Oberwolfach Workshop 2413:
Proof Complexity and Beyond
March 24–29, 2024

GENERAL INFORMATION

- Sunday afternoon is the official arrival time and Oberwolfach opens at 16:30. The institute offers free taxi transfer from the train station in Hausach on Sunday evening at 16:30, 17:30, and 18:30. Please check in at the reception from 17:00 to 19:00 or via the early/late arrivals list placed opposite the reception.
- Departure is on Friday after lunch. Check-out time from the rooms is at 9:30. There will be lunch at 12:30 but no dinner. Oberwolfach will organize a number of free taxi transfers to the train station in Hausach on Friday afternoon or evening.

MEALS

- Breakfast is served from 8:00 to 9:00.
- Lunch is served at 12:30.
- Cake is served 15:00–16:00 (except on Wednesday).
- Dinner is served at 18:30.

SCHEDULE

Sunday March 24

17:00–19:00	Check-in
18:30–	Dinner
20:00–	Informal gathering in the lounge (if desired)

Monday March 25

08:00–08:45	Breakfast
08:45–09:00	Welcome
09:00–10:00	Robert Robere *TFNP and Proof Complexity*
10:00–10:30	Coffee break
10:30–11:00	Noah Fleming *PPP Is Not Closed Under Turing Reductions*
11:00–11:30	Neil Thapen *TFNP Intersections and Feasible Disjunction*
11:30–12:00	Pavel Hrubeš *A Variant of Monotone Calculus*
12:00–12:30	Iddo Tzameret *Functional Lower Bounds in Algebraic Proofs: Symmetry, Lifting, and Barriers*
12:30	Lunch
15:00–16:00	Coffee and cake
16:00–17:00	Susanna F. de Rezende *MISSING TITLE AND ABSTRACT*
17:00–17:30	Break
17:30–18:00	Theodoros Papamakarios *On the Hardness of Automating Bounded Depth Frege Systems*
18:00–18:30	Presentation of participants
18:30	Dinner

Tuesday March 26

08:00–09:00 Breakfast
09:00–10:00 Kilian Risse *Clique Is Hard on Average for Unary Sherali-Adams*
10:00–10:30 Coffee break
10:30–11:00 Jonas Conneryd *Graph Colouring Is Hard on Average for Polynomial Calculus*
11:00–11:30 Jacobo Torán *Pebble Games and Algebraic Proof Systems*
11:30–12:00 Johan Håstad *On Small-Depth Frege Proofs for PHP*
12:00–12:30 Dmitry Itsykson *Lower Bounds for Regular Resolution Over Parities*
12:30 Lunch
15:00–16:00 Coffee and cake
16:00–17:00 Dmitry Sokolov *Some Applications of Sunflowers*
17:00–17:30 Break
17:30–18:00 Mika Göös *Hardness Condensation by Restriction*
18:00–18:30 Anastasiia Sofronova *Top-Down Lower Bounds for Depth-Four Circuits*
18:30 Dinner

Wednesday March 27

08:00–09:00 Breakfast
09:00–10:00 Pravesh Kothari *The Kikuchi Matrix Method*
10:00–10:30 Coffee break
10:30–11:00 Madhur Tulsiani *Decoding Codes via Proofs*
11:00–11:30 Grigoriy Blekherman *Graph Homomorphisms and Polynomials*
11:30–12:00 Nicola Galesi *On the Algebraic Proof Complexity of Tensor Isomorphism*
12:00–12:30 Edward Hirsch *Tropical Proof Systems*
12:30 Lunch & Hike
18:30 Dinner

