graphical models such as Bayesian networks. Languages for Probabilistic Programming typically support continuous probability distributions and have additional primitives for observations. In general, inference can only be done approximately, using sampling based approaches.

Clearly, the three directions are closely related. Moreover, program verification is key in all of them: While this is obvious for Randomised Algorithms and Probabilistic Model Checking, it turns out that verification and inference mostly coincide in the case of Probabilistic Programming. The aim of my research is twofold:

A. To help foster a common theoretical basis for the three areas: More specifically I am interested in the development of new verification logics in the spirit of classical Hoare logic and weakest precondition transformers [4,5] to facilitate and systemize the verification tasks mentioned above. This is closely related to program semantics—mathematical definitions of the meaning of a program—as different approaches to semantics lead to different verification rules.

B. Contributions to the ample field of Probabilistic Model Checking, more concretely:

   1. Stochastic games. Such games arise from controlled stochastic processes, additionally faced with unquantifiable uncertain external events, i. e., events whose occurrence cannot be described be means of probabilities, e.g. because relevant statistical data is unavailable. I plan to investigate the two-player turn-based variant of such games under non-standard multi-objectives [6].
   2. Recursive stochastic processes. These are naturally described by imperative probabilistic languages allowing (mutually) recursive function calls. I plan to work on Model Checking finite-state versions of such programs [7]. Applications include self-reproducing stochastic processes.
   3. Program rewriting. Another direction I intend to pursue is to rewrite probabilistic programs prior to Model Checking with the aim of simplifying the latter task, in particular by decreasing the size of the resulting finite-state model.

References:

1. Ted Herman. Probabilistic Self-Stabilization. Inf. Process. Lett. 35(2), p. 63–67 (1990)
2. Joost-Pieter Katoen. The Probabilistic Model Checking Landscape. LICS 2016, p. 31–45 (2016)
3. Andrew D. Gordon et al. Probabilistic Programming. FOSE 2014, p. 167–181 (2014)
4. Annabelle McIver and Carroll Morgan. Abstraction, Refinement and Proof for Probabilistic Systems. Monographs in Computer Science, Springer (2005)
5. Benjamin L. Kaminski. Advanced weakest precondition calculi for probabilistic programs. PhD Thesis (RWTH Aachen University), Germany, (2019)
6. Taolue Chen et al. On Stochastic Games with Multiple Objectives. MFCS 2013, p. 266–277 (2013)
7. Javier Esparza et al. Model Checking Probabilistic Pushdown Automata. LICS 2004, p. 12–21 (2004)

GRK 2428: ConVeY — Continuous Verification of Cyber-Physical Systems

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

Networks, computers, sensors, and actuators are being increasingly integrated into cyber-physical systems, i.e., software systems that interact with the physical world and must cope with its continuous behavior. An increasing number of cyber-physical systems operate in safety-critical domains, e.g., autonomous vehicles, robotic surgery, traffic control, human-robot collaboration, and smart grids. For this reason, their design and deployment should ideally be accompanied by a formal check of correct behavior. A fundamental challenge in the verification of cyber-physical systems is the fact that they are subject to change. The physical environment changes continuously, at runtime, and in ways that cannot be completely foreseen at the design stage. At the same time, the requirements may change. Sought-after aspects include more functionality, lower power consumption, or faster response. In many cases, the system should be migrated to a different hardware platform. To face this multi-level continuous change, we propose to

- develop verification and synthesis technology for robust system design, i.e., for the design of systems that maintain correct behavior under change
- develop verification and synthesis technology able to cope with frequent or even continuous change in the specification and the environment.

Areas of Research

Robust System Design. We will develop techniques to guarantee correct behavior under changes in plant parameters, under certain classes of perturbations including sensor measurement errors, and under uncertainties introduced by the implementation platform. In particular, we will investigate the design of controllers that are robust by construction against those changes.

Evolving Systems. Novel construction and verification techniques shall be investigated that adapt to offline changes in the specification, the hardware, or the implementation of control software, and reuse efforts from earlier stages as much as possible.

On-the-fly Synthesis and Verification. We will develop techniques for the online verification and synthesis of controllers that operate—and provide a correctness guarantee—only within a given time horizon. Repeated execution of this procedure, combined with availability of a fail-safe strategy, ensures safe operation.

Formal Verification and Synthesis of Stochastic Cyber-Physical Systems

Mahathi Anand (mahathi.anand@lmu.de)
Supervisor: Prof. Dr. Majid Zamani

Cyber-physical systems (CPS), *i.e.*, systems with interacting physical and software components, have achieved significant attentions in the past two decades. They model many applications such as power grids, air traffic networks, medical equipment, etc., and are often required to perform complex logic tasks. Examples of such tasks include those expressed as linear temporal logic or (in)finite strings over automata. Due to the large system size and the presence of random disturbances and uncertainities, the development and verification of safe CPSs is a challenging problem. Therefore, formal verification and synthesis of large-scale stochastic control systems against temporal logic specifications has received significant attentions in past few years. Traditionally, such systems have been analyzed using discretization-based methods [1]. These approaches suffer from the curse of dimensionality since the computational complexity grows exponentially with the number of state variables. More recently, discretization-free techniques using barrier certificates [2] have been developed to potentially alleviate this computational burden. In the context of stochastic control systems, barrier certificates take the form of inductive expectation invariants. They are non-negative real-valued functions that take higher values over the unsafe states of the system than in the initial states and satisfy the *supermartingale* property, *i.e.*, the expected value decreases as the system evolves. Then, the existence of suitable barrier certificates guarantees the satisfaction of logic specifications such as safety. However, the computation of barrier certificates is a difficult problem. First, imposing the supermartingale requirement on barrier certificates can be very restrictive. As a result, fewer classes of functions can behave as barrier certificates. In order to overcome this problem, we propose the notion of k-inductive barrier certificates which relax the traditional conditions and allow to improve the search for barrier certificates. Secondly, the computation of barrier certificates is not scalable to large-scale systems. To handle these limitations, we propose a compositional controller synthesis framework to construct barrier certificates for large-scale stochastic control systems. Utilizing these, the goal is to synthesize hybrid controllers enforcing specifications that are expressed by automata over (in)finite time horizons, while providing a (potentially tight) lower bound on the probability that the system satisfies the given specifications.

[1] A. Lavaei, S. Soudjani, and M. Zamani, "*Compositional (in)finite abstractions for large-scale interconnected stochastic systems*," IEEE Transactions on Automatic Control, vol. 65, no. 12, p. 5280–5295,2020.

[2] S. Prajna, A. Jadbabaie, and G. J. Pappas, "*A framework for worst-case and stochastic safety verification using barrier certificates*", IEEE Transactions on Automatic Control, vol. 52, no. 8, p. 1415–1428,2007

Energy-Efficient Scheduling Algorithms for Processor Systems

Gunther Bidlingmaier (g.bidlingmaier@tum.de)
Supervisor: Prof. Dr. Susanne Albers

Reducing the energy usage of computing systems has become a major concern in recent years. Reasons include ecological, economical and thermal concerns as well as wide adoption of battery powered devices. As of this writing in 2022, the conservation of energy is also a crucial political concern in Europe due to Europe's strategic dependence on oil and gas imports from Russia. The study of energy-efficient algorithms aims to reduce the energy usage of computer systems while still guaranteeing certain performance bounds.

I study a particular setting in which a set of n jobs with individual release times, deadlines, and processing times has to be scheduled across p homogeneous processors while minimizing the consumed energy. Idle processors can be turned off so as to save energy, while turning them on requires a fixed amount of energy. While there had not been any results for the general version of this basic scheduling problem for a long time, recent work[1] developed the first algorithm with significant mathematical guarantees. Their algorithm is based on Linear Programming and rounding and guarantees that the energy consumed by the resulting schedule is at most 3 times the minimum required energy. More recent work[2] slightly modified this Linear Program and improved the approximation guarantee to a factor of 2.

While Linear Programming is a powerful and generic algorithmic technique, it provides little insight into how a solution is constructed. On the other hand, Combinatorial Algorithms and in particular Greedy Algorithms, which operate by making locally optimal choices, often provide valuable insights into how a solution is constructed. Greedy Algorithms are also often preferred in practice since their implementation tends to be simpler.

I identified two simple Greedy Algorithms which are suitable for the problem and showed that their resulting schedules exhibit non-trivial structural properties. My further work aims at using these structural properties to provide constant-factor approximation guarantees for the two Greedy Algorithms.

[1] Antonios Antoniadis, Naveen Garg, Gunjan Kumar, Nikhil Kumar, "Parallel Machine Scheduling to Minimize Energy Consumption," Proceedings of the 2020 ACM-SIAM Symposium on Discrete Algorithms, SODA 2020, p. 2758-2769, 2020

[2] Antonios Antoniadis, Gunjan Kumar, Nikhil Kumar, "Skeletons and Minimum Energy Scheduling", 32nd International Symposium on Algorithms and Computation, ISAAC 2021, p. 51:1-51:16, 2021

Logical Safety Analysis of Concurrent Cyber-Physical Systems

Marvin Brieger (marvin.brieger@sosy.ifi.lmu.de)
Supervisor: Prof. Dr. André Platzer

Cyber-physical systems (CPSs) are ubiquitous in our everyday lives. They occur as cars, robots, airplanes, etc., and are often safety critical. However, due to their interlocked discrete and continuous dynamics CPSs are difficult to get right making them a natural target of verification [1].

Often a CPS can be better understood as several CPSs running in parallel. For example, each car in a convoy is a CPS on its own. However, the convoy needs to be studied as a whole including the interaction between the cars to answer questions about the convoy's safety. This verification of parallel CPSs is challenging as hybrid systems verification and concurrency verification are nontrivial challenges own their own. Additionally, parallel CPSs share physical time synchronously. The fact that parallelism is omnipresent in real world makes the development of verification techniques for parallel CPSs significant.

To tackle the CPS concurrency challenge, we aim for the development of a concurrency extension of differential dynamic logic $d\mathcal{L}$ [2]. In $d\mathcal{L}$ CPSs are modeled using hybrid programs and verified using dynamic logic. So far we extended hybrid programs with a parallel operator and communication primitives for modeling parallel CPS behavior. For verification, we adapted the assumption-commitment approach[3] to $d\mathcal{L}$, which allows for compositional reasoning about parallelism and communication behavior.

[1] André Platzer, "Logic and proofs for cyber-physical systems," Proc. 8th Intl. Joint Conf. Automated Reasoning (IJCAR), vol. 9706 of LNCS, p. 15 – 21, 2016

[2] André Platzer, "Logical Foundations of Cyber-Physical Systems," Springer, 2018

[3] Jayadev Misra and K. Mani Chandy, "Proofs of Networks of Processes," IEEE Transactions on Software Engineering, vol. 7(4), p. 417 – 426, 1981

Bridging the Gap between Hardware and Software Verification

Po-Chun Chien (po-chun.chien@sosy.ifi.lmu.de)
Supervisor: Dirk Beyer

Hardware verification and software verification are two research fields that share common theoretical foundations. The advancement in one field can often benefit the other. For example, some verification algorithms originally developed for hardware systems, such as bounded model checking and k-induction, have been successfully extended to software systems. Our recent study[1] shows that, via single-loop transformation and large-block encoding, interpolation-based model checking (IMC)[2] and interpolation-sequence based model checking (ISMC)[3] algorithms, both of which were designed for hardware, can also be adopted for software verification. The two algorithms have been implemented in the software verification framework CPAchecker[4] and were compared against several other verification algorithms. The evaluation shows that our adoption is successful and that both IMC and ISMC are competitive among other algorithms in terms effectiveness and efficiency.

In another line of research, we attempt to narrow the gap between hardware and software analysis by verifying hardware systems with software verifiers, and vice versa. One way to achieve this is by converting hardware systems into software programs. With such conversion, we could easily leverage all existing software verifiers to analyze hardware systems. Therefore, we develop Btor2C[5], a converter from word-level sequential circuits in Btor2[6] format to procedural C programs. Btor2 is a simple yet bit-precise language that can be deemed an intermediate representation tailored for analysis. Given a Btor2, Btor2C generates a behaviorally equivalent C program, which can then be taken as input by most software verifiers. The experimental results show that software-analysis tools performed quite decently on our benchmark tasks and was able complement hardware model checkers by uniquely solving several tasks that the latter could not. The proposed tool gives hardware designers and verification engineers an opportunity to try out software-analysis tools for enhanced quality assurance. In the future, we plan to bridge the gap from the other direction, i.e. by converting software programs into hardware circuits such that one can utilize hardware analyzers to solve software problems.

---

[1] D. Beyer, N.-Z. Lee, P. Wendler, "Interpolation and SAT-Based Model Checking Revisited: Adoption to Software Verification," arXiv:2208.05046, 2022.

[2] K. L. McMillan, "Interpolation and SAT-Based Model Checking," Proc. CAV, pp. 1-13, 2003.

[3] Y. Vizel, O. Grumberg, "Interpolation-sequence based model checking," Proc. FMCAD, pp. 1-8, 2009

[4] `https://cpachecker.sosy-lab.org/`

[5] `https://gitlab.com/sosy-lab/software/btor2c`

[6] A. Niemetz, M, Preiner, C. Wolf, A. Biere, "Btor2, BtorMC and Boolector 3.0," Proc. CAV, pp. 587-595, 2018

Study of Weak Models of Distributed Computing

Philipp Czerner (czerner@in.tum.de)
Supervisor: Prof. Dr. Javier Esparza

Many natural or artificial distributed systems, such as molecules, cells, microorganisms or nanorobots, consist of parts with limited computational capacities. These parts (called *agents*) can, for example, store only a small amount of information, have no identities, and interact stochastically. Various *weak* models of distributed computing have already been researched intensely in the literature, such as population protocols or chemical reaction networks.

The goal of this area of research is to find efficient protocols to perform distributed computations in these models and analyse their characteristics. Additionally, we want to develop automated procedures which can prove properties of specific protocols, such as their correctness or running-time.

I focus both on extending the existing theoretical knowledge on models such as population protocols, and on considering variants of known models.

Population protocols are a weak model of distributed computing, where agents have only finitely many states. They interact pairwise and stochastically – an agent has no knowledge about the global state of the population. Despite these limitations, they can compute global properties of the initial configuration, e.g. whether initially more "red" than "blue" agents exist in the population.

A natural topic of inquiry is the *succinctness* of population protocols: how many states does a protocol need to implement certain properties? Here, we showed the first elementary lower bound, by proving that protocols for properties of the form $x \geq k$, where k is a constant and x the number of agents in the population, have at least $\Omega(\log \log \log k)$ states. We since improved that bound to $\Omega(\log \log k)$ and very recently presented a $\mathcal{O}(\log \log k)$ construction, meaning that the bounds are tight. In a related investigation, we gave a construction for *arbitrary* predicates that is both succinct and fast, and close to optimal on both axes — showing that there is no space-speed tradeoff.

Chemical reactions are often assumed to be well-stirred, meaning that an agent does not have a fixed location and could interact with any other agent. For other, e.g. biological, systems this assumption does not hold, however, and an agent can communicate only with its neighbours in some fixed structure (a communication graph). We investigate protocols operating on these structures, where an agents perceives only the states of its neighbours. Based on a previous classification, we determine the expressive power for a number of classes. This enables comparisons between different models, and helps answering basic questions such as: "How important is randomness in this model?" or "How much information do agents need about their neighbours to decide certain properties?"

Controller synthesis for stochastic systems

Kush Grover (grover@in.tum.de)
Supervisor: Jan Křetínský

My research aims to develop techniques for synthesizing controllers with guarantees for safety critical systems. A safety-critical system is a system whose failure or malfunction may result in death/serious injury to people or loss of a lot of money. Therefore it is necessary to prove correctness of such systems. Markov decision processes (MDP) are widely used formalism for modeling non-deterministic and probabilistic behaviors of systems like a robot, warehouse storage management etc. Another popular stochastic model is Stochastic Games (SG) which can model interactions between a system and an agent or the environment.

Usually, for any continuous system, a model is generated by some sort of abstraction which discretizes the actual continuous space. Although, there exist sound analysis techniques which gives guarantees on the discrete models, these abstractions can be a source of errors in the final result. Hence, to tackle this problem, we have developed an algorithm to solve the rechability problem in a continuous space MDP directly while preserving the guarantees. This algorithm also generates an optimal controller for which the error is bounded by some given precision.

We modeled a robotic arm using a discrete MDP which incorporates the high level tasks the arm can perform. We use PRISM to generate the controller and dtControl to store and use it efficiently. We synthesize universal controllers that only depends on the current state of the system, making it faster to execute and have a fail-safe mechanism as well. We also give a way to improve the model of the robot by figuring out which states do not have a fail-safe action. This approach can be extended to work with more complicated models and also to find the best strategy w.r.t different reward structures. We also apply these methods in the context of fault detection, isolation and recoverability (FDIR) for satellites. We gave a way to find good strategies to isolate a fault by modeling the architecture of the satellite using MDPs.

We also solved a problem in the domain of motion planning that deals with finding a path for a robot satisfying some specification. We gave an algorithm which works in an unknown environment and tries to learn some semantic patterns that are present there and take advantage of them. It performs much better than the naïve “first explore, then plan” algorithm [**?**] if there are such patterns present in the environment. We solved this problem for LTL (Linear Temporal Logic) specifications and LTL is commonly used to specify high level specification. For low level specifications, Signal Temporal Logic (STL) is the usual choice. However, in STL, it is not possible to naturally express path segments and we want to develop a new logic in which it is possible to specify “fuzzy paths" which might be more useful in the context of low level motion planning.

Verification of Population Protocols and Chemical Reaction Networks

Martin Helfrich (helfrich@in.tum.de)
Supervisor: Javier Esparza

Population protocols are a model of distributed computation where a constant but unknown number of finite-state *agents* interact to decide a property. For example, in a majority protocol, there are initially agents that vote for "yes" and agents that vote for "no". The agents need to decide if there is a majority for "yes" by interacting in pairs. All agents follow the same protocol that determines how two agents in a rendez-vous interaction change their state. By interacting in a stochastic manner, the agents need to stabilize to the correct consensus in order to answer the property in question for every possible number of agents.

Population protocols are widely studied in the distributed computation community. Research areas are for example their *computational power*, their *computation speed*, and their *succinctness*. We proof that for every computable predicate there is a fast and succinct protocol computing it. In a different line of work, we presented a sound and complete method for the automatic verification of population protocols using witness in form of stage graphs that can be used to explain the correctness of in a visual manner.

While population protocols are a theoretical model, the closely-related model of *chemical reaction networks* has more practical applications such as modeling and analysis of biochemical systems, high-level programming of molecular devices and synthetic biology. In a chemical reaction network, molecules interact in reactions with different speeds that correspond to actual chemical reactions.

An important research topic is the efficient analysis of these complex and possibly infinite-state systems to accurately predict the evolution of a mixture of molecules without the need for an expensive and potentially dangerous wet lab. Because chemical reaction networks have an infinite state space, abstractions are used to make the system more tractable while preserving its global behavior.

To analyse the transient behaviour of a chemical reaction network, one can approximate the transient distribution of the system at a later time by repeated simulation. For this to yield a meaningful result, a large number of such simulations are needed. Because classical simulation of complex chemical reaction networks can be very time consuming, we proposed a novel memoization approach where small parts of already simulated trajectories, called segments, are reused efficiently. To make reusing segments feasible, we leverage population abstraction that splits the state space of the system into regions that behave similarly. To further scale our memoization approach we use the limited memory where it is most efficient. By leveraging other advanced simulation techniques, we can archive an even larger simulation speed-up.

