FSTTCS 2008 – Abstracts Collection
IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science

Ramesh Hariharan[1] and Madhavan Mukund[2] and V Vinay[3]

Strand, IN
and Chennai Mathematical Institute, IN
and Geodesic, IN

FSTTCS 2008 Preface – IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science

This volume contains the proceedings of the 28th international conference on the Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2008), organized under the auspices of the Indian Association for Research in Computing Science (IARCS). This year's conference attracted 117 submissions. Each submission was reviewed by at least three independent referees. The final selection of the papers making up the programme was done through an electronic discussion on EasyChair, spanning two weeks, without a physical meeting of the Programme Committee (PC). All PC members participated actively in the discussion. We have five invited speakers this year: Hubert Comon-Lundh, Uriel Feige, Erich Grädel, Simon Peyton Jones and Leslie Valiant. We thank them for having readily accepted our invitation to talk at the conference and for providing abstracts (and even full papers) for the proceedings. We thank all the reviewers and PC members, without whose dedicated effort the conference would not be possible. We thank the Organizing Committee for making the arrangements for the conference. This year, the conference is being held at the Indian Institute of Science, Bangalore, as part of its centenary year celebrations. It is a great honour and privilege for the conference to be recognized and associated with the institute on this occasion. Finally, this year we have taken a decisive step in democratizing the conference by moving away from commercial publishers. Instead, we will be hosting the proceedings online, electronically, via the Dagstuhl Research Online Publication Server (DROPS). A complete copy of the proceedings will also be hosted on the FSTTCS website (www.fsttcs.org). The copyrights to the papers will reside not with the publishers but with the respective authors. The copyright is now governed by the Creative Commons attribution NC-ND. We do hope this direction will be sustained in the future.

FSTTCS 2008
IARCS Annual Conference
on Foundations of Software Technology and Theoretical Computer Science
http://drops.dagstuhl.de/opus/volltexte/2008/1772

Keywords: Preface

Joint work of: Hariharan, Ramesh; Mukund, Madhavan; Vinay, V

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2008/1771

3-connected Planar Graph Isomorphism is in Log-space

We consider the isomorphism and canonization problem for 3-connected planar graphs. The problem was known to be L-hard and in ULcoUL [TW07]. In this paper, we give a deterministic log-space algorithm for 3-connected planar graph isomorphism and canonization. This gives an L-completeness result, thereby settling its complexity.

The algorithm uses the notion of universal exploration sequences from [Kou02] and [Rei05]. To our knowledge, this is a completely new approach to graph canonization.

Keywords: Planar graph isomorphism, three connected graphs, logspace, universal exploration sequence

Joint work of: Datta, Samir; Limaye, Nutan; Nimbhorkar, Prajakta

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1749

A Cubic-Vertex Kernel for Flip Consensus Tree

Given a bipartite graph $G = (V_c, V_t, E)$ and a non-negative integer k, the NP-complete Minimum-Flip Consensus Tree problem asks whether G can be transformed, using up to k edge insertions and deletions, into a graph that does not contain an induced P_5 with its first vertex in V_t (a so-called M-graph or Σ-graph). This problem plays an important role in computational phylogenetics, V_c standing for the characters and V_t standing for taxa. Chen et al. [IEEE/ACM TCBB 2006] showed that Minimum-Flip Consensus Tree is NP-complete and presented a parameterized algorithm with running time $O(6^k \cdot |V_t| \cdot |V_c|)$. Recently, Böcker et al. [IWPEC '08] presented a refined search tree algorithm with running time $O(4.83^k(|V_t| + |V_c|) + |V_t| \cdot |V_c|)$. We complement these results by polynomial-time executable data reduction rules yielding a problem kernel with $O(k^3)$ vertices.

Joint work of: Komusiewicz, Christian; Uhlmann, Johannes

Keywords: Fixed-parameter algorithm, problem kernel, NP-hard problem, graph modification problem, computational phylogenetics

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1760

A Hierarchy of Semantics for Non-deterministic Term Rewriting Systems

Formalisms involving some degree of nondeterminism are frequent in computer science. In particular, various programming or specification languages are based on term rewriting systems where confluence is not required. In this paper we examine three concrete possible semantics for non-determinism that can be assigned to those programs. Two of them –call-time choice and run-time choice– are quite well-known, while the third one –plural semantics– is investigated for the first time in the context of term rewriting based programming languages. We investigate some basic intrinsic properties of the semantics and establish some relationships between them: we show that the three semantics form a hierarchy in the sense of set inclusion, and we prove that call-time choice and plural semantics enjoy a remarkable compositionality property that fails for run-time choice; finally, we show how to express plural semantics within run-time choice by means of a program transformation, for which we prove its adequacy.