Thursday March 28

08:00–09:00 Breakfast
09:00–10:00 Igor Carboni Oliveira *Meta-Mathematics of Complexity Theory*
10:00–10:30 Coffee break
10:30–11:00 Emil Jeřábek *The Theory of Exponential Integer Parts*
11:00–11:30 Pavel Pudlák *On Quantified Propositional Calculus and Restricted Implicit Proofs*
11:30–12:00 Martin Grohe *Compressing CFI Graphs and Lower Bounds for the Weisfeiler-Leman Refinements*
12:00–12:30 Shuo Pang *A Supercritical and Robust Trade-off for Resolution Depth Versus Width and Weisfeiler-Leman*
12:30 Lunch
15:00–16:00 Coffee and cake
16:00–16:30 Olaf Beyersdorff *Proof Complexity and Solving of Quantified Boolean Formulas*
16:30–17:00 Abhimanyu Choudhury *Dependency Schemes in CDCL-Based QBF Solving: A Proof-Theoretic Study*
17:00–17:30 Break
17:30–18:00 Kaspar Kasche *Polynomial Calculus in QBF: Circuit Characterisation and Lower Bounds*
18:00–18:30 Ilario Bonacina *Proof Systems for MaxSAT*
18:30 Dinner

Friday March 29

08:00–09:00	Breakfast
09:00–09:30	TBD *TBD*
09:00–09:30	TBD *TBD*
10:00–10:30	Coffee break
10:30–11:00	TBD *TBD*
11:00–11:30	Aaron Potechin *Bounds on the Total Coefficient Size of Nullstellensatz Proofs of the Pigeonhole Principle*
11:30–12:00	TBD *TBD*
12:00–12:30	TBD *TBD*
12:30	Lunch
13:30–14:00	Coffee and cake
14:00–14:30	TBD *TBD*
14:30	Workshop ends

Olaf Beyersdorff: Proof Complexity and Solving of Quantified Boolean Formulas

I give an overview of proof systems and lower bound techniques for QBF. I will also explain the correspondence (or absence thereof) between QCDCL (the CDCL version for QBF) and QBF resolution systems.

Grigoriy Blekherman: Graph Homomorphisms and Polynomials

I would like to highlight recent interplay between problems in extremal combinatorics and real algebraic geometry. I will introduce graph homomorphism inequality problems, and discuss several topics including undecidability of certifying such inequalities and relations with the geometry of the Vandermonde map. I will then focus on structural properties of binomial inequalities and discuss some recent progress and open questions.

Ilario Bonacina: Proof Systems for MaxSAT

MaxSAT is the problem of finding an assignment satisfying the maximum number of clauses in a CNF formula. This talk gives an overview of recent results about proof systems for MaxSAT, i.e., formal systems that can be used to certify the optimum value of a MaxSAT problem. In particular, we show generalizations of Polynomial Calculus sound and complete both for MaxSAT and the natural generalization of MaxSAT to arbitrary sets of polynomials. We show how to view (semi-)algebraic static proof systems, such as Nullstellensatz and Sherali-Adams, in the language used to describe proof systems for MaxSAT, such as MaxSAT-Resolution. We give combinatorial principles capturing the strength of some (semi-)algebraic static proof systems. This talk is based on joint works with Maria Luisa Bonet and Jordi Levy.

Igor Carboni Oliveira: Meta-Mathematics of Complexity Theory

Despite significant efforts from computer scientists and mathematicians, the P vs. NP problem and other fundamental questions about the complexity of computations seem to remain out of reach for existing techniques. The difficulty of making progress on such problems has motivated a number of researchers to investigate the logical foundations of computational complexity. Over the last few decades, several works at the intersection of logic and complexity theory showed that certain fragments of Peano Arithmetic collectively known as Bounded Arithmetic can formalize a large fraction of results from algorithms and complexity (e.g., the PCP Theorem and complexity lower bounds against restricted classes of Boolean circuits). It is natural to consider if the same theories can settle longstanding problems about the inherent difficulty of computations.

In the first part of this talk, we survey a few recent results on the unprovability of statements of interest to complexity theory in theories of Bounded Arithmetic and highlighted some open problems. In the second part of the talk, we will cover new results on the reverse mathematics of complexity lower bounds, a research direction which seeks to determine which axioms are necessary to prove certain results. We explore reversals in the setting of bounded arithmetic, with Cook's theory PV_1 as the base theory, and show that several natural lower bound statements about communication complexity, error correcting codes, and Turing machines are equivalent to widely investigated combinatorial principles such as the weak pigeonhole principle for polynomial-time functions and its variants. As a consequence, complexity lower bounds can be formally seen as fundamental mathematical axioms with far-reaching implications. Time permitting, we will also present several implications of these results:

- Under a plausible cryptographic assumption, the classical single-tape Turing machine $\Omega(n^2)$-time lower bound for Palindrome is unprovable in Jeřábek's theory APC_1.

