Mathematisches Forschungsinstitut Oberwolfach

Report No. 27/2024

DOI: 10.4171/OWR/2024/27

Complexity Theory

Organized by
Peter Bürgisser, Berlin
Irit Dinur, Rehovot
Salil Vadhan, Cambridge MA

2 June – 7 June 2024

Abstract. Computational Complexity Theory is the mathematical study of the intrinsic power and limitations of computational resources like time, space, or randomness.

The current workshop focused on recent developments in various sub-areas including fine-grained complexity, algorithmic fairness, pseudorandomness, cryptography, arithmetic complexity, Markov Chain Monte Carlo, structure vs. randomness in combinatorics and complexity, meta-complexity, and the complexity of approximation problems. Many of the developments are related to diverse mathematical fields such as algebra, geometry, combinatorics, analysis, and coding theory.

Mathematics Subject Classification (2020): 68Q01, 68Q17, 68Q15.

Introduction by the Organizers

The workshop *Complexity Theory* was organized by Peter Bürgisser (TU Berlin), Irit Dinur (Weizmann Institute), and Salil Vadhan (Harvard). The workshop was held on June 2–7 2024. It was attended by approximately 50 participants spanning a wide range of interests within the field of Computational Complexity. The plenary program featured thirteen long lectures, plus three short (10-minute) reports by students and postdocs. In addition, intensive interaction took place in smaller groups.

The Oberwolfach Meeting on Complexity Theory is marked by a long tradition and a continuous transformation. Originally starting with a focus on algebraic and Boolean complexity, the meeting has continuously evolved to cover a wide variety of areas, most of which were not even in existence at the time of the first meeting (in 1972). While inviting many of the most prominent researchers in the field, the organizers try to identify and invite a fair number of promising young researchers and researchers involved in major developments in adjacent areas. In particular, approximately 30% of the participants in the 2024 meeting were not at either of our previous two meetings (2018 and 2021). The meeting usually features a few special focus topics which vary from meeting to meeting. The special focus topics of the current meeting were fine-grained complexity, algorithmic fairness, and structure vs. randomness in combinatorics.

Computational complexity (a.k.a. complexity theory) is a central field of theoretical computer science with a remarkable list of celebrated achievements as well as a vibrant research community. The field is concerned with the study of the *intrinsic complexity* of computational tasks, and this study tends to *aim at generality*: it focuses on natural computational resources, and considers the effect of limiting these resources on the class of problems that can be solved. Computational complexity is related to and has substantial interaction with other areas of mathematics such as algebra, analysis, combinatorics, geometry, number theory, optimization, probability theory, and quantum computation.

The workshop focused on several sub-areas of complexity theory and its nature may be best illustrated by a brief survey of some of the meeting's highlights.

Recent Developments in Fine-Grained Complexity. The goal of this active area is to understand the precise time complexity of fundamental computational problems in the class P. Amir Abboud surveyed the state of the art and current research directions. On the one hand, he mentioned recent algorithmic breakthroughs, e.g. for max-flow and matrix multiplication. On the other hand, Abboud highlighted the role of three primary conjectures, used to structure the landscape of the class P. The talk ended with a somewhat controversial discussion of the notion of "combinatorial algorithms" for triangle detection and Boolean matrix multiplication.

Algorithmic Fairness. The goal of *algorithmic fairness* is to ensure that algorithms, for example machine learning models, do not discriminate. Cynthia Dwork surveyed a variety of definitions that have been proposed for algorithmic fairness, and described how some of them are closely related to concepts in computational complexity and graph theory. In particular, the recently proposed notion of *multicalibration* (Hébert-Johnson et al. 2018) turns out to be a generalization of the graph regularity notion that appears in Szémeredi's Regularity Lemma and a strengthening of the complexity-theoretic notion of regularity proposed in 2009 by Trevisan, Tulsiani, and Vadhan. Several past applications of complexity-theoretic regularity become much more immediate consequences of multicalibration, and we expect that multicalibration will prove to be a powerful tool for future results in complexity theory. Informal presentations related to this topic were then given by Reingold and Vadhan.

New Frontiers In Structure vs Randomness. What is the largest cardinality of a subset $S \subseteq \{1, 2, ..., N\}$ that dos not have a three-term arithmetic progression? Behrend's construction (1946) of a large such set may be considered the starting point of the field of additive combinatorics. Raghu Meka's talk began with an overview of this problem. He then described his recent breakthrough on this question with Kelley, which gave another example of complexity-theoretic thinking yielding payoffs for problems in pure mathematics. The main idea is a new variant of the "structure vs. randomness" paradigm. This is a technique with many applications in complexity theory, algorithm design, and number theory, and the new variant may lead to further progress. The new idea was explained in detail for the analogous question for subsets of $\mathbb{F}_3^n$. The key concept is the notion of *spread* subsets $S \subseteq \mathbb{F}_3^n$ and the insight that simple operations on spread sets can lead to nearly-uniform distributions. Applications to communication complexity and algorithm design (triangle detection) were discussed, and were followed up by more detailed presentations in informal sessions by Meka and Fischer.

Reading Turing's papers. Avi Wigderson, recently announced recipient of the 2024 Turing Award (the highest prize in computer science), gave a wonderful preview of his "Turing Award Lecture" to be delivered a few weeks later at STOC conference. In his talk he covered several of Alan Turing's papers, giving a modern perspective on the same topics. A theme that came out was the power of modeling real world questions into a mathematical format. These topics span an amazingly broad range: from undecidability (Entscheidungsproblem), to code breaking (enigma in WW II) and advances in probability, statistics and information theory. Moreover, Alan Turing was a pioneer in machine intelligence (Turing test). Avi's talk ended with the discussion of Turing's influential paper in biology (morphogenesis). In this work, the symmetry breaking necessary for developing specialized cells is modelled by ordinary differential equations.

Advances in Polynomial Identity Testing. Pranjal Dutta presented a comprehensive overview on the history and recent advances on this important problem. A seminal paper by Kabanets and Impagliazzo from 2004 made it clear that finding fast *deterministic* algorithms for testing polynomial identities (PIT) and proving complexity lower bounds are intimately linked. In particular, it was shown that the assumed computational hardness of explicit polynomials can be used for solving the PIT problem without using randomness. This relied on a combinatorial construction due to Nisan and Wigderson (1994). For a long time, researchers sought to replace the combinatorial construction with a purely algebraic one, given that the problem at hand is algebraic. Recently, such construction was found by Guo, Kumar, Saptharishi, and Solomon (2022). Their result leads to a significantly better understanding of the parameter dependence, e.g., as seen from their optimal bootstrapping result. Besides explaining this breakthrough, the talk also overviewed the state of the art of unconditional derandomization of the PIT problem .

When Sunflowers Meet Thresholds. Jinyoung Park is a young mathematician working in combinatorics and random graph theory. In a brilliant talk, she reported on her recent work with several coauthors, in which two related conjectures were proven: the Kahn-Kalai Conjecture (2006) and its relaxation by Talagrand (2010). The motivation came from the famous, still unresolved Erdös-Rado Sunflower Conjecture, which has no randomness in it, and which is of relevance in complexity theory. A breakthrough on that conjecture was made by theoretical computer scientists Alweiss et al. (2021, presented in our previous meeting), which uses ideas of the structure versus randomness paradigm, which was also the topic of Raghu Meka's plenary talk.

Pseudorandom permutations. In this talk, Ryan O'Donnell surveyed recent developments in the construction of pseudorandom subsets of groups, with particular attention to symmetric groups and unitary groups. Such constructions have a variety of applications in theoretical computer science, including in classical and quantum cryptography. O'Donnell argued that a good notion of pseudorandomness is that of fooling group representations. In addition to the usual pseudorandomness goal of constructing small sets that are ε-approximately k-wise independent, significant attention has been paid recently to finding sets in which all elements have highly efficient reversible circuit representations.

Spectral Refutation and bounds for local codes. Pravesh Kothari presented a powerful new technique, based on the spectral analysis of *Kikuchi matrices*, which has been used to resolve several major open problems. The problems solved include exponential lower bounds on the length of 3-query "locally correctable" error-correcting codes, improved *refutation algorithms* for "smoothed" instances of the SAT problem (a model that lies between worst-case and average-case complexity), and a (positive) resolution of the Feige's conjecture on the hypergraph Moore bound. Related results were presented in the informal sessions by Guruswami, Kothari, Mohanty, and O'Donnell.

Brief Reports. In one plenary session, the postdocs Nick Fischer, Rahul Ilango, and Sidhanth Mohanty gave brief reports on their research interests.

Informal specialized sessions. Outside formal plenary program, intense interaction between the participants took place in smaller groups. Part of these took place in the form of specialized sessions, which included a mixture of interactive presentations (abstracts enclosed) and discussion/brainstorming. The topics of the specialized sessions included:

- Local characterizable expanders, or another benefit of the zig-zag construction (Goldreich), Computing polynomial gcd in AC^0 (Wigderson). What is in #P? (Ikenmeyer). Robust orbit problems and abc-conjecture (Bürgisser).
- Interactive proofs for verifying distrbution properties (Rothblum). Open problems on learning for indistinguishibility, regularity lemmas (Reingold). Multicalibration and the Hardcore Lemma (Vadhan).

- Near tight bounds for 3-query locally correctable binary codes (Guruswami). Quartic quantum speedups for Kikuchi-type problems (O'Donnell). Batch verification, recent progress (Rothblum).
- Explicit number-on-forehead separations in communication complexity (Meka). Combinatorial algorithms for triangle detection and new regularity lemma (Fischer).
- Update on complexity of matrix multiplication (Umans). Graph limits and Shannon capacity (Zuiddam).
- Attempts at explaining benign overfitting (Lin). Separating computational and statistical differential privacy (Ilango). New techniques in space complexity (Tal, Williams).
- Proving properties: answers of ML models (Goldwasser).
- Near optimal alphabet versus soundness tradeoff (Minzer). Feige's conjecture via Kuikui's matrix method (Kothari and Mohanty).
- Near-optimal average samplers (Zuckerman). Improved seedless condenser for Chor-Goldreich sources (Li).
- Depth reduction for algebraic formulas and circuits (Tavenas). Exponential lower bounds from Tau-Conjecture (Bläser).

Acknowledgement: The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-2230648, "US Junior Oberwolfach Fellows".

Workshop: Complexity Theory

Table of Contents

Abstracts

New Frontiers In Structure vs Randomness

Raghu Meka
(joint work with Amir Abboud, Nick Fischer, Zander Kelley, Shachar Lovett)

In 1936, Erdös and Turan asked the following: Suppose you have a set S of integers from $\{1, 2, ..., N\}$ that contains at least N/C elements. Then, for large enough N, must S have three equally spaced numbers (i.e., a 3-term arithmetic progression)? Behrend in 1946 showed that C can be at most $\exp(\Omega(\sqrt{\log N}))$. Since then, the problem has been a cornerstone of the area of additive combinatorics, with the best bound being $C = (\log N)^{1+c}$ for some constant $c > 0$. In a recent work with Zander Kelley [1], we obtained a sub-exponential improvement showing that C can be as big as $\exp(O(\log N)^{0.09})$, thus getting closer to Behrend's construction.

In this talk, I described this result and the main ingredient, a new variant of the "structure vs. randomness" paradigm. The latter is an old technique with many applications in complexity theory, algorithm design, and number theory, and the new variant can potentially lead to further progress.

The talk focused on presenting the main new ideas for the special case of the problem over finite fields $\mathbb{F}_3^n$. A key ingredient in the new technique is the idea that "spreadness implies mixing". A set $S \subseteq \mathbb{F}_3^n$ is d-spread if the density of S when restricted to any affine-space of co-dimension d is no more than a factor 1.01 larger than its original density. One of the main ingredients in the new improved bounds on 3-term arithmetic progressions is that while a spread set is only weakly pseudorandom, convolving two spread sets leads to a distribution that is very close to the uniform distribution on the entire space. That is, "spreadness implies mixing". The idea that simple operations on spread sets can lead to nearly-uniform distributions is key for the other applications discussed in the talk.

1. Communication complexity: An important question in communication complexity is to understand the relative powers of various communication models. In particular, the differences between randomized and deterministic protocols has been long-studied and well-understood in the two-party case. For example, the simple equality function, $EQ : [N] \times [N] \to \{0, 1\}$ defined by $EQ(x, y) = 1$ if and only if $x = y$ has deterministic communication complexity at least $\log_2 N - O(1)$, whereas its (public-coin) randomized communication complexity is $O(1)$.

However, the situation is vastly different when we have three communicating parties in the powerful "number-on-forehead" (NoF) communication model. Here, it is known that there exist functions that have as large a separation between randomized and deterministic communication protocols, but we did not have strong explicit separations. The talk described how the spreadness implies mixing framework could be used ([2]) to show such a separation for three-party NOF protocols leading to an explicit function $F : [N] \times [N] \times [N] \to \{0, 1\}$ whose randomized NoF complexity is $O(1)$ but deterministic NoF complexity is $\Omega((\log N)^{1/3})$.

2. Algorithm design: A classical question in algorithm design is to detect if a given input graph on N vertices has a triangle (three vertices with all edges present between them). The naive algorithm runs in time $O(N^3)$, whereas one can use fast matrix-multiplication to solve the problem in time $O(N^{2.37\cdots})$, i.e., get polynomial savings over the naive algorithm. However, for various applications and extensions (e.g., to hypergraphs) it is desirable to have "combinatorial algorithms" that could beat the naive algorithm. The techniques developed for the communication complexity application above, actually lead to a new "spread-regularity lemma" for graphs ([3]) which in turn can be used to obtain fast combinatorial algorithms for triangle detection: leading to a combinatorial algorithm for triangle detection that runs in time $N^3/2^{(\log N)^{\Omega(1)}}$.

References

[1] Z. Kelley, R. Meka, *Strong Bounds for Arithmetic Progressions*, FOCS 2023.

[2] Z. Kelley, S. Lovett, R. Meka, *Explicit separations between randomized and deterministic Number-on-Forehead communication*, STOC 2024.

[3] A. Abboud, N. Fischer, Z. Kelley, S. Lovett, R. Meka, New Graph Decompositions and Combinatorial Boolean Matrix Multiplication Algorithms, STOC 2024

Recent Developments in Fine-Grained Complexity

Amir Abboud

A large body of works, colloquially referred to as Fine-Grained Complexity or Hardness within P, aims to understand the precise time complexity of fundamental and important computational problems. While traditional complexity theory classifies problems into the polynomial time solvable ones and those that require super-polynomial time (under widely-believed conjectures), this more modern theory aims to classify problems based on the constant in the exponent of the polynomial.