Keywords: Functional-logic programming, term rewriting systems, constructor-based rewriting logic, non-determinism, call-time choice semantics, run-time choice

Joint work of: Rodríguez-Hortala, Juan

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1764

A new approach to the planted clique problem

We study the problem of finding a large planted clique in the random graph $G_{n,1/2}$. We reduce the problem to that of maximising a three dimensional tensor over the unit ball in n dimensions. This latter problem has not been well studied and so we hope that this reduction will eventually lead to an improved solution to the planted clique problem.

Keywords: Planted Clique, Tensor, Random Graph

Joint work of: Frieze, Alan; Kannan, Ravi

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1752

A new upper bound for 3-SAT

We show that a randomly chosen 3-CNF formula over n variables with clauses-to-variables ratio at least 4.4898 is asymptotically almost surely unsatisfiable. The previous best such bound, due to Dubois in 1999, was 4.506. The first such bound, independently discovered by many groups of researchers since 1983, was 5.19. Several decreasing values between 5.19 and 4.506 were published in the years between. The probabilistic techniques we use for the proof are, we believe, of independent interest.

Keywords: Satisfiability, 3-SAT, random, threshold

Joint work of: Diaz, Josep; Kirousis, Lefteris; Mitsche, Dieter; Perez-Gimenez, Xavier

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1750

About models of security protocols

In this paper, mostly consisting of definitions, we revisit the models of security protocols: we show that the symbolic and the computational models (as well as others) are instances of a same generic model. Our definitions are also parametrized by the security primitives, the notion of attacker and, to some extent, the process calculus.

Keywords: Protocols, security, concurrency, formal methods

Joint work of: Comon-Lundh, Hubert

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1766

Abstraction Refinement for Games with Incomplete Information

Counterexample-guided abstraction refinement (CEGAR) is used in automated software analysis to find suitable finite-state abstractions of infinite-state systems. In this paper, we extend CEGAR to games with incomplete information, as they commonly occur in controller synthesis and modular verification. The challenge is that, under incomplete information, one must carefully account for the knowledge available to the player: the strategy must not depend on information the player cannot see. We propose an abstraction mechanism for games under incomplete information that incorporates the approximation of the players' moves into a knowledge-based subset construction on the abstract state space. This abstraction results in a perfect-information game over a finite graph. The concretizability of abstract strategies can be encoded as the satisfiability of strategy-tree formulas. Based on this encoding, we present an interpolation-based approach for selecting new predicates and provide sufficient conditions for the termination of the resulting refinement loop.

Keywords: Automatic abstraction refinement, synthesis

Joint work of: Dimitrova, Rayna; Finkbeiner, Bernd

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1751

Algorithms for Game Metrics

Simulation and bisimulation metrics for stochastic systems provide a quantitative generalization of the classical simulation and bisimulation relations. These metrics capture the similarity of states with respect to quantitative specifications written in the quantitative μ-calculus and related probabilistic logics. We present algorithms for computing the metrics on Markov decision processes (MDPs), turn-based stochastic games, and concurrent games. For turn-based games and MDPs, we provide a polynomial-time algorithm based on linear programming for the computation of the one-step metric distance between states. The algorithm improves on the previously known exponential-time algorithm based on a reduction to the theory of reals. We then present PSPACE algorithms for both the decision problem and the problem of approximating the metric distance between two states, matching the best known bound for Markov chains. For the bisimulation kernel of the metric, which corresponds to probabilistic bisimulation, our algorithm works in time $\mathcal{O}(n^4)$ for both turn-based games and MDPs; improving the previously best known $\mathcal{O}(n^9 \cdot \log(n))$ time algorithm for MDPs. For a concurrent game G, we show that computing the exact distance between states is at least as hard as computing the value of concurrent reachability games and the square-root-sum problem in computational geometry. We show that checking whether the metric distance is bounded by a rational r, can be accomplished via a reduction to the theory of real closed fields, involving a formula with three quantifier alternations, yielding $\mathcal{O}(|G|^{\mathcal{O}(|G|^5)})$ time complexity, improving the previously known reduction with $\mathcal{O}(|G|^{\mathcal{O}(|G|^7)})$ time complexity. These algorithms can be iterated to approximate the metrics using binary search.