- While APC_1 proves one-way communication lower bounds for Set Disjointness, it does not prove one-way communication lower bounds for Equality, under a plausible cryptographic assumption.
- An amplification phenomenon connected to the (un)provability of some lower bounds, under which a quantitatively weak $n^{(1+\varepsilon)}$ lower bound is provable if and only if a stronger (and often tight) n^c lower bound is provable.
- Feasibly definable randomized algorithms can be feasibly defined deterministically (APC_1 is $\forall\Sigma^1_1$-conservative over PV_1) if and only if one-way communication complexity lower bound for Set Disjointness are provable in PV_1.

Abhimanyu Choudhury: Dependency Schemes in CDCL-Based QBF Solving: A Proof-Theoretic Study

In Quantified Boolean Formulas QBFs, dependency schemes help to detect spurious or superfluous dependencies that are implied by the variable ordering in the quantifier prefix but are not essential for constructing countermodels. This detection can provably shorten refutations in specific proof systems, and is expected to speed up runs of QBF solvers. The proof system QCDCL recently defined by Beyersdorff and Boehm (LMCS 2023) abstracts the reasoning employed by QBF solvers based on conflict-driven clause-learning (CDCL) techniques. We show how to incorporate the use of dependency schemes into this proof system, either in a preprocessing phase, or in the propagations and clause learning, or both. We then show that when the reflexive resolution path dependency scheme D^{rrs} is used, a mixed picture emerges: the proof systems that add D^{rrs} to QCDCL in these three ways are not only incomparable with each other, but are also incomparable with the basic QCDCL proof system that does not use D^{rrs} at all, as well as with several other resolution-based QBF proof systems. A notable fact is that all our separations are achieved through QBFs with bounded quantifier alternation.

(Joint work with Meena Mahajan. Appeared in FSTTCS2023.)

Jonas Conneryd: Graph Colouring Is Hard on Average for Polynomial Calculus

We give an overview of the ideas behind our FOCS 2023 paper proving that the polynomial calculus proof system over any field requires linear degree to refute that sparse random regular graphs, as well as sparse Erdős-Rényi random graphs, are 3-colourable. Using the known relation between size and degree for polynomial calculus proofs, this implies strongly exponential lower bounds on proof size.

This is joint work with Susanna F. de Rezende, Jakob Nordström, Shuo Pang, and Kilian Risse.

Noah Fleming: PPP Is Not Closed Under Turing Reductions

We show that the TFNP class PPP, corresponding to the totality of the Pigeonhole Principle, is not closed under Turing reductions in the black-box model, even non-adaptively. All other classical TFNP subclasses (e.g. PLS, PPA, PPAD, PPADS, etc.) are known to be closed under Turing reductions, and the closely related subclass PWPP (corresponding to the weak pigeonhole principle) is closed under non-adaptive Turing reductions. This differentiates PPP from all other well-studied TFNP subclasses, and resolves a conjecture of Buss and Johnson which was recently highlighted in Daskalakis' IMU Abacus Medal Lecture.

To prove our results we develop new lower bound tools in proof complexity. In particular, we introduce a new type of pseudoexpectation operator that is tailored to proving lower bounds for black-box PPP, which may be of independent interest. If time permits, we also show how to

use our pseudoexpectation operator to prove that the classical Ramsey problem is not black-box reducible to PPP, resolving another open problem in the complexity of TFNP. This talk is based on two joint papers currently in submission: Noah Fleming, Stefan Grosser, Toniann Pitassi, Robert Robere. Black-Box PPP is Not Turing-Closed. Siddhartha Jain, Jiawei Li, Robert Robere, Zhiyang Xun. On Pigeonhole Principles and Ramsey in TFNP.