The first part of the talk motivates this theory (e.g. by referring to practical considerations), presents the general technical framework (namely, a web of fine-grained reductions that translate a small set of conjectures about the complexity of certain core problems into a large number of tight conditional lower bounds), and offers a high-level overview of the state of affairs.

The second part of the talk surveys the research directions taken by the community in recent years, while going into the details of only a small fraction. The research directions can be categorized into three kinds.

- The first kind aims to boost the theory by making its hardness results more robust and applicable in settings beyond the basic worst-case setting. For example, the community has been trying to obtain *hardness of approximation* results, hardness for the *average-case*, and an analysis of the fine-grained *quantum* time complexity. Each of these topics deserves its own survey, and this talk will focus only on the hardness of approximation. We will discuss the main open questions, e.g. whether there is a $(1+\varepsilon)$-approximation for the Edit-Distance between two strings of length

n in near-linear time. Then, we will survey the known techniques for fine-grained gap amplification and present a recent technique called *Short Cycle Removal* [2] that has lead to strong lower bounds for approximate shortest path problems and distance oracles.

- The second kind are the works that aim to close any remaining gaps that exist for the most basic problems. As an example, we will present an open question asking whether subgraph isomorphism, i.e. checking whether a constant-size pattern graph H exists as a subgraph of an input graph G, can be solved in near-linear time if and only if H is acyclic. We will also discuss the impact of recent algorithmic breakthroughs on fine-grained complexity, e.g. for max-flow, matrix multiplication, and all-pairs max-flow. We will focus on the latter and discuss a surprising separation between all-pairs shortest-paths and all-pairs max-flow, as well as the credit due to fine-grained lower bounds towards making such algorithmic breakthroughs [3].
- The third kind investigates the conjectures that are the foundation of this theory. Why this many conjectures? Why these? Can we unify them? We will discuss some barriers for reductions between certain problems, which stand in the way of unifying the conjectures. We will also attempt to make order in the increasing number of conjectures used in the field, by distinguishing between the three *primary* conjectures and the more than ten *secondary* conjectures that can be derived from them.

The third and final part of the talk will discuss the notion of "combinatorial algorithms" for Triangle Detection and Boolean Matrix Multiplication, and the (lack of a) formal definition of this notion. It is based on the discussion in [1].

References

[1] A. Abboud, N. Fischer, Z. Kelly, S. Lovett, and R. Meka, *New Graph Decompositions and Combinatorial Boolean Matrix Multiplication Algorithms*, STOC 2024.

[2] A. Abboud, K. Bringmann, S. Khoury, and O. Zamir, *Hardness of Approximation in P via Short Cycle Removal: Cycle Detection, Distance Oracles, and Beyond*, STOC 2022.

[3] A. Abboud, R. Krauthgamer, J. Li, D. Panigrahi, T. Saranurak, and O. Trabelsi, *Breaking the Cubic Barrier for All-Pairs Max-Flow: Gomory-Hu Tree in Nearly Quadratic Time*, FOCS 2022.

Echoes of Rorschach: Complexity Theory and the Inkblots of Multi-group Fairness

Cynthia Dwork

(joint work with Silvia Casacuberta, Daniel Lee, Rachel Lin, Pranay Tankala, Salil Vadhan)

We identify and explore connections between the recent literature on multi-group fairness for prediction algorithms and classical results in graph regularity and computational complexity.

A *predictor* $\tilde{p} : \mathcal{X} \to [0,1]$ maps individuals in a domain $\mathcal{X}$ to a number in $[0,1]$ that is often interpreted as a probability, for example, the probability that individual x will complete college within four years of matriculation. While the meaning of the probability of a non-repeatable event is an open question in the philosophy of probability, we assume that "real-life" probabilities $p^*(x) \in [0,1]$ exist and that the real-life outcome for $x \in \mathcal{X}$ is a draw from the Bernoulli distribution $\mathrm{Ber}(p^*(x))$.

Multiaccuracy and multicalibration [5] are two widely-studied desiderata that arose in the study of the theory of algorithmic fairness [2]. Let $\mathcal{C} \subseteq 2^{\mathcal{X}}$ be a collection of arbitrarily intersecting subsets of $\mathcal{X}$, and let $\varepsilon \geq 0$. Abusing notation, let $c : \mathcal{X} \to \{0,1\}$ denote the characteristic function for the set $c \in \mathcal{C}$. Formally, $\tilde{p}$ is $(\mathcal{C}, \varepsilon)$-multiaccurate iff $\forall c \in \mathcal{C}$,

$$|\mathbb{E}[c(x)(\tilde{p}(x) - p^*(x))]| \leq \varepsilon.$$

Multicalibration is a strengthening of multiaccuracy requiring that $\tilde{p}$ be *calibrated* on each $c \in \mathcal{C}$.

A key result in [5] is the existence of low-complexity multicalibrated predictors. The level sets of a predictor $\tilde{p}$ induce a partition on the domain $\mathcal{X}$. A particularly useful form of the multicalibration theorem says that there is a low-complexity partitioning of $\mathcal{X}$ such that (1) the level sets are few ($O(1/\varepsilon)$); determining for $i \in X$ which piece of the partition contains i requires few ($O(1/\varepsilon^2)$) calls to functions $c \in \mathcal{C}$, and within each (sufficiently heavy) level set P, p^* is $(\mathcal{C}, \varepsilon)$-indistinguishable from the constant-Bernoulli function with parameter equal to $\mathbb{E}_{x \in P}[p^*(x)]$ [4]. (The definition in [5] (calibration on each $c \in C$) is slightly weaker than this partition form, but their algorithm achieves this "strict" notion.)

The complexity-theoretic regularity lemma [6] says, informally, that, given any class $\mathcal{F}$ of functions $f : \mathcal{X} \to \{0,1\}$, an arbitrary function $g : \mathcal{X} \to [0,1]$ can be approximated by a low-complexity function h that makes a small number of oracle calls to $\mathcal{F}$, in the sense that h is $(\mathcal{F}, \varepsilon)$-indistinguishable from g: $\forall f \in \mathcal{F}$,

$$|\mathbb{E}[f(x)(h(x) - g(x))]| \leq \varepsilon.$$

The regularity lemma has powerful consequences [6, 7], including Impagliazzo's hardcore lemma (1995); the Dense Model Theorem (Greene and Tao, 2008; Tao and Ziegler (2008)); Frieze-Kannan (1996) graph regularity; and a complete characterization [7] of pseudo-average min-entropy, a computational analogue of average min-entropy defined by Dodis, Ostrovsky, Reyzin and Smith (2008).

The starting point for our work is the observation that multiaccuracy *is exactly* regularity: simply substitute p^* for g, $\tilde{p}$ for h, and $c \in \mathcal{C}$ for $f \in \mathcal{F}$. Given that multiaccuracy ("TTV regularity") is so generous, what can the more powerful multicalibration give us?

Complexity Theory ([1]). By definition, each piece of an $(\mathcal{F}, \varepsilon)$-multicalibrated partition for an arbitrary function g enjoys $(\mathcal{F}, \varepsilon)$-multiaccuracy, so we can apply the results of [6] to each piece independently. However, by exploiting the fact that on each piece of the partition the function g is $(\mathcal{F}, \varepsilon)$-indistinguishable from a *constant-Bernoulli* function with parameter $v_P = \mathbb{E}_{x \in P}[g(x)]$, we can do more. Each of the complexity-theoretic applications of TTV regularity requires a hardness assumption. For example, Impagliazzo's hardcore theorem assumes that g is $(\mathcal{F}, \delta)$-weakly hard. Extending Yao's lemma (1982) on the equivalence of unpredictability and pseudorandomness (indistinguishability from a constant 1/2 Bernoulli function) to the case of general constant-Bernoulli functions, we get (some) unpredictability on each piece of the partition *with no assumptions.* The precise degree of unpredictability is governed by the bias $b_P = \min\{v_P, 1 - v_P\}$ of the constant v_P-Bernoulli function (and the ε of multicalibration). This yields, without assumptions, a collection of "little hard cores," one on each (sufficiently heavy) piece of the partition, leading to a characterization of the average-case hardness of a function in terms of a weighted sum of the $O(1/\varepsilon)$ biases b_P, for $P \in \mathcal{P}$. Moreover, by stitching together the little hardcore sets, we can recover the hardcore theorem with optimal parameters (Holenstein 2005). We also obtain analogous extensions of the results in [6] for pseudo-average min-entropy and the dense model theorem.

Graph Regularity ([3]). Szemerédi's regularity lemma (1975) states that any large, dense graph can be decomposed into parts that behave "pseudorandomly" in a certain precise sense. The Frieze-Kannan weak regularity lemma (1996) is a related result with a qualitatively weaker conclusion but parameter dependencies much better suited for algorithmic applications.

As noted in [6], given a graph $G = (V, E)$, we can relate graph regularity to complexity-theoretic regularity by setting the domain $\mathcal{X}$ to be $V \times V$, and letting $g : V \times V \to \{0, 1\}$ be the indicator function for E. A regular partition of the graph is a partitioning of the *vertex set* (not the domain $\mathcal{X}$), so that the densities of the cross-partition cuts capture the behavior of the graph. Every partitioning $\mathcal{P}$ of V immediately yields a partitioning of $V \times V$, but the converse is false.

For a graph $G = (V, E)$, the two regularity requirements can be rephrased in terms of the fairness (multiaccuracy and strict multicalibration) of the paritioning $\mathcal{P} \times \mathcal{P}$ of the domain $\mathcal{X} = V \times V$, where $\mathcal{P}$ is in turn a partitioning of V into m parts $V_1, \ldots, V_m$, with the collection of sets $\mathcal{C}$ being given (in both cases) by $\mathcal{C} = \{S \times T \mid S, T \subseteq V\}$. Letting d_{jk} be the edge density for the (V_j, V_k) cut, $j, k \in [m]$, and $e(A, B)$ denote the number of edges between $A, B \subseteq V$, we have:

Frieze-Kannan regularity:

$$\max_{S,T \subseteq V} \left| \sum_{j=1}^{m} \sum_{k=1}^{m} e(S \cap V_j, T \cap V_k) - d_{jk} |S \cap V_j||T \cap V_k| \right| \leq \varepsilon |V|^2;$$

equivalently, $\mathcal{P} \times \mathcal{P}$ is $(\mathcal{C}, \varepsilon^{\Theta(1)})$-multiaccurate.

Szemerédi regularity:

$$\sum_{j=1}^{m} \sum_{k=1}^{m} \max_{S,T \subseteq V} |e(S \cap V_j, T \cap V_k) - d_{jk} |S \cap V_j||T \cap V_k|| \leq \varepsilon |V|^2;$$

equivalently, $\mathcal{P} \times \mathcal{P}$ is $(\mathcal{C}, \varepsilon^{\Theta(1)})$-strictly multicalibrated.

Phrased in this way, we immediately see the possibility of an intermediate regularity notion fitting strictly between Frieze-Kannan and Szemerédi regularity:

$$\max_{S,T\subseteq V}\sum_{j=1}^{m}\sum_{k=1}^{m}|e(S\cap V_j,T\cap V_k)-d_{jk}|S\cap V_j||T\cap V_k||\leq\varepsilon|V|^2;$$

equivalently, $\mathcal{P}\times\mathcal{P}$ is $(\mathcal{C},\varepsilon^{\Theta(1)})$-multicalibrated as originally defined in [5]. This intermediate notion has part complexity $m=4^{1/\varepsilon^2}$ equal to that of Frieze-Kannan regularity, much smaller than the tower of $O(1/\varepsilon^2)$ 2's required for Szemerédi regularity (Fox and Lovàsz 2014).

For the case of unstructured partitions (and Boolean-valued outcomes), the original (not strict) definition of multicalibration [5] most closely resembles this intermediate notion. Unlike in the case with the structured partitions $\mathcal{P}\times\mathcal{P}$, in the unstructured case ordinary multicalibration and strict multicalibration are closely related (provided the number of level sets is small, which is easily obtained in the unstructured case because adjacent level sets can be merged).

References

[1] S. Casacuberta, C. Dwork, and S. Vadhan, *Complexity-Theoretic Implications of Multicalibration*, 56th Annual ACM Symposium on Theory of Computing (2024), 1071–1082.

[2] C. Dwork, M. Hardt, T. Pitassi, O. Reingold, and R. Zemel, *Fairness through awareness*, Innovations in Theoretical Computer Science (2012), 214–226.

[3] C. Dwork, D. Lee, H. Lin, and P. Tankala, *From pseudorandomness to multi-group fairness and back*, Thirty Sixth Annual Conference on Learning Theory, PMLR (2023), 3566–3614.

[4] P. Gopalan, O. Reingold, V. Sharan, and U. Wieder, *Multicalibrated Partitions for Importance Weights*, International Conference on Algorithmic Learning Theory, PMLR (2022) 408–435.

[5] U. Hébert-Johnson, M.P. Kim, O. Reingold, and G.N. Rothblum, *Multicalibration: Calibration for the (computationally-identifiable) masses*, International Conference on Machine Learning, PMLR (2018), 1939–1948.

[6] L. Trevisan, M. Tulsiani, and S. Vadhan, *Regularity, boosting, and efficiently simulating every high-entropy distribution*, 24th Annual IEEE Conference on Computational Complexity (2009), 126–136.

[7] S. Vadhan and C. Zheng, *Characterizing pseudoentropy and simplifying pseudorandom generator constructions*, 44th Symposium on Theory of Computing Conference (2012), 817–836.

Spectral Independence and Applications to Analysis of Markov chains

Kuikui Liu

(joint work with Dorna Abdolazimi, Nima Anari, Zongchen Chen, Shayan Oveis Gharan, Nitya Mani, Ankur Moitra, Eric Vigoda, Cynthia Vinzant, Thuy-Duong Vuong)

Let μ be a probability distribution over an exponentially large domain Ω; for simplicity, we take $\Omega=\{\pm1\}^n$. We study the complexity of sampling from the distribution μ, assuming we have query access to a function $w:\Omega\to\mathbb{R}_{\geq0}$ such that $\mu(x)\propto w(x)$ for all $x\in\Omega$. One of the most ubiquitous approaches to sampling, both in theory and in practice, is to simulate a Markov chain whose equilibrium distribution is μ. Over the Boolean cube, one natural Markov chain is given by *Glauber dynamics*, whose evolution can be described as follows. In each step, the chain

(1) selects a uniformly random coordinate $i \sim [n]$, and
(2) resamples the assignment σ_i conditioned on the current assignments σ_{-i} to the remaining coordinates; in other words, $\sigma_i \leftarrow +1$ with probability $\frac{\mu(\sigma_{-i},+1)}{\mu(\sigma_{-i},+1)+\mu(\sigma_{-i},-1)}$ and $\sigma_i \leftarrow -1$ otherwise.