Formal Synthesis of Controllers for Interconnected Stochastic Control Systems with Partial Information

Niloofar Jahanshahi (niloofar.jahanshahi@lmu.de)
Supervisor: Majid Zamani

In the past decade, CPSs have become ubiquitous and an integral part of our daily lives. Examples of such systems range from autonomous vehicles, drones, and aircraft to robots and advanced manufacturing. In many applications, these systems are expected to do complex logic tasks. Such tasks can usually be expressed using temporal logic formulae or as (in)finite strings over finite automata. In the past few years, abstraction-based techniques have been very promising for the formal synthesis of controllers. Since these techniques are based on the discretization of state and input sets, when dealing with large-scale systems, unfortunately, they suffer severely from the curse of dimensionality (*i.e.*, the computational complexity grows exponentially with the dimension of the state set). In order to overcome the large computational burden, a discretization-free approach based on *control barrier functions* has shown great potential to solve formal synthesis problems. In our research, we provide a systematic approach to synthesize a hybrid control policy for partially-observable (stochastic) control systems without discretizing the state sets. In many real-life applications, full-state information is not always available (due to the cost of sensing or the unavailability of the measurements). Therefore, in our research, we consider partially-observable (stochastic) control systems. Given proper state estimators, our goal is to utilize a notion of control barrier functions to synthesize control policies that provide (and potentially maximize) a lower bound on the probability that the trajectories of the partially-observable (stochastic) control system satisfy complex logic specifications such as safety and those that can be expressed as deterministic finite automata (DFA). To overcome the challenges encountered with large-scale systems, we develop approaches to reduce the computational complexity. In particular, by considering a large-scale partially-observable control system as an interconnection of lower-dimensional subsystems, we compute so-called *local control barrier functions* for subsystems along with the corresponding local controllers. By assuming some small-gain type conditions, we then utilize local control barrier functions of subsystems to compositionally construct an overall control barrier function for the overall interconnected system. Finally, since closed-form mathematical models of many physical systems are either unavailable or too complicated to be of any use, we also extend our work to the synthesis of safety controllers for partially-observable systems with unknown dynamics. To tackle this problem, we utilize a data-driven approach and construct control barrier functions and their corresponding controllers via sets of data collected from the output trajectories of the systems and the trajectories of the estimators.

Provably Safe Reinforcement Learning for Motion Planning of Autonomous Systems

Hanna Krasowski (hanna.krasowski@tum.de)
Supervisor: Matthias Althoff

For real-world motion planning tasks of autonomous cars, vessels, drones or other mobile robots, it is necessary to guarantee that the system behavior satisfies safety specifications. At the same time these tasks are highly complex, so that data-driven methods are often favored over standard control approaches. For motion planning tasks, reinforcement learning is well suited. However, reinforcement learning agents usually explore at random and unsafe actions are potentially executed, which impedes broad applicability to real-world tasks.

We aim to develop methods to decrease the randomness in reinforcement learning such that no unsafe states are explored during training and deployment. To this end, we use online verification techniques to verify actions before their execution. The resulting approaches are provably safe and can be applied to safety-critical tasks since they guarantee that the safety specifications always hold. In particular, we are interested in motion planning tasks of cyber-physical systems that interact with the physical world and humans.

As the field of provably safe reinforcement learning was not well distinguished from other safe reinforcement learning approaches, we specified the properties of provably safe reinforcement learning and developed an intuitive categorization for these methods. Next to this survey, we have been investigating: autonomous driving, autonomous vessels and cyber-physical systems. For autonomous driving, we showed that we can achieve provably safe reinforcement learning for highway driving and urban driving at intersections. For autonomous vessels, we formalized traffic rules to use them for verification later in this project. Furthermore, we developed CommonOcean, which is benchmarking suite for motion planning on water. For cyber-physical systems, we developed an approach that detects unsafe actions directly via reachability analysis and if necessary corrects them to the closest safe action. This approach evolved from our application-specific approaches and is more general.

We also are investigating how to integrate safety specifications that are more complex than reach-avoid in the online verification process. To this end, we developed a concept to achieve probabilistic guarantees for temporal logic specifications for a reinforcement learning agent.

For the remainder of the doctoral project, we want to research on more integrated methods for including temporal logic specifications and compliance to them in the reinforcement learning process. Here, we aim for an approach that can deal with a variety of specifications such as traffic rules and collision avoidance with dynamic obstacles and is as automatic as possible. In particular, we want to look at the use case of motion planning for autonomous vessels on the open ocean.

Formalization and Verification of Post-Quantum Cryptography

Katharina Kreuzer (k.kreuzer@tum.de)
Supervisor: Tobias Nipkow

Since communication is a key point in cyber-physical systems, it is important to ensure a safe communication. Especially since quantum computers come ito reach more and more, the threat of breaking current, widely used crypto systems is imminent. Developing quantum resistant cryptography – and verifying it – is a major task of modern research. For the long term goal of my research, the focus lies on verifying post-quantum crypto algorithms applicable to cyber physical systems, using the proof assistant Isabelle.

For the main project, the post-quantum crypto system Kyber was formalized and its correctness and some security properties were verified in the theorem prover Isabelle [1]. An extended version [2] was submitted to a cryptography conference. Kyber is a lattice-based post-quantum public-key encryption (PKE) scheme based on the module Learing-with-Errors problem and was chosen as the first winner of the NIST standardisation process for post-quantum PKE schemes. Since several error terms in the algorithms are chosen to blur the keys and the message, one has to make sure that the message is indeed decoded correctly. This has been verified in Isabelle. During the formalization, an error in the original proof was uncovered.

For the future, my goal is to formalize and verify security properties against quantum adversaries. The One-Way-to-Hiding (O2H) Lemma is the core theorem in this area. However, the O2H Lemma was axiomatized in the "qrhl-tool", currently the only tool that allows formalization of security properties against quantum adversaries. A foundational formalization of the O2H Lemma would thus significantly improve the trustworthiness of security proofs against quantum adversaries.

As a secondary project, the NP-hardness of lattice problems was inspected. First of all, the classical NP-reduction proofs of the partition problem to the closest vector problem and the shortest vector problem in the ℓ_∞ norm (according to [3] and [4]) were formalized and submitted to an appropriate conference. This will be the first formalization of NP-hardness reduction proofs underlining the security of post-quantum crypto systems in Isabelle. For the ℓ_2 norm, there only exist randomized reduction proofs. My next goal in this area is to implement a framework to formalize and verify randomized reduction proofs as well. In my knowledge, this has not been attempted so far.

[1] `https://isa-afp.org/entries/CRYSTALS-Kyber.html`

[2] `https://eprint.iacr.org/2023/087`

[3] D. Micciancio and S. Goldwasser, "Complexity of Lattice Problems" Springer US, p. 48-52, 2002

[4] P. van Emde-Boas, "Another NP-complete Partition Problem and the Complexity of Computing Short Vectors in a Lattice" Department of Mathematics University of Amsterdam, vol. 81, 1981

Neural Network Abstraction for Accelerating Verification

Stefanie Mohr (mohr@in.tum.de)
Supervisor: Prof. Dr. Jan Krestinsky

Neural Networks (NN) are successfully used to solve many hard problems reasonably well in practice. However, there is an increasing desire to use them also in safety-critical settings, such as perception in autonomous cars, where reliability has to be on a very high level and that level has to be guaranteed, preferably by a rigorous proof. This is a great challenge, in particular, since NN are naturally very susceptible to adversarial attacks, as many works have demonstrated in the recent years [1]. Consequently, various verification techniques for NN are being developed these days. Most verification techniques focus on proving robustness of the neural networks, i.e. for a classification task, when the input is perturbed by a small ε, the resulting output should be labeled the same as the output of the original input. Unfortunately, verification tools struggle to scale when faced with real-world neural networks. Reducing the size of a NN by abstraction leads to several possibilities. Firstly, since the abstracted NN is smaller, it may be preferred in practice because generally smaller networks are often more robust, smoother, and obviously less resource-demanding to run. Note that there is a large body of work on distilling smaller NN from larger ones, e.g. re naturally very susceptible to adversarial attacks, as many works have demonstrated in the recent years [2], i.e. training a smaller NN based on the output of a bigger one. Secondly, and more interestingly in the safety-critical context, we can use the smaller abstract NN to obtain a guaranteed solution (robust or satisfying other properties) to the original problem: We can analyze the abstract NN more easily as it is smaller and then transfer the results to the original one, provided the differences are small enough.

We already developed an abstraction framework for NN. In contrast to syntactic similarities, such as having similar weights on the edges from the previous layer [3], our aim is to provide a behavioral, semantic notion of similarity, such as those of predicate abstraction, since such notions are more powerful. Additionally, we investigate the behavior of neurons not only in the sense of similarity based on weights, but also in their linear dependence. It can be seen that neurons often span a space that is smaller than their number which leads to the assumption that some of them are linearly dependent.

In future, we want to extend the tool for application to more complex settings and create a full CEGAR-loop.

[1] Akhtar, Naveed and Mian, Ajmal, "Threat of adversarial attacks on deep learning in computer vision: A survey," IEEE, 2018
[2] Hinton, et al., "Distilling the Knowledge in a Neural Network," 2015
[3] Guoqiang Zhong et al., "Merging Neurons for Structure Compression of Deep Networks," ICPR, 2018

Theoretical Analysis and Formal Guarantees of Machine Learning Algorithms

Mahalakshmi Sabanayagam (maha.sabanayagam@tum.de)
Supervisor: Prof. Dr. Debarghya Ghoshdastidar

Machine learning has become the preferred choice for problems in a wide range of fields, from microbiology to cosmology due to their remarkable performances. For instance, Deep Neural Networks (DNNs), a modern machine learning method, predicted the protein structure with very high accuracy, incomparable to any other methods. Despite their phenomenal success, these networks are poorly understood as classical learning theory fails to explain the behavior of modern machine/deep learning[1] and therefore, these methods require exploration of non traditional analysis.

In the recent years, interesting research directions are developed by rigorous theoretical and empirical study of shallow neural networks. One approach is to analyse the network in *infinite width limit* theoretically, which resulted in establishing an interesting connection between neural networks and kernel machines[2]. Another breakthrough is the discovery of a peculiar phenomenon in deep over-parameterized neural networks called *double descent*[3].

One of our research goals is to explain the behavior of neural networks developed specifically for graph data called graph neural networks using the infinite width analysis. Graph neural networks are of particular interest as it exhibits different characteristics compared to DNNs when made deeper. As a first step, we studied the effect of an aspect of the network called normalisation [4] and further continuing to explore other components of the network. Another direction of our research aims at theoretically deriving the double descent phenomenon for a simplified neural network architecture.

We further focus on studying robustness of DNNs theoretically as DNNs are vulnerable to noise in the ground truth labels and to indistinguishable modification to the input data, both cause the model to misclassify it. Different methods are developed to increase robustness, but this comes at the expense of accuracy. We specifically analyse this tradeoff between accuracy and robustness of DNNs with the larger goal to reason the unreliability of the networks and with the possibility to develop effective techniques to overcome it.

[1] V. Nagarajan, and J. Z. Kolter. "Uniform convergence may be unable to explain generalization in deep learning." Neural Information Processing Systems, 2019

[2] A. Jacot, F. Gabriel, and C. Hongler. "Neural tangent kernel: Convergence and generalization in neural networks." Neural Information Processing Systems, 2018.

[3] M. Belkin, D. Hsu, S. Ma, and S. Mandal. "Reconciling modern machine learning and the bias-variance trade-off." Proceedings of the National Academy of Sciences, 2019

[4] M. Sabanayagam, P. Esser, and D. Ghoshdastidar. "New Insights into Graph Convolutional Networks using Neural Tangent Kernels." arXiv:2110.04060, 2021.

Verified Solution Methods for Markov Decision Processes

Maximilian Schäffeler (maximilian.schaeffeler@tum.de)
Supervisor: Tobias Nipkow

Markov decision processes (MDPs) are a standard model for decision-making problems in probabilistic systems. In MDPs, a decision-maker selects actions with random outcomes to maximize long-term rewards. MDPs are widely used in reinforcement learning, planning, model checking and operations research. Since algorithms on MDPs have applications in safety-critical scenarios, we require a high level of trustworthiness from both the underlying theory and the implementation.

A methodology with notable success in developing provably correct software involves the use of interactive theorem provers (ITPs). In our project, we study the application of the ITP Isabelle/HOL to the development of trustworthy software for solving MDPs. Compared to developing other types of verified algorithms, algorithms on MDPs bring their own particular set of challenges. First, formal proofs of correctness of MDP solving algorithms in ITPs need a combination of non-trivial formal mathematical libraries and concepts. Second, at an implementation level, multiple challenges exist, e.g. what kind of implementation of numerics should be used. Last is the overall architecture of the verified system: should it be a verified implementation, or should we use an unverified system to produce a certificate, which is later validated using a formally verified certificate checker. Previous verification efforts in the realm of MDPs have all focused on the abstract mathematical challenges, while we also address the problem of deriving efficient executable code.

As a first step, we have already verified dynamic programming algorithms that can solve tabular MDPs optimally. For infinite-horizon problems, we model four fundamental iteration-based methods: value iteration, policy iteration, modified policy iteration, and splitting-based methods. In the process, we fix a mistake in a textbook correctness proof of Gauss-Seidel value iteration.

We experimentally evaluate our implementations of the four algorithms on standard probabilistic planning problems and show that they are practical. Finally, we experimentally show that combining our verified implementations with an unverified implementation yields significant performance improvements: one can use a fast floating-point implementation to perform all the iterations and then use the formally verified implementation for the last iteration.

Our goal is to build on these developments and use them as a basis for the formalization of more practically relevant algorithms on MDPs, e.g. the verification of safe reinforcement learning algorithms or factored MDPs. We also investigate the viability of using ceritification of linear programming solutions to solve MDPs. We have published our formalization efforts on tabular MDPs in the Archive of Formal Proofs and at AAAI-23.

Thread-Modular Abstract Interpretation for Multi-Threaded Code

Michael Schwarz (m.schwarz@tum.de)
Supervisor: Helmut Seidl

Larger software systems tend to be multi-threaded where their correctness depends on the possible ways in which different threads can interact with each other. In particular, correctness may depend on the set of possible values of global variables.

However, analyzing all possible interleavings of different threads of larger programs is expensive in analysis time — in some cases even prohibitively so. Ideally, such analyses should be *thread-modular*, implying that their complexity does not increase exponentially with the number of threads.

As a reference semantics, we rely on a *local* trace semantics that is formulated by means of side-effecting constraint systems.[1] *Local* here means that each thread has only a *local view* of the system, i.e., it only knows things about its own past and those actions of different threads that are observable by it, but not about other, non-observable, actions of different threads.

Based on this setting, we provided thread-modular non-relational value analyses and showed that a generalization of the analysis provided by the static analyzer Goblint[2] as well as a natural improvement of Antoine Miné's approach [3] can be obtained as instances of this general scheme.[4]

More recently, we gave a framework to improve the precision of such analyses by splitting the control locations based on further finite abstractions of the reaching *local* trace. As one instance of this framework, we, e.g., obtained an analysis of dynamically generated thread ids, and thus which threads *may-happen-in-parallel*.[5]

We designed new thread-modular relational analyses of the values of global variables. In further work, we will investigate further useful abstractions of the local traces to further improve precision and obtain, e.g., and analyses of signaling and waiting in multi-threaded programs.

[1] Apinis K., Seidl H., Vojdani V., "Side-Effecting Constraint Systems: A Swiss Army Knife for Program Analysis.", APLAS, vol. 7705, p. 157-172, 2012

[2] https://goblint.in.tum.de/

[3] Miné A., "Static Analysis of Run-Time Errors in Embedded Real-Time Parallel C Programs", LMCS, vol. 8, 2012

[4] Schwarz, M., Saan, S., Seidl, H., Apinis, K., Erhard, J., Vojdani, V., "Improving Thread-Modular Abstract Interpretation.", SAS, vol 12913, p. 359-383, 2021

[5] Schwarz, M., Saan, S., Seidl, H., Erhard, J., Vojdani, V., "Clustered Relational Thread-Modular Abstract Interpretation with Local Traces.", ESOP 2023, to appear

Incremental Automatic Software Verification

Martin Spiessl (spiessl@sosy.ifi.lmu.de)
Supervisor: Dirk Beyer

Automatic Software Verification has become more and more powerful over the recent years, but still there are easy ways to generate verification tasks that cannot be solved by any of the currenty state-of-the-art tools. One of the reasons for this is that different analyses often have orthogonal weaknesses, and specific combination of techniques would be needed to proof a certain program correct. This lead to the development of Conditional Model Checking [1] [2], which we try to improve upon by further increasing the ways via which different tools, approaches, and the users can interact with each other.

One obvious way is to leverage the information exchange of invariants that are contained in the verification witnesses. Currently the main purpose of these witnesses is to validate the results of verification, and their usefulness in exchange between tools is limited.

As a first step we enable verifiers to directly reuse this information by encoding the information in the witnesses into a new verification problem that is potentially easier to solve. [3].

To better understand the information that is really important for a particular verification approach, a next step is to enable automatic verifiers to be used like interactive verifiers, i.e., provide easy ways for the users to add annotations and proof hints that can be transparently translated into verification tasks. Of course one can also use the information generated by the verifiers to automatically generate annotations. This can make the verification results more clear to the user, and help tool developers improve the quality of the exported information. For example, currently there is no way to make quantified invariants available in the verification witnesses, and more features like this might be revealed as necessary to further improve the state-of-the-art.

Lastly we envision a way for a precision-based parametric analysis that can choose between different verification approaches either automatically via CEGAR or interactively via user-provided annotations (very similar to how interactive proof assistants work). The goal is to use the insights gained in the previous steps to create new ways of designing powerful analyses that can apply working strategies for different subproblems in a larger verification task.

[1] D. Beyer and T. A. Henzinger and M. E. Keremoglu and P. Wendler,
Conditional Model Checking: A Technique to Pass Information between Verifiers,
Proc. FSE 2012, article no. 57, https://doi.org/10.1145/2393596.2393664

[2] D. Beyer and M.-C. Jakobs and T. Lemberger and H. Wehrheim, Reducer-Based Construction of Conditional Verifiers, Proc. ICSE 2018, pp. 1182-1193,
https://doi.org/10.1145/3180155.3180259

[3] D. Beyer and M. Spiessl, Witness Validation via Verification,
Proc. CAV 2020, pp. 165-177,https://doi.org/10.1007/978-3-030-53291-8_10

Verification of Top-Down Solvers

Sarah Tilscher (sarah.tilscher@tum.de)
Supervisor: Helmut Seidl

For program analysis, fixpoint solvers are essential to computing a solution to the constraint system generated from the control flow of the program. The **TD** is a generic and demand-driven top-down solver that tracks the dependencies between unknowns on-the-fly. It is implemented in the static analyzer Goblint[1] for multithreaded C programs. By now, several improvements to the initial **TD** have been proposed, such as the dynamic detection of widening/narrowing points[2].

While the improved **TD** is convenient to use for program analysis, the interplay of the advanced solving strategies is often difficult to understand, and every further extension makes it harder to reason about its correctness. This makes the implementation of the solver fragile and vulnerable to bugs. Therefore, we want to back up its correctness with a formal verification in the interactive theorem prover Isabelle and prove that the assignment returned by the solver is indeed a partial solution of the input constraint system. We started by reducing the **TD** to a minimal version that has no mechanism to avoid unnecessary re-evalutations and could be verified more easily. We introduced the concept of the solver's *trace* as a tree of all recursive calls that are called during solving, including their parameters and return values. Interestingly, existing extensions of the solver can be viewed as an abstract interpretation of the abstract interpreter (A²I)[3] itself: they are optimizations of the minimal solver that keep track of an abstraction of the reaching left-context of the trace as state and react according to it. This is the case for the original **TD** with the additional mechanism to avoid unnecessary re-evaluations of unknowns where the fixpoint was already reached, as well as a solver with dynamic detection of widening/narrowing points. Additionally, we derived another optimized solver, that also skips those re-evaluations that are redundant because the abstract values of all unknowns on the right-hand side have not changed since its last evaluation.