Keywords: Automated Verification, Computational Complexity

Joint work of: Chatterjee, Krishnendu; de Alfaro, Luca; Majumdar, Rupak; Raman, Vishwanath

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1745

All-Norms and All-L_p-Norms Approximation Algorithms

In many optimization problems, a solution can be viewed as ascribing a "cost" to each client, and the goal is to optimize some aggregation of the per-client costs. We often optimize some L_p-norm (or some other symmetric convex function or norm) of the vector of costs—though different applications may suggest different norms to use. Ideally, we could obtain a solution that optimizes several norms simultaneously. In this paper, we examine approximation algorithms that simultaneously perform well on all norms, or on all L_p norms. A natural problem in this framework is the L_p Set Cover problem, which generalizes Set Cover and Min-Sum Set Cover. We show that the greedy algorithm *simultaneously gives a* $(p + \ln p + O(1))$*-approximation for all* p*, and show that this approximation*

ratio is optimal up to constants under reasonable complexity-theoretic assumptions. We additionally show how to use our analysis techniques to give similar results for the more general *submodular set cover*, and prove some results for the so-called *pipelined set cover* problem. We then go on to examine approximation algorithms in the "all-norms" and the "all-L_p-norms" frameworks more broadly, and present algorithms and structural results for other problems such as k-facility-location, TSP, and average flow-time minimization, extending and unifying previously known results.

Keywords: Approximation algorithms, set-cover problems, combinatorial optimization, sampling minkowski norms

Joint work of: Golovin, Daniel; Gupta, Anupam; Kumar, Amit; Tangwongsan, Kanat

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1753

An Optimal Construction of Finite Automata from Regular Expressions

We consider the construction of finite automata from their corresponding regular expressions by a series of digraph-transformations along the expression's structure. Each intermediate graph represents an extended finite automaton accepting the same language. The character of our construction allows a fine-grained analysis of the emerging automaton's size, eventually leading to an optimality result.

Keywords: Finite automata, regular expressions, descriptional complexity

Joint work of: Gulan, Stefan; Fernau, Henning

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1754

Analyzing Asynchronous Programs with Preemption

Multiset pushdown systems have been introduced by Sen and Viswanathan as an adequate model for asynchronous programs where some procedure calls can be stored as tasks to be processed later. The model is a pushdown system supplied with a multiset of pending tasks. Tasks may be added to the multiset at each transition, whereas a task is taken from the multiset only when the stack is empty. In this paper, we consider an extension of these models where tasks may be of different priority level, and can be preempted at any point of their execution by tasks of higher priority. We investigate the control point reachability problem for these models. Our main result is that this problem is decidable by reduction to the reachability problem for a decidable class of Petri nets with inhibitor arcs. We also identify two subclasses of these models for which the control point reachability problem is reducible respectively to the reachability problem and to the coverability problem for Petri nets (without inhibitor arcs).

Keywords: Multiset Pushdown Systems, Multithreaded Asynchronous Programs, Program verification, Verification algorithms

Joint work of: Atig, Mohamed Faouzi; Bouajjani, Ahmed; Touili, Tayssir

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1739

Analyzing the Implicit Computational Complexity of object-oriented programs

A sup-interpretation is a tool which provides upper bounds on the size of the values computed by the function symbols of a program. Sup-interpretations have shown their interest to deal with the complexity of first order functional programs. This paper is an attempt to adapt the framework of sup-interpretations to a fragment of object-oriented programs, including loop and while constructs and methods with side effects. We give a criterion, called brotherly criterion, which uses the notion of sup-interpretation to ensure that each brotherly program computes objects whose size is polynomially bounded by the inputs sizes. Moreover we give some heuristics in order to compute the sup-interpretation of a given method.

Keywords: Implicit computational complexity, object-oriented programs, sup-interpretation, resource upper bounds

Joint work of: Marion, Jean-Yves ; Pechoux, Romain

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1763

Average-Time Games

An average-time game is played on the infinite graph of configurations of a finite timed automaton. The two players, Min and Max, construct an infinite run of the automaton by taking turns to perform a timed transition. Player Min wants to minimize the average time per transition and player Max wants to maximize it. A solution of average-time games is presented using a reduction to average-price game on a finite graph. A direct consequence is an elementary proof of determinacy for average-time games. This complements our results for reachability-time games and partially solves a problem posed by Bouyer et al., to design an algorithm for solving average-price games on priced timed automata. The paper also establishes the exact computational complexity of solving average-time games: the problem is EXPTIME-complete for timed automata with at least two clocks.