Since each step can be implemented efficiently, the fundamental question is how long to simulate the chain. In other words, we wish to bound the mixing time of the chain

$$T_{\mathsf{mix}} := \min\{t \in \mathbb{N} : \mathscr{D}_{\mathsf{TV}}(\delta_x P^t, \mu) \le \epsilon, \forall x \in \Omega\},$$

where P denotes the chain's transition probability matrix. In this talk, we survey a recently developed technique for bounding mixing times of Markov chains called *spectral independence.*

Definition 1 (Spectral Independence (Boolean Case); [3])**.** Let μ be a probability distribution over $\{\pm 1\}^n$. Define its *conditional influence matrix* $\Psi_\mu \in \mathbb{R}^{n \times n}$ by

$$\Psi_\mu(i \to j) := \Pr_{\sigma\sim\mu}[\sigma_j = +1 \mid \sigma_i = +1] - \Pr_{\sigma\sim\mu}[\sigma_j = +1 \mid \sigma_i = -1], \qquad \forall i, j \in [n].$$

We say μ is *η-spectrally independent* if $\lambda_{\max}(\Psi_\mu) \le 1 + \eta$.

Note that $\Psi_\mu = D_\mu^{-1}\Sigma_\mu$, where $\Sigma_\mu(i,j) = \mathsf{Cov}_{\sigma\sim\mu}(\sigma_i, \sigma_j)$ is the usual covariance matrix, and D_μ is a diagonal matrix with entries given by the variance of each coordinate; in particular, the eigenvalues of Ψ_μ are all real. If μ is a product measure (e.g. uniform over $\{\pm 1\}^n$), then μ is 0-spectrally independent. At the other extreme, if $\mu = \frac{1}{2}\delta_{+\mathbf{1}} + \frac{1}{2}\delta_{-\mathbf{1}}$, then $\Psi_\mu = \mathbf{1}\mathbf{1}^\top$ and so μ is $(n-1)$-spectrally independent. This property of the distribution μ was originally distilled from the recently emerging theory of high-dimensional expanders. We have the following local-to-global theorems connecting spectral independence with the theory of mixing times.

Theorem 1 (Informal; [1, 3] building on [25, 21, 26])**.** *Suppose there exists $\eta \le O(1)$ such that for every $S \subseteq [n]$ with $|S| \le n-2$ and every partial assignment $\tau : S \to \{\pm 1\}$, the distribution of $\sigma \sim \mu$ conditioned on agreeing with τ on S is η-spectrally independent. Then Glauber dynamics mixes in $O(n^{2+\eta})$-steps.*

If we impose an additional graphical assumption on the structure of μ, then we can improve the mixing time to the optimal $O(n \log n)$. More specifically, we say μ satisfies the global Markov property w.r.t. a graph $G = ([n], E)$ if for every partition of $[n]$ into three sets A, S, B such that S separates A from B, and every partial assignment $\tau : S \to \{\pm 1\}$ on the separator, the marginal assignments σ_A, σ_B are independent conditioned on $\sigma_S = \tau$.

Theorem 2 (Informal; [16])**.** *Suppose μ satisfies the following properties.*

(1) μ and all of its conditional distributions are all η-spectrally independent for some $\eta \le O(1)$.

(2) μ satisfies the global Markov property w.r.t. a graph of bounded maximum degree $\Delta \leq O(1)$.

(3) For every $i \in [n]$, $S \subseteq [n] \setminus \{i\}$, and $\tau : S \to \{\pm 1\}$, the marginals $\Pr_{\sigma\sim\mu}[\sigma_i = +1 \mid \sigma_S = \tau], \Pr_{\sigma\sim\mu}[\sigma_i = -1 \mid \sigma_S = \tau]$ are both lower bounded by a constant $b \geq \Omega(1)$

Then Glauber dynamics mixes in $O_{\eta,\Delta,b}(n \log n)$ steps.

The spectral independence technique has led to the resolution of several long-standing open problems in the theory of approximate counting and sampling.

- **Bases of Matroids:** It was shown in [5] that the uniform distribution over bases of any matroid is 0-spectrally independent.[1] Hence, the natural basis exchange walk mixes in $O(r^2 \log n)$-steps, where r is the rank of the matroid and n is the number of elements in the ground set. In particular, this led to the first provably correct algorithm for sampling forests in graphs. The mixing time has been subsequently improved to $O(r \log r)$ [12, 6], leading to the first nearly-linear time sampler for spanning trees.
- **Hardcore Gas Model:** For a graph $G = (V, E)$ and a parameter $\lambda \geq 0$, define the Gibbs distribution of the hardcore gas model on G to the distribution $\mu(I) \propto \lambda^{|I|}$ for all independent sets $I \subseteq V$. This a discretization of the classical hard spheres model of a gas in statistical mechanics. It is well-known that there is a critical threshold $\lambda_c(\Delta)$, depending on the maximum degree of the graph, such that approximate counting and sampling is NP-hard when $\lambda > \lambda_c(\Delta)$ [29, 30], and efficient algorithms exist when $\lambda < \lambda_c(\Delta)$ [31]. We proved that whenever $\lambda < \lambda_c(\Delta)$, the Gibbs distribution is $O(1)$-spectrally independent, and hence Glauber dynamics furnishes a nearly-linear time sampling algorithm [3, 15, 16]. In particular, there is an extremely sharp complexity phase transition.

Several classes of techniques for establishing spectral independence have also been developed.

- **Correlation Decay:** In a sequence of works [3, 15, 16, 13, 23], it was established that correlation decay implies spectral independence. Correlation decay is a well-studied property of graphical distributions in statistical physics, which says that

$$\left|\Pr_{\sigma\sim\mu}[\sigma_v = +1 \mid \sigma_S = \tau] - \Pr_{\sigma\sim\mu}[\sigma_v = +1 \mid \sigma_S = \tau']\right| \lesssim \exp(-O(\mathsf{dist}_G(v, S)))$$

  for all $v \in [n]$, $S \subseteq [n] \setminus \{v\}$ and $\tau, \tau' : S \to \{\pm 1\}$.
- **Geometry of Polynomials:** The distribution μ can be fruitfully encoded into its generating polynomial $g_\mu(\mathbf{z}) := \sum_{\sigma\in\{\pm 1\}^n} \mu(\sigma) \prod_{i:\sigma_i=+1} z_i$. Analytic and algebraic properties of g_μ, such as zero-freeness and log-concavity, can then be leveraged to bound the spectral independence of μ [5, 2, 17].

[1] As this distribution is supported over sets of a fixed size, a minor adjustment to the definition of spectral independence is required.

- **Measure Decompositions:** If one can find a decomposition of μ into a mixture ξ of component distributions μ_ι such that ξ satisfies some nice mixing properties (e.g. a Poincaré Inequality), and each component μ_ι is $O(1)$-spectrally independent, then one can deduce $O(1)$-spectral independence for μ itself. Trickle-down-type methods [28, 4, 9], as well as techniques based on localization and the Hubbard–Stratonovich transform all fall under this umbrella [22, 10, 27, 8].
- **Disagreement Percolation:** Similar to correlation decay, one can establish spectral independence by exhibiting a coupling ξ of the conditional distributions $\mu^{i\leftarrow +1}$ and $\mu^{i\leftarrow -1}$ such that $\mathbb{E}_{(\tau,\sigma)\sim\xi}[d_H(\tau,\sigma)] \le O(1)$, where $d_H(\cdot,\cdot)$ denotes Hamming distance. Constructing such couplings has been used to great effect in several works on sampling solutions to constraint satisfaction problems [19, 20, 18, 14, 11, 24].

The spectral independence technique has since been strengthened and generalized considerably [10, 7]. We conclude with an open problem.

Conjecture 1. *Let $G = (V, E)$ be a graph of maximum degree Δ. Then for every $q \ge \Delta + 2$, the uniform distribution over proper q-colorings of G is $O(1)$-spectrally independent.*

This has been verified for $q \ge \Delta + 3$ for graphs of girth at least some constant depending only on Δ [14], and for $q \ge (1 + o_\Delta(1)) \cdot \Delta$ for line graphs [32]. Establishing various spatial and temporal mixing properties of random colorings on general graphs is a major open problem in approximate counting and sampling.

References

[1] V. Alev and L. Lau, *Improved Analysis of Higher Order Random Walks and Applications*, STOC 2020, 1198–1211

[2] Y. Alimohammadi, N. Anari, K. Shiragur, and T. Vuong, *Fractionally Log-Concave and Sector-Stable Polynomials: Counting Planar Matchings and More*, STOC 2021, 433–446

[3] N. Anari, K. Liu, and S. O. Gharan, *Spectral Independence in High-Dimensional Expanders and Applications to the Hardcore Model*, SIAM Journal on Computing (2021).

[4] D. Abdolazimi, K. Liu, and S. O. Gharan, *A Matrix Trickle-Down Theorem on Simplicial Complexes and Applications to Sampling Colorings*, FOCS 2022, 161–172

[5] N. Anari, K. Liu, S. O. Gharan, and C. Vinzant, *Log-Concave Polynomials II: High-Dimensional Walks and an FPRAS for Counting Bases of a Matroid*, STOC 2019, 1–12

[6] N. Anari, K. Liu, S. O. Gharan, C. Vinzant, and T. Vuong, *Log-Concave Polynomials IV: Approximate Exchange, Tight Mixing Times, and near-Optimal Sampling of Forests*, STOC 2021, 408–420

[7] N. Anari, Vishesh Jain, F. Koehler, H. T. Pham, and T. Vuong, *Entropic Independence: Optimal Mixing of down-up Random Walks*, STOC 2022, 1418–1430

[8] N. Anari, Vishesh Jain, F. Koehler, H. T. Pham, and T. Vuong, *Universality of Spectral Independence with Applications to Fast Mixing in Spin Glasses*, SODA 2024, 5029–5056

[9] N. Anari, F. Koehler, and T. Vuong, *Trickle-Down in Localization Schemes and Applications*, STOC 2024, 1094–1105

[10] Y. Chen and R. Eldan, *Localization Schemes: A Framework for Proving Mixing Bounds for Markov Chains*, FOCS 2022, 110–122

[11] Z. Chen and Y. Gu, *Fast Sampling of b-Matchings and b-Edge Covers*, SODA 2024, 4972–4987

[12] M. Cryan, H. Guo, and G. Mousa, *Modified log-Sobolev inequalities for strongly log-concave distributions*, Annals of Probability (2021), 506–525

[13] Z. Chen, A. Galanis, D. Štefankovič, and E. Vigoda, *Rapid Mixing for Colorings via Spectral Independence*, SODA 2021, 1548–1557

[14] Z. Chen, K. Liu, N. Mani, and A. Moitra, *Strong spatial mixing for colorings on trees and its algorithmic applications*, FOCS 2023, 810–845

[15] Z. Chen, K. Liu, and E. Vigoda, *Rapid Mixing of Glauber Dynamics up to Uniqueness via Contraction*, FOCS 2020, 1307–1318

[16] Z. Chen, K. Liu, and E. Vigoda, *Optimal Mixing of Glauber Dynamics: Entropy Factorization via High-Dimensional Expansion*, STOC 2021, 1537–1550

[17] Z. Chen, K. Liu, and E. Vigoda, *Spectral Independence via Stability and Applications to Holant-Type Problems*, FOCS 2021, 149–160

[18] Z. Chen, N. Mani, and A. Moitra, *From Algorithms to Connectivity and Back: Finding a Giant Component in Random k-SAT*, SODA 2023, 3437–3470

[19] A. Galanis, L. A. Goldberg, H. Guo, A. Herrera-Poyatos, *Fast sampling of satisfying assignments from random k-SAT*, arXiv:2206.15308 (2022)

[20] X. Chen and X. Zhang, *A Near-Linear Time Sampler for the Ising Model*, SODA 2023, 4478–4503

[21] I. Dinur and T. Kaufman, *High Dimensional Expanders Imply Agreement Expanders*, FOCS 2017, 974–985

[22] R. Eldan, F. Koehler, and O. Zeitouni, *A spectral condition for spectral gap: fast mixing in high-temperature Ising models*, Probability Theory and Related Fields 182 (2022), 1035–1051

[23] W. Feng, H. Guo, Y. Yin, and C. Zhang, *Rapid Mixing from Spectral Independence beyond the Boolean Domain*, SODA 2021, 1558–1577

[24] M. Jerrum, *Glauber dynamics for the hard-core model on bounded-degree H-free graphs*, arXiv:2404.07615 (2024)

[25] T. Kaufman and D. Mass, *High Dimensional Random Walks and Colorful Expansion*, ITCS 2017

[26] T. Kaufman and I. Oppenheim, *High Order Random Walks: Beyond Spectral Gap*, Combinatorica **40** (2020), 245–281

[27] K. Liu, S. Mohanty, A. Rajaram, and D. X. Wu, *Fast Mixing in Sparse Random Ising Models*, FOCS 2024

[28] I. Oppenheim, *Local spectral expansion approach to high dimensional expanders part I: Descent of spectral gaps*, Discrete and Computational Geometry **59.2** (2018), 293–330

[29] A. Sly, *Computational Transition at the Uniqueness Threshold*, FOCS (2010), 287–296

[30] A. Sly and N. Sun, *The Computational Hardness of Counting in Two-Spin Models on d-Regular Graphs*, The Annals of Probability **42.6** (2014), 2383–2416

[31] D. Weitz, *Counting Independent Sets Up to the Tree Threshold*, STOC 2006, 140–149

[32] Y. Wang, C. Zhang, and Z. Zhang, *Sampling Proper Colorings on Line Graphs Using $(1+o(1))\Delta$ Colors*, STOC 2024

Reading Turing's Papers

Avi Wigderson

Note from reporter: In this session, Avi Wigderson gave a preview of his 2024 Turing Award lecture.

Alan Turing was a giant intellectual figure of the 20th century. During his short life he thought deeply about a stunning variety of fundamental issues in several disciplines, and has contributed uniquely original models and results about them, which science (especially, but not only computer science) follow and develop. We review some of the ideas in his papers, and discuss how some evolved within TCS.