While we have verified the simple version of the top-down solver in Isabelle, it remains to show its equivalence to the optimized versions that skip certain unnecessary re-evaluations of unknowns. Beyond that, we would also like to formally verify versions of the solver with more advanced extensions, like *side-effects*.

Since fixpoint algorithms are widely used, not only in program analysis but for example also for parser generation, we would like to generalize our approach of reasoning over the solver's trace. By generating the trace from the specification of a functional program we could provide the structure of necessary inductions for a more powerful framework for the verification of functional programs in Isabelle HOL.

[1] https://goblint.in.tum.de/

[2] Apinis, K., Seidl, H. and Vojdani, V., "Enhancing top-down solving with widening and narrowing", LNCS, vol. 9560, p. 272-288, 2016

[3] Cousout P., Giacobazzi R. and Ranzato F., "A²I: abstract² interpretation", POPL, vol. 3, 2019

Incremental and Cooperative Software Verification

Henrik Wachowitz (henrik.wachowitz@ifi.lmu.de)
Supervisor: Dirk Beyer

As software enriches more aspects of our daily lives, it becomes increasingly important to ensure its correctness. With safety-critical systems, such as cyber-physical systems (CPS), mere testing is not enough. We need strong guarantees of Software Verification. However, there are limitations: Software Verification techniques can consume large amounts of resources and time, making it often difficult to integrate Software Verification throughout the development process.

With Incremental Verification, we want to close this gap. Reusing knowledge gained from verifying earlier versions of a software system increases speed and lowers resource consumption of successive verification tasks. Embedding this incremental framework in a service infrastructure further improves its accessibility, creating an ideal fit for continuous integration.

Another way of improving Software Verification results is through cooperation. Nowadays, we have access to a plenitude of Software Verification tools. These tools can serve as actors working towards a common goal. In CPS, we can use cooperative verification approach to combine the strength of tools specialized for hardware and those intended for software. However, for cooperation to thrive we need an expressive, unified and standardized exchange format between the tools. I built on the project of Nico Weise: He devised a new witness format that is more expressive and is embedded in a yaml file. This enables more explicit information interchange between tools. Using the established yaml format supports developers integrating this format as they may rely on existing well tested parsing libraries. Weise also derived a prototype for stateful verification. Right now cooperation is rarely happening in a way where two tools exchange information at runtime. The proposed prototype showcased how a verification tool might read and write information it runtime – potentially benefiting from the newly read inputs. In my work at ConVeY I want to improve on this prototype making verification as a service [**?**] even more viable. Finally, we combine cooperation with the incremental framework, sourcing the strengths of a repository of tools for specialized increments.

Automated Formal Verification of Dynamical Systems Using Reachability Analysis

Mark Wetzlinger (m.wetzlinger@tum.de)
Supervisor: Matthias Althoff

Applying cyber-physical systems in safety-critical environments requires formal verification techniques to ensure correct functionality with respect to safety specifications. A contemporary example is the launch of a rover to another planet, where even small failures are critical as they might lead to severe consequences. One of the main techniques to provide safety guarantees is *reachability analysis* where all possible system behaviors over time are computed under the influence of uncertainty in the initial state and control input or disturbances. If the exact reachable set does not intersect an unsafe set defined via unwanted system behavior, safety is formally guaranteed.

Since reachable sets cannot be computed exactly in general, we revert to algorithms that return either outer-approximations or inner-approximations, which together can be used to verify or falsify a given system specification. We first investigated an automated parameter tuning approach for reachability analysis of linear systems, which allowed to tune the accuracy of the outer-approximation by setting a single scalar value. As a next step, we rigorously considered all approximation errors so that the resulting accuracy value is interpretable as a bound for the set distance between the outer-approximation and the exact solution, which can then also be utilized to compute an inner-approximation. We combined the outer- and inner-approximations in an automated verification algorithm, which refines the tightness of the approximation until safety can be proven or disproven. An alternative approach has also been developed which exploits potential simplicity in the given safety specification allowing for an analysis of very high-dimensional systems.

In reachability analysis of nonlinear systems, we currently cannot compute a rigorous bound on the approximation error. Instead, we have devised an algorithm that balances the main sources of over-approximation by solving an optimization problem, which outputs locally optimal parameters in order to compute a tight outer-approximation. As a consequence, we took a deeper dive into the foundations of the approximation error and its relation to the time step size, similarly to the analysis of classical solvers for ordinary differential equations.

The final stage of the doctoral project will be dedicated to proposing a novel set-based algorithm for backward reachability analysis, which computes the set of states that can reach a given target set under competing influence of control inputs and disturbances; this set is practically relevant, e.g., for motion planning tasks or collision avoidance. In contrast to current state-of-the-art methods with exponential runtime complexity, our algorithm is designed to run in polynomial time.

GRK 2475: Cybercrime and Forensic Computing

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

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

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

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

Graded Semantics and Logics and their Applications in Digital Forensics and Security

Üsame Cengiz (uesame.cengiz@fau.de)
Supervisor: Prof. Dr. Lutz Schröder

State-based systems are a useful formal method for modeling process behaviour. In its most basic form, a system consists of states and transitions between them. Over the years many different system types have emerged, such as labelled, weighted, probabilistic, and game-based systems. The category-theoretic framework of universal coalgebra provides a generalization of all these settings.

But even when one restricts to just a simple system type, there is a wide variety of pertinent semantics. Two systems which behave differently under a finer semantics may be indistinguishable under a coarser semantics. The desired semantics always depends on the use case. Processes can thus be compared in different ways, ranging from just their outputs to their exact internal behaviour. All of these types of process equivalences can be used in e.g. specifying the degree of strength of an attacker model for verifying security features of protocols. This is done by modeling implementation and specification and checking for their equivalence under the appropriate semantics.

In recent years, the idea to use graded monads in the study of process semantics has emerged. An advantage of taking this approach, in addition to its coalgebraic generality, is that in some cases one can systematically extract the so called characteristic logic of a semantics. Simply put, a logic consists of certain kinds of formulas and a definition of when they are satisfied by, in our case, a process. The characteristic logic for a semantics defines the types of formulas in such a way that whenever two processes are semantically equivalent, there is no formula, i.e. property, that distinguishes them from each other, e.g. is satisfied by one and not by the other. In the case of inequivalence, distinguishing formulas serve as an easily verifiable certificate of this fact.

The first goal is to extend the framework of graded semantics to include temporal logics, which enable reasoning over unspecified depth of steps. Temporal logics are used in model checking and can be useful in e.g. checking for properties of unspecified depth in data analysis such as “Was program A executed before program B?”.

The study of these semantics and extending the theoretical foundation for their applications in digital forensics and cybersecurity is the main aim of the thesis.

Coalgebraic Automata and Learning Algorithms and their Application in Forensics

Hans-Peter Deifel (hans-peter.deifel@fau.de)
Supervisor: Prof. Dr. Stefan Milius

The study of dynamic systems has a long and rich history in computer science, spanning fields such as classical automata theory, concurrency theory, and IT security. Such systems include deterministic automata, (labeled) transition systems, and probabilistic systems. Historically, algorithms developed for one type of system had to be adapted or reinvented for another one. In contrast, the theory of *Universal Coalgebra* aims to provide a generic framework for systems that encompasses the instances mentioned above and many others.

The use of coalgebraic techniques has recently facilitated the development of a generic *partition refinement algorithm*, which we implemented in a tool that can efficiently minimize a wide array of state based systems. In fact, for many of the studied system types, the generic algorithm matches the run-time complexity of the best known specialized algorithm and for some system types even surpasses it. Genericity is achieved by varying the coalgebraic type functor, but the base category is assumed to be the category of sets.

In the above algorithm, partition refinement is used to compute the state space of a minimal system w.r.t. behavioral equivalence. In this thesis we will, as a first step, extend the algorithm into a fully fledged minimization procedure. This entails moving from computing the state space to also computing the transition structure of the minimal system, while retaining the full genericity.

We will also add support for data automata to the algorithm, by porting it to another base category. Data automata deal with infinite alphabets that are accessible only by a limited API. They arise e.g. when dealing with user data in XML processing.

Another class of algorithms that has recently seen the introduction of coalgebraic techniques is active automata learning, which allows to infer automata models by querying a black-box system. E.g. Angluin's original learning algorithm reconstructs a deterministic finite automaton by posting a series of questions to an adequate *teacher*. Since this pioneering work, similar learning algorithms have been developed for a variety of different systems, motivating the search for a generic method. Advances in this direction were made using coalgebraic methods by Silva et al. with their Coalgebraic Automata Learning Framework and more recently, by Barlocco et al. The latest development is an algebraic approach by Schröder and Urbat. All of these approaches have various shortcomings, in particular, they do not yield a concrete ready-to-use generic algorithm. In this thesis, we will investigate the applicability of those approaches and hope to devise a concrete algorithm with a high level of genericity.

As a case study, we will apply active learning techniques in the field of digital forensics, e.g. by constructing accurate models of black-box systems in digital evidence.

Viktimologie Cybercrime

Julia Drafz (julia.drafz@fau.de)
Supervisor: Prof. Dr. Gabriele Kett-Straub

Die Digitalisierung schreitet in unserer Gesellschaft immer weiter voran und bringt neue Technologien hervor. Nach der JIM-Studie 2019 des Medienpädagogischen Forschungsverbunds Südwest ist von einer flächendeckenden Vollausstattung sowohl mit dem Internet als auch Smartphone in den deutschen Haushalten auszugehen. Das Internet ist somit nicht mehr aus dem Berufsleben und privaten Alltag wegzudenken. Doch die technischen Errungenschaften gehen jedoch nicht nur mit positiven Aspekten einher, da auch Kriminelle das Potential des Internets zum Missbrauch für ihre eigenen Zwecke entdeckt haben. Während das Schadensausmaß enorm ist, ist das Aufdeckungsrisiko aufgrund der Anonymität des Internets und fortschreitenden technischen Entwicklungen gering. Im Gegensatz zu anderen Kriminalitätsbereichen steht die Forschung im Gebiet der Internetkriminalität noch am Anfang. Insbesondere in der (Cyber-)Viktimologie, einem Teilbereich der Kriminologie, das sich mit verschiedenen Facetten der Kriminalitätsopfer beschäftigt, besteht ein großes Forschungsdesiderat.

Bisherige Studien beliefen sich bisher relativ erfolglos auf die ausschließliche Anwendung quantitativer Methoden zur Identifizierung von Risikofaktoren bei Opfern von Cyberkriminalität in der allgemeinen Bevölkerung. Um den Opfern nach einer Viktimisierung zu helfen und Taten im Vorfeld zu verhindern, erfordert es eine Forschung, die sich nicht alleine auf statistische Analysen beschränkt und sich neben der Aufdeckung von Risikofaktoren auch anderen viktimologischen Themenfeldern widmet.

Im Rahmen der Dissertation steht deshalb neben der Aufarbeitung des aktuellen Stands der Opferforschung sowie einer grundlegenden Darstellung des Phänomens Cyberkriminalität die Durchführung einer eigenen empirischen Studie im Vordergrund. Mithilife eines standardisierten Fragebogens sollen Opfererfahrungen von Privatnutzer*innen im Internet und ihr Online-Verhalten erfasst und Daten für eine statistische Analyse gewonnen werden. Im anschließenden qualitativen Forschungsteil werden ausgewählte Cybercrime-Opfer zu ihrem Umgang mit der Tat und der Bewältigung der Tatfolgen interviewt. Diese kombinierte Vorgehensweise schafft zum einen die Möglichkeit, statistische Kennwerte zu erhalten und zum anderen mittels einer qualitativen Inhaltsanalyse nach Mayring Wissen über den Umgang mit der Tat von Cybercrime-Opfer zu generieren, welche dann in die Opferhilfe und Präventionsarbeit einfließen können.

Digital Stratigraphy: Chronological Dating for Digital Forensics

Lisa Marie Dreier (lisa.dreier@fau.de)
Supervisor: Prof. Dr.-Ing. Felix Freiling

In criminal investigations, understanding temporal relationships often is crucial to interrelate evidence or exonerate suspects. In the case of digital evidence such temporal relationships are usually established by collecting and interrelating timestamps in file systems or log files. Although this can be a good approach in general, such an analysis entirely depends on the existence of reliable timestamps. But these do not necessarily exist, as illustrated in the case of file recovery in file systems: Even though deleted files often can be recovered fully or partially, associated metadata (and thus corresponding timestamps) might already be overwritten. Besides, some recovery methods (e.g., file carving) do not recover the associated timestamps by design.

But temporal relationships can not only be established by interpreting a set of timestamps. Instead, Casey proposed a method to estimate a time frame for the creation date of a deleted file based on the file's location on disk combined with time specifications of neighboring files.[1]. It is part of a bundle of methods and observations summarized under the term digital stratigraphy, with their concepts transferred from archaeology and geology. In these two disciplines, stratigraphy is a well-known method for establishing a relative chronology (and thus temporal relationships) between different sediment or rock layers (including the objects they contain). As establishing temporal relationships and assigning dates to objects is an essential objective in both disciplines, they have a wide range of such methods summarized under the term chronological dating.

Thus, this thesis will explore different ways of chronological dating in different disciplines and investigate which of these methods can be transferred to digital forensics. For this purpose, it will focus on the inherent concepts of the methods and constitute an overview of their characteristics before investigating how they can be applied to digital forensics. Nevertheless, one main focus of the work will still be digital stratigraphy, with the aim of improving and extending its capabilities to establish temporal relationships: this thesis will extend the method in a way that makes it applicable for further digital media, e.g., databases, and refine it with additional concepts transferred from other disciplines, such as the Harris-Matrix taken from archeology.

[1] Eoghan Casey, "Digital Stratigraphy: Contextual Analysis of File System Traces in Forensic Science", Journal of Forensic Sciences, vol. 63, p. 1383-1391, 2018.

Investigations into Automata for Data Languages and their Applications in Forensics

Florian Frank (florian.ff.frank@fau.de)
Supervisor: Prof. Dr. Stefan Milius

Infinite alphabets are used to model the communication of values from infinite data types such as nonces, channel names, process identifiers, URLs, data values in XML documents, object identities, or abstract resources. Automata models for *data languages*, which are languages over an infinite alphabet, have received considerable attention in recent research. Typically, these languages are accepted by register automata, first introduced by Kaminski and Francez[1] and extended by Kaminski and Zeitlin[2]. These automata have a finite state description, which then generates an infinite configuration space by use of the infinite alphabet. Another model for data languages are *nominal automata*, first introduced by Bojańczyk, Klin, and Lasota[3]. These automata have infinitely many states but are often required to be *orbit-finite*: they have only finitely many states up to renaming implicitly stored data values. Both types of automata have shown to be equi-expressive, yet nominal automata enjoy many properties convenient for talking about them in an abstract manner.

In this thesis we shall explore different topics arising at the interface of automata theory, logic, and (co-)algebras: We will look at new automata models for data languages and work out the details of their semantics and equivalent descriptions. In addition, we will describe equivalent logics for the class of data languages accepted by these automata models. In particular, we have started an investigation of *presheaf automata*. During this, we found a class of languages accepted by specific presheaf automata, which had wonderful properties for reasoning about them. We found a characterization of these by using monadic second order logic with equality tests and also equivalences to other automata types already studied before. Later we will also work out the coalgebraic semantics for presheaf automata, similarly to our previous work where this was done for non-deterministic orbit-finite nominial automata (NOFAs) and regular non-deterministic nominal automata (RNNAs).[4] With these presheaf automata we will use the internal logics of toposes.

Finally, we will discuss applications of these automata in different fields of digital forensics. Nominal automata have previously been used for model checking, where an automaton model is exhaustively verified against a property specified in an expressive logic. We aim to extend this towards other automata models and to properties of interest in forensics.

[1] M. Kaminski, N. Francez, "Finite-memory automata", *Theoretical Computer Science*, Volume 134, Issue 2, 1994, Pages 329-363, ISSN 0304-3975

[2] M. Kaminski, D. Zeitlin, "Finite-Memory Automata with Non-Deterministic Reassignment", *Int. J. Found. Comput. Sci.*, Volume 21, Issue 5, 2010, Pages 741-760

[3] M. Bojańczyk, B. Klin, S. Lasota, "Automata theory in nominal sets", *Logical Methods in Computer Science*, Volume 10, Issue 3, 2014

[4] F. Frank, S. Milius, H. Urbat, "Coalgebraic Semantics for Nominal Automata", In Helle Hansen, Fabio Zanasi, eds.: *Coalgebraic Methods in Computer Science. CMCS 2022*. Lecture Notes in Computer Science, vol 13225. Springer, Cham.

Foundations of Adaptor Signatures

Paul Gerhart (paul.gerhart@fau.de)
Supervisor: Prof. Dr. Dominique Schröder

Adaptor signatures are a novel cryptographic primitive with numerous applications to payment channels, blind conditional signatures, and verifiable witness encryption. On a high level, this primitive allows the signer to compute pre-signatures on messages for statements of NP relations. Pre-signatures are publicly verifiable that simultaneously hide and commit to a signature of an underlying signature scheme on that message. Anybody possessing a corresponding witness for the statement can adapt the pre-signature to obtain the "regular" signature. These properties allow building some sort of smart contracts on blockchains that only allow the storage of transactions on chain. Unfortunately, the formal security notions of adaptor signatures are not well understood. The security of many works building on top of adaptor signatures relies on stronger security assumptions not necessarily covered by adaptor signatures. Therefore, we try to build a new formal security model for adaptor signatures that allows building solid proofs. Furthermore, we want to build protocols that do fair exchange based on these new definitions and explore applications in digital forensics.

Forensic Application of Side-Channel Analysis

Paul Krüger (paul.krueger@fau.de)
Supervisor: Prof. Dr. Jürgen Teich

With the ever-increasing spread of embedded systems used in, for example, smart devices and the Internet of Things, and the public's heightened consciousness regarding privacy and data security, the need for secure computing and communication was never higher. While current standards for cryptographic algorithms can be considered mostly secure the issue of side-channel vulnerabilities is omnipresent. Side-channel vulnerabilities may occur when an algorithm implemented on a physical platform is executed generating traces possibly containing information related to a confidential part of the system. This issue is exacerbated when considering the implementation of cryptographic algorithms on embedded systems, where side-channel security is often traded for computational efficiency, further increasing the risk of side-channel attacks. However, these vulnerabilities also present an opportunity for forensic investigation, as systems that might be otherwise unbreakable may still be susceptible to side-channel attacks, enabling investigators to access possibly critical information.

In order to apply side-channel attacks in forensic investigations it is necessary to handle emerging issues due to discrepancies between side-channel attack research and forensic practice: While research usually focuses on often simplistic target platforms, the devices encountered in practical forensic investigations are usually much more complex. Device-specific attacks from the research literature therefore regularly have to be adapted.