Keywords: Games on Timed Automata, Mean-payoff Games, Average-Time Games, Game Theory

Joint work of: Jurdzinski, Marcin; Trivedi, Ashutosh

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1765

Banach-Mazur Games on Graphs

We survey determinacy, definability, and complexity issues of Banach-Mazur games on finite and infinite graphs. Infinite games where two players take turns to move a token through a directed graph, thus tracing out an infinite path, have numerous applications in different branches of mathematics and computer science. In the usual format, the possible moves of the players are given by the edges of the graph; in each move a player takes the token from its current position along an edge to a next position. In Banach-Mazur games the players instead select in each move a *path* of arbitrary finite length rather than just an edge. In both cases the outcome of a play is an infinite path. A winning condition is thus given by a set of infinite paths which is often specified by a logical formula, for instance from S1S, LTL, or first-order logic. Banach-Mazur games have a long tradition in descriptive set theory and topology, and they have recently been shown to have interesting applications also in computer science, for instance for planning in nondeterministic domains, for the study of fairness in concurrent systems, and for the semantics of timed automata. It turns out that Banach-Mazur games behave quite differently than the usual graph games. Often they admit simpler winning strategies and more efficient algorithmic solutions. For instance, Banach-Mazur games with ω-regular winning conditions always have positional winning strategies, and winning positions for finite Banach-Mazur games with Muller winning condition are computable in polynomial time.

Keywords: Games, strategies, determinacy, positional determinacy, definability, complexity

Joint work of: Graedel, Erich

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1768

Boolean algebras of unambiguous context-free languages

Several recent works have studied subfamilies of deterministic context-free languages with good closure properties, for instance the families of input-driven or visibly pushdown languages, or more generally families of languages accepted by pushdown automata whose stack height can be uniquely determined by the input word read so far. These ideas can be described as a notion of synchronization. In this paper we present an extension of synchronization to all context-free languages using graph grammars. This generalization allows one to define boolean algebras of non-deterministic but unambiguous context-free languages containing regular languages.

Keywords: Synchronization, deterministic graph grammars

Joint work of: Caucal, Didier

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1743

Complexity Analysis of Term Rewriting Based on Matrix and Context Dependent Interpretations

For a given (terminating) term rewriting system one can often estimate its *derivational complexity* indirectly by looking at the proof method that established termination. In this spirit we investigate two instances of the interpretation method: *matrix interpretations* and *context dependent interpretations*. We introduce a subclass of matrix interpretations, denoted as *triangular matrix interpretations*, which induce polynomial derivational complexity and establish tight correspondence results between a subclass of context dependent interpretations and restricted triangular matrix interpretations. The thus obtained new results are easy to implement and considerably extend the analytic power of existing results. We provide ample numerical data for assessing the viability of the method.

Keywords: Term Rewriting, Derivational Complexity, Termination, Automation

Joint work of: Moser, Georg; Schnabl, Andreas; Waldmann, Johannes

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1762

Dynamic matrix rank with partial lookahead

We consider the problem of maintaining information about the rank of a matrix M under changes to its entries. For an $n \times n$ matrix M, we show an amortized upper bound of $O(n^{\omega-1})$ arithmetic operations per change for this problem, where $\omega < 2.376$ is the exponent for matrix multiplication, under the assumption that there is a *lookahead* of up to $\Theta(n)$ locations. That is, we know up to the next $\Theta(n)$ locations $(i_1, j_1), (i_2, j_2), \ldots$, whose entries are going to change, in advance; however we do not know the new entries in these locations in advance. We get the new entries in these locations in a dynamic manner.

Keywords: Matrix rank, dynamic algorithm, fast matrix multiplication

Joint work of: Kavitha, Telikepalli

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1759

Explicit Muller Games are PTIME

Regular games provide a very useful model for the synthesis of controllers in reactive systems. The complexity of these games depends on the representation of the winning condition: if it is represented through a win-set, a coloured condition, a Zielonka-DAG or Emerson-Lei formulae, the winner problem is PSPACE-complete; if the winning condition is represented as a Zielonka tree, the winner problem belongs to NP and CO-NP. In this paper, we show that explicit Muller games can be solved in polynomial time, and provide an effective algorithm to compute the winning regions.