Recent Advances in Polynomial Identity Testing

Pranjal Dutta

Polynomial Identity Testing (PIT) is the problem of checking whether an n-variate polynomial over a field $\mathbb{F}$ is identically zero. For e.g., $(x+y)(x-y)-x^2-y^2$ is an identically zero polynomial. PIT is easy to solve if the polynomial is given in the sum of monomials form: $f(x_1,x_2,\ldots,x_n) = \sum_{0\le e_1,\cdots,e_n\le d} c_{e_1,\cdots,e_n}\, x_1^{e_1}\cdots x_n^{e_n}$, simply by checking whether all coefficients $c_{e_1,\cdots,e_n} \in \mathbb{F}$ are zero. However, it is often inefficient to have such an explicit representation of polynomials. In our context, we consider a compact representation of polynomials known as *algebraic circuits.* An *algebraic circuit* is a directed acyclic graph whose input nodes (nodes of in-degree zero) are labeled by variables $\{x_1,x_2,\ldots,x_n\}$, and constants from the underlying field $\mathbb{F}$, the internal nodes labeled by '+' (addition gate) and '$\times$' (multiplication gate). The two main complexity parameters of a circuit are the following: (1) *size*: the number of edges in the graph which is equal to the number of addition and multiplication we perform to compute the polynomial, (2) *depth*: the length of the longest path in the graph which captures the notion of parallel complexity. A circuit can compute a polynomial with exponentially large degree w.r.t. its size. For our purpose, we only focus on *low degree* circuits.

For algebraic circuits, the PIT problem is defined as follows. Given a circuit C, decide whether C computes the *zero* polynomial. One trivial way to compute the sum of monomials representation *fails* because it can have exponentially many monomials. For example, $f(x_1,x_2,\ldots,x_n)=\prod_{i=1}^n(1+\alpha_i x_i)+\prod_{i=1}^n(1+\beta_i x_i)$ has a circuit of size $O(n)$, but the number of nonzero monomials in f can be as large as 2^n. Therefore, this trivial approach does not produce an efficient solution for PIT. However, we can evaluate a circuit at any point in size(C) many operations over $\mathbb{F}$ by assigning values to the variables in the input nodes. This gives us a simple polynomial-time randomized algorithm for PIT due to the following.

Lemma 1 (Polynomial Identity Lemma [1, 4, 2, 3])**.** Let $f \in \mathbb{F}[x_1,x_2,\ldots,x_n]$ be a nonzero polynomial of degree at most d and $S \subseteq \mathbb{F}$. Then,

$$\Pr_{a_1,\ldots,a_n\in S}[f(a_1,\ldots,a_n)] \neq 0] \;\geq\; 1-\frac{d}{|S|}\ .$$

In *blackbox* PIT setting, we are *not* allowed to see the internal structure of the circuit, instead we are only allowed to evaluate the circuit at points from $\mathbb{F}^n$. Additionally, we assume that the information about the size, degree, and the number of variables of the input circuit is given in *unary.* A *hitting set* for a set of n-variate polynomials $\mathcal{P}$ is a set of points $\mathcal{H} \subseteq \mathbb{F}^n$ such that for any nonzero polynomial $f \in \mathcal{P}$ there exists a point $\mathbf{a} \in \mathcal{H}$ for which $f(\mathbf{a}) \neq 0$. A polynomial map $\mathsf{Gen}(\mathbf{y}) = (g_1,g_2,\ldots,g_n)$ from $\mathbb{F}^\ell$ to $\mathbb{F}^n$ is called a *hitting set generator* (HSG) for a class $\mathcal{P}$ if for every $P \in \mathcal{P}$, $P \neq 0$ if and only if $P \circ \mathsf{Gen} \neq 0$. Typically, we want ℓ to be as small as possible. These notions are known to be *equivalent.*

The PIT lemma ensures that for any n-variate nonzero polynomial f with *individual degree* at most d, the set S^n contains a point $\mathbf{a} \in S^n$ such that $f(\mathbf{a}) \neq 0$. Therefore, S^n works as a hitting set for the set of all n-variate polynomials of degree at most d. If we consider $\mathcal{C}(n,s,d)$, defined as the set of all size s circuits computing n-variate polynomials of degree at most d, then $\mathsf{poly}(sn)$-size hitting set for $\mathcal{C}(n,s,d)$ exists as shown by Heintz and Schnorr [5]. To derandomize PIT in the blackbox setting, our goal is to *explicitly* construct a hitting set of size $\mathsf{poly}(snd)$ for $\mathcal{C}(n,s,d)$ in time $\mathsf{poly}(snd)$. However, the current best explicit construction puts this problem in PSPACE [6].

We organize the known PIT results in two different categories; (1) *conditional* and (2) *unconditional.* Under these categories, we try to chronologically cover some of the major results,

Conditional PIT. In this regime, we design efficient PIT algorithms based on unproven complexity-theoretic assumptions like the existence of an explicit hard polynomial family. Let $(P_d)_d$ be an explicit univariate polynomial family where $\mathsf{deg}(P_d) = d$. We say that P_d is *hard* if $\mathsf{size}(P_d) = (\log d)^{\omega(1)}$. A random univariate polynomial requires $d^{\Omega(1)}$ size circuit. Although there are *non-explicit* hard polynomials, e.g. $P_d \in \{\sum_{i=0}^{d} 2^{2^{i^2}} x^i, \sum_{i=0}^{d} \sqrt{p_i} x^i, \ldots\}$, no *explicit* univariate polynomial family is shown to be hard. Here, explicitness means that the coefficients are polynomially large and computable efficiently.

Interestingly, explicit and hard univariate polynomial P_d can be uniquely converted into multilinear explicit hard multivariate polynomial $\tilde{P}_n$, where $n = \lceil \log(d+1) \rceil$ by *reverse Kronecker* map: $\tilde{P}_n(x^{2^0}, \ldots, x^{2^{n-1}}) := P_d$. In fact, $\mathsf{size}(P_d) = d^{\Omega(1)} \implies \mathsf{size}(\tilde{P}_n) = 2^{\Omega(n)}$.

It turns out that not only univariate hard polynomials can be converted into hard multivariate polynomials, it can also be used to design efficient PIT algorithms. Kabanets and Impagliazzo [7] showed how to use (optimal) hard univariate polynomials to get a quasipolynomial-time algorithm for PIT for the class $\mathcal{C}(s,s,s)$. The proof is based on NW-design families. Nisan and Wigderson [8] showed that there exists a family of subsets $S_1, S_2, \ldots, S_s \subseteq [\ell]$ with $\ell = O(m^2/\log s)$, $|S_i| = m$, and $|S_i \cap S_j| \le \log s$ for all $i \neq j$. Furthermore, they constructed such a design deterministically in time $\mathsf{poly}(s, 2^\ell)$. Such a family is called a NW-design.

Let $\tilde{P}$ be an explicit, multilinear and exponentially hard polynomial. Such polynomials can be found by converting a hard univariate polynomial by the reverse Kronecker map as mentioned above. Given an NW-design, let $S_i = \{i_1 < i_2 < \cdots < i_m\}$, and $\mathbf{y}|_{S_i} = (y_{i_1}, y_{i_2}, \ldots y_{i_m})$. The HSG in [7] (KI generator) is defined as follows: $\mathsf{Gen}_{\mathsf{KI}}^{\tilde{P}} = (\tilde{P}(\mathbf{y}|_{S_1}), \tilde{P}(\mathbf{y}|_{S_2}), \ldots, \tilde{P}(\mathbf{y}|_{S_s}))$. They showed $C \neq 0 \iff C \circ \mathsf{Gen}_{\mathsf{KI}}^{\tilde{P}} \neq 0$.

Building upon the template provided in [7], Dvir, Shpilka, and Yehudayoff [9] gave a more fine-grained version of the KI generator, which yielded an efficient black-box PIT for $\Delta - 5$ depth circuits of *bounded individual degree*, assuming P does not have small size Δ depth circuits. Later, Chou, Kumar, and Solomon [10] removed the bounded individual degree restriction in the conclusion, but they need a stronger hardness assumption in the hypothesis, that is, the degree of P is *low.*

In [11], Guo etal. gave a different construction of HSG from an explicit univariate hard degree d polynomial P. Their generator does not rely on combinatorial designs like NW-design, and is purely algebraic. The HSG $\mathsf{Gen}^P_{\mathsf{GKSS}} : \mathbb{F}^\ell \to \mathbb{F}^s$ by Guo etal. is defined as follows:

$$\mathsf{Gen}^P_{\mathsf{GKSS}}(\mathbf{y}, \mathbf{z}) \ := \ (\Delta_0(P)(\mathbf{y}, \mathbf{z}), \Delta_1(P)(\mathbf{y}, \mathbf{z}), \ldots, \Delta_{s-1}(P)(\mathbf{y}, \mathbf{z})) \ ,$$

where $\Delta_i(P)$ is the degree i (in $\mathbf{z}$) of the Taylor expansion of $P(\mathbf{y} + \mathbf{z})$. The analysis of $\mathsf{Gen}^P_{\mathsf{GKSS}}$ is quite different from the analysis of the KI generator. [11] constructed a small circuit for P from the equation $C \circ \mathsf{Gen}^P_{\mathsf{GKSS}} = 0$, via a careful inductive analysis similar to Newton iteration. This shows that $\mathsf{size}(P) = d^{\Omega(1)}$, then there is a $\mathsf{poly}(s)$-size explicit HSG for $\mathcal{C}(s, s, s)$. Combining this with PIT-to-hardness result of [12], one gets the surprising bootstrapping results. A general template of the bootstrapping results assumes a hypothesis that there is a slightly better-than-the-trivial hitting set for a restricted class of circuits and then one aims to *bootstrap* it to get a hitting set for general $\mathcal{C}(s, s, s)$. In the same spirit, [11] achieves the following.

Theorem 2 (Optimal Bootstrapping [11])**.** Let k, δ be constants. Let $\mathcal{C}(k, \mathsf{ind} : s, s^\delta)$ be the class of k-variate polynomials of individual degree s which are computable by s^δ size circuits. Suppose, there is an explicit hitting set of size $\leq (s+1)^k - 1$ (1 less than the trivial hitting set). Then, there is a $\mathsf{poly}(s)$ size explicit hitting set for $\mathcal{C}(s, s, s)$.

Unconditional PIT. Due to various structural results in algebraic circuits [13, 14], it is known that complete derandomization of restricted classes like depth-3 and depth-4 will lead to significant progress in derandomizing PIT for general circuits. Thus, restricted classes not only provide various challenges to generate new techniques but they can also be seen as stepping stones toward the general problem. For depth-2 circuits $\Sigma\Pi$, often referred as *sparse polynomials*, there is a polynomial-size explicit hitting set due to Klivans and Spielman [15].

A depth-3 diagonal circuit, denoted by $\Sigma \wedge \Sigma$, is of the form $f(\mathbf{x}) := \sum_{i=1}^k \ell_i^{d_i}$, where ℓ_i are linear polynomials. The best-known hitting set for this model is due to Forbes and Shpilka [17], and Gurjar, Korwar and Saxena [18], which has size $(knd)^{O(\log \log kd)}$, where $d = \max d_i$. On the other hand, when the number of variables is small, then Forbes, Ghosh and Saxena [16] designed a $\mathsf{poly}(kd2^n)$-size explicit hitting set. Coming up with a polynomial-size hitting set remains open.

A depth-3 circuit computes a polynomial of the form $\sum_{i=1}^k \prod_{j=1}^d \ell_{i,j}$, where $\ell_{i,j}$ are linear polynomials. For this model, there is an $(knd)^{O(k)}$-size hitting set due to Saxena and Seshadri [19].

A depth-4 circuit computes a polynomial of the form $\sum_{i=1}^k \prod_{j=1}^d f_{i,j}$, where $f_{i,j}$ are sparse polynomials. When the top fanin k and $\deg(f_{i,j}) \leq \delta$, are arbitrary constants Dutta, Dwivedi and Saxena [20] designed a quasipolynomial-size explicit hitting set using Jacobian techniques. For general constant-depth circuits, Limaye, Srinivasan and Tavenas [21] designed a subexponential-size explicit hitting set. Coming up with a better size hitting sets for both these models remain open.

References

[1] Øystein Ore, *Über höhere Kongruenzen*, Norsk Mat. Forenings Skrifter **1** (1922), 1-15.

[2] Richard Zippel, *Probabilistic algorithms for sparse polynomials*, EUROSAM LNCS **72** (1979), 216–226.

[3] Jacob T. Schwartz, *Fast Probabilistic Algorithms for Verification of Polynomial Identities*, J. ACM **27** (1980), 701–717.

[4] Richard A. DeMillo and Richard J. Lipton,*A Probabilistic Remark on Algebraic Program Testing*, Information Processing Letters **7** (1978), 193–195.

[5] Joos Heintz and Claus-Peter Schnorr, *Testing polynomials which are easy to compute*, Proceedings of the twelfth annual ACM Symposium on Theory of Computing (1980), 262–272.

[6] Ketan Mulmuley, *Geometric complexity theory V: Efficient algorithms for Noether normalization*, Journal of the American Mathematical Society **30** (2017), 225–309.

[7] Valentine Kabanets and Russell Impagliazzo, *Derandomizing polynomial identity tests means proving circuit lower bounds*, Computational Complexity **13** (2004), 1–46.

[8] Noam Nisan and Avi Wigderson, *Hardness vs Randomness*, J. Comput. Syst. Sci. **49** (1994), 149–167.

[9] Zeev Dvir and Amir Shpilka and Amir Yehudayoff, *Hardness-Randomness Tradeoffs for Bounded Depth Arithmetic Circuits*, SIAM J. Comput. **39** (2009), 1279–1293.

[10] Chi-Ning Chou and Mrinal Kumar and Noam Solomon, *Closure Results for Polynomial Factorization*, Theory Comput. **15** (2019), 1–34.

[11] Zeyu Guo and Mrinal Kumar and Ramprasad Saptharishi and Noam Solomon, *Derandomization from Algebraic Hardness*, SIAM J. Comput. **51** (2022), 315–335.

[12] Manindra Agrawal, *Proving Lower Bounds Via Pseudo-random Generators*, FSTTCS LNCS **3821** (2005), 92–105.

[13] Manindra Agrawal and V. Vinay, *Arithmetic Circuits: A Chasm at Depth Four*, FOCS (2008), 67–75.