In particular, the issue of *Systemic Noise* in power side-channel attacks is investigated. In this context the Systemic Noise of a device is an encapsulation of all noise directly originating from the device's hard- or software components. These noise components may negatively affect side-channel attacks as they can introduce for an observer non-deterministic execution behavior and may invalidate the attacker's assumptions about the system behavior. This thesis mainly investigates the effects of Systemic Noise on the current standards for cryptographic algorithms, namely the Advanced Encryption Standard (AES) and its related modes of operation. The overall goal of this thesis is to enable efficient cross-device application of side-channel attacks by providing generic solutions to Systemic Noise issues that can be applied to different classes of target devices. For this the following three approaches are pursued:

First, we adapt current side-channel attack techniques to enable them to detect, interpret and adapt to Systemic Noise. Second, we investigate side-channel attack techniques that approach Systemic Noise as an additional side channel to attack and obtain further information about the system. And third, we develop side-channel attacks completely circumventing the issue of Systemic Noise by relying on sources of information unaffected by Systemic Noise.

Cyberangriffe auf kritische Infrastrukturen

Mathis Ohlig (mathis.ohlig@fau.de)
Supervisor: Prof. Dr. Hans Kudlich

Immer wieder gibt es Schlagzeilen, dass Infrastrukturen und deren IT-Systeme von Akteuren jedweder Art angegriffen wurden. Eine ausführliche Untersuchung des strafrechtlichen Umgangs mit diesem Phänomen unter Berücksichtigung des geltenden Rechts ist indes — obwohl sie geboten ist — bislang nicht erfolgt. Auch mögliche Rechtsentwicklungen bedürfen aufgrund aktueller Gesetzesvorhaben verschiedener Akteure schon jetzt einer ausführlichen Würdigung.

Im Fokus der Analyse der aktuellen Rechtslage steht die Frage, ob die bestehenden Straftatbestände und die bestehende strafrechtliche Dogmatik Cyberangriffe auf kritische Infrastrukturen angemessen erfassen. Dabei ist vorweg freilich die Frage zu beantworten, was überhaupt „kritische Infrastrukturen“ nach der aktuellen Rechtslage sein können. Auch wenn es bisher keine strafrechtliche Legaldefinition gibt und noch keine Straftatbestände besondere Folgen an die Kritikalität von angegriffenen Infrastrukturen knüpfen, ist die Begriffsdefinition doch deshalb relevant, weil es denkbar ist, dass sich aus der Einstufung als kritische Infrastruktur im Rahmen normativer Kriterien besondere dogmatische Folgen ergeben. Es stellen sich im Rahmen der besonderen Fallgruppe der Cyberangriffe auf kritische Infrastrukturen bis dato unbehandelte Probleme. Es fragt sich u.a., welche Computerdelikte im engeren und im weiteren Sinne bei Cyberangriffen auf kritische Infrastrukturen verwirklicht sein können und wer Täter im Kontext von Cyberangriffen auf kritische Infrastrukturen sein kann. Es ist das Ziel der Dissertation, die gefundenen Probleme in der gegebenen Rechtslage unter Berücksichtigung der Besonderheiten der Fallgruppe dogmatisch zu lösen.

Schließlich stellt sich noch die Folgefrage, ob und welcher Regelungsbedarf im Detail tatsächlich besteht. Im Detail ist zu überlegen, welche Deliktstypen einzuführen sinnvoll und mit der bestehenden Dogmatik — unter Berücksichtigung der erörterten Besonderheiten — und Strafzwecken vereinbar wäre.

Bringing Science to Mobile Device Forensics

Jenny Ottmann (jenny.ottmann@fau.de)
Supervisor: Prof. Dr.-Ing. Felix Freiling

Mobile devices like smartphones have become an irreplaceable companion for many people today and are used for a multitude of activities such as navigation, communication and entertainment. Therefore, the data stored on a smartphone can serve as a valuable source of evidence during a criminal investigation. Accessing data on a mobile device can be a technical challenge. In smartphones, for example, many measures are employed to protect the users' data, and various methods, some hardware-based, others software-based, have been developed to facilitate data extraction and subsequent analysis[1]. When such extraction methods are used it is important to know if they make any changes to the device under investigation and how reliable their results are as this influences their usability in court proceedings.

To establish under which circumstances an extraction method is reliable and in what cases the produced data could contain errors, testing needs to be performed. With regard to the ever evolving hard- and software, it is important that testing is continously performed under the new circumstances. Because of the possible importance of digital evidence it is not enough to rely upon the word of the tool vendors that they are performing this continuous testing. And, in some cases, the number of different settings in which a method could be used is too big to rely upon one entity to perform testing for all of them. Therefore, it is necessary that practitioners and researchers also perform tool and method validation. However, there are obstacles to this like limited resources and a lack of reference data. More testing could also help to establish the limitations of tools better[2].

As testing is an important factor for the extracted data to serve as reliable evidence, in this thesis possibilities to validate data extraction methods used in the context of mobile device forensics are explored. First, an extensive overview of methods that could be used in digital investigations will be given and the methods classified according to the maximal data access they can provide. Then quality criteria need to be defined and different possibilities for a validation setup assessed. Finally validation methods should be implemented and evaluated regarding their usability and the transferability of results between different devices.

[1] Maxim Chernyshev, Sherali Zeadally, Zubair Baig and Andrew Woodward, "Mobile Forensics: Advances, Challenges, and Research Opportunities", IEEE Security and Privacy, vol. 6_15, p. 42-51, 2017

[2] Graeme Horsman. ""I couldn't find it your honour, it mustn't be there!" – Tool errors, tool limitations and user error in digital forensics". In: Science and Justice 58.6 (Nov. 2018), pp. 433–440.

Understanding Privacy in Cryptocurrencies

Viktoria Ronge (vikoria.ronge@fau.de)
Supervisor: Prof. Dr. Dominique Schröder

Cryptocurrencies are digital currencies normally not issued by a government or other central authority relying on cryptographic tools. They enable users to transfer money all over the world in a secure way, where there is no need for intermediaries like banks or exchange the money into different currency. Thereby, no user can be prevented from transferring money, no one can spend money they do not own or spend it twice and money can only be created under rules everyone agrees to. They further provide different nuances of privacy, where somewhat fully private ones are rare. The largest two are Monero[1] and Zcash[2]. They pursue different approaches, which are, with our current knowledge about privacy, at least partly incomparable.

This research project focusses on the foundations of anonymous cryptocurrencies from different angles. One is to understand the theory behind different anonymous cryptocurrencies and to formalize them. This is necessary as without formalizing no security can be proven and no statements about actual privacy for users can be done. Another one is to extend our knowledge and comprehension of different anonymity measures and to use them for comparison of currencies. This would help us to answer simple questions like which currency offers better anonymity, but this research is also important from a legal perspective, because anonymous cryptocurrencies often are used by criminals. Understanding privacy of different systems might lead to ideas on how to attack a system. This raises the fundamental question if this is proportional in relation to the violation of privacy of honest users. Moreover, when using results from such attacks in prosecution, we need an understanding of the results' quality. For genetic tests we know well about the accuracy based on past experiences. For deanonymising we are lacking such a ground truth that exists in other areas used for evidence. Therefore it is urgent to gain confidence in the accuracy of deanonymisation to make sure no innocent is falsely accused.

We hope to help giving an overview of these issues to provide the community with a better understanding of what privacy means in this subfield and how reliable we can talk about it. A first step was already done in formalizing Monero as a whole[3]. We further gave a better understanding of choosing anonymity sets in Monero[4] and are working on a followup.

[1] The Monero Project, `https://www.getmonero.org/`, last visited March, 27^{th}, 2020

[2] Electric Coin Company, `https://z.cash/`, last visited March, 27^{th}, 2020

[3] *Omniring: Scaling Private Payments Without Trusted Setup*, R. W. F. Lai and V. Ronge and T. Ruffing and D. Schröder and S. A. K. Thyagarajan and J. Wang, *Proceedings of the 2019 ACM SIGSAC CCS 2019*

[4] *Foundations of Ring Sampling*, V. Ronge, C. Egger, R. W. F. Lai, D. Schröder, and H. H. F. Yin, *Proceedings of PETS 2021*

"Der IT-Sachverständige im Strafverfahren" — Heuristik und Beweiswürdigung

Nicole Scheler (nicole.scheler@fau.de)
Supervisor: Prof. Dr. Christoph Safferling

Nicht nur viele unserer Lebensinhalte spielen sich nunmehr digital ab, auch die Beweismittel haben längst die analoge Welt verlassen ("eEvidence"). Durch die Allgegenwärtigkeit der Informationstechnik in unserem Alltag (Smartphones, Laptops, Wearables, Navigationsgeräte, Sprachassistenten, etc.), können anhand der dabei entstehenden Daten umfassende Persönlichkeits- und Aktivitätsprofile erstellt und digitale Abbilder gespeichert werden. Diese Daten können umfangreiche Spuren enthalten, die auf Sachverhalte aus der körperlichen Welt schließen lassen und menschliches Verhalten nachweisbar machen. Sie zu finden, zu sichern und gerichtsverwertbar auszuwerten ist Gegenstand der IT-Forensik. Diese digitalen Spuren müssen als gerichtsfestes Beweismittel in die Hauptverhandlung eines Strafverfahrens eingeführt werden. Neben den Herausforderungen der Massendatenauswertung, der Heterogenität von Daten sowie der Verschlüsselung der Kommunikation und von Festplatten, stellt sich u.a. auch der "Übersetzungsvorgang" von digitalen Beweismitteln durch IT-Sachverständige für die anderen Prozessbeteiligten vor Gericht als problematisch dar. Die Gerichte können in vielen Verfahren nicht mehr auf die Hilfe von IT-Sachverständigen verzichten. Aufgrund der steigenden Komplexität informationstechnischer Systeme ist hierfür — neben der reinen Übersetzungstätigkeit in eine menschenlesbare Form durch Software — in zunehmendem Maße auch eine tiefgehende Erläuterung der Ergebnisse von Datenverarbeitungsvorgängen durch menschliche IT-Forensik-Expertinnen und Experten notwendig. Bei mangelnder Kompetenz der Gerichte im Bereich der IT-Forensik besteht die ernstzunehmende Gefahr, dass nicht mehr die Richterinnen und Richter (allein) über Schuld oder Unschuld befinden (§261 StPO), sondern die IT-Sachverständigen in weiten Teilen das Ergebnis hinsichtlich der Schuldfrage determinieren. Um dieser Gefahr vorzubeugen, sollen verschiedene Lösungsansätze entwickelt werden. Zum einen soll ein Vergleich zu den Anfängen anderer forensischer Wissenschaften vor Gericht hergestellt (u.a. DNA-Analysen, Rechtsmedizin, Glaubwürdigkeitsgutachten) und ggf. die dabei entwickelten Regeln auf die IT-Forensik übertragen werden. Standardisierte Verfahren sowohl in der IT-Forensik als auch bei der Bewertung und Würdigung digitaler Beweise sind dringend notwendig für eine vertrauenswürdige und nachvollziehbare Tatsachenqualität, die juristischen und grundrechtseinschränkenden Entscheidungen (wie Ermittlungsmaßnahmen und Verurteilungen) zugrundeliegen. Zum anderen könnte eine präzisere Kommunikation zwischen verfahrensbeteiligten Juristinnen und Juristen und IT-Sachverständigen notwendig sein, sowie Grundkenntnisse aller Verfahrensbeteiligten hinsichtlich der Besonderheit der IT-Forensik und Daten als Beweismittel, um die Ergebnisse der Gutachten im Rahmen der Beweiswürdigung auf Plausibilität überprüfen zu können.

Tempting Bytes: Vergleiche der Neigung zu Cyberkriminalität und herkömmlicher Kriminalität

Laurin Schwemer (laurin.schwemer@fau.de)
Supervisor: Prof. Dr. Gabriele Kett-Straub

Im November 2022 veröffentlichte das Bundeskriminalamt (BKA) die Ergebnisse der Dunkelfeldstudie „Sicherheit und Kriminalität in Deutschland“ (SKiD). Der Studie zufolge sind die Menschen in Deutschland am häufigsten von Straftaten betroffen, die sich dem Bereich der Cyberkriminalität zuordnen lassen. Gleichzeitig sind die Anzeigequoten in diesem Bereich recht gering und das Dunkelfeld daher vergleichsweise groß. Mit der fortschreitenden Digitalisierung in der Gesellschaft nimmt die Bedeutung digital verübter Kriminalität offenbar zu, während herkömmliche Kriminalität vom Volumen her etwas in den Hintergrund rückt. Obwohl Cyberkriminalität häufig grenzüberschreitend ist und die hohe Zahl an Betroffenen in Deutschland nicht unbedingt auf eine hohe Zahl an Tatbegehenden aus Deutschland schließen lässt, stellt sich doch die Frage, ob in einer digitalisierten Gesellschaft die Kriminalitätsneigung zu Cyberkriminalität womöglich höher ist, als zu herkömmlicher Kriminalität. Vor diesem Hintergrund rückt das Internet nicht nur als „Tatort“, sondern als digitaler Raum generell in den Fokus der Betrachtung. Immerhin schafft es neben neuen Möglichkeiten der Tatbegehung auch neue Wege der Kommunikation, des Austauschs, der Bildung, es formt durch seine Inhalte, Logiken und Strukturen eine eigene Kultur (z.B. Memes) und wirkt auf verschiedene Weise auf seine Nutzerinnen und Nutzer zurück. Bestimmte Merkmale des Internets, zum Beispiel der globale Charakter und die Suggestion von Anonymität, lassen es für die Nutzer und Nutzerinnen unter Umständen als regellos erscheinen. Das Internet kann mit Durkheim und Merton folglich als eine Quelle von Anomie oder gar als ein anomischer Raum konzipiert werden. Dieser Überlegung folgend, könnte die Wahrnehmung des Netzes als anomisch die Kriminalitätsneigung zu Cyberkriminalität möglicher Täterinnen und Täter weiter begünstigen. Das Dissertationsvorhaben, will also zum einen herausfinden, inwiefern in der deutschen Bevölkerung eine Kriminalitätsneigung zu Cyberkriminalität besteht und in welchem Maße sich diese von der Kriminalitätsneigung zu herkömmlicher Kriminalität unterscheidet. Zum anderen soll dabei betrachtet werden, welche Rolle das Internet als anomischer Raum für die Kriminalitätsneigung spielt.

Noch zu füllende Forschungslücken betreffen die Tatgelegenheitsstruktur, mögliche Tatmittel und notwendige Kompetenzen im „Tatort“ Internet sowie generelle Konzeption des Internets als anomischer Raum, die bisher unterblieben ist. Des Weiteren wurden bisher fast nie kriminologische Theorien eingesetzt, um das unterschiedliche Ausmaß an Kriminalität im Cyberspace im Vergleich zur Realität beziehungsweise die unterschiedliche Kriminalitätsneigung zu Cyberkriminalität und herkömmlicher Kriminalität zu erklären. Dies möchte das Dissertationsvorhaben ändern, indem es sich den Fragen widmet: Welche technischen Faktoren und Merkmale des digitalen Raumes lassen die Begehung von Cyberkriminalität im engeren Sinne rational oder attraktiv erscheinen?, Wie kann das Internet im Rahmen von Anomie-Theorien und der Situational Action Theory überhaupt konzipiert werden? und: Besteht in Deutschland (als Beispiel für eine digitalisierte Gesellschaft) eine höhere Neigung zu Cyberkriminalität im engeren Sinne als zu herkömmlicher Kriminalität?

Zur Beantwortung der Fragen sollen mehrere Experteninterviews geführt werden, um die tatsächliche Tatgelegenheitsstruktur im Internet besser einschätzen zu können und zu erfahren, welche Mittel und Kompetenzen für die Begehung von Cyberkriminalität im engeren Sinne vonnöten sind. Daran anschließend soll ein Fragebogen für eine allgemeine Bevölkerungsbefragung entworfen und angewendet werden, um das theoretische Konzept des digitalen Raumes als

anomisch zu überprüfen und die deliktspezifische Kriminalitätsneigung in der Gesellschaft zu erheben. Mit den Ergebnissen lassen sich die Erkenntnisse von SKiD weiter komplementieren und es wird ein Beitrag zur theoretischen Weiterentwicklung geleistet.

Open Source Ermittlungen im Strafverfahren

Tabea Seum (tabea.seum@fau.de)
Supervisor: Prof. Dr. Christoph Safferling

Das Internet beeinflusst und erleichtert nicht nur die Recherche im Privaten, sondern unterstützt auch die Ermittlungen der Polizei und Staatsanwaltschaft. Zur Nachforschung und Durchsuchung im Internet werden Suchmaschinen, wie Google, Yahoo oder duck-duck-go, genutzt. Dabei gibt es neben den genannten kommerziellen Suchdiensten auch spezielle für die Ermittlungen im Netz. Im Rahmen dieser Recherchen sind sensible Daten frei zugänglich und können auf den verschiedenen Plattformen, wie beispielsweise Facebook, Instagram, TikTok usw. gefunden werden. Diese privaten Daten können dann mit anderen Ermittlungsergebnissen verknüpft und abgeglichen werden. Es besteht somit eine Fülle an neuer, möglicher Beweisergebnisse und Indizien im Rahmen der Ermittlungen. Als Kehrseite muss jedoch ein strenger Blick auf das Vorgehen der Datengewinnung durch die Ermittler geworfen werden. Aufgrund von Fakeprofilen und Fakeinformationen kann die Gefahr bestehen, dass diese nicht authentisch und integer sind. Das vorliegende Promotionsverfahren befasst sich mit den aufkommenden, rechtlichen Problematiken bei der Verwendung solcher Suchmaschinen durch die Ermittlungsbehörden, die sich sowohl im Ermittlungsverfahren als auch in der Hauptverhandlung ergeben können.

Primär stellt sich die Frage nach einer angemessenen Rechtsgrundlage. Aktuell wird § 161 StPO, die Allgemeine Ermittlungsbefugnis, verwendet. Dabei ist fraglich, ob die Norm das Spannungsfeld der schutzwürdigen Daten zum einen und der Eingriffsintensität zum anderen erfasst und diese somit als ausreichend erachtet werden kann oder ob zur Gewährleistung der ausgewogenen Beachtung der Individualrechte des Beschuldigten/Angeklagten und einer effizienten Strafverfolgung der Gesetzgeber tätig werden müsste.

Weiterhin kann die Verknüpfung der digitalen Ermittlungsergebnisse mit anderen Ergebnissen aus den Ermittlungen zu einem gesonderten Eingriff in die Privatsphäre führen. Daraus folgt das Bedürfnis einer genaueren Untersuchung, ob ein solcher Eingriff vorliegen kann und wenn dies zu bejahen ist, wie der Eingriff rechtlich zu behandeln ist.

Auch die einzelnen Suchmaschinen, die die Ermittler verwenden, müssen genauer betrachtet werden. Je nach Ausgestaltung beinhalten diese KI-Anteile. Insoweit ist es notwendig, die Funktionsweise genauer zu untersuchen und zu verstehen. Aufgrund des gewonnenen Verständnisses können dann etwaige rechtliche Probleme erkannt, behandelt und gelöst werden.

Im Rahmen der Hauptverhandlung muss sich das Gericht dann kritisch mit der Herkunft und dem Vorgang der Beweisgewinnung auseinandersetzen. Nur durch eine sorgfältige Analyse kann eine Fehleinschätzung des Beweiswertes vermieden werden. Es wird somit die Frage untersucht, welche Anforderungen und Kriterien an die Vorlage der Open-Source Beweismittel zu stellen sind.

Automated Side-Channel Evaluation of Embedded Devices

Jens Trautmann (jens.trautmann@fau.de)
Supervisor: Dr. Stefan Wildermann

The always increasing abundance of embedded devices dealing with sensitive or security critical data should incentivize side-channel security evaluations not only for vendors but also forensic investigators. Hereby, side-channels like electromagnetic radiation can compromise mathematically safe cryptography by leaking information about the key. This is of special interest, as smart home devices and the Internet of Things are on the rise and many devices can provide valuable information when their cryptographic key is revealed. To analyze the side-channel information of a specific device, emissions of several cryptographic operations need to be recorded, synchronized, and compared to detect leakage. In order to enable easier and faster ways to evaluate generic embedded devices, new approaches have to be developed.