Keywords: Games, authomata, model checking

Joint work of: Horn, Florian

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1756

Graph Games on Ordinals

We consider an extension of Church's synthesis problem to ordinals by adding limit transitions to graph games. We consider game arenas where these limit transitions are defined using the sets of cofinal states. In a previous paper, we have shown that such games of ordinal length are determined and that the winner problem is PSPACE-complete, for a subclass of arenas where the length of plays is always smaller than ω^ω. However, the proof uses a rather involved reduction to classical Muller games, and the resulting strategies need infinite memory. We adapt the LAR reduction to prove the determinacy in the general case, and to generate strategies with finite memory, using a reduction to games where the limit transitions are defined by priorities. We provide an algorithm for computing the winning regions of both players in these games, with a complexity similar to parity games. Its analysis yields three results: determinacy without hypothesis on the length of the plays, existence of memoryless strategies, and membership of the winner problem in $\text{NP} \cap co - \text{NP}$.

Keywords: Games, ordinals, zeno

Joint work of: Cristau, Julien; Horn, Florian

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1748

Harnessing the Multicores: Nested Data Parallelism in Haskell

If you want to program a parallel computer, a purely functional language like Haskell is a promising starting point. Since the language is pure, it is by-default safe for parallel evaluation, whereas imperative languages are by-default unsafe. But that doesn't make it easy! Indeed it has proved quite difficult to get robust, scalable performance increases through parallel functional programming, especially as the number of processors increases. A particularly promising and well-studied approach to employing large numbers of processors is data parallelism. Blelloch's pioneering work on NESL showed that it was possible to combine a rather flexible programming model (nested data parallelism) with a fast, scalable execution model (flat data parallelism). In this paper we describe Data Parallel Haskell, which embodies nested data parallelism in a modern, general-purpose language, implemented in a state-of-the-art compiler, GHC. We focus particularly on the vectorisation transformation, which transforms nested to flat data parallelism.

Keywords: Nested data parallelism, Vectorisation, Haskell, Program transformation

Joint work of: Peyton Jones, Simon; Leshchinskiy, Roman; Keller, Gabriele; Chakravarty, Manuel M T

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1769

Implicit Branching and Parameterized Partial Cover Problems (Extended Abstract)

Covering problems are fundamental classical problems in optimization, computer science and complexity theory. Typically an input to these problems is a family of sets over a finite universe and the goal is to cover the elements of the universe with as few sets of the family as possible. The variations of covering problems include well known problems like Set Cover, Vertex Cover, Dominating Set and Facility Location to name a few. Recently there has been a lot of study on partial covering problems, a natural generalization of covering problems. Here, the goal is not to cover all the elements but to cover the specified number of elements with the minimum number of sets.

Keywords: Implicit Branching, Parameterized Algorithms, Partial Dominating Set, Partial Vertex Cover, Local Treewidth

Joint work of: Amini, Omid; Fomin, Fedor; Saurabh, Saket

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1736

Increasing the power of the verifier in Quantum Zero Knowledge

In quantum zero knowledge, the assumption was made that the verifier is only using unitary operations. Under this assumption, many nice properties have been shown about quantum zero knowledge, including the fact that Honest-Verifier Quantum Statistical Zero Knowledge ($HVQSZK$) is equal to Cheating-Verifier Quantum Statistical Zero Knowledge ($QSZK$) (see [Wat02,Wat06]). In this paper, we study what happens when we allow an honest verifier to flip some coins in addition to using unitary operations. Flipping a coin is a non-unitary operation but doesn't seem at first to enhance the cheating possibilities of the verifier since a classical honest verifier can flip coins. In this setting, we show an unexpected result: any classical Interactive Proof has an Honest-Verifier Quantum Statistical Zero Knowledge proof with coins. Note that in the classical case, honest verifier SZK is no more powerful than SZK and hence it is not believed to contain even NP. On the other hand, in the case of cheating verifiers, we show that Quantum Statistical Zero Knowledge where the verifier applies any non-unitary operation is equal to Quantum Zero-Knowledge where the verifier

uses only unitaries. One can think of our results in two complementary ways. If we would like to use the honest verifier model as a means to study the general model by taking advantage of their equivalence, then it is imperative to use the unitary definition without coins, since with the general one this equivalence is most probably not true. On the other hand, if we would like to use quantum zero knowledge protocols in a cryptographic scenario where the honest-but-curious model is sufficient, then adding the unitary constraint severely decreases the power of quantum zero knowledge protocols.

