ISSN 2186-7437

NII Shonan Meeting Report

No. 2017-13

Logic and Computational Complexity
NII Shonan Meeting Report

Yijia Chen
Rodney Downey
Jörg Flum

September 18–22, 2017

National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-Ku, Tokyo, Japan

Logic and Computational Complexity
NII Shonan Meeting Report

Organizers:
Yijia Chen (Fudan University, China)
Rodney Downey (Victoria University of Wellington, New Zealand)
Jörg Flum (Albert-Ludwigs Universität Freiburg, Germany)

September 18–22, 2017

The discipline of theoretical computer science has its early roots in the pioneering work of Church, Turing, and Gödel. Two important branches of theoretical computer science were already visible right from the beginning: One oriented to computational complexity and algorithms, the other to logic, semantics, and formal methods. The two branches have quite different goals and problems, each developed methods of its own, and they partly use different mathematical tools. Even though their division has been growing steadily during the last 30 years, the two branches come together from time to time as witnessed by the work in areas as descriptive theory, proof complexity, and more recently, parameterized complexity. The main focus of the planned meeting are those areas.

Probably the theorem of Büchi and Trahtenbrot characterizing the languages accepted by finite automata in terms of monadic second-order logic (MSO) can be viewed as the first main result in the area of **descriptive complexity**. However, the systematic development of descriptive complexity (or finite model theory at large) started with Fagin's seminal work. It shows that the complexity class NP consists precisely of the problems definable in existential second-order logic (ESO). It is well known that all major complexity classes have such a characterization in terms of an appropriate logic. For example, the class P corresponds to least fixed-point logic (LFP) on ordered structures. Therefore, the separation of P and NP, the central problem in computational complexity, amounts to show that LFP and ESO have different expressive power on ordered structures. Although it hasn't panned out as hoped, finite model theorists have the long-term goal to settle some major complexity problems using methods from logic. In the converse direction, computational complexity has proved to be very useful to resolve some difficult questions in finite model theory. One example is Rossman's result that on ordered structures the expressive power of k-variable first-order logic strictly increases with k. His proof uses Håstad's Switching Lemma, a major tool from circuit complexity.

Of course, also in **proof complexity** the central open problem is the P versus NP question of whether there exists a polynomial time method of recognizing tautologies. A related research area is the question of proof lengths. In this area, the central questions concern the minimum lengths of proofs needed

for tautologies in proof systems. A proof system P is polynomially optimal if for any other proof system P' there is a polynomial algorithm transforming every proof in P' of a tautology into a proof in P of the same tautology. In particular, the length of the proof in P is polynomially bounded in the length of the proof in P'. Recently, it was shown that the existence of a polynomially optimal proof system for tautologies is equivalent to the fact that a certain logic, introduced by Blass and Gurevich, is a logic for P.

Parameterized complexity theory provides a framework for a refined analysis of hard algorithmic problems A specific structural property of a given problem is identified (called the parameter). It is expected to be small in typical instances of the problem. Then, the (parameterized) complexity of the problem is measured in terms of its parameter and input length.

Logic shows up in this area in many different ways. For example, logic yields the framework for algorithmic meta-theorems. These theorems give sweeping explanations for the existence of many efficient algorithms on special graph classes. For instance, Courcelle's Theorem yields linear time algorithms for all problems definable by MSO on graphs of bounded tree-width. The area of algorithmic meta-theorems uses deep tools from both model theory and structural graph theory.

Furthermore, computational problems from logic, e.g., weighted satisfiability problems for propositional logic and model-checking problems for first-order logic, are used to define (or, to characterize) classes of parameterized intractability.

In this Shonan meeting, we have brought together researchers from both communities, complexity and logic, working in the areas mentioned above. So they were able to share their recent work and discuss research problems. The meeting consisted a number of tutorials, survey talks, and research talks.