Forensic investigations have specific requirements for side-channel analysis, as they should not modify or tamper with evidence during the task. Therefore, electromagnetic radiation probes can be used to measure the emissions. However, current side-channel evaluation techniques use highly device-specific training or information which is not feasible due to the diversity of embedded systems. Therefore, expensive experts and a lot of time and effort would be needed to retrieve side-channel information at a crime scene. As this is not feasible for every crime scene, valuable information may be lost.

To tackle these problems, this thesis investigates new approaches which will enable highly automated side-channel evaluation of embedded devices. With a main focus on the Advanced Encryption Standard (AES) as it is widely spread for embedded systems as a symmetric, round based block cipher. The goal is a system that automatically evaluates a device which uses AES without preliminary knowledge about the device. Furthermore, other block ciphers are evaluated as well as other cryptographic routines. Specifically, the following challenges are faced:

First, detecting and characterizing of cryptographic operations on a power trace with multiple recorded cryptographic operations without device-specific knowledge. Second, the approach shall be independent of the measuring setup as well as independent of the specific implementation of the cryptographic algorithm in software or hardware. A final goal is to build a framework that can do a live side-channel evaluation of a target device without modifying it physically.

Detection of AI-Generated Images

Lea Uhlenbrock (lea.uhlenbrock@fau.de)
Supervisor: PD Dr. Christian Riess

In forensic investigations, images can show valuable leads or they can serve as evidence in court. A variety of digital tools has been developed to validate the origin and authenticity of images. Conversely, there also exist tools for detecting image tampering. This includes, for example, image splicing, object removal or copied image regions. One new challenge for image forensics analysis is the emergence of images generated by artificial intelligence (AI). With only minimal human interaction, such AI-based generators are able to create image content that is visually highly plausible. The detection of such generated content is an open problem. Currently, the most promising approach for forensic detectors is to use machine learning (ML).

The subject of this thesis is to add to the state of the art in ML-based image forensics with neural networks. The pursued research addresses the following questions: Which traces are left by AI-based image generators? Which neural network architecture is best suited for detecting generated images? How can a learning-based detector framework be constructed, such that the results of the image analysis provide as much interpretability and explainability to an analyst as possible?

Towards answering these questions, first results were found for images that are generated from Generative Adversarial Networks (GANs): GANs exhibit specific traces in transform domains, and it was even found that specific model architectures leave fingerprints in the images. However, these insights only form the beginning of understanding the specific representations of generated images. For example, the current state-of-the-art Diffusion Models are considerably more difficult to detect by established forensic techniques. This shows that we need a broader and deeper understanding of the representation of synthetic images in order to be able to reliably analyze them.

Two aspects are considered particularly important for the pursued research on forensic detectors. First, the technology behind forensic detectors has to be sufficiently flexible to be able to keep up with the rapid progress in the state of the art in synthetic image generation. This aspect encourages research in features and representations that capture inherent properties of generated content. Second, forensic detectors have to be designed with interpretability and explainability in mind. This is a critical component for an analyst to understand whether a detection result is reliable and justified. Such understanding is on one hand important when considering that also pristine images are created nowadays with an increasingly large amount of advanced image processing. Hence, an analyst must distinguish between such "expected" image processing and post-hoc artificially generated content. On the other hand, forensic detection methods for generated content almost exclusively rely on black-box learning-based methods, which make it challenging for an analyst to recognize the circumstances when she can trust the results.

To tackle these challenges, we investigate a learning framework that consists of multiple neural networks. Each network is specialized in extracting one type of trace. One system containing the different networks then adapts their combined output to create a final result. This ensures generalizability to different scenarios and generator models. As each sub-network is specialized on finding specific traces, this framework also implies a certain level of explainability and interpretability of the end result. Our research analyzes and discusses the conceptional details of this framework and its implementation to allow valuable insights into the detection of synthetic images.

Forensic Disk Image Generation Revisited

Lena Lucia Voigt (lena.lucia.voigt@fau.de)
Supervisor: Prof. Dr.-Ing. Felix Freiling

Various usage scenarios that necessitate realistic forensic data have been identified in the past. Some of the most prominent ones are education and training, tool testing, malware analysis, and research and development. In most cases, the deployment of generated data is inevitable as the use of real-world data is severely restricted due to privacy concerns as well as non-disclosure obligations. However, generated data often contains traces of its *artificial* creation and lacks realistic background noise or wear-and-tear artifacts that are irrelevant to the case under consideration but contribute to the comparability of generated data to real-world data.

For more than a decade, separate approaches have been introduced by the scientific community – with various concrete objectives in mind – to enhance the creation of forensic data, resulting in frameworks like Forensig^2, EviPlant, TraceGen, or ForTrace. Nevertheless, the authors of previous work uniformly acknowledge that there still does not seem to be an adequate solution.

In this work, we build upon existing strategies in the field of forensic data generation, but take a novel viewpoint by integrating ideas known from other research areas, such as malware sandbox detection and generative adversarial networks. However, the first step towards tackling the problem of creating realistic data, is to precisely define and formalize the concept of *realistic* data, contrasting them to *artificial* data. Subsequently, ways to evaluate the realism of generated data will be studied. Moreover, we will distinguish the concrete requirements on generated data that are implied by different usage scenarios.

While different starting points are conceivable, in this thesis we will first focus our attention on the generation of realistic disk images for education and training purposes. An extension of the approach and evaluation of its suitability for other applications or data types is intended in the future.

GRK 2535: Knowledge- and Data-Driven Personalization of Medicine at the Point of Care (WisPerMed)

Prof. Dr. Britta Böckmann
Email: britta.boeckmann@uk-essen.de
University of Duisburg-Essen & Fachhochschule Dortmund
Internet: https://wispermed.com/

Thanks to increasing digitization in medicine, more and more data is becoming available, for example in electronic patient records, through laboratory analyses, or even in treatment guidelines. One challenge is to make the knowledge contained in this very diverse data available and usable at the point of treatment for concrete individual therapy decisions. Existing clinical information systems allow the collection and storage of important information, but usually in a relatively unstructured way and without an individual, context-related compilation of the facts relevant for a treatment decision. The aim of the research training group is to train young researchers from the fields of medical informatics, computer science, statistics, epidemiology, and psychology so that they obtain a holistic overview of the state of research on knowledge- and data-based personalization of medical decision-making processes and learn to design new methods on an interdisciplinary basis and implement them prototypically using the example of malignant melanoma. For this purpose, methods from the fields of information extraction, knowledge representation with machine learning methods, and insights into user interaction at the point of care will be combined in a novel way. Through interdisciplinary measures, in particular through job shadowing in the dermatology clinic, barriers to understanding between the disciplines are broken down. Unique for a research training group is the cross-institutional cooperation between the Dortmund University of Applied Sciences and Arts, the University of Duisburg-Essen, and the University Hospital Essen, which is based on an already existing cooperation through a joint study program in medical informatics. Together, the applicants represent broad expertise in the fields of medical informatics, bioinformatics, epidemiology, artificial intelligence, psychology, radiology, and melanoma research. Graduates of our program will be able to take leading roles in the digitization process of healthcare and further improve treatment pathways using artificial intelligence techniques, taking into account the direct feedback and experience of the treating physicians.

Context Modeling and Mapping of Guidelines and Standard Operating Procedures

Catharina Lena Beckmann (catharina.beckmann@fh-dortmund.de)
Supervisor: Prof. Dr. Britta Böckmann

Clinical guidelines and hospital-specific standard operating procedures (SOPs) provide useful knowledge for evidence-based care. However, identifying appropriate guideline- or SOP-based information linked to a concrete patient context currently requires time-consuming searches by physicians. Reasons are the unstructured text form[1] and the missing link of existing modeling and mapping procedures for guidelines to specific patient or user context.

In the presented project we will examine to what extent modeling and mapping approaches to unstructured SOPs and guidelines can improve the decision for patient-specific therapy at the point of care and at the same time reduce time for treatment preparation.

First, important passages necessary at the point of care are identified in the documents in collaboration with dermatooncologists of the University Hospital Essen. Thereby, patient-specific comorbidities, comedications and the patient's general condition are relevant for the identification of these passages, and the inclusion of user-specific expertise.

The identified text passages are then formalized as patient-specific checklists for defined decision points and mapped to a suitable ontology to establish semantic interoperability. Subsequently, we will evaluate the developed model in terms of improved decision-making and time savings in the clinical context.

As preliminary result, guideline-based context-sensitive Business Process Model And Notation modeling for the melanoma patient treatment was performed and iteratively validated by dermatooncologists. Afterwards, Fast Healthcare Interoperability Resource (FHIR) resources were assigned to each modeled decision point to enable patient context sensitivity[2].

By providing physicians with information needed for following treatment steps in a standardized and guideline-compliant form, we aim to make a significant contribution to rapid and patient-specific medical decision-making for melanoma patients in the clinical setting.

[1] Vandvik PO, Brandt L, Alonso Coello P, et al. Creating clinical practice guidelines we can trust, use, and share: a new era is imminent. Chest. 2013 Aug; 144(2): 381-389. doi:10.1378/chest.13-0746 .

[2] Beckmann CL, Lodde G, Livingstone E, Schadendorf D, Böckmann B. Guideline-Based Context-Sensitive Decision Modeling for Melanoma Patients. In: German Medical Data Sciences 2022-Future Medicine: More Precise, More Integrative, More Sustainable!. IOS Press, 2022. S. 50 57. doi:10.3233/SHTI220803.

Extraction of Argumentation Structures

Jeanette Bewersdorff (jeanette.bewersdorff@fernuni-hagen.de)
Supervisor: Prof. Dr. Torsten Zesch

To help medical professionals at the point of care, it's important to give them access to documents that are relevant to their specific patient and case. In order to do so, not only must relevant entities like FINDING X and THERAPY Y be found and extracted, but also the argumentation structure in which the entities are used must be considered, as the mere mention of an entity does not provide enough information to determine the relevance of the corresponding document for the specific case. For example, an entity could be referenced in a negation (because X was not found, Y was started) or used implicitly in another section of the document (because of the previous findings, Y is no therapy option).

The purpose of this research project is thus to create information extraction models that can recognize and extract argumentation structures from German medical texts in the field of malignant melanoma. Implicit arguments will be given special attention. To achieve this, a corpus of medical documents based on or connected to malignant melanoma will be constructed, with the argumentation structures manually annotated. Information extraction models will be developed based on this dataset, with the goal of eventually being able to automatically annotate the argumentation structure of unread medical documents linked to malignant melanoma.

The diverse documentation style of doctors and other medical professionals is one of the two key problems that are currently noticeable. Each person has their own writing style, which can range from short notes with a lot of abbreviations to long, syntactically difficult texts. The models have to be capable of annotating the argumentation structure on all writing and documentation styles. Possible mistakes, such as spelling errors, must also be considered.

The availability and accessibility of medical documents for the corpus is another major challenge. Although many medical guidelines and most of the related literature are written in English, the clinical documents on which this project focuses are written in German. Another consideration is that medical records frequently contain personal information about the patient, such as his full name, residence, and medical history. Because this type of material is protected by privacy rules, it is almost always impossible to use and distribute un-anonymized documents. Even anonymized data is rarely made public, thus acquiring medical documents of sufficient quality and quantity for the corpus and then being able to publicly disclose the corpus remains a challenge. The transfer of medical corpora from other languages to German could be one approach to solve this issue.

Analysis of clinical image data including further clinical data – Explainable Radiomics

Katarzyna Borys (katarzyna.borys@uk-essen.de)
Supervisor: Prof. Dr. med. Felix Nensa

Motivation: As Artificial Intelligence (AI) rapidly reshapes medical research and promotes personalized clinical care, alongside its increasing usage, arises an urgent need for a deep understanding of its inner workings and the effects of interaction between AI systems and clinicians. A crucial requirement is that AI systems communicate the origin of their results reasonably, as transparency supports physicians' and patients' trust and enables the identification of errors, biases, and system limitations.

Research Question: This work aims to investigate the interpretability and explainability of Radiomics-based AI models developed for predicting the treatment response of metastasized melanoma patients to immune and targeted therapies by implementing standard eXplainable AI (XAI) methods at the Point of Care (PoC). Using these models, the primary focus is examining how XAI can contribute to integrating AI at the PoC and which factors are decisive for a successful interaction between AI systems and healthcare professionals.

Methodology: The present work builds upon AI models obtained within a DFG-funded project and developed to predict treatment response using radiomic features extracted from Computed Tomography scans and clinical characteristics of 120 malignant melanoma patients. The models and predictions will be interpreted with established XAI approaches and integrated into an app available within the Hospital Information System (HIS). With this setup and corresponding XAI results, a user study including dermato-oncologists from the University Hospital Essen will be conducted to investigate the research questions.

Preliminary Results: A preliminary examination of the radiomic and clinical attributes indicates that frequently the models rely on influenceable features like therapy medication and therapy lines. These observations are particularly interesting for contrastive XAI approaches such as counterfactuals or *What if?*-assumptions potentially enabling a first estimation of response before treatment. Additionally, Radiomic features are relevant for many predictions, which raises the question of how to suitably integrate such observations at the PoC. Subsequently, after optimizing the preliminary app prototype, the system will be deployed within the HIS and used to carry out the user-centered evaluation.

Context-sensitive, personalized search at the Point of Care

Sameh Frihat (Sameh.Frihat@uni-due.de)
Supervisor: Prof. Dr. -Ing. Norbert Fuhr

Recent developments in medical data science have made it possible to retrieve similar cases, related treatments, and supportive information. However, existing medical search engines like PubMed only retrieve health documents based on simple similarity without considering users' situational and contextual features. As a result, medical information systems fail to personalize searches or consider case contexts, leading to time-consuming searches that medical practitioners cannot afford.

This research project aims to create a search engine for medical practitioners that takes into account case context and personalization. Our research questions include: (RQ1) identifying contextual aspects related to context and personalization in medical information retrieval, (RQ2) extracting context-feature values at the document and query levels, and automatically or manually configuring personalization features, and (RQ3) integrating these features into the retrieval process to improve answers using interactive information retrieval.

Our project aims to contribute to context and personalization features in medical information retrieval. We investigate technicality, topicality, ease of reading, treatment stage, and level of evidence as contextual features, and field of expertise, years of experience, average number of patients handled, age, gender, and language as personalization aspects. We develop machine learning and natural language processing models to extract feature values and study techniques for integrating contextual features, such as integrating variables into PageRank. We also aim to improve the retrieval process by placing users at the center of the process through interactive information retrieval methods like query formulation, updating context feature values, explaining the context values of retrieved documents, or enabling new user guidance procedures such as scaffolding.

The primary outcomes of this research project are identifying contextual features like level of evidence, field of expertise, and readability level. Natural language processing techniques are used to extract knowledge at the document level, and a search engine integrating all contextual features is being developed.

Treatment decision for melanoma patients: Identification of similar patients at the point of care

Wolfgang Galetzka (wolfgang.galetzka@uk-essen.de)
Supervisor: Prof. Dr. Andreas Stang, MPH

In the treatment of melanoma patients, unusual constellations occur frequently. For those cases, making a treatment decision can be difficult. Comparison of the currently treated patient with similar previously treated melanoma patients, can support the physician's decision-making process by contrasting their received treatments and outcomes.

Similarity of patients can be viewed from different angles. One requirement might be that similar patients have similar outcomes, i.e. progression-free survival in the case of cancer patients. In this case, one can learn a similarity measure to optimize the precision of the prediction of progression-free survival via kernels. The challenge here is the time-to-event nature of the outcomes. This means that not all outcomes are observed, some are censored. Preliminary results show that kernel prediction via an optimized metric performs comparable to well-established like the random survival forest[1] and is better suited in the case of non-proportional hazards.

Similarity can however also be seen as being eligible for the same treatment which can be modeled as the probability of receiving a certain treatment. This approach is related to the propensity score method from causal inference. However, unlike for the propensity score method we not only aim at the propensity score to be similar for the patients in question but also the decisive attributes. This problem is approached in two ways; for the first one manually defined decision points in the patient trajectories are defined and a separate, traditional machine learning model is fitted for each of these decision points. In the second approach, methods that can incorporate longitudinal data such as RNNs or LSTMs[2] will be used. The first approach will serve as a baseline for the second approach.

[1] Ishwaran H, Gerds TA, Kogalur UB, Moore RD, Gange SJ, Lau BM. Random survival forests for competing risks. Biostatistics. 2014 ; 15:757–73

[2] Pham T, Tran T, Phung D, Venkatesh S. Predicting healthcare trajectories from medical records: A deep learning approach. J Biomed Inform. 2017; 69:218–29

Development and Evaluation of a Context-Aware Adaptive User Interface for Decision Support at the Point of Care in the Treatment of Patients with Malignant Melanoma

Eva Maria Hartmann (eva.hartmann@fh-dortmund.de)
Supervisor: Prof. Dr. rer. nat. Sabine Sachweh

Motivation: For the treatment of patients with malignant melanoma physicians need to get an overview of the patient's status within no time. In Hospitals though many different information systems are used at the same time resulting in disparate incoherent and duplicated data. To give an easier access to the relevant data of the patients conditions the aim of this project is to analyze the data and processes at the point of care to develop a dashboard aware of the context as well as the user experience.

Research Question: For the design and development of a user- and context-aware dashboard this project investigates the structure of data, used knowledge sources and which user accesses which data at which step and intent. Furthermore, it will be researched how this data can be visualized, grouped, organized, and termed optimized for users' needs bringing important data into focus.

Methodology: User-centered methodology will be used in various iterations to reveal the different aspects of the research questions. In the first iteration the focus lies on the discovery of the data format, its sources, and its flow as well as on the definition of user (groups) and the (sub-)contexts. Therefore, a combination of the Think Aloud Method, Contextual Inquiry, Design Thinking, and a questionnaire will be used. Based on the insights gathered the information will be illustrated in contextual models. Furthermore, these will be used to develop a first prototype of the dashboard. The prototype will be evaluated in this cycle by conducting usability testing and a questionnaire. Starting with the next iteration gained findings will be integrated and the focus of research will shift towards the preferences regarding visualization of the data while respecting the psychological and social characteristics of the users. By this approach the interactions between user and software at the point of care will gradually become more precise by the results of each cycle. This will manifest in the generation and revision of models as well as in the redesign of the dashboard.

Preliminary Results: The conduction of the Think Aloud Method and Contextual Inquiry revealed the user groups and differences in data prioritized regarding to different tasks, resulting in variant dashboard designs. By designing reusable sub modules which will be combined according to the task these differences are addressed. In the next step the design will be evaluated and the insights in data used will be modeled in FHIR profiles.

Evaluation and Proposal System for Current and Relevant Literature at the PoC

Ahmad Idrissi-Yaghir (ahmad.idrissi-yaghir@fh-dortmund.de)
Supervisor: Prof. Dr.-Ing Christoph M. Friedrich

Clinical Practice Guidelines (CPGs) are systematically developed statements that provide evidence-based recommendations to support decision-making and reduce variability in clinical practice. To maintain their relevance, CPGs need to be regularly updated with the latest research findings. However, the traditional process of updating CPGs is complex, slow, and time-consuming, causing a lag between research advancements and their implementation in clinical practice. This research project aims to improve the updating process of CPGs by leveraging machine learning, information retrieval, and natural language processing techniques.