Keywords: Quantum cryptography, zero-knowledge protocols, honest-verifier, quantum semi-honest model, hiddenquantum cryptography, zero-knowledge protocols, honest-verifier, quantum semi-honest model, hidden-bits

Joint work of: Chailloux, Andre; Kerenidis, Iordanis

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1744

Knowledge Infusion: In Pursuit of Robustness in Artificial Intelligence

Endowing computers with the ability to apply commonsense knowledge with human-level performance is a primary challenge for computer science, comparable in importance to past great challenges in other fields of science such as the sequencing of the human genome. The right approach to this problem is still under debate. Here we shall discuss and attempt to justify one approach, that of *knowledge infusion*. This approach is based on the view that the fundamental objective that needs to be achieved is *robustness* in the following sense: a framework is needed in which a computer system can represent pieces of knowledge about the world, each piece having some uncertainty, and the interactions among the pieces having even more uncertainty, such that the system can nevertheless reason from these pieces so that the uncertainties in its conclusions are at least controlled. In knowledge infusion rules are learned from the world in a principled way so that subsequent reasoning using these rules will also be principled, and subject only to errors that can be bounded in terms of the inverse of the effort invested in the learning process.

Keywords: Artificial intelligence, knowledge acquisition, knowledge representation,learning, reasoning, robustness

Joint work of: Valiant, Leslie G.

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1770

Leaf languages and string compression

Tight connections between leafs languages and strings compressed via straight-line programs (SLPs) are established. It is shown that the compressed membership problem for a language L is complete for the leaf language class defined by

L via logspace machines. A more difficult variant of the compressed membership problem for L is shown to be complete for the leaf language class defined by L via polynomial time machines. As a corollary, a fixed linear visibly pushdown language with a PSPACE-complete compressed membership problem is obtained. For XML languages, the compressed membership problem is shown to be coNP-complete.

Keywords: Leaf languages, string compression, grammar-based compression, complexity theory

Joint work of: Lohrey, Markus

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1761

On Estimation Algorithms vs Approximation Algorithms

In a combinatorial optimization problem, when given an input instance, one seeks a feasible solution that optimizes the value of the objective function. Many combinatorial optimization problems are NP-hard. A way of coping with NP-hardness is by considering approximation algorithms. These algorithms run in polynomial time, and their performance is measured by their approximation ratio: the worst case ratio between the value of the solution produced and the value of the (unknown) optimal solution. In some cases the design of approximation algorithms includes a nonconstructive component. As a result, the algorithms become estimation algorithms rather than approximation algorithms: they allow one to estimate the value of the optimal solution, without actually producing a solution whose value is close to optimal. We shall present a few such examples, and discuss some open questions.

Keywords: Estimation Algorithms, Approximation Algorithms, Combinatorial Optimization

Joint work of: Feige, Uriel

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1767

On the Power of Imperfect Information

We present a polynomial-time reduction from parity games with imperfect information to safety games with imperfect information. Similar reductions for games with perfect information typically increase the game size exponentially. Our construction avoids such a blow-up by using imperfect information to realise succinct counters which cover a range exponentially larger than their size. In particular, the reduction shows that the problem of solving imperfect-information games with safety conditions is EXPTIME-complete.

Keywords: Infinite games, imperfect information

Joint work of: Berwanger, Dietmar; Doyen, Laurent

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1742

Pruning 2-Connected Graphs

Given an edge-weighted undirected graph G with a specified set of terminals, let the *density* of any subgraph be the ratio of its weight/cost to the number of terminals it contains. If G is 2-connected, does it contain smaller 2-connected subgraphs of density comparable to that of G? We answer this question in the affirmative by giving an algorithm to *prune* G and find such subgraphs of any desired size, at the cost of only a logarithmic increase in density (plus a small additive factor). We apply the pruning techniques to give algorithms for two NP-Hard problems on finding large 2-vertex-connected subgraphs of low cost; no previous approximation algorithm was known for either problem. In the k-2VC problem, we are given an undirected graph G with edge costs and an integer k; the goal is to find a minimum-cost 2-vertex-connected subgraph of G containing at least k vertices. In the Budget-2VC problem, we are given the graph G with edge costs, and a budget B; the goal is to find a 2-vertex-connected subgraph H of G with total edge cost at most B that maximizes the number of vertices in H. We describe an $O(\log n \log k)$ approximation for the k-2VC problem, and a bicriteria approximation for the Budget-2VC problem that gives an $O(\frac{1}{\epsilon}\log^2 n)$ approximation, while violating the budget by a factor of at most $3+\epsilon$.