[14] Ankit Gupta and Pritish Kamath and Neeraj Kayal and Ramprasad Saptharishi, *Arithmetic Circuits: A Chasm at Depth 3*, SIAM J. Comput. **45** (2016), 1064–1079.

[15] Adam R. Klivans and Daniel A. Spielman, *Randomness efficient identity testing of multivariate polynomials*, STOC (2001), 216–223.

[16] Michael A. Forbes and Sumanta Ghosh and Nitin Saxena, *Towards Blackbox Identity Testing of Log-Variate Circuits*, ICALP (2018), 54:1–54:16.

[17] Michael A. Forbes and Amir Shpilka, *Quasipolynomial-Time Identity Testing of Non-commutative and Read-Once Oblivious Algebraic Branching Programs*, FOCS (2013), 243–252.

[18] Rohit Gurjar and Arpita Korwar and Nitin Saxena, *Identity Testing for Constant-Width, and Any-Order, Read-Once Oblivious Arithmetic Branching Programs*, Theory Comput. **13** (2017), 1–21.

[19] Nitin Saxena and C. Seshadhri, *Blackbox Identity Testing for Bounded Top-Fanin Depth-3 Circuits: The Field Doesn't Matter*, SIAM J. Comput. **41** (2012), 1285–1298.

[20] Pranjal Dutta and Prateek Dwivedi and Nitin Saxena, *Deterministic Identity Testing Paradigms for Bounded Top-Fanin Depth-4 Circuits*, CCC 2021, 11:1–11:27.

[21] Nutan Limaye and Srikanth Srinivasan and Sébastien Tavenas, *Superpolynomial Lower Bounds Against Low-Depth Algebraic Circuits*, FOCS 2021, 804–814.

When Sunflowers Meet Thresholds

Jinyoung Park
(joint work with Keith Frankston, Jeff Kahn, Bhargav Narayanan, Huy Tuan Pham)

In this survey talk, we discuss the connection between Alweiss-Lovett-Wu-Zhang's breakthrough [1] on the Erdos-Rado Sunflower Conjecture and the recent developments around thresholds in probabilistic combinatorics, including the resolution of a conjecture of Talagrand due to Frankston-Kahn-Narayanan-Park [2] and the Kahn-Kalai Conjecture due to Park-Pham [4].

A collection of sets $S_1, \dots, S_r$ is an *r-sunflower* if

$$S_i \cap S_j = S_1 \cap \cdots \cap S_r \quad \forall i \neq j,$$

and the celebrated Erdős-Rado Sunflower Conjecture is:

Conjecture 1. Let $r \geq 3$. There exists $c = c(r)$ such that any k-set system $\mathcal{F}$ of size $|\mathcal{F}| \geq c^k$ contains an r-sunflower.
(a k-set system means every set in $\mathcal{F}$ has size at most k.)

A few years ago, Alweiss, Lovett, Wu, and Zhang [1] made a huge breakthrough towards Conjecture 1, showing that the conjecture holds if

$$|\mathcal{F}| \geq (Cr^3 \log k \log\log k)^k.$$

Actually, Alweiss-Lovett-Wu-Zhang's result was stronger, using the notion of *robust sunflower.*

Definition 2. (Robust sunflower) $0 < \alpha, \beta < 1$, $\mathcal{F}$ a set system on X, $K = \bigcap_{S \in \mathcal{F}} S$. We say $\mathcal{F}$ is an (α, β)-robust sunflower if

(1) $K \notin \mathcal{F}$
(2) $\mathcal{F}_K$ satisfies
$$\mathbb{P}(X_\alpha \text{ contains some member of } \mathcal{F}_K) > 1 - \beta.$$

($\mathcal{F}_K := \{S \setminus K : S \in \mathcal{F}, K \subseteq S\}$, and X_α is an α-random subset of X.)

It is easy to see that any $(1/r, 1/r)$-robust sunflower contains an r-sunflower.

Theorem 3. (Alweiss-Lovett-Wu-Zhang [1]) There exists C such that any k-set system $\mathcal{F}$ of size $|\mathcal{F}| \geq (Cr^3 \log k \log\log k)^k$ contains a $(1/r, 1/r)$-robust sunflower.

The proof of Theorem 3 uses the framework of "structured vs. pseudorandom." The key part is the pseudorandomness, which uses the notion of "κ-spread." In fact, the key theorem in [1] is:

Theorem 4. If $\kappa \geq (Cr^3 \log k \log\log k)^k$, then any κ-spread $\mathcal{F}$ satisfies

$$\mathbb{P}(X_{1/r} \text{ contains some member of } \mathcal{F}) > 1 - 1/r.$$

Theorem 4 provides a sufficient condition (i.e., spread) for an α-random subset of X contains a member of given set system $\mathcal{F}$ with a certain probability, which is closely related to the notion of *thresholds* in random graph theory.

As usual, we use $G_{n,p}$ for the Erdős-Renyi random graph, and say $\mathcal{F}_n \subseteq 2^{E(K_n)}$ is an *increasing property* if $A \supseteq B \in \mathcal{F}_n$, then $A \in \mathcal{F}_n$. Given an increasing property $\mathcal{F}_n$, $p_0 = p_0(n)$ is the *threshold* for $\mathcal{F}_n$ if

$$\mathbb{P}(G_{n,p} \text{ satisfies } \mathcal{F}_n) \to \begin{cases} 0 & \text{if } p \ll p_0; \\ 1 & \text{if } p \gg p_0 \end{cases}$$

as $n \to \infty$.

In 2006, Kahn and Kalai [3] suggested an extremely bold conjecture, which roughly says that, given an increasing property $\mathcal{F}_n$, if p is large enough to avoid both "first moment" and "coupon collector" constraints, then $G_{n,p}$ contains a member of $\mathcal{F}$ with a good probability.

The result by Alweiss-Lovett-Wu-Zhang and the Kahn-Kalai Conjecture, which are seemingly unrelated, turned out to be surprisingly closely related. By taking a linear relaxation of the integral constraints in the Kahn-Kalai Conjecture and applying the linear programming duality, Talagrand [5] suggested the following conjecture that is weaker than the Kahn-Kalai Conjecture. This is proved by Frankston, Kahn, Narayanan, and Park [2]:

Theorem 5.(Frankston-Kahn-Narayanan-Park [2]) There exists $K > 0$ such that, for any finite X and increasing $\mathcal{F} \subseteq 2^X$, if there is a q-spread probability measure supported on $\mathcal{F}$, then for $p = Kq \log \ell(\mathcal{F})$,

$$\mathbb{P}(X_p \text{ contains a member of } \mathcal{F}) \geq 1/2.$$

($\ell(\mathcal{F})$ is the size of a largest minimal element of $\mathcal{F}$.)

Here "q-spread" is essentially equivalent to the notion of κ-spread in [1], in the sense that the only difference is that q is the reciprocal of κ. The proof of Theorem 5 is based on the ingenious algorithm in [1], and [2] tightened the analysis of the algorithm to obtain the optimal bound of $p = \Theta(q \log \ell)$.

Theorem 5 has been very influential in random graph theory, often providing tight thresholds for many interesting increasing properties, some of which have been historically very hard. The algorithm used in [1] inspired the resolution of the Kahn-Kalai Conjecture [3] due to Park and Pham [4]. In the following statement, we use $q(\mathcal{F})$ for the "expectation threshold" given in [3].

Theorem 6. There exists $K > 0$ such that for any finite X and increasing $\mathcal{F} \subseteq 2^X$, if $p \geq Kq(\mathcal{F}) \log \ell(\mathcal{F})$, then

$$\mathbb{P}(X_p \text{ contains a member of } \mathcal{F}) \geq 1/2.$$

As a final remark, we note that the "graphic" Kahn-Kalai Conjecture, which was the original motivation for Theorem 6, is still open. We define the *graphic expectation threshold* for a graph H to be

$$p_{\mathbb{E}}(H) := \min\{p : \mathbb{E}\,[\#F\text{'s in } G_{n,p}] \geq 1 \quad \forall F \subseteq H\}.$$

Conjecture 7. (Conjecture 2 in [3]) There exists $K > 0$ such that for any graph $H \subseteq K_n$, if $p \geq Kp_{\mathbb{E}}(H) \log v(H)$, then

$$\mathbb{P}(G_{n,p} \text{ contains } H) \geq 1/2.$$

References

[1] R. Alweiss, S. Lovett, K. Wu, and J. Zhang, *Improved bounds for the sunflower lemma*, Ann. of Math. **194** (2021), 795-815.

[2] K. Frankston, J. Kahn, B. Narayanan, and J. Park, *Thresholds versus fractional expectation-thresholds*, Ann. of Math. **194** (2021), 475-495.

[3] J. Kahn and G. Kalai, *Thresholds and expectation thresholds*, Combin. Probab. Comput. **16** (2007), no. 3, 495–502.

[4] J. Park and H. T. Pham, *A proof of the Kahn-Kalai Conjecture*, J. Amer. Math. Soc. **37** (2024), 235-243

[5] M. Talagrand, *Are many small sets explicitly small?* Proc. 2010 ACM Int. Sympos. Theory Comput, New York (2010), 13–35.

Spectral Refutation for Semirandom CSPs and Applications to Local Codes

Pravesh K. Kothari

A 3-SAT formula is a collection of disjunctive 3-clauses (i.e., OR of 3 literals) on a given collection of n truth variables. In the well-known 3-SAT problem, we are given such a 3-SAT formula with m clauses on n variables and our goal is to find an assignment that satisfies all the constraints (if one exists) and if not, find a short (i.e., polynomial size in n) *witness* or *certificate* of unsatisfiability of the formula. 3-SAT is a well-known (and in many a sense, the *first*) NP-complete problem. It is also a problem that turns out to be hard to approximate. In a more fine-grained picture, denser instances of 3-SAT (i.e., when m grows super-linearly in n) appear intuitively easier (more "easily accessible" information about the satisfying assignment, in the form of additional clauses, if there is one or more "likelihood" of a short contradiction when there are more clauses) but this ease only amounts to an asymptotic gain for formulas with $\omega(n^2)$ constraints. Specifically, we know a $2^{O(n^{1-\delta})}$ time algorithm to find an assignment that gets within $(1-\epsilon)$ factor of the optimal (along with a certificate of approximate optimality) if the formula has at least $\tilde{O}(n^{2+\delta})$ constraints and a polynomial time algorithm if the formula has at least $O(n^3)$ constraints. Back in the late 1980s, in the context of proof complexity, researchers [5] posed the question of whether *random* 3-SAT formulas could be easier than the worst-case. Such formulas are unsatisfiable with high probability if $m \geq O(n)$. Indications of comparative easiness of such formulas finally arrived with the work of Goerdt and Krivilevich [9] and Coja-Oghlan, Goerdt and Lanka [6] in 2004 who proved that random 3-SAT formulas with $\tilde{O}(n^{1.5})$ clauses admit efficient *refutation* algorithms, i.e., polynomial time algorithms that generate a certificate of unsatisfiability of the given formula. And about a decade later, Raghavendra, Rao and Schramm [15], building on the work of Allen, O'Donnell and Witmer [2] proved that there is a $2^{n^{1-\delta}}$ time algorithm to find certificates of unsatisfiability with high probability for formulas with at least $\tilde{O}(n^{1.5-\delta/2})$ clauses. To top this work off, while we lack tools for proving NP-hardness of such *average-case* problems, there are lower bounds in various restricted models [14] (e.g., the sum-of-squares hierarchy of convex relaxations) that show that the running time vs clause density trade-offs achieved in the above works are nearly tight. Finally, all the above story extends naturally to k-SAT (and in fact, all constraint satisfaction problems that generalize k-SAT) for any constant $k \in \mathbb{N}$ with the two relevant threshold values of m being $\tilde{O}(n^{k/2})$ and $\tilde{O}(n^{1+(1-\delta)(k/2-1)})$.

Random k-SAT formulas appear a lot easier than their worst-case counterparts. But could this ease simply be a quirk of the specific random model? Said differently, how "robust" are our conclusions (and our algorithms) with respect to the specific, and rather arbitrary, choice of the random model for the formulas? Such questions [8] were posed in pioneering works of Blum and Spencer and later Feige and Kilian in the 1990s for graph problems. In 2007, Feige [7] proposed a *semi-random* model to formally tackle this question for k-SAT. Feige's goal was to pose a model where an instance is chosen by a combination of random and worst-case choices. The random choices will hopefully steer clear of the worst-case hard formulas while the worst-case component would, in principle, prevent overfitting to specific, brittle properties of a specific random model. Formally, he proposed the *smoothed model* of j-SAT where a formula is chosen by 1) starting with an arbitrary, worst-case k-SAT formula, and, 2) perturbing each literal pattern (i.e., negation pattern on each literal appearing in every clause) independently with some small constant probability, say, 0.1. If the number of clauses $m \geq O(n)$ then such a formula is unsatisfiable with high probability no matter what formula we begin with. Feige asked the question of whether such smoothed k-SAT formulas admit efficient refutation algorithms and in particular, are they easier than worst-case and in fact, as easy as random k-SAT formulas?

The algorithms that work for random k-SAT formulas strongly exploit the randomness in the variables appearing in the clauses – an aspect completely lost in the smoothed model where the only randomness is the random perturbation of worst-case literal patterns that we begin with. Nevertheless, he managed to find new combinatorial techniques that, when combined with some spectral methods allow *weak*[1] refutation algorithms for such smoothed 3-SAT formulas. These ideas, however, did not yield strong refutation algorithms for 3-SAT and did not generalize to k-SAT for any $k \geq 4$.

In this talk, we presented recent progress and some surprising applications thereof on Feige's smoothed model. In a joint work with Abascal and Guruswami [1], we found *strong* refutation algorithms for smoothed k-SAT formulas with $\tilde{O}(n^{k/2})$ clauses based on new combination of combinatorial and spectral methods. These results were then generalized to obtain the same running time vs clause density trade-off (i.e., $2^{n^{1-\delta}}$ time for formulas with $\tilde{O}(n^{1+(1-\delta)(k/2-1)})$ clauses) in a later joint work with Manohar and Guruswami [10] based on a new tool called *Kikuchi matrices* combined with a new *regularity decomposition* for hypergraphs.

[1] A weak refutation algorithm certifies unsatisfiability of a 3-SAT formula, as opposed to a strong refutation algorithm that certifies that the every assignment must violate a constant fraction of the clauses in the input formula. The results discussed for random 3-SAT above all yield strong refutation algorithms.

Simpler proof was later found in a joint work with Hsieh and Mohanty [11] and with Munha-Correia and Sudakov.