The primary objective of this project is to develop systems that can efficiently identify and recommend current, relevant publications for inclusion in updated clinical guidelines. Furthermore, the project investigates quantitative and qualitative methods to evaluate the performance of such systems. Another significant goal of this project is to investigate techniques for automatically assessing the quality of evidence in biomedical publications. The project will make use of evidence grading systems like the Strength of Recommendation Taxonomy (SORT) to identify and evaluate studies based on their level of evidence.

Initial experiments employ both an older and a current version of the German melanoma clinical guidelines to evaluate the performance of various information retrieval approaches, such as classical information retrieval, bibliometric-enhanced information retrieval, and semantic search based on dense embeddings of transformer-based language models. Additional methods being investigated include machine learning algorithms for abstractive summarization techniques that can generate concise summaries of relevant publications. This approach can assist guideline developers in quickly identifying the most important research findings. The project is also exploring methods to model the relationships between publications, which can aid in identifying the most influential studies and help guide the updating process. The experiments aim to predict the publications included in the current guidelines based on those in the older version, using PubMed as the source for retrieving biomedical publications.

Results indicate that while relevant publications can be identified using these approaches, ranking the literature from the current guidelines among the higher-ranked publications remains challenging. Consequently, the project is exploring additional assessment and scoring methods, such as combinations of the different approaches, to enhance the CPG updating process. By incorporating these new methods, the research aims to improve the effectiveness and efficiency of updating CPGs, ultimately leading to better patient care and outcomes.

Mitigating Cognitive Bias with Clinical Decision Support Systems

Alisa Küper (alisa.kueper@uni-due.de)
Supervisor: Prof. Dr. phil. Nicole Krämer

Motivation: When physicians make clinical decisions they make use of two different systems of decision making: a fast, intuitive system that operates subconsciously and a slower analytical system[1]. When under time constrains physicians potentially rely on the intuitive mode to make use of heuristics, rules of thumb derived from prior experience. However, these are prone to trigger cognitive bias, which can lead to diagnostic error. Bias has been identified as one of the major sources of diagnostic error [2]. With technology supporting physicians in many different areas in the clinical setting, a clinical decision support systems that not only suggests possible diagnosis but additionally provides information to mitigate cognitive bias, could support physicians in finding the correct diagnosis.

Research Question: The goals of this study are: 1) To test debiasing methods that were proposed by previous research and find out whether they can succeed in mitigating biases. 2) To investigate further influencing factors like confidence and experience on the probability to elicit bias and remedy the decision after receiving decision aid. 3) To investigate whether the time of support and the possibility to form a first opinion without decision aid makes a difference.

Methodology: A between subject three-group design was employed. Participants were presented with a decision-making task under the influence of either availability or representativeness bias. These tasks consisted of different vignettes depicting hypothetical clinical scenarios, formulated in a way to elicit the aforementioned biases, with a choice of three to four differential diagnosis. Depending on the test group, participants received additional information, such as base rate probability or prototypical data for the diagnosis, to potentially mitigate bias. Furthermore, participants were asked to rate their confidence in their decision. Demographic data, including years of experience, were collected.

Results: Analysis showed that presentation of prevalence data to mitigate availability bias changed the final probability estimate of the diagnosis significantly. Prototypical data to counteract representativeness bias showed no significant change. Neither medical experience nor confidence in the decision had a significant influence on the probability to change the estimate. Timing of support after or before forming a first uninfluenced opinion made no significant difference for the final decision.

[1] Kahneman, D., “Thinking, fast and slow", 2011

[2] Croskerry, P., “From Mindless to Mindful Practice — Cognitive Bias and Clinical Decision Making.," New England Journal of Medicine, 368(26), 2013

Explainable multi-modal prediction models based on patient history data

Meijie Li (meijie.li@uni-due.de)
Supervisor: Prof. Dr. Christin Seifert

A treatment plan for cancer is a series of decisions made during the treatment phase based on the progression of the disease and the patient's condition. From a computer science perspective, diagnostics are characterized by the collection and aggregation of information. Treatment decisions are then made based on the clinical information gathered for the patient to date. This includes structured information obtained through initial patient histories (patient referral, anamneses), clinical reports, imaging data, and sequential information in genome sequencing data. In the case of malignant melanoma, treatment decisions are made by a panel of experts, the "Tumorboard" considering the diagnosis, expected side effects of each treatment option.

The dissertation project will develop a predictive model that can "act as an expert on the tumor board", which can predict patient outcomes(survival time, side effects), explain the reasons for their decision, and analyze the patterns' contribution to the overall decision.

Preliminary Results

As a first step, we created an overview of the patient's diagnostic and treatment pathway. Based on data provided by University Hospital Essen (UKE) in FHIR[1] format, relevant data attributes are selected, transformed in JSON, and visualized using the anychart library[2](cf.Figure1, left) . The patient history visualization (cf. Figure1, right) provides an overview of all clinical information collected so far for the patient. At the same time, we also hope that the patient trajectory can help clinicians more easily to grasp the patient's disease progression and physical condition to help them formulate the best treatment plan for the patient.

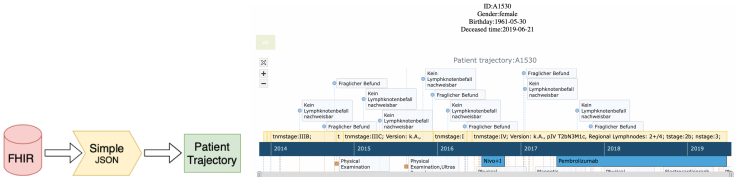


Figure 1: Visuaztilzation pipeline (left) and Example Visualization for a realistic, but artificial patient (right).

[1] https://www.hl7.org/fhir/
[2] https://www.anychart.com

Analysis of Preclinical Image Data Including Additional Clinical Data

Daniel Sauter (daniel.sauter@fh-dortmund.de)
Supervisor: Prof. Dr. rer. nat. Markus Kukuk

Malignant melanoma have a high mortality rate when diagnosed at a late stage[1]. Fortunately, there is recent progress in melanoma treatment[2]. Here, histopathological examination is an important element in the clinical practice[3]. There are numerous applications of deep learning (DL) to histopathology for predicting clinical endpoints[4]. Specifically for malignant melanoma, research is mainly based on the diagnosis using supervised DL (e.g., Hekler et al.[5]). Other technical approaches (like multiple instance learning) promise to address challenges like the high labeling effort in histopathology. Another relevant aspect is reproducibility[6]. Therefore, there is some effort on explainable AI (XAI) for DL-based computational melanoma pathology[7].

This thesis aims at predicting clinical endpoints from digital histopathology slides using DL. As a first step, we already performed a study on a concept-based XAI method called automated concept-based explanation (ACE)[8]. Our study validated the technical validity of ACE for bias discovery in histopathological CNNs[9]. ACE provided insight into the CNNs beyond a heatmap-based control method called Guided Grad-CAM[10]. Next, we will identify suitable techniques in the literature on DL and computational pathology using the systematic literature review methodology. Those techniques should then be applied to develop CNNs, for example on BRAF mutation prediction.

[1] Robert Koch-Institut, "Krebs in Deutschland für 2017/2018," Berlin, 2021, Accessed: Dec. 11th 2022, Available: `https://www.krebsdaten.de/Krebs/DE/Content/Publikationen/Krebs_in_Deutschland/kid_2021/krebs_in_deutschland_2021.pdf`

[2] D. Schadendorf et al., "Melanoma," Lancet, vol. 392, no. 10151, pp. 971–984, 2018

[3] R. A. Scolyer, R. V. Rawson, J. E. Gershenwald, P. M. Ferguson, and V. G. Prieto, "Melanoma pathology reporting and staging," Mod. Pathol., vol. 33, no. 1, pp. 15–24, 2020

[4] C. L. Srinidhi, O. Ciga, and A. L. Martel, "Deep neural network models for computational histopathology: A survey," Med. Image Anal., vol. 67, no. 1, paper 101813, 2021

[5] A. Hekler et al., "Deep learning outperformed 11 pathologists in the classification of histopathological melanoma images," Eur. J. Cancer, vol. 118, pp. 91–96, 2019

[6] B. Haibe-Kains et al., "Transparency and reproducibility in artificial intelligence," Nature, vol. 586, no. 7829, pp. E14–E16, 2020

[7] K. Hauser et al., "Explainable artificial intelligence in skin cancer recognition: A systematic review," Eur. J. Cancer, vol. 167, pp. 54–69, 2022

[8] A. Ghorbani et al., "Towards Automatic Concept-based Explanations," in NeurIPS 2019 Proc., Vancouver, Canada, 2019, pp. 9277–9286

[9] D. Sauter et al., "Validating Automatic Concept-Based Explanations for AI-Based Digital Histopathology," Sensors, vol. 22, no. 14, paper 5346, 2022

[10] R. R. Selvaraju et al., "Grad-CAM: Visual Explanations from Deep Networks via Gradient-Based Localization," in ICCV 2017 Proc., Venice, Italy, 2017, pp. 618–626

Leveraging English Datasets and Annotation Transfer for Pre-annotating German Clinical Texts

Henning Schäfer (henning.schaefer@uk-essen.de)
Supervisor: Prof. Dr. Christoph M. Friedrich

Clinical texts contain a wealth of critical information on etiology, family history, treatment types, and success rates. These texts can be found in various sources such as publications (PubMed) or electronic health records (EHRs). Systematically analyzing this vast pool of data can lead to improved clinical care and better decision support. However, clinical text is often written as unstructured free text by physicians who are under time pressure. Consequently, these texts are characterized by heterogeneity in abbreviations, omission of words, and the use of medical jargon to maintain high information density.[1]

With regard to the availability of natural language processing (NLP) tools for other languages than English, there are major differences, for example in the processing of German clinical texts: Anonymization is left to individual institutions, data protection officers and ethics committees, which means that there are no uniform regulations. The state-of-the-art for German texts lags behind and, despite great efforts [2], continues to be limited to rule-based systems [3] or is often based on in-house data, which means that neither the data nor the trained models can be shared [4].

By employing a methodology that combines cross-language span prediction and contextualized word embedding models with neural machine translation, English datasets can be transferred alongside annotation alignment to German as a pre-annotation. These pre-annotations can then be verified and serve as a valuable starting point for generating pre-annotations and training models in cases where no data would otherwise be available.

[1] Leaman, R., Khare, R., and Lu, Z. (2015). Challenges in clinical natural language processing for automated disorder normalization. Journal of biomedical informatics, 57, 28-37.

[2] Hahn, U., Matthies, F., Lohr, C., and Löffler, M. (2018). 3000PA-Towards a National Reference Corpus of German Clinical Language. Studies in health technology and informatics, 247, 26-30.

[3] Roller, R., Seiffe, L., Ayach, A., Möller, S., Marten, O., Mikhailov, M., ... and Budde, K. (2020). Information Extraction Models for German Clinical Text. In 2020 IEEE International Conference on Healthcare Informatics (ICHI) (pp. 1-2). IEEE.

[4] Carlini, N., Tramer, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., ... and Raffel, C. (2021). Extracting training data from large language models. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 2633-2650).

Predictive Modeling Based on a Clinical Concept Model of Melanoma using Patient Similarity

Jessica Swoboda (jessica.swoboda@uk-essen.de)
Supervisor: Prof. Dr. Britta Böckmann

Patient-specific predictions, using patient data and similarity to calculate individual probabilities for possible outcomes, have great potential to improve medical care[1]. Individual predictive modeling uses regularly documented medical data rather than specifically collected cohort data[2] to find a variety of possible predictors that might not have been considered in a cohort study.

The aim of this study is to assess whether prediction models can be developed, which predict different patient specific and probabilistic treatment outcomes of melanoma patients, based on electronic health record (EHR) data and patient similarities, thereby improving the decision making of dermatooncologists.

To standardize aspects of retrospective EHRs of patients diagnosed with malignant melanoma from the University Hospital Essen, we created initial clinical concept models as basis for predictions. They describe clinical concepts as patterns using artifacts and can be combined into use cases. The standard Fast Healthcare Interoperability Resources (FHIR) is used for modeling due to its widespread use in the German inpatient sector. Metrics will be constructed with covariates of an outcome. A first approach will be based on predicting side effects. The model will be trained on EHR data, using supervised machine learning algorithms for classification such as random forest and gradient tree boosting. To prove robustness, we will perform model validation using nested/k fold cross validation. Several performance measurement parameters, such as positive predictive value, and precision recall curve, will be determined using test data to be compared to the assessment of dermatooncologists.

We analyzed the German evidence-based guideline on malignant melanoma regarding medications and possible side effects. An analysis of different treatment relevant FHIR resources was performed using ten non anonymized EHRs of melanoma patients for their use at the University Hospital Essen. This provided insights into the data structure and available information regarding primary tumor diagnoses, comorbidities, patient visits, tumor boards, treatment planning, etc.

By providing probabilistic patient specific predictions for potential side effects of different drug therapy options, we aim to improve decision making for melanoma patients in routine clinical practice using regularly documented data.

[1] Jenkins, D. A., Sperrin, M., Martin, G. P. and Peek, N. (2018). Dynamic models to predict health outcomes: current status and methodological challenges. Diagnostic and prognostic research 2, 23.

[2] Goldstein, B. A., Navar, A. M., Pencina, M. J. and Ioannidis, J. P. A. (2017).Opportunities and challenges in developing risk prediction models with electronic health records data: a systematic review. Journal of the American Medical Informatics Association : JAMIA 24, 198–208.

Uncertainty-aware HLA typing at subclone resolution

Hamdiye Uzuner (hamdiye.uzuner@uni-due.de)
Supervisor: Dr. Johannes Köster

HLA (Human Leukocyte Antigen) haplotypes are a large group of genes that bear extreme sequence polymorphism as well as sequence similarity. The HLA system is referred to as the human version of the Major Histocompatibility Complex (MHC), with all three classes (Class I, II and III) located on the chromosome 6[1]. Class I and II HLAs are known to present antigens to T cells,[1] thereby their role in certain diseases including cancer and its treatment is stressed at this point, particularly immunotherapy. Therefore, accurate and precise identification of HLA haplotypes is necessary considering the heterogenity of tumors. In this project, a Bayesian latent variable model is developed for the quantification of haplotypes that allows a resolution of subclonal levels, using Next Generation Sequencing (NGS) data. The framework is named as ORThogonal evidence HAplotype Quantification (ORTHANQ), being reachable under `https://github.com/orthanq/orthanq`.

Orthanq uses Maximum Likelihood Estimates (MLE) of Variant Allele Frequencies (VAFs) that come from Varlociraptor[2], a variant caller than can deal with all types of biases and uncertainties, and it uses these to formulate a linear optimisation problem that is solved to acquire a prefiltered set of haplotypes. Then, VAF distributions are used as evidence for the calculation of likelihood of fractions. Afterwards, depending on the priors that is configurable for normal and tumor samples, every combination of haplotype fractions is explored and the posterior probabilities of combination of haplotype fractions are reported, together with their uncertainty estimates. The model is continuously tested on simulated samples that are generated artificially from HLA haplotypes. Moreover, public datasets, e.g. International HapMap Project, are also used to evaluate the performance of the model.

Besides the ability to quantify HLA haplotypes at subclonal resolution, the model can be applied to quantify virus lineages, for example in the current and (SARS-CoV-2) and future viral outbreaks.

[1] Choo S. Y. (2007). The HLA system: genetics, immunology, clinical testing, and clinical implications. Yonsei medical journal, 48(1), 11–23. https://doi.org/10.3349/ymj.2007.48.1.11

[2] Köster, J., Dijkstra, L. J., Marschall, T., and Schönhuth, A. (2020). Varlociraptor: enhancing sensitivity and controlling false discovery rate in somatic indel discovery. Genome biology, 21(1), 98. https://doi.org/10.1186/s13059-020-01993-6

Research School on Data Science and Engineering

Prof. Dr. Felix Naumann
Email: felix.naumann@hpi.de
Hasso Plattner Institute, University of Potsdam
Internet: https://hpi.de/research-schools/hpi-dse.html

The increasing abundance of data in science and in industry creates many challenges and opportunities. Data science has grown to be a foundational discipline in information technology, allowing new insights from data and creating ever more intelligent applications. Simultaneously, it is becoming increasingly difficult to collect, clean and deliver the vast amounts of data and apply and maintain complex data science processes. Targeting these challenges, the discipline of data engineering has become equally foundational.

The 2019 newly established research school „Data Science and Engineering" unites top PhD students in all areas of data-driven research and technology, including scalable storage, stream processing, data cleaning, machine learning and deep learning, text processing, data visualization, digital health and more. We apply our research to many different use cases across the participating interdisciplinary research groups, joining forces whenever possible.

Mixer Flow: A computationally efficient normalising flow

Eshant English (eshant.english@hpi.de)
Supervisor: Prof. Dr. Christoph Lippert

Normalising flows are invertible neural networks used for generative modelling. They utilise the change of variable formula to normalise the unknown distribution to a distribution of choice, generally chosen to be multivariate standard Gaussian. The extensive knowledge of the properties of the normalised distribution along with invertibility facilitates Density Estimation and Sampling by using the change of variable formula.

Change of Variables: Let $p_X(x)$ be the unknown distribution and $p_Z(z)$ be the known normalised distribution where $z = f(x)$.

$$p_X(x) = p_Z(f^{-1}(x)) \left| det \left(\frac{\partial f^{-1}(x)}{\partial x} \right) \right|$$

Currently, Glow architecture is the state-of-the-art Normalising Flow model for image synthesis. However, it is computationally inefficient and a 32*32 image generation costs approx. 45 Million parameters. In comparison, the state-of-the-art Style-GAN has approx. 30 Million parameters and generates images of better quality. In this work, we propose an architecture, which uses only 7.5 Million parameters for 32*32 image generation and generates images of non-inferior quality than the Glow architecture.

Efficient Round-Based Decentralized Aggregation for Count-Based Windows

Wang Yue (Wang.Yue@hpi.de)
Supervisor: Prof. Dr. Tilmann Rabl

In the field of IoT, there are many devices are employed in industry as well as in research. These devices are used by many applications and are connected in huge decentralized networks. They produce large data streams that need to be processed in a timely fashion. Current stream processing engines (SPEs) typically compute queries on such streams in centralized data centers. Given that data streams are distributed among a decentralized network, SPEs have to collect the events centrally. To reduce the amount of data sent in decentralized networks, state-of-the-art solutions off-load partial computations on machines that are close to data sources and collect partial results in a logical center. However, these solutions only focus on time-based windows. For count-based windows, they still need to send all data via the network and all computations is performed centrally.

We present Deco, a decentralized round-based aggregation approach for count-based windows. For each count-based window, there is at least one communication round between the center and devices, which is the same as current solutions processing time-based windows. To process count-based windows, Deco partitions events locally close to the data source and sends only a fraction of events to the data center. Based on these fractions, the data center computes and sends local window sizes for each local node. Then count-based windows are partially aggregated on the edge devices. Although there are multiple rounds between the center and devices, only partial results and few events are transmitted to the data center. Deco adapts local window sizes to changing event generation rates and also supports both decomposable functions and non-decomposable functions. Deco outperforms centralized solutions by orders of magnitude when processing count-based windows. Deco reduces network traffic by up to 99% and its throughput scales linearly with the number of nodes.

Prediction of Physical Responses During Resistance Training Using Markerless Motion Tracking

Justin Albert (justin.albert@hpi.de)
Supervisor: Prof. Dr. Bert Arnrich

Intensity quantification is essential in weight training to adjust training routines. Overtraining can increase the risk of injuries, while undertraining does not deliver optimal training results. In this project, we aim to develop an unobtrusive exercise feedback system that works contactless for the athlete. Toward this goal, we develop models that can predict multiple physical and subjective responses during resistance training, including the heart rate, the subjective rating of perceived exertion (RPE), and the power progression over time. An RPE scale is validated to give a good overview of athletes' physical states. A standard RPE scale is the Borg scale, which usually ranges from 6 to 20, where six refers to minimal exertion, and 20 refers to maximal exertion.