Overview of Talks

Testing logically defined properties on structures of bounded degree

Isolde Adler, University of Leeds, UK

Property testing (for a property P) asks for a given input, whether it has property P, or is "far" from having that property. A "testing algorithm" is a probabilistic algorithm that answers this question with high probability correctly, by only looking at small parts of the input. Testing algorithms are thought of as "extremely efficient", making them relevant in the context of big data.

We extend the bounded degree model of property testing from graphs to relational structures, and we show that in this model, every property definable in monadic second-order logic is testable with a constant number of queries in polylogarithmic time on structures of bounded tree-width.

This is joint work with Frederik Harwath.

A proof of Courcelles Conjecture on recognisable graph classes

Mikołaj Bojańczyk, University of Warsaw, Poland

Courcelles conjecture says that for classes of bounded treewidth, definability in MSO is the same as recognisability. More precisely, consider the following notions: (D) a class of graphs is called MSO definable if it can be defined in monadic second-order logic (with counting quantifiers). (R) a class of graphs is called recognisable if for each k there is a tree automaton which recognises width k tree decompositions of graphs in the class. Many natural graph classes are easily seen to satisfy (D), e.g. graphs with Hamiltonian (or Euler) paths, or 3-colourable graphs. Courcelles Theorem says that (D) implies (R). Courcelles Conjecture says that (R) implies (D) for classes of bounded tree width. In the talk, I will discuss a proof of this conjecture.

Joint work with Michał Pilipczuk.

Parameterised Computational Topology

Benjamin Burton, The University of Queensland, Australia

In recent years there has been great progress on the parameterised complexity of topological problems, involving computations on knots, surfaces and 3-manifolds. We begin by surveying the current state of progress, where there are now many positive complexity results backed up by practical mathematical software. We then discuss normal surface theory, a core algorithmic machine behind many topological problems, which offers a potential route for proving that unknot recognition is fixed-parameter tractable in the treewidth of the underlying graph.

Some NP functions, proof complexity and completeness

Samuel Buss, UC San Diego, USA

We discuss Total NP Search Problems from the three viewpoints of the complexity theory of TFNP classes, of propositional proof complexity, and of bounded arithmetic. We consider first the classic example of the pigeonhole principle. We then discuss polynomial size proofs for Lovasz's theorem on the chromatic number of Kneser graphs. We conclude with discussing the Frege Consistency problem which is many-one complete for the provable NP Search Problems of the second order theory U-1-2 of bounded arithmetic which corresponds to polynomial space computation.

One hierarchy spawns another: graph deconstructions and the complexity classification of conjunctive queries

Hubie Chen, Univ. Pais Vasco and Ikerbasque, Spain

We study the classical problem of conjunctive query evaluation. This problem admits multiple formulations and has been studied in numerous contexts; for example, it is a formulation of the constraint satisfaction problem, as well as the problem of deciding if there is a homomorphism from one relational structure to another (which transparently generalizes the graph homomorphism problem).

We here restrict the problem according to the set of permissible queries; the particular formulation we work with is the relational homomorphism problem over a class of structures $\mathbf{A}$, wherein each instance must be a pair of structures such that the first structure is an element of $\mathbf{A}$. We present a comprehensive complexity classification of these problems, which strongly links graph-theoretic properties of $\mathbf{A}$ to the complexity of the corresponding homomorphism problem. In particular, we define a binary relation on graph classes and completely describe the resulting hierarchy given by this relation. This binary relation is defined in terms of a notion which we call graph deconstruction and which is a variant of the well-known notion of tree decomposition. We then use this graph hierarchy to infer a complexity hierarchy of homomorphism problems which is comprehensive up to a computationally very weak notion of reduction, namely, a parameterized form of quantifier-free reductions. We obtain a significantly refined complexity classification of left-hand side restricted homomorphism problems, as well as a unifying, modular, and conceptually clean treatment of existing complexity classifications, such as the classifications by Grohe-Schwentick-Segoufin (STOC 2001) and Grohe (FOCS 2003, JACM 2007).