Somewhat surprisingly, these new algorithms have applications to problems in combinatorics and coding theory that we also discussed in the talk. The principle behind these applications is simple if somewhat strange. In principle, the truth of any mathematical statement can be efficiently encoded into a satisfiability of a 3-SAT formula thus reducing a mathematical problem to understanding whether the formula produced by the reduction is satisfiable. This abstract idea, however, is too general to be useful as a tool for actually establishing mathematical results. In our applications, however, we'd be able to encode the truth of certain kinds of combinatorial statements as the satisfiability of a *family of* SAT formulas and thus, to disprove the truth of such a statement, it is enough to prove that one of these formulas, say a *randomly* chosen member, is unsatisfiable. While this may appear to get us closer to random SAT formulas, the resulting formulas are far from random. In fact, in a precise sense, they can be described by a number of random bits that is significantly smaller (in applications n^ϵ for $\epsilon \ll 1$ or even $\mathsf{poly}\log n$) than the number of variables that disallows straightforward probabilistic analyses. Nevertheless, it turns out that the *analysis of the refutation algorithms for smoothed formulas* above can be adapted with some work to apply to even such randomness-starved formulas. Notice that we do not need any efficient algorithm for proving unsatisfiability of the SAT formula in such an application. The algorithm arises purely as a tool for arguing the unsatisfiability (indeed, we know of no other proofs, in general, for establishing such a result).

The applications of this technique so far include a new cubic (improving on the quadratic) lower bounds on the blocklength of a 3-query locally decodable codes [3], exponential (improving on cubic) lower bounds [12] on the block length of 3-query, linear, locally correctable codes (with applications to almost resolving the Hamada conjecture from the theory of algebraic designs for 4-designs), a super-polynomial lower bound [13] for non-linear 3-query locally correctable codes, the resolution of Feige's conjecture [10] on the hypergraph Moore bound, and improved bounds on three-term arithmetic progressions with random common differences [3, 4]. In the talk, we focused largely on the lower bounds on the local codes.

References

[1] J. Abascal, V. Guruswami, and P. K. Kothari. Strongly refuting all semi-random boolean csps. In *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms, SODA 2021, Virtual Conference, January 10 - 13, 2021*, pages 454–472. SIAM, 2021.

[2] S. R. Allen, R. O'Donnell, and D. Witmer. How to refute a random CSP. *CoRR*, abs/1505.04383, 2015.

[3] O. Alrabiah, V. Guruswami, P. K. Kothari, and P. Manohar. A near-cubic lower bound for 3-query locally decodable codes from semirandom CSP refutation. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20 - 23, 2023*, pages 1438–1448. ACM, 2023.

[4] J. Briët and D. Castro-Silva. On the threshold for szemerédi's theorem with random differences, 2023.

[5] V. Chvátal and E. Szemerédi. Many hard examples for resolution. *J. ACM*, 35(4):759–768, 1988.

[6] A. Coja-Oghlan, A. Goerdt, and A. Lanka. Strong refutation heuristics for random k-sat. In *8th International Workshop on Randomization and Computation, RANDOM 2004, Cambridge, MA, USA, August 22 - 24, 2004, Proceedings*, volume 3122 of *Lecture Notes in Computer Science*, pages 310–321. Springer, 2004.

[7] U. Feige. Refuting smoothed 3cnf formulas. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2007), October 20 - 23, 2007, Providence, RI, USA, Proceedings*, pages 407–417. IEEE Computer Society, 2007.

[8] U. Feige. Introduction to semirandom models. In *Beyond the Worst-Case Analysis of Algorithms*, pages 189–211. Cambridge University Press, 2020.

[9] A. Goerdt and M. Krivelevich. Efficient recognition of random unsatisfiable k-sat instances by spectral methods. In *STACS 2001, 18th Annual Symposium on Theoretical Aspects of Computer Science, Dresden, Germany, February 15 - 17, 2001, Proceedings*, volume 2010 of *Lecture Notes in Computer Science*, pages 294–304. Springer, 2001.

[10] V. Guruswami, P. K. Kothari, and P. Manohar. Algorithms and certificates for boolean CSP refutation: smoothed is no harder than random. In *STOC '22: 54th Annual ACM SIGACT Symposium on Theory of Computing, Rome, Italy, June 20 - 24, 2022*, pages 678–689. ACM, 2022.

[11] J. Hsieh, P. K. Kothari, and S. Mohanty. A simple and sharper proof of the hypergraph moore bound. In *Proceedings of the 2023 ACM-SIAM Symposium on Discrete Algorithms, SODA 2023, Florence, Italy, January 22 - 25, 2023*, pages 2324–2344. SIAM, 2023.

[12] P. K. Kothari and P. Manohar. An exponential lower bound for linear 3-query locally correctable codes. *CoRR*, abs/2311.00558, 2023.

[13] P. K. Kothari and P. Manohar. Superpolynomial lower bounds for smooth 3-lccs and sharp bounds for designs. *FOCS*, 2024.

[14] P. K. Kothari, R. Mori, R. O'Donnell, and D. Witmer. Sum of squares lower bounds for refuting any CSP. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19 - 23, 2017*, pages 132–145. ACM, 2017.

[15] P. Raghavendra, S. Rao, and T. Schramm. Strongly refuting random csps below the spectral threshold. *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19 - 23, 2017*, pages 121–131, 2017.

Meta-complexity, One-way Functions and Zero Knowledge

Shuichi Hirahara

(joint work with Mikito Nanashima)

This talk consists of two parts. In the first part, I survey recent progress towards eliminating Heuristica via meta-complexity. In the second part, I present new characterizations of the existence of one-way functions by worst-case complexities of zero knowledge, based on the joint work with Mikito Nanashima [HN24].

1. Meta-complexity

Although $\mathsf{P} \neq \mathsf{NP}$ is the central open problem in complexity theory, it does not provide an efficient way to generate hard instances of NP, which makes $\mathsf{P} \neq \mathsf{NP}$ irrelevant in practice. More relevant is whether NP is hard on average, e.g., $\mathsf{DistNP} \not\subseteq \mathsf{AvgP}$, which means that there exists a polynomial-time samplable distribution with respect to which NP is hard on average. Whether $\mathsf{P} \neq \mathsf{NP}$ and

$\mathsf{DistNP} \not\subseteq \mathsf{AvgP}$ are equivalent is a central open problem in complexity theory, known as “excluding Heuristica from Impagliazzo’s five possible worlds [Imp95]”. This is an important step towards another significant problem of constructing a one-way function whose security is based on the worst-case hardness of NP, known as the problem of excluding Heuristica and Pessiland from Impagliazzo’s five possible worlds.

There are three types of barriers that explain why standard proof techniques are incapable of ruling out Heuristica: limits of (nonadaptive) black-box reductions [FF93, BT06], impossibility of hardness amplification [Vio05], and relativization barriers [Imp11, HN21]. Thus, it is crucial to develop new proof techniques that are not subject to these barriers.

Meta-complexity — complexity of problems that ask for complexity — played a key role in developing proof techniques that bypass the barriers. The Minimum Circuit Size Problem (MCSP) asks for the size of a minimum circuit that computes a given function $f\colon \{0,1\}^n \to \{0,1\}$ (encoded as the truth table of length 2^n). Using such meta-computational problems, it was shown that each barrier can be overcome:

- In [Hir23], we showed the equivalence between the average-case complexity of MCSP with respect to the uniform distribution and the worst-case complexity of $\mathsf{GapMCSP}$ (an approximate version of MCSP). This is proved by non-black-box reductions and bypasses the limits of black-box reductions [BT06].
- In [Hir21], we showed that $\mathsf{NP} \not\subseteq \mathsf{DTIME}(2^{O(n/\log n)})$ implies $\mathsf{DistNP} \not\subseteq \mathsf{Avg_P P}$, which eliminates a strong variant of Heuristica. This result cannot be proved by neither black-box reductions [BT06] nor hardness amplification [Vio05].
- In [Hir22], we showed that the partial function variant of $\mathsf{GapMCSP}$, denoted by $\mathsf{GapMCSP}^*$, is NP-complete. This result does not relativize [Ko91].

What remains to rule out Heuristica is to combine these proof techniques and to bypass the barriers *simultaneously.* A specific approach for ruling out Heuristica is to extend the NP-completeness of $\mathsf{GapMCSP}^*$ to $\mathsf{GapMCSP}$. Then, it follows from the worst-case to average-case connection of [Hir23] that the worst- and average-case complexities of NP are equivalent. Ilango [Ila23] showed that this approach can be realized under the random oracle model, by proving that NP reduces to $\mathsf{GapMCSP}^{\mathcal{O}}$ for a random oracle $\mathcal{O}$.

2. One-way functions and zero knowledge

Although it remains open whether Heuristica can be ruled out unconditionally, Hirahara and Nanashima [HN24] ruled out Heuristica and Pessiland *if* NP has zero knowledge systems, which provides new worst-case characterizations of one-way functions.

A zero knowledge proof system for a language L is a system in which a prover convinces a polynomial-time verifier that an input is in L without revealing any other information. The celebrated theorem of Goldreich, Micali and Wigderson [GMW91] shows that a one-way function is *sufficient* for constructing a zero knowledge proof system for every problem in NP. Ostrovsky and Wigderson [OW93] studied whether a one-way function is *necessary*, and showed that the average-case hardness of computational zero knowledge implies the existence of a one-way function. Their work leaves as a main open problem a gap between the average- and worst-case complexities of zero knowledge.

[HN24] presents characterizations of the existence of a one-way function based on worst-case complexities of zero knowledge. Specifically, the following are equivalent.

- A one-way function exists.
- Every problem in NP has a computational zero knowledge proof system, and $\mathsf{NP} \not\subseteq \mathsf{i.o.P/poly}$ (i.e., NP is hard in the worst case for polynomial-size circuits).

This equivalence does not refer to meta-complexity, yet meta-complexity plays a key role in the proof.[1]

The statements above are also equivalent to the following.

- $\mathsf{GapMCSP}$ has a computational zero knowledge proof system, and some worst-case hard problem has a computational zero knowledge proof system.

References

[BT06] Andrej Bogdanov and Luca Trevisan. On Worst-Case to Average-Case Reductions for NP Problems. *SIAM J. Comput.*, 36(4):1119–1159, 2006.

[FF93] Joan Feigenbaum and Lance Fortnow. Random-Self-Reducibility of Complete Sets. *SIAM J. Comput.*, 22(5):994–1005, 1993.

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that Yield Nothing But Their Validity for All Languages in NP Have Zero-Knowledge Proof Systems. *J. ACM*, 38(3):691–729, 1991.

[Hir21] Shuichi Hirahara. Average-case hardness of NP from exponential worst-case hardness assumptions. In *Proceedings of the Symposium on Theory of Computing (STOC)*, pages 292–302, 2021.

[Hir22] Shuichi Hirahara. NP-Hardness of Learning Programs and Partial MCSP. In *Proceedings of the Symposium on Foundations of Computer Science (FOCS)*, pages 968–979, 2022.

[Hir23] Shuichi Hirahara. Non-Black-Box Worst-Case to Average-Case Reductions Within NP. *SIAM J. Comput.*, 52(6):S18–349, 2023. A preliminary version appeared in FOCS'18.

[HN21] Shuichi Hirahara and Mikito Nanashima. On Worst-Case Learning in Relativized Heuristica. In *Proceedings of the Symposium on Foundations of Computer Science (FOCS)*, pages 751–758, 2021.

[HN24] Shuichi Hirahara and Mikito Nanashima. One-Way Functions and Zero Knowledge. In *Proceedings of the Symposium on Theory of Computing (STOC)*, pages 1731–1738, 2024.

[1] Although it is possible to present a proof without explicitly using meta-complexity, the proof is more natural if meta-computational problems, such as $\mathsf{GapMCSP}$ and $\mathsf{GapMINKT}$, are used.

[Ila23] Rahul Ilango. SAT Reduces to the Minimum Circuit Size Problem with a Random Oracle. In *Proceedings of the Symposium on Foundations of Computer Science (FOCS)*, pages 733–742, 2023.

[Imp95] Russell Impagliazzo. A Personal View of Average-Case Complexity. In *Proceedings of the Structure in Complexity Theory Conference*, pages 134–147, 1995.

[Imp11] Russell Impagliazzo. Relativized Separations of Worst-Case and Average-Case Complexities for NP. In *Proceedings of the Conference on Computational Complexity (CCC)*, pages 104–114, 2011.

[Ko91] Ker-I Ko. On the Complexity of Learning Minimum Time-Bounded Turing Machines. *SIAM J. Comput.*, 20(5):962–986, 1991.

[OW93] Rafail Ostrovsky and Avi Wigderson. One-Way Fuctions are Essential for Non-Trivial Zero-Knowledge. In *Proceedings of the Symposium on Theory of Computing (STOC)*, pages 3–17, 1993.

[Vio05] Emanuele Viola. On Constructing Parallel Pseudorandom Generators from One-Way Functions. In *Proceedings of the Conference on Computational Complexity (CCC)*, pages 183–197, 2005.

The Lens of Abelian Embedding

Dor Minzer
(joint work with Amey Bhangale, Subhash Khot)

The primary topic of this talk is the approximation dichotomy conjecture and some progress towards it. We also discuss relations to discrete Fourier analysis, multi-player parallel repetition, additive combinatorics and more. To describe the conjecture we begin with some background.

Setup: let Σ be a finite alphabet and let $k \in \mathbb{N}$ be a parameter; we think of both $|\Sigma|$ and of k as constants. Given a collection of predicates $\mathcal{P} \subseteq \{P\colon \Sigma^k \to \{0,1\}\}$, we define an associated constraints satisfaction problem CSP-$\mathcal{P}$, as follows. An instance (X, E) of CSP-$\mathcal{P}$ is composed of a set of variables X and a collection E of constraints of the form $P(x_{i_1}, \ldots, x_{i_k}) = 1$, where $x_{i_1}, \ldots, x_{i_k} \in X$ are variables and P is a predicate from the collection $\mathcal{P}$.