We have recorded a dataset of 16 participants performing the squat exercise on a Flywheel machine for 12 sets and 12 repetitions each. Subjects were measured using a full-body Inertial Measurement Unit setup consisting of six sensors, electrocardiography (ECG), and two Microsoft Azure Kinect RGB-D cameras. The Flywheel also measured the power output for each repetition. We obtained temporally stable skeletons from the Kinect cameras using camera calibration, signal filtering, and inverse kinematics. Based on the obtained joint positions and orientations, the goal is to train models to predict the power, heart rate, and RPE responses. We utilize and compare various approaches, such as sliding windows, exercise segmentation, statistical features, and deep learning. Further, we introduce temporal context to the models, either by gradients of individual repetitions or time-series machine learning models. With the predictions of these models, athletes could get training feedback in real-time during the exercise without the need to wear sensors and react accordingly to the output.

Wearable multi-modal on-body sensor systems for real-time classification of mental workload and stress

Christoph Anders (christoph.anders@hpi.de)
Supervisor: Prof. Dr. Bert Arnrich

High levels of mental workload and stress, especially if prolonged, can lead to mistakes, incur mental health issues, and reduce the quality of life of individuals. Currently, individuals are on their own with the task of identifying and coping with challenging times. The timely self-identification of stress and high mental workload requires active, truthful, and reflected actions of the individual. While subject-matter experts could provide guidance, there will always be a shortage of timely and affordable external evaluations. Ultimately, the application of on-body sensor systems for monitoring the psychophysiological signals of individuals is seen as the solution to this problem. Some work has already been performed on the classification of mental states using on-body sensor systems, yet many open questions remain [1].

To bring wearable devices and their assistance in healthcare closer to society, plenty of challenges in the application of wearable devices have to be overcome. Common challenges are the contamination of recorded time series with noise, the partial absence of ground-truth labels, and the synchronization of the utilized wearable systems. No one-solution-fits-all can be provided, and benchmarks usually do not encapsulate challenging aspects of recordings in uncontrolled environments due to the unavailability of such data. In order to broaden knowledge in this field, we are working towards collecting and publishing data sets that will investigate mental workload and stress in controlled, semi-controlled, and uncontrolled environments. We are utilizing affordable, consumer-grade multi-modal on-body sensor systems which are widely used by consumers in the market today. We aim to collect equal amounts of data from healthy and sick participants.

Our goals are to increase the amount of publicly available data, develop algorithms to alleviate noise and artefacts, automatically clean data, and to implement new methods for time-series data augmentation as well as data forecasting. To achieve this, we have so far collected a dataset of stress and mental workload elicitation in twenty-five healthy participants in controlled and uncontrolled environments and are performing the first analysis steps on a subset thereof. Planned and prepared projects will investigate interventions for mental workload and stress as well as dive into these topics with respect to reading comprehension.

[1] Christoph Anders and Bert Arnrich, "Wearable electroencephalography and multi-modal mental state classification: A systematic literature review", Computers in Biology and Medicine, Volume 150, November 2022, DOI: 10.1016/j.compbiomed.2022.106088

Integrating Knowledge and Graph-Based Strategies for Text

Margarita Bugueño (margarita.bugueno@hpi.de)
Supervisor: Prof. Dr. Gerard de Melo, Prof. Dr. Bert Arnrich

Natural Language Processing (NLP) involves applying algorithms to face natural language in a rule-based approach. In order to extract the meaning associated with a piece of text, NLP transforms the language data into a structure that computers can understand. However, it is considered a challenge. Understanding both the words and the way concepts are associated is required. For this reason, it is common to use different techniques to handle the multiple language aspects, each establishing learning restrictions.

Given the success of Graph Neural Networks (GNNs) for structure-aware machine learning, numerous studies have explored their application to text classification by proposing an alternative to traditional feature representation models, such as vector representation, which most of the time fail to map the full richness of the text.

Although several graph-based models for text representation, document summarization, and question-answering have been proposed giving a considerable boost to those tasks, most strategies were domain-specific and validated on data with particular characteristics, making it difficult to compare and extend them to new scenarios for assessing their merits in modern settings. Furthermore, the graph methods generally base their construction strategy on the co-occurrence of terms, leaving aside critical factors such as syntax, semantics, and co-reference.

All this reflects that the graph-based text representation area requires further study and in-depth exploration.

Improving the Linguistic Capabilities of Vision-and-Language Models

Marco Cipriano (marco.cipriano@hpi.de)
Supervisor: Prof. Dr. Gerard de Melo

Vision-and-Language models have achieved impressive success in learning multimodal representations, which noticeably improved the performances of those models in tasks like image captioning, retrieval, and Visual Question Answering (VQA). However, among all the fields where multimodal deep learning algorithms have reached extraordinary results, the medical domain is one where their full potential still remains undug. The reason relies on the lack of large annotated datasets and the complexity of those tasks, which often require medical expertise to be fully understood.

In recent years, Medical VQA has raised a growing interest in the research community [1], due to its considerable potential to benefit healthcare systems. In the future, Medical VQA models may aid clinicians in interpreting medical images, obtaining more accurate diagnoses, and ultimately, improving patient care. We are working towards improving the performance of Vision-and-Language models for this task. We created a large multi-organ dataset by collecting, extracting, and merging images from many 3D public datasets. Those datasets contain single and multi-organ annotations from various parts of the human body. We have extracted slices out of 3D CT and MRI and X-ray scans to create a dataset of more than 23 thousand annotated images covering the brain, heart, spleen, kidneys, bladder, lungs, and liver. We plan to increase the number of images and covered organs in the future. The current target organs were chosen to reflect the most common and relevant organs for the medical VQA benchmarks. We are now working on semi-supervised pre-training objectives [2] to enable state-of-the-art VQA models with better segmentation capabilities and organ awareness.

[1] Liu Bo, Zhan Li-Ming, Wu Xiao-Ming, "Contrastive pre-training and representation distillation for medical visual question answering based on radiology images" Medical Image Computing and Computer Assisted Intervention–MICCAI, 2021

[2] Pengfei Li, Gang Liu, Lin Tan, Jinying Liao, Shenjun Zhong, "Self-supervised vision-language pretraining for Medical visual question answering" arXiv preprint arXiv:2211.13594, 2022

Analysis and Design of Privacy Preserving Protocols

Tarek Galal (tarek.abdelsalam@hpi.de)
Supervisor: Prof. Dr. Anja Lehmann

Digital Covid certificates are the first widely deployed end-user cryptographic certificates. For service providers, such as airlines or event ticket vendors, that needed to check that their (global) customers satisfy certain health policies, the verification of such Covid certificates was challenging though - not because of the cryptography involved, but due to the multitude of issuers, different certificate types and the evolving nature of country-specific policies that had to be supported. As Covid certificates contain sensitive health information, their (online) presentation to non-health related entities also poses clear privacy risk. To address both challenges, the EU proposed a specification for outsourcing the verification process to a validator service, that executes the process and informs service providers of the result. The WHO announced to adapt this approach for general vaccination credentials beyond Covid-19. While being beneficial to improve security and privacy for service providers, their solution requires strong trust assumption for the (central) validation service that learns all health-related details of the users.

In our first project, we propose and formally model a privacy-preserving variant of such an outsourced validation service. Therein the validator learns the attributes it is supposed to verify, but not the users identity. Still, the validator's assertion is blindly bound to the user's identity to ensure the desired user-binding. We analyze the EU specification in our model and show that it only meets a subset of those goals. Our analysis further shows that the EU protocol is unnecessarily complex and can be significantly simplified while maintaining the same (weak) level of security. Finally, we propose a new construction for privacy-preserving certificate validation that provably satisfies all desired goals.

TAHARAT: Cleaning ill-formed Rows in CSV Files

Mazhar Hameed (mazhar.hameed@hpi.uni-potsdam.de)
Supervisor: Prof. Dr. Felix Naumann

Comma-separated value (CSV) files follow a useful and widespread format for data exchange due to their flexible standard. However, due to this flexibility and plain text format, such files often have structural issues, such as unescaped quote characters within quoted fields, columns containing different value formats, rows with different numbers of cells, etc. We refer to rows that contain such structural inconsistencies as *ill-formed*. Consequently, ingesting them into a host system, such as a database or an analytics platform, often requires prior data preparation steps.

Traditionally, data scientists write custom code to clean ill-formed rows, even before they can use data cleaning tools and libraries, which assume all data to be properly loaded. These tasks are tedious and time-consuming, requiring expertise and frequent human intervention. To automate this process, we propose TAHARAT[1], a system that automatically detects ill-formed rows containing data and then standardizes their structure into a uniform format based on the structure of well-formed rows. Of $2,003,514$ manually annotated rows from four different sources, TAHARAT was able to correctly detect 95.53% of data rows and accurately generate transformations for 87.83% of them.

[1] TAHARAT is an Urdu word that means the state or quality of being clean.

Computational methods for the characterization of the human post-translational modification landscape

Yannick Hartmaring (yannick.hartmaring@hpi.de)
Supervisor: Prof. Dr. Bernhard Renard

A post-translational Modification (PTM) is an alteration on a protein that changes the amino acid sequence into a functional proteoform. Such a modification has the ability to change the protein function and therefore highly increase the complexity of the overall proteome. PTMs regulate not only the physical or chemical properties of proteins but also their structure, stability and cellular location. Overall, they affect almost all cellular processes. [1]

In addition to more than 300 known PTMs, the individual modifications also often interact and rely on each other. Therefore a much higher degree of combinatorial variation occurs. This type of communication is called crosstalk. Discrepancies in these interaction is linked to the development of various diseases like Alzheimer's disease and diabetes. [2]

Due to fragmentation during the analysis of protein sequences it is no longer possible to make statements about the crosstalk of PTMs across different peptides, since it is not clear which PTMs are located simultaneously on the same protein molecule and which do not occur together.

To get a better overview of the human PTM-landscape, we will first analyse which PTMs generally occur in human samples across different tissues and conditions. Therefore we will utilize already available public datasets and map all peptides and PTMs against their original protein sequences to establish a unique mapping of modification sites. Secondly, we will utilize the PTM identifications and peptide quantitive information from step one to identify which PTMs do co-occur. Due to alternative splicing and variable modification events, different non-linear proteoforms arise. To account for these alternative paths in the unique PTM mapping, we will develop a graph-based proteome approach so each PTM can be connect to a unique site. The quantity information is used to build weighted edges to connect the individual positions of the peptides. Through this graph-based approach it will be possible to identify co-occuring PTMs across different non-overlapping peptides by using statistical and graph-based deep learning models.

The new knowledge gained from proteoform identification and PTM co-expression will provide new insights into cellular protein regulation and highlight modifications of interest in a variety of human tissues and conditions. Accordingly, it will be possible to develop new approaches to understanding and treating diseases.

[1] Schlaffner et al, 'FLEXIQuant-LF to quantify protein modification extent in label-free proteomics data, eLife, vol. 9, p. e58783, 2020

[2] Laarse et al., Crosstalk between phosphorylation and O-GlcNAcylation: friend or foe, FEBS J., vol. 17, p. 3152-3167, 2018

Network-based multi-drug response prediction using multi-omics data

Pauline Hiort (pauline.hiort@hpi.de)
Supervisor: Bernhard Renard

Networks are an important tool for the analysis of interactions in complex systems. Networks have been shown to be especially beneficial when investigating molecular interactions in biological cells, e.g., in human cells. In these cells, different types of molecules interact and regulate each other. Especially in disease states, for example in cancer, the interactions can be altered, giving rise to disease-specific networks.
We developed a pipeline to use these disease-specific networks for single drug response prediction[1]. The associated R package is published on CRAN. It enables differential predictions between two conditions, e.g., two groups of patients. Using correlations of abundance measurements, condition-specific molecular networks are generated. Multiple layers of information from different types of molecules, such as genes and proteins, are combined into multi-layer networks. The condition-specific networks are further processed by computing a novel semi-local, path-based integration. Differential predictions on drug responses are inferred by contrasting the condition-specific integrated multi-layer networks. The differential drug responses are explainable, so that the differences in the molecular interactions contributing to a differential drug response score can be retrieved. As a case study, we predict differential drug response in breast cancer contrasting patients of two cancer sub-types.
Currently, we develop a network-based analysis pipeline for predicting drug-drug interactions. Treatments of diseases with drug combinations can improve their therapeutic effect, but can also cause undesired adverse effects. We focus on classifying drug-drug combinations as advantageous or adverse. Our pipeline combines disease-specific distance information from protein-protein interaction networks with machine learning classification methods. Distance measures are computed using the interaction network, drug target information, and disease gene information. Previously, these measures have been used to define drug interaction motifs and thus classify drug combinations based on a fixed distance threshold[2]. To improve the classification based on the distance measures, we test several machine learning approaches. For model training, we rely on ground truth data comprising FDA-approved drug combinations and combinations with adverse effects from Cheng and Kovács et al. (2019)[2]. We apply our method on the case of cancer as disease and anti-cancer drug combinations.

[1] Hiort et al. (2022). DrDimont: explainable drug response prediction from differential analysis of multi-omics networks. *Bioinformatics*, 38(Supplement_2), ii113–ii119.
[2] Cheng and Kovács et al. (2019). Network-based prediction of drug combinations. *Nature Communications*, 10(1), 1197.

Privacy-Preserving Identity Management

Maximilian Kroschewski (maximilian.kroschewski@hpi.de)
Supervisor: Prof. Dr. Anja Lehmann

In our research, we are interested in privacy-preserving solutions that meet the desired functional requirements in a secure and privacy-friendly way. This includes the definition of a security model, the design of a cryptographic protocol, proving its security under precise assumptions, and, optionally, demonstrating its applicability with an implementation.

Our first research project aimed to enhance the privacy of Single Sign-On (SSO) protocols, specifically focusing on the OpenID Connect (OIDC) protocol. We identified the lack of privacy in OIDC, which allows the Identity Provider (IdP) to learn the Relying Party's (RP) identity at each user login. We proposed a privacy-preserving approach to incorporate RP authentication into the Implicit Flow, a OIDC sub-protocol, ensuring users only access properly registered RPs while preventing the IdP from acquiring knowledge of which user is accessing which RP. Our approach formally defines the desired security and privacy properties, and we proposed a provably secure construction using generic building blocks. Finally, we reported on the implementation of our approach.

Evaluation of post-hoc attribution methods on genomic motif interactions

Marta Lemanczyk (marta.lemanczyk@hpi.de)
Supervisor: Prof. Dr. Bernhard Renard

Deep Neural Networks excel at complex prediction tasks since they are capable to learn complex interactions between features. Especially convolutional neural networks (CNN) are suitable for sequence-based tasks in the biological domain due to their capability to learn patterns of biologically relevant sub-sequences (so-called motifs). To understand a model's decision for specific inputs, post-hoc attribution methods are often used to highlight the parts of an input that impact the decision for the given outcome. Those methods have in common that they are applied to an already-trained model so no re-training is required. However, feature dependencies and interactions can lead to erroneous interpretability due to the additive nature of those methods.
In this project, we investigate the interpretability performance of post-hoc attribution methods (including DeepLIFT[1], Integrated Gradients[2] and Feature Permutation[3]) on CNNs trained on genomic data containing motif interactions. First, we formalize interactions to enable the generation of data containing various interactions. We include different logical relationships, represented by the presence or absence of motifs in a sequence, as well as the effects of interactions on the outcome encoded in the target value. Additionally, we focus on the following aspects: (1) Negative data with unavailable motif subsets in the training, (2) the effects of additive and non-additive relationships between motifs, and (3) subpopulations in classification tasks. For all experiments, we distinguish between subsets with homologous motifs and subsets with heterologous motifs to see if motif similarity between interacting motifs influences interpretability. We use motif sequences from the JASPAR database for transcription factor binding sites[4] to ensure a realistic simulation.

[1] Shrikumar, Avanti, Peyton Greenside, and Anshul Kundaje. *"Learning important features through propagating activation differences."* International conference on machine learning. PMLR (2017).

[2] Sundararajan, Mukund, Ankur Taly, and Qiqi Yan. *"Axiomatic attribution for deep networks."* International conference on machine learning. PMLR (2017).

[3] Fisher, Aaron, Cynthia Rudin, and Francesca Dominici. *"All Models are Wrong, but Many are Useful: Learning a Variable's Importance by Studying an Entire Class of Prediction Models Simultaneously."* J. Mach. Learn. Res. 20.177 (2019): 1-81.

[4] Castro-Mondragon, Jaime A., et al. *"JASPAR 2022: the 9th release of the open-access database of transcription factor binding profiles."* Nucleic acids research 50.D1 (2022): D165-D173

TopGeoNet: Topological-Geometric Graph Neural Network

Tahir Miriyev (tahir.miriyev@hpi.de)
Supervisor: Prof.,Dr.,Christoph Lippert

A standard representation for graph neural networks (GNNs) is widely accepted to be node-centered, considering the low complexity of such architecture. However, in practice, many applications assume potential interactions between larger groups of nodes, as well as between distant nodes. Standard GNNs fail in capturing valuable features related to these cases, resulting in expensive computational time, inefficient representation learning, and poor interpretability of results. In my research, I try to go beyond the classical choice by "lifting up" the architecture to characterize relationships between N number of nodes via N-dimensional topological simplices, rather than nodes and edges. This included the development of the novel Message Passing algorithm and the Attention mechanism to achieve an optimized feature update and explainability, respectively. The aim is to provide a better computational fabric for GNNs with the following advantages:

- Expressive power. Defining Message Passing between more than two nodes can lead to the discovery of potentially new types of features, and consequently, improve the accuracy in tasks such as classification, prediction, and knowledge discovery.
- Avoid under-reaching, over-smoothing, and bottlenecks. N-simplices may alleviate these problems because of the higher dimensional structure that connects nodes, hence creating an instant feature update for all nodes within the simplex and achieving more efficient information propagation.
- Hierarchical modeling. We can define computations performed by a novel Message Passing algorithm to be hierarchical, with information flowing from lower-dimensional simplices to higher-dimensional ones, and backward.
- Natural integration of notions from mathematics. Such a redefined architecture of GNNs allows us to exploit mathematical tools in Algebraic Topology and Graph Theory, such as a Mapper algorithm and Persistence Diagrams for studying explainable clustering and node connectivity, respectively.
- Parallelization for GPU-optimized training. Every subgraph containing only N-simplices can be processed in parallel, and the final results can be aggregated.

Affective Computing with Multi-modal Wearable Sensors: A Potential Tool for Early Detection of Epileptic Seizures.

Sidratul Moontaha (sidratul.moontaha@hpi.de)
Supervisor: Prof. Dr. Bert Arnrich

The autonomous nervous system, responsible for regulating bodily functions such as heart rate, is triggered by negative emotions, stress, and mental workload, just as it is by epileptic seizures. These factors have also been identified as potential premonitory factors of epileptic seizures. An affective computing system can detect patterns that may indicate an impending seizure by analyzing physiological and behavioral signals, such as heart rate, brain activity, and skin conductivity. As proposed in our concept study[1], early detection can provide medical interventions promptly, thereby improving the quality of life for individuals with epilepsy.