Nicola Galesi: On the Algebraic Proof Complexity of Tensor Isomorphism

We initiate the study of (algebraic) proof complexity approaches to proving that two tensors are non-isomorphic. The Tensor Isomorphism problem (TI) has recently emerged as having connections to multiple areas of research within complexity and beyond, but the current best upper bound is essentially the brute force algorithm. Our main results are an $\Omega(n)$ lower bounds on PC degree or SoS degree for Tensor Isomorphism, and a nontrivial upper bound for testing isomorphism of tensors of bounded rank. We also show that PC cannot perform basic linear algebra in sub-linear degree, such as comparing the rank of two matrices, or deriving $BA = I$ from $AB = I$. As linear algebra is a key tool for understanding tensors, we introduce a strictly stronger proof system, $PC + \text{Inv}$, which allows as derivation rules all substitution instances of the implication $AB = I \implies BA = I$. We conjecture that even $PC + \text{Inv}$ cannot solve TI in polynomial time either, but leave open getting lower bounds on $PC + \text{Inv}$ for any system of equations, let alone those for TI.

Martin Grohe: Compressing CFI Graphs and Lower Bounds for the Weisfeiler-Leman Refinements

The k-dimensional Weisfeiler-Leman (k-WL) algorithm is a simple combinatorial algorithm that was originally designed as a graph isomorphism heuristic. It naturally finds applications in Babai's quasipolynomial-time isomorphism algorithm, practical isomorphism solvers, and algebraic graph theory. However, it also has surprising connections to other areas such as logic, combinatorial optimization, machine learning, and proof complexity.

The algorithm iteratively computes a coloring of the k-tuples of vertices of a graph. Since Fürer's linear lower bound [ICALP 2001], it has been an open question whether there is a super-linear lower bound for the iteration number for k-WL on graphs. We answer this question affirmatively, establishing an $\Omega(n^{k/2})$-lower bound for all k.

This is joint work with Moritz Lichter, Daniel Neuen, and Pascal Schweitzer.

Mika Göös: Hardness Condensation by Restriction

Can every n-bit boolean function with deterministic query complexity $k \ll n$ be restricted to $O(k)$ variables such that the query complexity remains $\Omega(k)$? That is, can query complexity be condensed via restriction? We study such hardness condensation questions in both query and communication complexity, proving two main results:

(Negative): Query complexity cannot be condensed in general: There is a function f with query complexity k such that any restriction of f to $O(k)$ variables has query complexity $O(k^{3/4})$.

(Positive): Randomised communication complexity can be condensed for the sink-of-xor function. This yields a quantitatively improved counterexample to the log-approximate-rank conjecture, achieving parameters conjectured by Chattopadhyay, Garg, and Sherif (2021).

Along the way we show the existence of Shearer extractors—a new type of seeded extractor whose output bits satisfy prescribed dependencies across distinct seeds.

Joint work with Ilan Newman, Artur Riazanov, and Dmitry Sokolov.

Edward Hirsch: Tropical Proof Systems

Tropical (min-plus) arithmetic has many applications in various areas of mathematics. The operations are the real addition (as the tropical multiplication) and the minimum (as the tropical addition). Recently, in several papers a version of Nullstellensatz in the tropical setting was demonstrated.

We introduce (semi)algebraic proof systems that use min-plus arithmetic. This allows us to view some known proof systems from a different angle. In particular, we provide a static Nullstellensatz-based tropical proof system that polynomially simulates daglike resolution and also has short proofs for the propositional pigeon-hole principle. Its dynamic version strengthened by an additional derivation rule (tropical analogue of resolution by linear inequality) is equivalent to R(LP), which derives nonnegative linear combinations of linear inequalities; this latter system is known to polynomially simulate Krajicek's R(CP) with unary coefficients. Lower bound results for these new systems are limited so far (I will mention a few), but they seem to be a promising direction.

Joint work with Y. Alekseev and D. Grigoriev.