After presenting this new advance, we will compare this line of research with another that aims to classify the complexity of the homomorphism problem where the second (target) structure is fixed, and that is currently being studied using universal-algebraic methods. We will also present and discuss two intriguing variants, injective homomorphism (also called embedding) and surjective homomorphism.

This talk is mostly based on joint work with Moritz Müller that appeared in CSL-LICS'14.

Parameterized AC^0 – some upper and lower bounds

Yijia Chen, Fudan University, China

In parameterized complexity, FPT plays the same role as P in classical complexity. Similarly, parameterized AC^0 is the parameterized analog of the circuit complexity class AC^0. In this talk, I will discuss some upper and lower bounds for parameterized AC^0. For the lower bounds, we exploit a result of Rossman [STOC'08] and a strong AC^0 version of the planted clique conjecture. For the upper bounds, we implement the color-coding method of Alon, Yuster, and Zwick [JACM 1995] in first-order logic using bounded number of quantifiers. The latter turns out to be essential for a descriptive characterization of parameterized AC^0.

This is joint work with Jörg Flum and Xuangui Huang.

Tree-width, clique-width and fly-automata

Bruno Courcelle, LaBRI/ Bordeaux University, France

The verification of MSO (monadic second-order) graph properties and the computation of related evaluations (like the number of 3-colorings) is FPT w.r.t. to clique-width and tree-width. To make these algorithms usable, one can use automata on terms representing the input graphs, but these automata have huge numbers of states and cannot be implemented by tables of transitions. We use instead "fly-automata" that compute their transitions instead of looking into tables. Such automata can have infinite sets of states: a state may comprise integers, for instance for the computation of the number of satisfying answers to an MSO query, or for checking if a graph is regular (which is not an MSO property). These automata are easier to construct for the algebraic terms denoting graphs of bounded clique-width than for tree-decompositions of graphs of bounded tree-width. For bounded tree-width, one can check even MSO expressions using edge-set quantifications (MSO_2 formulas).

What can we do for graphs of bounded tree-width? The corresponding clique-width may be exponential in the tree-width, however in many cases of interest (planar graphs, bounded degree) it is only linear which makes fly-automata on clique-width terms usable. Furthermore, the clique-width of the incidence graph of a graph of tree-width k is at most $k+3$. Via incidence graphs, one can check MSO_2 properties.

The symmetry barrier in combinatorial optimization

Anuj Dawar, University of Cambridge, UK

The expressive power of fixed-point logic with counting (FPC) forms a powerful fragment of the complexity class P. It can be characterised in a natural way through symmetric circuits. We show that methods for solving combinatorial optimization problems based on linear and semi-definite programming can be expressed in FPC and this provides a means to prove strong lower bounds on these methods.

Logics with invariantly used relations

Kord Eickmeyer, Technische Universität Darmstadt, Germany

Natural extensions of well-known logics such as FO and MSO arise if formulae are allowed to speak of a linear order on the elements of a structure, as long as truth values do not depend on the particular choice of a linear order. The resulting logics are referred to as order-invariant FO/MSO, and are strictly more expressive than plain FO and MSO on finite structures. Analogously one may define other variants such as successor-invariant or addition-invariant logics.

Many powerful tools from finite model theory fail to be applicable to these logics: Since the subformulae of an order-invariant formula are not themselves order-invariant (except for trivial cases), proofs by syntactic induction are not available. Furthermore, there are no Ehrenfeucht-Fraïssé games for these logics.

We survey known results about the expressive power and model checking complexity of logics with invariant relations, in particular successor-invariant FO and order-invariant MSO.