The Dichotomy Theorem: with the definition of CSP-$\mathcal{P}$ in mind, one can consider the decision problem of determining satisfiability of instances CSP-$\mathcal{P}$. By that, we mean that for a fixed collection $\mathcal{P}$, we may consider the problem of deciding whether an instance $\Psi = (X, E)$ of CSP-$\mathcal{P}$ is satisfiable or not. Schaefer Theorem [15] asserts that for Boolean alphabets, i.e. for $|\Sigma| = 2$, the decision problem CSP-$\mathcal{P}$ is always either in the class P or else it is NP-hard. Feder and Vardi [17] conjectured that this result extends to all finite alphabets: this is the well known dichotomy conjecture. The dichotomy conjecture has been open for a long time until it was resolved independently by Zhuk [16] and Bulatov [11]. In words, the dichotomy theorem asserts that the complexity of CSP-$\mathcal{P}$ can never be intermediate: it is either computationally tractable (in the class P), or else it is computationally hard (namely, NP-hard).

Raghavendra's Theorem: Raghavendra [14] established a similar dichotomy behaviour for approximation problems, albeit in the case of almost satisfiable instances. Towards stating this result, we define the promise problem gap-CSP-$\mathcal{P}[c,s]$ for $0 \leq s \leq c \leq 1$: in this problem one is given an instance Ψ of CSP-$\mathcal{P}$ promised to either be at least c-satisfiable (namely, there is an assignment satisfying at least c fraction of the constraints), or at most s-satisfiable (namely, no assignment satisfies more than s fraction of the constraints), and the goal is to distinguish between these two cases. With this in mind, Raghavendra proved that for all finite alphabets, k and collections of predicates $\mathcal{P}$ and for all $0 < c < 1$, there exists a number s such that gap-CSP-$\mathcal{P}[c,s]$ can be solved in polynomial time, but for all $\delta > 0$ the problem gap-CSP-$\mathcal{P}[c,s+\delta]$ is NP-hard (assuming the Unique-Games Conjecture [13]). In fact, Raghavendra gives a polynomial time algorithm for solving gap-CSP-$\mathcal{P}[c,s]$, which consists of solving the natural semidefinite programming relaxation of the problem and then applying an appropriate Gaussian rounding scheme.

Satisfiable instances versus almost satisfiable instances: Ragahvendra's theorem [14] does not address the case of satisfiable instances, and at first glance it may seem as a mere technicality. After all, what is the big difference between almost satisfiable instances and fully satisfiable instances? Alas, it turns out that this makes a dramatic difference for some problems. Consider, for instance, the problem 3-Lin$_{\mathbb{F}_2}$, in which one is given a system of linear equations over $\mathbb{F}_2$ wherein each equation contains 3 variables; the goal is to find an assignment satisfying as many of the equations as possible. If the instance is promised to be satisfiable, then one can perform the Gaussian elimination algorithm and thereby find a satisfying assignment in polynomial time. Thus, gap-CSP-3LIN$[1,s]$ is in P for every $s < 1$. However, if the instance is only promised to be c-satisfiable for $c < 1$ (which may be very close to 1), a well known result of Håstad [12] shows that the best one can do is a random guessing algorithm, and in fact that gap-CSP-3LIN$[c,1/2+\delta]$ is NP-hard for all $\delta > 0$. This brings us to the main question that we considered in the talk: for what predicates can there be such a dramatic difference between satisfiable instances and almost satisfiable instances?

Abelian embeddings: in [3], we suggest that the notion of Abelian embeddings plays a crucial role in the above question. We say a predicate $P\colon \Sigma_1 \times \cdots \times \Sigma_k \to \{0,1\}$ has a non-trivial Abelian embedding if there exists an Abelian group $(G,+)$ and maps $\sigma_i\colon \Sigma_i \to G$ for $i = 1,\ldots,k$, not all constant, such that

$$\forall (x_1,\ldots,x_k) \in \prod_{i=1}^{k} \Sigma_i, \qquad P(x_1,\ldots,x_k) = 1 \Rightarrow \sigma_1(x_1) + \ldots + \sigma_k(x_k) = 0_G.$$

In words, the definition says that after applying the re-labelings $\sigma_1,\ldots,\sigma_k$ of the alphabets $\Sigma_1,\ldots,\Sigma_k$, the support of P is contained in the set of solutions to a linear equation over G. We conjecture that, in some sense, there could only be a difference between the complexity of the problems gap-CSP-$P[1,s]$ and gap-CSP-$P[1-\varepsilon,s]$ if P admits non-trivial Abelian embeddings.[1] In the talk we discussed

[1] The precise formulation has to do with the structure of integrality gaps for the natural semidefinite programming relaxation of gap-CSP-$P[1,s]$, and we do not elaborate on it for simplicity.

relationship between this problem and the following analytical problem: let μ be a distribution over $P^{-1}(1)$; what 1-bounded functions $f_i\colon \Sigma_i^k \to \mathbb{C}$ can satisfy that

$$\left| \mathop{\mathbb{E}}_{(x_1,\ldots,x_k)\sim\mu^{\otimes n}} [f_1(x_1)\cdots f_k(x_k)] \right| \geq \Omega(1)?$$

We discussed some progress on the case that $k = 3$ from the works [5, 6, 7, 8]. In particular, we discussed the solution to the above inverse problem and argued that under mild assumptions about μ, any f_1, f_2, f_3 achieving such non-trivial 3-wise correlations must come from "Fourier characters" and "low-degree functions". We discussed applications of this result to the problem of restricted 3-AP free subsets of $\mathbb{F}_p^n$ from [4] and to 3-player parallel repetition theorem of the GHZ game [9] and more generally of 3-XOR games [1, 2].

The hybrid algorithm: lastly, we discussed the hybrid algorithm from [8]. This is a candidate optimal approximation algorithm for certain classes of constraints satisfaction problems (that include CPSs with sufficient symmetries). This algorithm consists of solving the natural semi-definite programming relaxation of the problem as well as solving a certain system of linear equations over an Abelian group associated with the predicate, and then applying some rounding function. We analyze this algorithm for some class of predicates and show a dictatorship test that matches the performance of this algorithm, giving evidence that this is indeed the best efficient approximation algorithm (assuming a variant of the Unique-Games Conjecture called the Rich 2-to-1 Games Conjecture [10]).

References

[1] Amey Bhangale, Mark Braverman, Subhash Khot, Yang P. Liu, and Dor Minzer. Parallel repetition for 3-player XOR games.

[2] Amey Bhangale, Mark Braverman, Subhash Khot, Yang P. Liu, and Dor Minzer. Parallel repetition of k-player projection games. *Electron. Colloquium Comput. Complex.*, TR23-198, 2023.

[3] Amey Bhangale, Subhash Khot, and Dor Minzer. On approximability of satisfiable k-csps: I. In STOC 2022.

[4] Amey Bhangale, Subhash Khot, and Dor Minzer. Effective bounds for restricted 3-arithmetic progressions in fp^{n}. *CoRR*, abs/2308.06600, 2023.

[5] Amey Bhangale, Subhash Khot, and Dor Minzer. On approximability of satisfiable k-csps: II. In STOC 2023.

[6] Amey Bhangale, Subhash Khot, and Dor Minzer. On approximability of satisfiable k-csps: III. In STOC 2023.

[7] Amey Bhangale, Subhash Khot, and Dor Minzer. On approximability of satisfiable k-csps: IV. In STOC 2024.

[8] Amey Bhangale, Subhash Khot, and Dor Minzer. On approximability of satisfiable k-csps: V. 2024+.

[9] Mark Braverman, Subhash Khot, and Dor Minzer. Parallel repetition for the GHZ game: Exponential decay. In FOCS 2023.

[10] Mark Braverman, Subhash Khot, and Dor Minzer. On rich 2-to-1 games. In ITCS 2021.

[11] Andrei A. Bulatov. A dichotomy theorem for nonuniform csps. In FOCS 2017.

[12] Johan Håstad. Some optimal inapproximability results. *J. ACM*, 48(4):798–859, 2001.

[13] Subhash Khot. On the power of unique 2-prover 1-round games. In CCC 2002.

[14] Prasad Raghavendra. Optimal algorithms and inapproximability results for every csp? In STOC 2008.
[15] Thomas J Schaefer. The complexity of satisfiability problems. In STOC 1978.
[16] Dmitriy Zhuk. A proof of the CSP dichotomy conjecture. *J. ACM*, 67(5):30:1–30:78, 2020.
[17] Tomás Feder and Moshe Y Vardi. Monotone monadic snp and constraint satisfaction. In STOC 1993.

Pseudorandom permutations and unitaries: recent developments

Ryan O'Donnell

In this talk, we survey some recent developments in the construction of pseudorandom subsets of (families of)groups G_N, with particular attention being paid to the symmetric groups $G_N = \mathrm{Sym}(N)$ and the unitary groups $G_N = \mathrm{U}(N)$, where $N = 2^n$. Other possibilities include $G_N = \mathbb{F}_2^N$ (though this is already extremely well-studied) and the orthogonal groups $G_N = \mathrm{O}(N)$.

We first argue that a good notion of pseudorandomness is that of fooling *representations*. Specifically, if $\rho : G_N \to \{d \times d \text{ matrices}\}$ is a representation (meaning $\rho(gh) = \rho(g)\rho(h)$), we say that a (multi)set $D \subseteq G_N$ *ϵ-fools* ρ if

$$\left\| \mathop{\mathbf{E}}_{\mathbf{g}\sim D}[\rho(\mathbf{g})] - \mathop{\mathbf{E}}_{\mathbf{g}\sim G_N}[\rho(\mathbf{g})] \right\| \leq \epsilon. \tag{1}$$

Here $\mathbf{g} \sim G_N$ denotes that $\mathbf{g}$ is drawn from the uniform/Haar distribution. As an example, when $G_N = \mathbb{F}_2^N$ we have the $d = 1$ representations $\rho = \chi_S : x \mapsto \prod_{i\in S}(-1)^{x_i}$. If D ϵ-fools all of these it is an ""ϵ-biased set"; if D ϵ-fools just those with $|S| \leq k$, it is "ϵ-approximate k-wise independent".

The main case we focus on is when G_N is a group of $N \times N$ matrices (e.g., $\mathrm{Sym}(N)$ thought of as permutation matrices, or $\mathrm{U}(N)$), and when ρ is the representation $\rho_k : M \mapsto M^{\otimes k/2} \otimes \overline{M}^{\otimes k/2}$. (This is just $M \mapsto M^{\otimes k}$ for real matrices M.) In this case, $\rho_k(M)$ encodes all the degree-k monomials in the entries of M, and a set $D \subseteq G_N$ that ϵ-fools ρ_k can be thought of as "ϵ-approximately k-wise independent" (or an "ϵ-approximate k-design").

In addition to the usual pseudorandomness goal of constructing small sets D that are ϵ-approximately k-wise independent, significant attention has been paid recently to finding sets D in which all elements $g \in D$ have *highly efficient circuit representations.* Here, in the case of $G_N = \mathrm{Sym}(2^n)$, we wish for each $g \in D$ to be computable by a small n-bit *reversible circuit* with gates of fan-in/out, say, 3. In the case of $G_N = \mathrm{U}(2^n)$, we wish for each $g \in D$ to be computable by a small n-qubit *quantum circuit* with gates of fan-in/out at most 2 or 3. For practical reasons, we may even wish for additional structure/simplicity, such as circuits of low *depth*, circuits with only nearest-neighbor gates, or "brickwork" circuits (meaning ones with complete layers of nearest-neighbor gates). See Figure 1 for depictions.

One way to construct small k-designs is to show that the set $D_1 = \{\text{a single gate}\}$ is $(1 - \delta)$-fooling for ρ_k. Then it is not hard to show that $D_T = \{\text{all circuits of } T \text{ gates}\}$ is ϵ-fooling provided $T \geq \ln(1/\epsilon)/\delta$. One most often wants $\epsilon = 1/N^{Ck}$

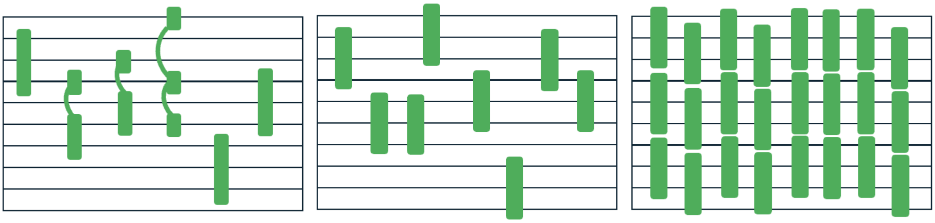

FIGURE 1. The first circuit is an example of a circuit with generic 3-bit gates. The second is an example of a circuit with 1D nearest-neighbor 3-bit gates. The third is an example of a brickwork circuit.

(since $\rho_k(g)$ is $N^k \times N^k$ when $g \in G_N$), and this means that circuits of size $T = O(nk/\text{"gap"})$ suffice, where "gap" denotes δ.

In the last part of the talk, we describe past and present results for constructing ϵ-approximate k-wise independent subsets of $\mathrm{Sym}(N)$ and $\mathrm{U}(N)$, including:

- Works [Gow96, HMMR05, BH08, FI24, HO24] that bound "gap" for a single classical reversible gate. The last work mentioned shows the gap is at least $\frac{1}{n \cdot \tilde{O}(k)}$, meaning that random reversible circuits of size $n^2 \cdot \tilde{O}(k)$ are good k-designs for $\mathrm{Sym}(2^n)$. Indeed, this is shown even for brickwork circuits of depth $n \cdot \tilde{O}(k)$.
- Works [BHH16, HHJ21, OSP23] that bound "gap" for a single quantum gate. These works achieve that gap is at least $\frac{1}{n \cdot \mathrm{poly}(k)}$, meaning that random quantum circuits of size $n^2 \cdot \mathrm{poly}(k)$ are good k-designs for $\mathrm{U}(2^n)$. Again, this is shown even for brickwork circuits of depth $n \cdot \mathrm{poly}(k)$.
- Works [KNR09, OSP23] that use pseudorandomness technology to show that only $O(nk)$ bits of true randomness are needed to draw from such designs.
- Works [Kas07, CK23] giving constant-size sets $D \subseteq \mathrm{Sym}(N)$ (of seemingly small circuit complexity) that $(1 - \Omega(1))$-fool *all* representations.

Connections to classical and quantum cryptography were also discussed, as well as additional works with improved results appearing online right around the time of the talk, including [GHP24, CHH$^+$24].

References

[BH08] Alex Brodsky and Shlomo Hoory. Simple Permutations Mix Even Better. *Random Structures & Algorithms*, 32(3):274–289, 2008.

[BHH16] Fernando G.S.L. Brandao, Aram W. Harrow, and Michał Horodecki. Local Random Quantum Circuits are Approximate Polynomial-Designs. *Communications in Mathematical Physics*, 346:397–434, 2016.