Pavel Hrubeš: A Variant of Monotone Calculus

Monotone calculus is a Frege-style system which operates with implications $A \implies B$ where A and B are monotone. I will define a weakening of this system and show its connections with monotone arithmetic circuits.

Johan Håstad: On Small-Depth Frege Proofs for PHP

We study Frege proofs for the one-to-one graph Pigeon Hole Principle defined on the $n \times n$ grid where n is odd. We are interested in the case where each formula in the proof is a depth d formula in the basis given by $\wedge$, $\vee$, and $\neg$. We prove that in this situation the proof needs to be of size exponential in $n^{\Omega(1/d)}$. If we restrict the size of each line in the proof to be of size M then the number of lines needed is exponential in $n/(\log M)^{O(d)}$. The main technical component of the proofs is to design a new family of random restrictions and to prove the appropriate switching lemmas.

Dmitry Itsykson: Lower Bounds for Regular Resolution Over Parities

The proof system resolution over parities (Res($\oplus$)) operates with disjunctions of linear equations (linear clauses) over GF(2); it extends the resolution proof system by incorporating linear algebra over GF(2). Over the years, several exponential lower bounds on the size of tree-like Res($\oplus$) refutations have been established. However, proving a superpolynomial lower bound on the size of dag-like Res($\oplus$) refutations remains a highly challenging open question.

We prove an exponential lower bound for regular Res($\oplus$). Regular Res($\oplus$) is a subsystem of dag-like Res($\oplus$) that naturally extends regular resolution. This is the first known superpolynomial lower bound for a fragment of dag-like Res($\oplus$) which is exponentially stronger than tree-like Res($\oplus$).

The talk is based on the joint paper with Klim Efremenko and Michal Garlik to appear at STOC 2024.

Emil Jeřábek: The Theory of Exponential Integer Parts

An integer part (IP) of an ordered ring is a discretely ordered subring D such that every element is within distance 1 from D. A classical result of Shepherdson characterizes models of the arithmetical theory IOpen as IPs of real-closed fields. Motivated by connections to bounded arithmetic, we are interested in extensions of Shepherdson's theorem to IPs closed under 2^x (=

exponential IP = EIP) of real-closed exponential fields. In this talk, we axiomatize the first-order theories of such EIPs in a language with 2^x, in a language with a predicate for the powers of 2, and in the basic language of ordered rings; we investigate some properties of these theories, and a certain associated 2-player game on the integers.

Kaspar Kasche: Polynomial Calculus in QBF: Circuit Characterisation and Lower Bounds

We investigate a natural generalisation of polynomial calculus to QBFs. We show a circuit characterisation of proof size in QBF PC, a size-degree relation (different from the size-degree relation in PC) and new lower bounds for proof size.

Pravesh Kothari: The Kikuchi Matrix Method

This method shows how to solve problems in combinatorics/coding theory by reducing them to finding refutations for semirandom XOR instances (which are then found using a new class of spectral methods). The following are the applications of this method so far:

1. Smoothed CSP Refutation `https://arxiv.org/abs/2109.04415`
2. Resolving Feige's Conjecture on short even covers in arbitrary hypergraphs `https://arxiv.org/abs/2109.04415andhttps://arxiv.org/abs/2207.10850`
3. Polynomially-improved Lower bounds on locally decodable codes `https://eccc.weizmann.ac.il/report/2022/101`
4. Exponential Lower bound on locally correctable codes `https://arxiv.org/abs/2311.00558`
5. Bounds on Restricted k-term Arithmetic Progressions in dense subsets of integers (this one is due to Castro-Silva and Briet) `https://arxiv.org/abs/2304.03234`

Shuo Pang: A Supercritical and Robust Trade-off for Resolution Depth Versus Width and Weisfeiler—Leman

We present the first robust trade-offs for resolution where low width implies depth superlinear in the formula size. We give analogous results for the Weisfeiler–Leman algorithm, which also translate into trade-offs between number of variables and quantifier depth in first-order logic.

