Colloquium FoCS

CS & BME

It is a pleasure to invite you to the colloquium for our Professorship in Human Computer Interaction at Graz University of Technology. The public part will be a short educational presentation at Bachelor's level 4th semester in Computer Science on topic Hough Transformation, a scientific talk (titles below), and a discussion with the audience.

Colloquium **Foundation of Computer Science – 12th to 16th February 24**

Data House – Showroom (DHEG136E) – Sandgasse 36 EG

De Neville Hans: " Partial Higher-Order Logic with Interfaces "
12th February 2024 | 09:30 h

Abstract

This presentation is about a calculus for formal verification of mathematical proofs that I am trying to develop. I have used existing verification systems (Coq, HOL-light, Isabelle, and Mizar), but I think there is room for improvement. PHOLI means 'Partial Higher-Order Logic with Interfaces'.It is based on a 3-valued logic for partial functions that I developed in 2014. I want to evolve this logic into a user-friendly calculus for mathematical proof checking. In order to do this, higher-order must be added, methods for definitions of types, and methods for proof structuring.I have worked on different versions of PHOLI at various times since 2014. I spent half of 2014 implementing the first version, and was disappointed in the result. The calculus had flaws that made it effectively unusable. During 2018 I tried to implement an improved version, and concluded that implementing logic takes too much time in every programming language that I know, including functional languages. During 2020-23 I worked on techniques for implementing logic. Last year, I made much progress. I developed a compiler that automatically generates recursive data structures in C++. I believe that the implementation problem is now completely solved. Now I want to implement PHOLI again, but I do not want to repeat previous mistakes. So I will be writing proofs in text until I am completely satisfied with the calculus. I believe that this approach is working. During the presentation, I will show how standard automata theory can be developed in PHOLI. Although these are simple proofs using constructions that are well-known, looking at them using PHOLI gives fresh perspectives at basic questions: What is the best way to define words over an alphabet? How does one define functions on words? How does one prove existence of words? In order to make a non-deterministic finite automaton deterministic, one needs the subset construction, for which one needs set theory. But what is the right set theory for computer scientists? How much set theory does a computer scientist need?

Aucher Guillaume: " Atomic and Molecular Logics: some Model Theoretic Aspects "
12th February 2024 | 13:30 h

Abstract

After observing that the truth conditions of connectives of non-classical logics are generally defined in terms of formulas of first-order logic, we introduce 'protologics', a class of logics whose connectives are defined by arbitrary first-order formulas. Then, we also introduce atomic and molecular logics, which are two subclasses of protologics. It turns out that the class of protologics is equally expressive as the class of molecular logics and this result formally supports our claim that atomic and molecular logics are somehow 'universal'. Then, we show that notions of bisimulations can be automatically defined for any atomic or molecular logic. For atomic and molecular connectives which are called 'normal', we state a generic van Benthem theorem which generalizes a number of existing results of this kind for various logics. We provide examples of such automatic bisimulation generations, recovering in doing so the usual bisimulation notions associated to logics such as modal logic, the Lambek calculus or modal intuitionistic logic. Finally, after having embedded first-order logic into some atomic logic, we show that the notion of automatic bisimulation obtained for this embedding is equivalent to the classical notion of partial isomorphism.

Aichholzer Oswin: " Combinatorial reconfiguration in plane graphs - classic and new challenges "
13th February 2024 | 09:30 h

Abstract

Reconfiguration is the process of changing a structure into another - either through continuous motion or through discrete changes. We will concentrate on plane graphs and discrete reconfiguration steps of bounded complexity, like exchanging one edge of the graph for another edge. This operation is usually called a flip, and the flip graph is defined as the graph having a vertex for each configuration and an edge for each flip. Three questions are central: studying the connectivity of the flip graph, its diameter, and the complexity of finding the shortest flip sequence between two given configurations. We will survey classic results and open problems -- for example for flips in triangulations which are related to the transformation of binary trees --as well as recent observations and new open challenges.

Kling Peter
13th February 2024 | 13:30 h

Klein Karen: " Provable security guarantees for real-world cryptographic protocols "
14th February 2024 | 09:30 h

Abstract

In this talk I will focus on my research in the area of group messaging protocols, in particular the central building block of group key agreement. While messaging systems with strong security guarantees are widely used in practice, designing a protocol that scales efficiently to large groups and enjoys similar security guarantees is far from trivial. The candidate construction of group key agreement considered by the IETF is called "TreeKEM" and was recently standardized in RFC 9420. While TreeKEM is a very promising solution, neither its concrete efficiency nor its precise security guarantees are fully understood yet. I will give an overview on the results I had with my coauthors in this context.

Kral Daniel: " Structural sparsity and algorithm design "
14th February 2024 | 13:30 h

Abstract

Many algorithmic problems, which are computationally hard in general, are tractable for simply structured inputs, with trees serving as a prototypical example of such inputs. A seminal result of Courcelle from the early 1980s asserts that all decision problems expressible in the monadic second order logic are tractable for graphs with bounded tree-width, i.e., tree-like shaped graphs. In this talk, we survey some of many structural and algorithmic results on graphs and matroids that belong to a large area of research in computer science sparked by Courcelle's metatheorem. In particular, we will discuss inherently sparse graphs and the existence of efficient algorithms for various problems involving such graphs. We will also discuss extensions of the presented graph concepts to matroids, a combinatorial structure capturing linear independence, and demonstrate how matroid based techniques can be used to uncover a hidden Dantzig-Wolfe-like structure of instances of optimization problems.

Muehlebach Michael: " Machine learning for cyber-physical systems “
15th February 2024 | 13:30 h

Abstract

My talk will be divided into two parts. The first part views learning and optimization algorithms as dynamical systems and exploits system theoretic ideas for deriving convergence rates in nonconvex settings. The analogies to dynamical systems will also guide the design of new algorithms for constrained optimization, which have applications in signal processing, traffic predictions, and online learning.

The second part of my talk will illustrate how learning algorithms can be used to control dynamical systems. I will present an algorithm for robot learning that reduces reinforcement learning tasks to supervised learning. The method incorporates prior knowledge about the system dynamics and by optimizing over feedforward actions, the risk of instability during deployment is mitigated. Experiments with a robot arm that is actuated by pneumatic artificial muscles highlight the sample-efficiency and reliability of the approach.

Maus Yannic
16th February 2024 | 09:30 h