Completeness and improved algorithms for first-order properties on sparse structures

Jiawei Gao, UC San Diego, USA

Properties definable in first-order logic are algorithmically interesting for both theoretical and pragmatic reasons. Many of the most studied algorithmic problems, such as Hitting Set and Orthogonal Vectors, are first-order, and the first-order properties naturally arise as relational database queries. A relatively straightforward algorithm for evaluating a property with k+1 quantifiers takes time $O(m^k)$ and, assuming the Strong Exponential Time Hypothesis (SETH), some such properties require $O(m^{k-\epsilon})$ time for any $\epsilon > 0$. (Here, m represents the size of the input structure, i.e. the number of tuples in all relations.) We give algorithms for every first-order property that improves this upper bound to $m^k/2^{\Theta(\sqrt{\log n})}$, i.e., an improvement by a factor more than any poly-log, but less than the polynomial required to refute SETH. Moreover, we show that further improvement is equivalent to improving algorithms for sparse instances of the well-studied Orthogonal Vectors problem. Surprisingly, both results are obtained by showing completeness of the Sparse Orthogonal Vectors problem for the class of first-order properties under fine-grained reductions. To obtain improved algorithms, we apply the fast Orthogonal Vectors algorithm of [AWY15, CW16]. While fine-grained reductions (reductions that closely preserve the conjectured complexities of problems) have been used to relate the hardness of disparate specific problems both within P and beyond, this is the first such completeness result for a standard complexity class.

Joint work with Russell Impagliazzo, Antonina Kolokolova and Ryan Williams.

Definability of path- and branch-decompositions: another view

Petr Hliněný, Masaryk University, Czech Republic

We will present an alternative way of defining a path-decomposition and a branch-decomposition in MSO logic, a result which has been first shown in a LICS2016 paper by Bojańczyk and Pilipczuk. The aim of our modified approach is to simplify some technical parts of the mentioned original paper, and to provide a smooth extension to matroids over finite fields. This talk is based on joint research with Eunjung Kim and Jan Obdrzálek.

The uncanny usefulness of constructive proofs of pseudorandomness

Valentine Kabanets, Simon Fraser University, Canada

Explicit constructions of pseudorandom objects (e.g., pseudorandom generators, expander graphs, or boolean functions of large circuit complexity) often come with very constructive proofs of existence. For example,

1. the Nisan-Wigderson (NW) generator based on an assumed "hard" function f (of large circuit complexity) has the constructive analysis: There is an efficient uniform reduction (with oracle access to f) taking an algorithm "breaking" the generator into a small circuit for f;

2. the Natural Proofs framework of Razborov and Rudich argues that most circuit lower bound proofs come with an efficiently testable property that distinguishes "easy" functions (with small circuit complexity) from random functions;

3. the analysis of the iterative Zig-Zag construction of expanders due to Reingold, Vadhan, and Wigderson contains an efficient algorithm taking a non-expanding set of vertices in the graph at any given stage i into a non-expanding set of vertices in the graph at the previous stage $(i-1)$.

I'll talk about several recent applications of such constructive proofs. In particular, properties (1) + (2) yield an efficient agnostic learning query algorithm for every sufficiently strong circuit class that has a natural proof of circuit lower bounds. As an application, the class $\mathrm{AC}^0[p]$, for any prime p, is agnostically learnable in quasi-polynomial time. (Previously, only the case of AC^0 was known by the results of Linial, Mansour, and Nisan.) [joint with Carmosino, Impagliazzo, and Kolokolova, CCC'16 & RANDOM'17] The analysis of the zig-zag construction in (3) can be made even more constructive: it is formalizable in the theory VNC^1 of NC^1-reasoning. This implies (using the previous work by Jerabek) that monotone LK (MLK) proof system polynomially simulates LK proof system on monotone sequents, strengthening the quasi-polynomial simulation result by Atserias, Galesi, and Pudlak. [joint with S. Buss, Kolokolova, and Koucky.]

Proof complexity of SMT

Antonina Kolokolova, Memorial University of Newfoundland, Canada

Over the last decade, SAT solvers have been gaining popularity as a generic method for solving decision problems. Proof complexity, in particular results about resolution proof system and its variants, has been instrumental in analysing their performance and limitations.