Theodoros Papamakarios: On the Hardness of Automating Bounded Depth Frege Systems

The problem of proof search is central to automated theorem proving, and has been the driving force behind many theoretical advances: Provided that short proofs of a statement exist, how hard is to find one? More concretely, a proof system P is called *automatable* if there is an algorithm that, given a formula F, finds a P-proof of F in time polynomial in the size of the shortest P-proof of F. Starting with [Atserias, Muller, JACM, 2020], many weak proof systems, including resolution, Res(k), cutting planes, various algebraic proof systems and bounded depth Frege, have been shown to be as hard to automate as possible. I would like to propose a talk focusing on the hardness of automating bounded depth Frege systems.

Aaron Potechin: Bounds on the Total Coefficient Size of Nullstellensatz Proofs of the Pigeonhole Principle

When studying algebraic proof systems such as Nullstellensatz, Sherali-Adams, and the sum of squares hierarchy, we are generally interested in the size and degree of proofs. A natural question is what happens when we take the size of the coefficients of the proof into account.

There are several approaches for studying this. One approach is to look at unary Nullstellensatz and unary Sherali-Adams where all coefficients of the proof must be integers and we take the proof size to be the sum of the magnitudes of the coefficients. As shown by the paper "Separations in Proof Complexity and TFNP" by Göös et. al., this approach has several advantages. Two of the results in this paper (out of many) are that unary Nullstellensatz is closely connected to the TFNP class PPAD and unary Sherali-Adams is closely connected to the TFNP class PPADS. A second approach is to look at the bit complexity of the proofs. While this is generally quite challenging, there is one formula, the Binary Value Principle, for which several strong lower bounds have been shown. In particular, there are conditional superpolynomial lower bounds for the extremely powerful Ideal Proof System and unconditional exponential lower bounds for Res-Lin and for polynomial calculus with square roots and extension variables.

In our work, we take a third approach where we investigate the total coefficient size of proofs without requiring that the coefficients are integers. This approach has the advantage that the minimum total coefficient size of a proof can be computed using a linear program. This approach also allows us to investigate the question of whether having fractional coefficients reduces the total coefficient size needed. In this talk, I will give a direct proof that any Nullstellensatz proof of the pigeonhole principle must have exponential total coefficient size.

Pavel Pudlák: On Quantified Propositional Calculus and Restricted Implicit Proofs

We will show that the restricted implicit proof system of G_i is polynomially equivalent to G_{i+1}.

Kilian Risse: Clique Is Hard on Average for Unary Sherali-Adams

We show that unary Sherali-Adams requires proofs of size $n^{\Omega(d)}$ to refute the existence of an $n^{0.1}$-clique in Erdős-Rényi random graphs whose maximum clique is of size $d \leq 2 \log n$. We obtain this result by introducing a technique inspired by pseudo-calibration which may be of independent interest. The technique involves defining a measure on monomials that precisely captures the contribution of a monomial to a refutation. This measure intuitively captures progress and should have further applications in proof complexity.

Based on joint work with Susanna de Rezende and Aaron Potechin.

Robert Robere: TFNP and Proof Complexity

A recent line of work has demonstrated many deep connections between propositional proof systems and total NP search problems (TFNP). The basic correspondence allows us to associate a total search problem S with each propositional proof system P such that the following holds: for every tautology T, T has a short proof in P if and only if proving T can be "efficiently reduced" to proving the totality of S. This allows us to define a theory of reducibility for proof systems that is analogous to classical reducibility in complexity theory, it has led to the resolution of a number of open problems in both proof complexity and the theory of TFNP, and also has suggested new directions of study in both of these areas. In this talk we will survey this connection, the recent progress that has been made, and outline some next steps for the development to take.

Anastasiia Sofronova: Top-Down Lower Bounds for Depth-Four Circuits

We present a top-down lower-bound method for depth-4 boolean circuits. In particular, we give a new proof of the well-known result that the parity function requires depth-4 circuits of size exponential in $n^{1/3}$. Our proof is an application of robust sunflowers and block unpredictability. This is a joint work with Mika Göös, Artur Riazanov and Dmitry Sokolov.