Keywords: 2-Connected Graphs, k-MST, Density, Approximation

Joint work of: Chekuri, Chandra; Korula, Nitish

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1746

Runtime Monitoring of Metric First-order Temporal Properties

We introduce a novel approach to the runtime monitoring of complex system properties. In particular, we present an online algorithm for a safety fragment of metric first-order temporal logic that is considerably more expressive than the logics supported by prior monitoring methods. Our approach, based on automatic structures, allows the unrestricted use of negation, universal and existential quantification over infinite domains, and the arbitrary nesting of both past and bounded future operators. Moreover, we show how to optimize our approach for the common case where structures consist of only finite relations, over possibly infinite domains. Under an additional restriction, we prove that the space consumed by our monitor is polynomially bounded by the cardinality of the data appearing in the processed prefix of the temporal structure being monitored.

Keywords: Runtime Monitoring, Metric First-order Temporal Logic, Automatic Structures, Temporal Databases

Joint work of: Basin, David; Klaedtke, Felix; Müller, Samuel; Pfitzmann, Birgit

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1740

Single-Sink Network Design with Vertex Connectivity Requirements

We study single-sink network design problems in undirected graphs with vertex connectivity requirements. The input to these problems is an edge-weighted undirected graph $G = (V, E)$, a sink/root vertex r, a set of terminals $T \subseteq V$, and integer k. The goal is to connect each terminal $t \in T$ to r via k *vertex-disjoint* paths. In the *connectivity* problem, the objective is to find a min-cost subgraph of G that contains the desired paths. There is a 2-approximation for this problem when $k \leq 2$ [FleischerJW] but for $k \geq 3$, the first non-trivial approximation was obtained in the recent work of Chakraborty, Chuzhoy and Khanna [ChakCK08]; they describe and analyze an algorithm with an approximation ratio of $O(k^{O(k^2)} \log^4 n)$ where $n = |V|$. In this paper, inspired by the results and ideas in [ChakCK08], we show an $O(k^{O(k)} \log |T|)$-approximation bound for a simple greedy algorithm. Our analysis is based on the dual of a natural linear program and is of independent technical interest. We use the insights from this analysis to obtain an $O(k^{O(k)} \log |T|)$-approximation for the more general single-sink *rent-or-buy* network design problem with vertex connectivity requirements. We further extend the ideas to obtain a poly-logarithmic approximation for the single-sink *buy-at-bulk* problem when $k = 2$ and the number of cable-types is a fixed constant; we believe that this should extend to any fixed k. We also show that for the non-uniform buy-at-bulk problem, for each fixed k, a small variant of a simple algorithm suggested by Charikar and Kargiazova [CharikarK05] for the case of $k = 1$ gives an $2^{O(\sqrt{\log |T|})}$ approximation for larger k. These results show that for each of these problems, simple and natural algorithms that have been developed for $k = 1$ have good performance for small $k > 1$.

Keywords: Network Design, Vertex Connectivity, Buy-at-Bulk, Rent-or-Buy, Approximation

Joint work of: Chekuri, Chandra ; Korula, Nitish

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1747

Some Sieving Algorithms for Lattice Problems

We study the algorithmic complexity of lattice problems based on the sieving technique due to Ajtai, Kumar, and Sivakumar [AKS01]. Given a k-dimensional

subspace $M \subseteq IR^n$ and a full rank integer lattice $L \subseteq Q^n$, the *subspace avoiding problem* SAP, defined by Blömer and Naewe [BN07], is to find a shortest vector in $L \setminus M$. We first give a $2^{O(n+k \log k)}$ time algorithm to solve *the subspace avoiding problem*. Applying this algorithm we obtain the following results.