Whereas for SAT solvers inputs are encoded by propositional formulas, it is often more natural to encode problems using a richer language, for example, encoding numerical problems using Boolean combinations of equations and inequalities. This gave rise to the Satisfiability Modulo Theories (SMT) paradigm, where a combination of a SAT solver and a solver for the underlying theory (such as linear arithmetic) is used to tackle such problems more efficiently. Though SMT solvers are widely used in practice, there has not been much theoretical, proof complexity, work on understanding their power.

Here, we develop a proof complexity framework for studying SMT solvers, building upon results relating resolution and SAT solvers. We introduce a class of proof systems Res(T), with resolution over atoms of a theory T augmented with a theory rule, and show that Res(T) is equivalent to SMT systems based on conflict-driven SAT solvers. We also look at several common underlying theories, showing, in particular, that a SAT solver with a solver for the theory of equality with uninterpreted functions can effectively p-simulate Frege proofs.

Joint work with Vijay Ganesh and Robert Robere.

The distinctive power and complexity of counting generalized colorings: new results and challenges

Johann Makowsky, Technion – Israel Institute of Technology, Israel

Let P be a graph property. We look at graph colorings with k colors where each color class induces a graph satisfying P. By a result of Makowsky and Zilber (2005) the number of such colorings $\chi_P(G;k)$ is a polynomial in k. We discuss the distinctive power of these polynomials and present recent results and open problems on the complexity of evaluating $\chi_P(G;\lambda)$ for various properties P and (not only integer) values of λ.

This is joint work with A. Goodall, M. Hermann, T. Kotek and S. Noble which was initiated during last year's program "Counting Complexity and Phase Transitions". See also arXiv:1701.06639v1 [math.CO].

Definability and recognizability for graphs of bounded linear cliquewidth

Michał Pilipczuk, University of Warsaw, Poland

Motivated by the recent resolution of Courcelle's conjecture, we investigate the same question for graphs of bounded cliquewidth. Precisely, is it true that every graph property that is recognizable with respect to the algebra of k-clique expressions, for every k, is also MSO_1-definable on graphs of cliquewidth at

most k, for every k? We apply a similar general scheme as for the treewidth case to prove this statement for classes with bounded linear cliquewidth.

The talk will be a continuation of the talk of Mikołaj Bojańczyk and is based on a joint work with Mikołaj Bojańczyk and Martin Grohe.

Deciding parity games in quasipolynomial time

Frank Stephan, National University of Singapore, Singapore

It is shown that the parity game can be solved in quasipolynomial time. The parameterised parity game – with n nodes and m distinct values (aka colours or priorities) – is proven to be in the class of fixed parameter tractable (FPT) problems when parameterised over m. Both results improve known bounds, from runtime $n^{O(\sqrt{n})}$ to $O(n^{\log(m)+6})$ and from an XP-algorithm with runtime $O(n^{\Theta(m)})$ for fixed parameter m to an FPT-algorithm with runtime $O(n^5+m^{1.001m})$. As an application it is proven that coloured Muller games with n nodes and m colours can be decided in time $O((m^m \cdot n)^5)$; it is also shown that this bound cannot be improved to $2^{o(m \cdot \log(m))} \cdot n^{O(1)}$ unless FPT = W[1]. Further investigations deal with memoryless Muller games and multi-dimensional parity games.

Joint work with Cristian S. Calude, Sanjay Jain, Bakhadyr Khoussainov, and Wei Li.