Dmitry Sokolov: Some Applications of Sunflowers

We consider the notion of sunflowers and robust sunflowers. Through examples of sunflower applications we will try to answer the following questions:

a) Which properties of sunflowers can help to solve the problem?

b) Why "robust sunflower" is a sunflower?

c) How we can find a robust sunflower?

During this talk we go over classical applications like monotone circuit lower bounds as well as recent results DNF sparsification (and Res(k) lower bounds), depth-4 circuit lower bounds.

Jacobo Torán: Pebble Games and Algebraic Proof Systems

We give some new connections between pebble games and algebraic proof systems, showing that there is a parallelism between the reversible, black and black-white pebbling games on one side, and the three algebraic proof systems NS, MC and PC on the other side. In particular we will provide: Very similar results as those proven in [deRezendeMNR21] for reversible pebbling and Nullstellensatz, for the case of black pebbling and Monomial Calculus (pebbling space and time correspond to degree and size). These results imply degree separations between NS and MC as well as strong degree-size tradeoffs for MC. These are joint results with my student Lisa-Marie Jaser.

Madhur Tulsiani: Decoding Codes via Proofs

The problem of finding the nearest codeword to a possibly corrupted received word, can naturally be viewed as an optimization problem. Over the past few years, continuous relaxations of this problem have led to new unique decoding and list decoding algorithms for several code families. In this talk, we will discuss a general framework for obtaining such algorithms using relaxations based on the Sum-of-Squares (SoS) hierarchy of semidefinite programs. In particular, this framework is an adaptation of the well-known "proofs to algorithms" paradigm to the setting of codes. If the proof of the fact that all pairs of codewords have large distance can be expressed in a proof system corresponding to the SoS hierarchy, then one can use it to obtain a list decoding algorithm for the corresponding code. We will discuss a few examples of this phenomenon.

Iddo Tzameret: Functional Lower Bounds in Algebraic Proofs: Symmetry, Lifting, and Barriers

Strong algebraic proof systems such as IPS (Ideal Proof System; Grochow-Pitassi 2018) offer a general model for deriving polynomials in an ideal and refuting unsatisfiable propositional formulas, subsuming most standard propositional proof systems. A major approach for lower bounding the size of IPS refutations is the Functional Lower Bound Method (Forbes, Shpilka, Tzameret and Wigderson 2021), which reduces the hardness of refuting a polynomial equation $f(x) = 0$ with no Boolean solutions to the hardness of computing the function $1/f(x)$ over the Boolean cube with an algebraic circuit. Using symmetry we provide a general way to obtain many new hard instances against fragments of IPS via the functional lower bound method. This

includes hardness over finite fields and hard instances different from Subset Sum variants both of which were unknown before, and significantly improved constant-depth IPS lower bounds. Conversely, we expose the limitation of this method by showing it cannot lead to proof complexity lower bounds for any hard Boolean instance (e.g., CNFs) for any sufficiently strong proof systems (including $\mathrm{AC}^0[p]$-Frege).

Joint work with Tuomas Hakoniemi and Nutan Limaye.

Susanna F. de Rezende: MISSING TITLE AND ABSTRACT

Neil Thapen: TFNP Intersections and Feasible Disjunction

MISSING ABSTRACT

Jakob Nordström: Certifying Combinatorial Solving Using Cutting Planes with Strengthening Rules

A talk like this might or might not be scheduled on Friday

The last couple of decades has witnessed a revolution in combinatorial optimization, with modern algorithms being used routinely to solve large-scale real-world problems, but the scientific understanding how these so-called combinatorial solvers can perform so well is quite poor. More importantly, even mature commercial solvers are known to sometimes produce wrong answers, which can be fatal for some types of applications.

We will discuss how proof complexity can be leveraged to design so-called certifying solvers, which output not only an answer but also a machine-verifiable proof that this answer is correct. Quite surprisingly, it turns out that cutting planes, if suitably extended, seems to hit a sweet spot between simplicity and expressivity, making it a suitable proof system for not only advanced Boolean satisfiability (SAT) solving but also MaxSAT solving, pseudo-Boolean optimization, and constraint programming.