1. We give a $2^{O(n)}$ time algorithm to compute i^{th} successive minima of a full rank lattice $L \subset Q^n$ if i is $O(\frac{n}{\log n})$.
2. We give a $2^{O(n)}$ time algorithm to solve a restricted *closest vector problem CVP* where the inputs fulfil a promise about the distance of the input vector from the lattice.
3. We also show that unrestricted CVP has a $2^{O(n)}$ exact algorithm if there is a $2^{O(n)}$ time exact algorithm for solving CVP with additional input $v_i \in$, $1 \leq i \leq n$, where $\|v_i\|_p$ is the i^{th} successive minima of for each i.

We also give a new approximation algorithm for SAP and the *Convex Body Avoiding problem* which is a generalization of SAP. Several of our algorithms work for *gauge* functions as metric, where the gauge function has a natural restriction and is accessed by an oracle.

Keywords: Lattice problems, sieving algorithm, closest vector problem

Joint work of: Arvind, V.; Joglekar, Pushkar S.

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1738

Sound Lemma Generation for Proving Inductive Validity of Equations

In many automated methods for proving inductive theorems, finding a suitable generalization of a conjecture is a key for the success of proof attempts. On the other hand, an obtained generalized conjecture may not be a theorem, and in this case hopeless proof attempts for the incorrect conjecture are made, which is against the success and efficiency of theorem proving. Urso and Kounalis (2004) proposed a generalization method for proving inductive validity of equations, called sound generalization, that avoids such an over-generalization. Their method guarantees that if the original conjecture is an inductive theorem then so is the obtained generalization. In this paper, we revise and extend their method. We restore a condition on one of the characteristic argument positions imposed in their previous paper and show that otherwise there exists a counterexample to their main theorem. We also relax a condition imposed in their framework and add some flexibilities to some of other characteristic argument positions so as to enlarge the scope of the technique.

Keywords: Sound generalization, inductive theorem, automated theorem proving, term rewriting

Joint work of: Aoto, Takahito

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1737

STCON in Directed Unique-Path Graphs

We study the problem of space-efficient polynomial-time algorithms for *directed st-connectivity* (STCON). Given a directed graph G, and a pair of vertices s, t, the STCON problem is to decide if there exists a path from s to t in G. For general graphs, the best polynomial-time algorithm for STCON uses space that is only slightly sublinear. However, for special classes of directed graphs, polynomial-time poly-logarithmic-space algorithms are known for STCON. In this paper, we continue this thread of research and study a class of graphs called *unique-path graphs with respect to source s*, where there is at most one simple path from s to any vertex in the graph. For these graphs, we give a polynomial-time algorithm that uses $\tilde{O}(n^{\varepsilon})$ space for any constant $\varepsilon \in (0, 1]$. We also give a polynomial-time, $\tilde{O}(n^{\varepsilon})$-space algorithm to *recognize* unique-path graphs. Unique-path graphs are related to configuration graphs of unambiguous log-space computations, but they can have some directed cycles. Our results may be viewed along the continuum of sublinear-space polynomial-time algorithms for STCON in different classes of directed graphs - from slightly sublinear-space algorithms for general graphs to $O(\log n)$ space algorithms for trees.

Keywords: Algorithm, complexity, st-connectivity

Joint work of: Kannan, Sampath; Khanna, Sanjeev; Roy, Sudeepa

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1758

The Complexity of Tree Transducer Output Languages

Two complexity results are shown for the output languages generated by compositions of macro tree transducers. They are in NSPACE(n) and hence are context-sensitive, and the class is NP-complete.

Keywords: Complexity, Tree Transducer, OI-hierarchy, Context-Sensitive

Joint work of: Inaba, Kazuhiro; Maneth, Sebastian

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1757

The unfolding of general Petri nets

The unfolding of (1-)safe Petri nets to occurrence nets is well understood. There is a universal characterization of the unfolding of a safe net which is part and parcel of a coreflection from the category of occurrence nets to the category of safe nets. The unfolding of general Petri nets, nets with multiplicities on arcs whose markings are multisets of places, does not possess a directly analogous universal characterization, essentially because there is an implicit symmetry in the multiplicities of general nets, and that symmetry is not expressed in their traditional occurrence net unfoldings. In the present paper, we show how to recover

a universal characterization by representing the symmetry in the behaviour of the occurrence net unfoldings of general Petri nets. We show that this is part of a coreflection between enriched categories of general Petri nets with symmetry and occurrence nets with symmetry.

Keywords: Petri nets, symmetry, unfolding

Joint work of: Hayman, Jonathan; Winskel, Glynn

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2008/1755