List of Participants

- Isolde Adler, University of Leeds, UK
- Mikołaj Bojańczyk, University of Warsaw, Poland
- Benjamin Burton, The University of Queensland, Australia
- Samuel Buss, UC San Diego, USA
- Hubie Chen, Univ. Pais Vasco and Ikerbasque, Spain
- Yijia Chen, Fudan University, China
- Bruno Courcelle, LaBRI/ Bordeaux University, France
- Radu Curticapean, Hungarian Academy of Sciences, Hungary
- Anuj Dawar, University of Cambridge, UK
- Holger Dell, Saarland University, Germany
- Rodney Downey, Victoria University of Wellington, New Zealand
- Kord Eickmeyer, Technische Universität Darmstadt, Germany
- Jörg Flum, Albert-Ludwigs Universität Freiburg, Germany
- Jiawei Gao, UC San Diego, USA
- Serge Gaspers, The University of New South Wales, Australia
- Petr Hliněný, Masaryk University, Czech Republic
- Bart M. P. Jansen, Eindhoven University of Technology, the Netherlands
- Valentine Kabanets, Simon Fraser University, Canada
- Antonina Kolokolova, Memorial University of Newfoundland, Canada
- Johann Makowsky, Technion C- Israel Institute of Technology, Israel
- Catherine McCartin, Massey University, New Zealand
- Michał Pilipczuk, University of Warsaw, Poland
- Frank Stephan, National University of Singapore, Singapore
- Osamu Watanabe, Tokyo Institute of Technology, Japan
- Keita Yokoyama, Japan Advanced Institute of Science and Technology, Japan

Meeting Schedule

Check-in Day: September 17 (Sunday)

15:00 Check-in

19:00 Welcome Banquet

Day 1: September 18 (Monday)

9:00-10:00 *Introduction*

10:00-11:00 Bruno Courcelle: *Tree-width, clique-width and fly-automata*

11:00-12:00 Mikołaj Bojańczyk: *A proof of Courcelle's conjecture on recognisable graph classes*

12:00 *Lunch*

13:30 *Group Photo*

14:00-15:00 MichałPilipczuk: *Definability and recognizability for graphs of bounded linear cliquewidth*

15:00-15:30 *Coffee Break*

15:30-16:30 Petr Hliněný: *Definability of path- and branch decompositions: another view*

18:00 *Dinner*

Day 2: September 19 (Tuesday)

9:00-10:00 Hubie Chen: *One hierarchy spawns another: graph deconstructions and the complexity classification of conjunctive queries*

10:00-10:30 *Coffee Break*

10:30-11:30 Isolde Adler: *Testing logically defined properties on structures of bounded degree*

12:00 *Lunch*

14:00-15:00 Kord Eickmeyer: *Logics with invariantly used relations*

15:00-15:30 *Coffee Break*

15:30-16:30 Yijia Chen: *Parameterized* AC^0 *– some upper and lower bounds*

18:00 *Dinner*

Day 3: September 20 (Wednesday)

9:00-10:00 Samuel Buss: *Some* NP *functions and their proof complexity and completeness*

10:00-10:30 *Coffee Break*

10:30-11:30 Valentine Kabanets: *The uncanny usefulness of constructive proofs of pseudorandomness*

12:00 *Lunch*

14:00 *Excursion: Engaku and Kencho Temple*

18:00 *Main Banquet*

Day 4: September 21 (Thursday)

9:00-10:00 Johann Makowsky: *The distinctive power and complexity of counting generalized colorings: new results and challenges*

10:00-10:30 *Coffee Break*

10:30-11:30 Anuj Dawar: *The symmetry barrier in combinatorial optimization*

12:00 *Lunch*

14:00-15:00 Antonina Kolokolova: *Proof complexity of SMT*

15:00-15:30 *Coffee Break*

15:30-16:30 Jiawei Gao: *Completeness and improved algorithms for first-order properties on sparse structures*

18:00 *Dinner*

Day 5: September 22 (Friday)

9:00-10:00 Frank Stephan: *Deciding parity games in quasipolynomial time*

10:00-10:30 *Coffee Break*

10:30-11:30 Benjamin Burton: *Parameterised computational topology*

12:00 *Lunch*

14:00 C 18:00 *Free Discussion and Departure*