Prior to measuring affects in epilepsy patients, we conducted several studies with the control group to develop a robust experimental framework for multi-modal baseline assessments. A test battery was designed, including stimuli and questionnaire presenters, without external interference. Moreover, using a single platform, multi-modal data can be recorded in parallel, such as Photoplethysmography (PPG), Electroencephalography (EEG), Acceleration, and Electrodermal Activity data. The developed framework was tested on eight participants in a controlled environment while performing tasks that elicit mental workload, and the synchronization was ensured using a shake detection tool[2]. Performing binary classification on high and low mental workload, our analysis reports that EEG asymmetry features contributed significantly over other EEG features [3]. Moreover, during the presentation of various emotional stimuli via the test battery, real-time EEG data was collected. The Valence and Arousal classification pipeline outperformed the reported metrics on the state-of-the-art dataset. The real-time emotion prediction also demonstrated potential for a practical system[4].

Currently, multi-modal data has been curated from 25 healthy participants performing mental workload-related tasks in controlled and uncontrolled environments. Part of the collected data has been synchronized, pre-processed, and classified for mental workload measurement and is ready to be submitted as a scientific contribution. Therefore, after establishing confidence in the proposed framework and classification pipeline, the next objective is to apply this methodology to measure mental workload and stress levels in patients with epilepsy. To this end, an ethics proposal has been submitted to the University Clinic in Bonn.

[1] https://doi.org/10.1145/3421937.3421943
[2] http://library.ijs.si/Stacks/Proceedings/InformationSociety/2022/IS2022_Volume-H%20-%20PHSS.pdf
[3] https://www.scitepress.org/Papers/2023/116283/116283.pdf
[4] https://doi.org/10.3390/s23052387

Graph partitioning in restricted graph classes

Aikaterini Niklanovits (Aikaterini.Niklanovits@hpi.de)
Supervisor: Prof. Dr. Tobias Friedrich

Structural properties of graphs have been proven to be interesting and useful when it comes to dealing with algorithmically hard problems. In particular through forbidding certain substructures some graph classes are defined in which NP-hard problems can be solved in polynomial time.

One way to define such a class is through focusing on the absence of certain induced subgraphs. A graph H is said to be an induced subgraph of a graph G if it can be obtained from G after only deleting a set of vertices and its incident edges. A popular such graph class is chordal graphs. When choosing a graph class to work on, it is important to have an algorithm that can quickly decide whether a given graph belongs in this class. Such polynomial time algorithm has been provided for chordal graphs, and apart from its independent significance, I also find it interesting as it uses some structural notions which we also used to develop efficient algorithms for graph partitioning.

The main focus of my research is developing efficient algorithms for various partitioning problems when restricted to such graph classes. The goal usually is to partition a given graph into a specific number k of connected components each satisfying a certain constrain. When this constrain is the size of each component, a well known objective is to partition the graph into components of roughly equal size. Gyori and Lovasz independently proved that if the given graph is k-connected then not only such a balanced partition is possible, but we can also chose the size and a terminal vertex of each component.

The approach to obtain efficient algorithms realizing this theorem used so far has been restricting the value of k. Specifically, such algorithms have been provided for the cases where k is at most four. Our approach for developing such algorithms for this problem is instead of restricting the value of k, restricting the graph class we are working on. Together with Katrin Casel, Tobias Friedrich, Davis Issaac and Ziena Zeif we developed a polynomial time algorithm for general k and the class of chordal graphs. On the same paper we also extended this result to a broader graph class we defined, HHI_4^2-free graphs, that also allows some induced cycles of length 4 to exist. In order to do that, we used the perfect elimination ordering chordal graphs have, and also the structural properties of HHI_4^2-free graphs to show the existence of certain k-contractible edges. Regarding future research on this direction we believe that focusing on the structure of the minimal separators will be fruitful.

Another constrain a graph partition that interests me refers to the density of it. In particular we aim at maximizing the sum of densities of the components of a partition without however restricting the number of parts this partition has. This problem has already been studied for various graph classes such as trees and dense bipartite graphs. We work on developing a parameterized by treewidth and maximum degree of a graph algorithm.

Privacy Enhancing Protocols

Cavit Özbay (cavit.oezbay@hpi.de)
Supervisor: Prof. Dr. Anja Lehmann

The main task of identity management systems is to provide an authentication mechanism that allows service providers to deliver the service to the correct parties. While authentication notion is mainly built upon the service providers' concerns, users of these applications may have concerns on their privacy. If the underlying authentication mechanism reveal the identity of a user to service providers, then service providers may learn various private information about the user which is irrelevant to the provided service.

Anonymous authentication mechanisms are proposed to solve this problem. Anonymous authentication schemes aim to prevent the systems from leaking information of the users which is irrelevant from the authentication process. These schemes may target different definitions of anonymity according to use cases. Unconditional anonymity is usually used to define the following notion. Users do not reveal any other information then they are required to reveal to authenticate. While this notion solves the privacy concerns of users, it makes impossible to have any accountability mechanism by the definition. Hence, service providers cannot take any action against a misbehaving user. Conditionally anonymous schemes propose solutions between two extremes, anonymity and accountability, considering different use cases adversarial models. We work on designing conditionally anonymous protocols or designing cryptographic tools that help constructing conditionally anonymous protocols.

Algorithmic Aspects of Gibbs Point Processes

Marcus Pappik (marcus.pappik@hpi.de)
Supervisor: Prof. Dr. Tobias Friedrich

Gibbs point processes are stochastic models for gasses and liquids of interacting particles in statistical physics. In the finite-volume setting, a Gibbs point process is defined via a probability density with respect to a Poisson point process of intensity $\lambda \in \mathbb{R}_{\geq 0}$. In general, this density is proportional to an exponential function of the energy of the particle configuration, which is often defined by a sum of interactions between pairs of particles via a potential ϕ. The normalizing constant of this density is usually referred to as the *partition function*, and the resulting distribution over particle configurations is called the *(finite-volume) Gibbs distribution*.

My main research area are computational aspects of Gibbs point processes. In particular, this includes designing algorithms for efficient sampling from the Gibbs distribution (exact or approximately) and approximation of the partition function. In a series of papers [1,2,3] with Tobias Friedrich, Andreas Göbel, Maximilian Katzmann and Martin Krejca, we have studied discretization-based algorithms for these computational tasks. The central idea of these algorithms is to map the computational task to a discrete hard-core model on a suitable graph. This reduction step allows us to use the heavy machinery of algorithms for discrete spin systems that was established by the computer science community within the last decade. While our results in [1,2] were restricted to the grand-canonical hard-sphere model, we recently extended this approach to arbitrary Gibbs point processes with repulsive pair potentials [3]. The key ingredient for this generalization was to carefully construct a graphon (a graph limit object), such that a hard-core model on a random graph generated by that graphon closely approximates the desired point process.

Besides these discretization-based algorithms, I am currently studying efficient exact sampling algorithms for Gibbs point processes together with Konrad Anand, Andreas Göbel and Will Perkins. The idea is that, similar to discrete spin systems, a sufficiently strong notion of correlation decay allows for exact sampling. However, the uncountable size of the considered state space imposes additional algorithmic challenges.

[1] T. Friedrich, A. Göbel, M. S. Krejca, and M. Pappik. A spectral independence view on hard spheres via block dynamics. SIAM Journal on Discrete Mathematics, 36(3):2282–2322, 2022.

[2] T. Friedrich, A. Göbel, M. Katzmann, M. S. Krejca, and M. Pappik. Algorithms for hard-constraint point processes via discretization. In Proc. of COCOON'22, pages 242–254.

[3] T. Friedrich, A. Göbel, M. Katzmann, M. Krejca, and M. Pappik. Using random graphs to sample repulsive gibbs point processes with arbitrary-range potentials. arXiv preprint arXiv:2204.01793, 2022.

Enhancing Knowledge Representation of German Interview Data on Current Global Crises using Fine-Tuned Small BERT Model

Anne Radunski (anne.radunski@hpi.de)
Supervisor: Prof. Dr. Katharina Hölzle

In this work, we introduce a domain-specific Named Entity Recognition (NER) annotation designed to identify the current global crises, such as the Russian war against Ukraine and the climate crisis, as triggers, and their cognitive consequences, such as loneliness or stress, based on German interviews. Using a fine-tuned Bidirectional Encoder Representations from Transformers (BERT) model is an effective approach for achieving state-of-the-art performance in custom NER labeling, as it enables the model to learn domain-specific features and capture the language semantics used in custom-related texts. To address the lack of annotated interview text data and demonstrate the usefulness of such data, we utilized interviews with (n=28) German entrepreneurs at two different time periods. We show that our proposed NER annotation scheme is suitable for identifying the different global crises and their corresponding cognitive consequences and serves as a valuable tool for non-experts due to the straightforward and self-explanatory representation of the knowledge graph. Understanding individual triggers and consequences are crucial for research and practice alike as it provides the base for deriving coping strategies for resilience and well-being.

Machine Learning in Clinical Proteomics and Metaproteomics

Hendrik Raetz (hendrik.raetz@hpi.de)
Supervisor: Prof. Dr. Bernhard Renard

In recent years, the discipline of proteomics mass spectrometry (MS) made it feasible to process proteomics data on a large scale and rivals genomics in analysis depth and scale. The analysis of protein data is desirable because proteins are much closer to the phenotype than genes and transcripts, as these are the molecules that define the function of an organism. However, their behavior cannot easily be inferred from the genome alone because there are many regulatory steps before, between, and after transcription and translation that alter the structure and function of the encoded proteins. The regulatory events that take place after translation are of special interest to my research. These are called post-translational modifications (PTMs). Recent studies showed that these PTMs contribute to diseases such as cancer and Alzheimer's disease. Thus, analyzing these PTMs can make a big difference in the correctness of disease prediction algorithms.

Proteomics data are usually obtained through MS experiments, which result in large amounts of high-dimensional data. Using current methods, this sheer mass of data is often hard to analyze because it is usually either a time- or resource-intensive process. Thus, it is important to develop improved processing methods that are not only faster but possess adequate sensitivity while keeping false discovery rates low. In recent years, methods from the field of machine learning have proven to be successful in the analysis of complex proteomics data, such as the detection and intensity estimation of peptide feature intensity.

I want to apply machine learning methods to efficiently analyze large amounts of MS data and research how they can be used to predict sample conditions without prior preprocessing, e.g., whether they belong to a healthy or disease-affected organism. For this, I will represent samples as image-like data structures so that they can be processed using fine-tuned deep-learning models from the computer vision domain. The encoded peptide and PTM information are the key to explaining the difference in health between samples. In a second step, it is also necessary to identify the specific PTMs to gain a deeper understanding of their interactions and potentially help advance drug development. For this, I also want to develop algorithms to further increase the efficiency of peptide and PTM identification. This project will take a completely novel approach and use spectrum similarity to build networks and aid a faster explanation of spectrum identity using protein database searching or even *de novo* identification approaches.

I plan on using the newly developed approaches to gain more insights into publicly available cancer data and hopefully increase the analysis speed of future cancer research.

Weakly-Supervised Disentanglement for Longitudinal Brain Imaging Studies

Alexander Rakowski (alexander.rakowski@hpi.de)
Supervisor: Prof. Dr. Christoph Lippert

Identifying a disentangled representation in a purely unsupervised setting has been proven impossible (Locatello et al. [1]). However, labeling of the dataset can be labor-intensive, especially when expert knowledge is required. In such cases, weakly-supervised algorithms can be employed, which leverage high-level auxiliary information about the data samples, for example labels indicating which samples have the same (although unknown) values for a subset of traits (Bengio et al.[2], Locatello et al.[3].

In this work we evaluate a weakly-supervised approach for learning disentangled representations of brain Magnetic Resonace Imaging(MRI) data. We leverage the longitudinal nature of brain imaging studies, such as the Alzheimer's Disease Neuroimaging Initiative (ADNI), using repeated measurements of the same subjects as the signal for weak supervision. We compare the proposed approach across a range of settings, measuring its disentanglement as well as performance in real-life downstream tasks, such as dementia score prediction or genome-wide association tests.

In a longitudinal study the measurements of interest (e.g., MRI scans) are repeated over several points in time for each participant. We assume that different scans from the same participant obtained at different time-points will be similar to each other, i.e., they will share certain underlying attributes, such as volumetric measures or disease state, even though we do not have direct access to these attributes. We leverage this assumption to construct pairs of samples from the same participants and use it to train a state-of-the-art weakly-supervised disentangled representation learning model - Adaptive-Group-Variational-Autoencoder (Ada-GVAE, Locatello et al.[3]). During training, the model compares encodings of each sample in a pair and adaptively selects a group of most similar dimensions. Values in these dimensions are then averaged inside each pair of samples to create modified, partially averaged encodings. The modified encodings are then used to reconstruct the original inputs. This forces the model to select only the features shared between two samples for averaging, effectively improving disentanglement of the representations.

[1] Locatello F, Bauer S, Lucic M, Raetsch G, Gelly S, Schölkopf B, Bachem O. Challenging Common Assumptions in the Unsupervised Learning of Disentangled Representations. In International Conference on Machine Learning 2019 May 24 (pp. 4114-4124).

[2] Bengio Y, Courville A, Vincent P. Representation Learning: A Review and New Perspectives. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2013 Mar 7;35(8):1798-828.

[3] F., Poole, B., Rätsch, G., Schölkopf, B., Bachem, O., Tschannen, M.: Weakly-supervised disentanglement without compromises. In: International Conference on Machine Learning. pp. 6348–6359. PMLR (2020)

Disentangling syntactic latent spaces in pre-trained language models to guide natural language understanding models

Alejandro Sierra-Múnera (alejandro.sierra@hpi.de)
Supervisor: Prof. Dr. Felix Naumann

Pre-trained language models (PLMs) have received significant attention in the last years because with them, many approaches are able to define new state-of-the-art models that solve a broad range of natural language processing (NLP) tasks.

The transformer model[1], which is the basis of most PLMs, encodes multiple aspects of text into rich contextualized vectors, representing lexical, syntactic, and semantic information captured during pre-training. But some of these representations are kept in the hidden layers and then aggregated to have a single final summarized representation to be used in downstream tasks. The research community has been able to empirically identify the presence of these structures within the pre-trained models [2] that were not necessary trained to find them, suggesting that with large amounts of text and sufficiently rich models, many linguistic structures were inferred in an unsupervised fashion.

Disentangling these structures from the multiple hidden layers, could open the possibility of improving natural language understanding models and create an opportunity of transferring structural representations of text from general-domain corpora, to low-resource domain-specific models.

In our work we intend to create models in which these structures are discovered from general-domain PLMs and fine-tuned to domain-specific versions of tasks like named entity recognition, relation extraction and open information extraction. As a case study, we plan to evaluate these models in the cultural-heritage domain, in which annotated data is very scarce.

[1] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Łukasz Kaiser, and Illia Polosukhin. Attention is all you need. In Proceedings of the 31st International Conference on Neural Information Processing Systems. 2017

[2] Anna Rogers, Olga Kovaleva, Anna Rumshisky; A primer in BERTology: What we know about how BERT works. Transactions of the Association for Computational Linguistics. 2020

A Physiological Assessment of Cognitive Load in Software Development using Wearable Sensors

Fabian Stolp (fabian.stolp@hpi.de)
Supervisor: Prof. Dr. Bert Arnrich

The quality of software and the performance of software developers are influenced by source code understandability[1][2]. The importance of this factor is underlined by the finding that code comprehension is one of the major tasks software developers are dealing with in terms of time spent[3]. Different ways, for example, interviews, think-aloud protocols, or behavioral measures, exist to evaluate the understandability of code. However, the downsides of corresponding methods, such as the interviewers unwittingly introducing bias, call for more direct and objective ways of assessment[4]. In this context, the concept of cognitive load can be explored. It helps in evaluating the mental resources a person utilizes for a task[5]. How to assess it using physiological sensors has been researched before, and in recent years, this knowledge has been applied to the software engineering area, among others, to evaluate code comprehensibility[6]. At the same time, the prices for body sensors are falling, and their usability is increasing so that they can be applied in more areas and environments. We work on using multimodal setups of low-cost wearable devices that can be applied in software engineering settings to robustly, continuously, and passively record developers' reactions to then analyze their cognitive load. The overall goal is to improve the evaluation of the understandability of code by considering cognitive processes and limitations. The results of this research could have implications for teaching programming, developing software and ensuring its quality in professional software engineering practice, and methods used in empirical software engineering research.[7]

[1] Schankin, A., Berger, A., Holt, D. V., Hofmeister, J. C., Riedel, T., and Beigl, M. (2018, May). Descriptive compound identifier names improve source code comprehension. In Proceedings of the 26th Conference on Program Comprehension (p. 31-40). IEEE.

[2] Siegmund, J., Brechmann, A., Apel, S., Kästner, C., Liebig, J., Leich, T., and Saake, G. (2012, November). Toward measuring program comprehension with functional magnetic resonance imaging. In Proceedings of the ACM SIGSOFT 20th International Symposium on the Foundations of Software Engineering (pp. 1-4).

[3] Schröter, I., Krüger, J., Siegmund, J., and Leich, T. (2017, May). Comprehending studies on program comprehension. In Proceedings of the 25th International Conference on Program Comprehension (pp. 308-311). IEEE.

[4] Peitek, N. (2022). A Neuro-Cognitive Perspective of Program Comprehension (Doctoral dissertation, Chemnitz University of Technology).

[5] Paas, F. G., and Van Merriënboer, J. J. (1994). Instructional control of cognitive load in the training of complex cognitive tasks. Educational psychology review, 6, 351-371.

[6] Weber, B., Fischer, T., and Riedl, R. (2021). Brain and autonomic nervous system activity measurement in software engineering: A systematic literature review. Journal of Systems and Software, 178, p. 110946.

[7] https://hpi.de/research-schools/hpi-dse/mitglieder/research-pages/fabian-stolp.html (accessed Mar. 20, 2023).

Bounded Graph Separators and their Structural Strength

Ziena Zeif (Ziena.zeif@hpi.de)
Supervisor: Prof. Dr. Tobias Friedrich

A network graph is a mathematical model consisting of vertices and pairs of vertices, called edges, that can describe structures in nature and technology. There are many practical applications, and research on graph theory is extensive. A separator in a graph is a group of vertices that fundamentally separate parts of the graph from each other while satisfying certain properties. In many real-world problems such as security, surveillance control, and epidemics, separators can be represented as significant points in a network. Moreover, separators can be used to efficiently solve many graph optimization problems by using them to develop divide-and-conquer strategies or to implement parallel processing algorithms. This generality and their wide applicability have made the study of separators a rich and active area of research. Although separators play an important role in graph theory, they are still not fully understood.

We are concerned with bounded separators, i.e., a set of vertices whose removal leads to small connected components, where the goal is to minimize this separator set. In general, scientific advances in bounded separators are very valuable because of their ability to decipher structures in graphs. It is interesting for us to understand how they relate to other problems and how structures arising from separators provide the ability to deal with problems that are difficult in terms of complexity. For example, through our results on bounded separators, we arrive at new insights into problems of partitioning connected subgraphs with different objectives. Another interesting example is the packing problem, where the goal is to find a maximal set of disjoint connected subgraphs with lower bounded sizes. This problem can be viewed as the dual of the bounded separator problem in a linear programming sense, and can also derive results for related problems through its structural insights. In summary, we have obtained several approximation and kernelization results for those problems, where kernelization can be interpreted as reduction rules for problem instances that allow faster brute-force algorithms to solve the objective accurately.

While the first part is more about evolving structural properties through bounded separators, the second part is about computing an optimal one. We have combined the field of parameterized complexity with evolutionary algorithms and shown that in expectation random meta-solvers can solve the bounded separator problem in a time that is only exponential to the size of an optimal separator and the desired size of the largest connected component after removing this separator. Our results show that evolutionary algorithms with different objectives guide the search and admit fixed parameterized runtimes to solve or approximate (even arbitrarily close) the bounded separator problem.

Author Index

DOI: 10.17185/duepublico/78280
URN: urn:nbn:de:hbz:465-20230508-084913-4