[CHH$^+$24] Chi-Fang Chen, Jeongwan Haah, Jonas Haferkamp, Yunchao Liu, Tony Metger, and Xinyu Tan. Incompressibility and spectral gaps of random circuits. *arXiv preprint arXiv:2406.07478*, 2024.

[CK23] Pierre-Emmanuel Caprace and Martin Kassabov. Tame automorphism groups of polynomial rings with property (T) and infinitely many alternating group quotients. *Transactions of the American Mathematical Society*, 376(11):7983–8021.

[FI24] Xiaozhou Feng and Matteo Ippoliti. Dynamics of pseudoentanglement. *arXiv preprint arXiv:2403.09619*, 2024.

[GHP24] Lucas Gretta, William He, and Angelos Pelecanos. More efficient approximate k-wise independent permutations from random reversible circuits via log-sobolev inequalities. *Cryptology ePrint Archive*, 2024.

[Gow96] W. Timothy Gowers. An Almost m-wise Independent Random Permutation of the Cube. *Combinatorics, Probability and Computing*, 5(2):119–130, 1996.

[HHJ21] Jonas Haferkamp and Nicholas Hunter-Jones. Improved Spectral Gaps for Random Quantum Circuits: Large Local Dimensions and All-to-All Interactions. *Physical Review A*, 104(2):022417, 2021.

[HMMR05] Shlomo Hoory, Avner Magen, Steven Myers, and Charles Rackoff. Simple Permutations Mix Well. *Theoretical Computer Science*, 348(2-3):251–261, 2005.

[HO24] William He and Ryan O'Donnell. Pseudorandom permutations from random reversible circuits. Manuscript.

[KNR09] Eyal Kaplan, Moni Naor, and Omer Reingold. Derandomized Constructions of k-wise (almost) Independent Permutations. *Algorithmica*, 55(1):113–133, 2009.

[Kas07] Martin Kassabov. Symmetric Groups and Expander Graphs. *Inventiones Mathematicae*, 170(2):327–354, 2007.

[OSP23] Ryan O'Donnell, Rocco A. Servedio, and Pedro Paredes. Explicit Orthogonal and Unitary Designs. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1240–1260. IEEE, 2023.

Recent Developments of SNARGs

Yael Tauman Kalai

In this talk we focused on the problem of constructing succinct non-interactive arguments (SNARGs) for NP. Fix any NP language L. For any $x \in L$ with a corresponding witness w, the goal is for a prover, who is given (x, w), to prove to a verifier that $x \in L$, where the length of the proof is succinct, i.e., significantly smaller than the length of the witness w. Both the prover and the verifier are required to be efficient. Namely, the prover is required to run in time $\mathsf{poly}(|x|, |w|)$ and the verifier who is given x and a proof π, is required to run in time $\mathsf{poly}(|x|, |\pi|)$.

This task is only possible if we relax the soundness condition to be a computational one, where we require soundness to hold only against cheating provers who are computationally bounded. The reason is that we do not expect that it is possible to shrink any witness w into a more succinct one that can be verified efficiently. Instead this is achieved by assuming that both the prover and verifier have access to a common random string (CRS), in which a cryptographic assumption is embedded. The (computational) soundness requirement is that for every $x \notin L$ and for every polynomial-time cheating prover P^*, the probability that $P^*(x, \mathsf{CRS})$ outputs an accepting proof π is negligible. A proof system where the soundness guarantee is only computational is called an *argument*, and such succinct non-interactive argument systems are called SNARGs.

The holy grail in this area is to construct SNARGs for all of NP under standard cryptographic assumptions. Starting with the seminal work of Micali [1] there were many results that construct SNARGs for NP under non-standard assumptions or in idealized models (such as the random oracle model). Sahai and Waters [2] construct a SNARG for NP assuming indistinguishability obfuscation (iO), though in this SNARG CRS is not random, and is instead structured and also long (as long as the instance and witness). While recently, Jain, Lin and Sahai [3] constructed iO under standard assumptions, these assumptions are quantumly broken and also rely on sub-exponential hardness.

In this talk we presented a recent result due to Jin, Kalai, Lombardi and Mathialagan that under the LWE assumption (which is a standard cryptographic assumption believed to be post-quantum secure), constructs a universal SNARG for NP. Namely, for every language $L \in \mathsf{NP}$ and for every length bounds ℓ_{crs} and ℓ_{proof}, they construct a SNARG with CRS of length $\mathsf{poly}(\ell_{\mathsf{crs}})$ and proof length $\mathsf{poly}(\ell_{\mathsf{proof}})$, and argue that if there *exists* any SNARG for L with CRS of length ℓ_{crs} and proof length ℓ_{proof} that has a poly-size Extended Proof of correctness, then their construction is sound under LWE.

Moreover, they prove something stronger: their SNARG is sound under LWE even if there exists a two-message argument for L where the first message from the verifier to the prover (which may depend on the instance x) is of length ℓ_{crs} and the second message from the prover to the verifier is of length ℓ_{proof} (and may require the secret state of the verifier to verify), assuming this 2-message argument has a poly-size Extended Proof of correctness. As a corollary they conclude that their SNARG is secure assuming the existence of a witness encryption which has a poly-size Extended Proof of correctness. A witness encryption is a weaker primitive than iO and is known to imply the existence of a two-message argument for NP where the message from the prover to the verifier is succinct. The techniques used to obtain this result heavily rely on a recent work due to Jin, Kalai, Lombardi and Vaikuntanathan [4].

References

[1] S. Micali, *CS Proofs (Extended Abstracts)*, 35th Annual Symposium on Foundations of Computer Science, 436–453.

[2] A. Sahai and B. Waters, *How to use indistinguishability obfuscation: deniable encryption, and more*, Symposium on Theory of Computing, STOC 2014, 475–484.

[3] A. Jain, H. Lin, and A. Sahai. *Indistinguishability Obfuscation from Well-Founded Assumptions*, Commun. ACM 67(3): 97-105 (2024)

[4] Z. Jin, Y. Kalai, A. Lombradi and V. Vaikuntanathan, *SNARGs under LWE via Propositional Proofs*, Symposium on Theory of Computing, STOC 2024, 24-28.

The Parameterized Inapproximability Hypothesis

Venkatesan Guruswami

(joint work with Bingkai Lin, Xuandi Ren, Yican Sun, Kewen Wu)

Abstract. The Parameterized Inapproximability Hypothesis (PIH) asserts that no fixed parameter tractable (FPT) algorithm can distinguish a satisfiable CSP instance, parameterized by the number of variables, from one where every assignment fails to satisfy an ϵ fraction of constraints for some absolute constant $\epsilon > 0$. PIH plays the role of the PCP theorem in parameterized complexity, with many downstream inapproximability consequences. This talk introduced the context and statement of the PIH, and then gave a high level view of a recent proof showing that the well-known Exponential Time Hypothesis (ETH) implies the PIH. Previously PIH had only been established under Gap-ETH, a very strong assumption with an inherent gap.

We begin with some basic definitions concerning parameterized complexity and CSP before stating the PIH formally.

Fixed parameter tractability. In parameterized complexity, each input instance x of a problem of interest is associated with a parameter $k := k(x)$, and we treat the input as the pair $(x; k)$. A fixed parameter tractable (FPT) algorithm is one which runs in time $f(k)|x|^c$ for an arbitrary computable function $f : \mathbb{N} \to \mathbb{N}$ and a finite c. That is, we decouple the dependence of the runtime on the parameter k and the instance size $|x|$, and allow super-polynomial (or indeed arbitrary) dependence on the parameter k which is to be thought of as a growing parameter that is much smaller than the instance size $n := |x|$.

A language L is said to belong to FPT if there is an FPT algorithm that on input instance $(x; k)$ correctly determines if $x \in L$ in time $f(k)|x|^c$.

For instance, the Vertex Cover problem, consisting of instances $(G; k)$ where G is a graph that has a vertex cover of size k is in FPT, as it admits an algorithm running in time $O(2^k n)$, that is much better than the brute force n^k algorithm for small values of the parameter k. The Clique problem, consisting of instances $(G; k)$ where G is a graph that has a clique of size k, on the other hand, is not believed to be in FPT. In fact, no algorithm with running time $n^{o(k)}$ is known for this problem, and indeed such an algorithm is ruled out under the ETH (which states that 3SAT on n variable instances requires $2^{\Omega(n)}$ time). The parameterized Clique problem is complete for the class $W[1]$ (under FPT reductions), and $W[1] \neq \text{FPT}$ is the counterpart of the NP $\neq$ P assumption in the parameterized world.

CSP. A constraint satisfaction problem (CSP) instance consists of a directed graph $G = (V, E)$, an alphabet Σ, and a relation $R_e \subseteq \Sigma \times \Sigma$ for each edge $e = (u, v) \in E$ which constrains the values to be assigned to u, v. (Here we are defining arity two CSPs, which are of sufficient generality for our purposes.) The goal is to find an assignment $\sigma : V \to \Sigma$ that maximizes the fraction of "satisfied" edges $e = (u, v)$ for which $(\sigma(u), \sigma(v)) \in R_e$, and in the optimization version to maximize the fraction of satisfied constraints/edges.

Parameterized CSP. Usually for a CSP, we treat the alphabet Σ as fixed and the number of variables $|V|$ as growing. For parameterized CSPs, the alphabet Σ is considered as growing (so $n := |\Sigma|$ is the input size) and we treat the number of variables $|V|$ as the parameter k. Note that there is a brute force $|\Sigma|^{|V|} = n^k$ time algorithm to determine the optimum solution to a parameterized CSP.

One can easily encode the $W[1]$-hard Multicolored k-Clique problem (where the vertices are partitioned into k parts and the goal is to find a k-clique with one vertex per part) as a parameterized CSP, and thus the problem in general is $W[1]$-hard. The PIH asserts the *inapproximability* of parameterized CSP, akin to how the PCP theorem shows hardness of approximating CSP.

Parameterized Inapproximability Hypothesis (PIH). There is an absolute constant $\epsilon > 0$ such that no FPT algorithm can distinguish satisfiable instances of a parameterized CSP (with number of variables as the parameter) from instances where every assignment fails to satisfy more than ϵ fraction of the constraints.

The PIH was implicitly mentioned in several works as the surrogate of the PCP theorem in the parameterized world, and explicitly highlighted in [6]. PIH unifies several inapproximability results for fundamental parameterized problems like k-Clique and k-Set-Cover that were established using ingenious, problem-specific techniques. It is thus a desirable goal for the theory of parameterized approximability.

The main result highlighted in this talk, shown in [4], can be compactly described as:

Theorem 3. *ETH implies PIH.*

In comparison, previously PIH was known under the assumption of linear-sized PCPs, or the implied Gap-ETH [3] which asserts that even approximating 3SAT within some constant factor (as opposed to solving it exactly) requires $2^{\Omega(n)}$ time.

The proof of Theorem 3 in [4] proceeds in two steps: (i) a reduction from 3SAT to a special vector-structured CSP called VecCSP , and (ii) a "short" PCP for testing satisfiability of VecCSP. The identification of the specific form of VecCSP, which is general enough to accommodate the reduction step (i), and at the same time highly structured enough to facilitate the design of the PCP in step (ii), is one of the crucial insights and contributions of our work [4].

The (parameterized) VecCSP instances have k variables V (where k is thought of as the parameter) each to take as values vectors in $\mathbb{F}^d$ over some fixed finite field. The constraints are of two kinds: (a) parallel, and (b) linear. A parallel constraint between $u, v \in V$ is specified by a relation $\Pi_{u,v} \subset \mathbb{F} \times \mathbb{F}$, and the vector assignments $\sigma(u), \sigma(v) \in \mathbb{F}^d$ should satisfy $(\sigma(u)_i, \sigma(v)_i) \in \Pi_{u,v}$ for each coordinate $i \in \{1, 2, \ldots, d\}$. The key point is that the *same* constraint is applied in parallel to the i'th coordinate for *every* i.

The advantage of parallel constraints is that one can take a PCP for the constraints involving each coordinate independently, and "stack" them together into a PCP that can be checked in parallel by making the same queries into each of the

PCPs. In each coordinate, we have a CSP with k variables and a constant-sized alphabet, so we can construct "short" PCPs whose size only depends on k.

Of course, a VecCSP with only parallel constraints will be easy to decide in FPT time, as one can solve the CSP instance for each coordinate independently. A linear constraint between $u, v \in V$ is specified by a matrix $M_{u,v} \in \mathbb{F}^{d \times d}$ and stipulates that $\sigma(u) = M_{u,v}\sigma(v)$.

The combination of parallel and linear constraints is surprisingly enough to make the VecCSP instance hard, in the sense that an FPT algorithm will lead to a sub-exponential algorithm for 3SAT, contradicting ETH. The talk sketched most details of this reduction, which is based on a sequence of elementary steps which bestow increasingly more structure on the constraints, culminating with the parallel-linear combination mentioned above.

At the same time, the linear constraints turn out to be amenable to testing via the well-known Walsh-Hadamard code PCP, of length exponential in k. Together, we get a reduction from 3SAT on n variables to a parameterized gapCSP on $k = 2^{O(k'^4)}$ variables over an alphabet Σ of size $2^{O(n/k')}$ with a constant gap between completeness and soundness. Chasing through the parameters, assuming ETH this implies a $|\Sigma|^{\Omega(\sqrt[4]{\log k})}$ running time lower bound for approximating parameterized CSP, which in turn rules out an FPT algorithm.

In a recent follow-up to [4], the authors improved the running time lower bound for approximating parameterized CSP within a constant factor to $|\Sigma|^{k^{1-o(1)}}$ which is near-tight [5]. This is based on an even more structured form of VecCSP, and using the Reed-Muller code to design a near-linear size PCP for it, employing constructions and ideas from [2, 1].

References

[1] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, and S. Vadhan. Robust PCPs of proximity, shorter PCPs, and applications to coding. *SIAM Journal on Computing,* 36(4):889?974, 2006.

[2] E. Ben-Sasson, M. Sudan, S. Vadhan, and A. Wigderson. Randomness- efficient low degree tests and short PCPs via epsilon-biased sets. In *Proceedings of the 35th ACM Symposium on Theory of Computing,* pages 612?621, 2003.

[3] P. Chalermsook, M. Cygan, G. Kortsarz, B. Laekhanukit, P. Manurangsi, D. Nanongkai, and L. Trevisan. From gap-ETH to FPT- inapproximability: Clique, dominating set, and more. In *58th IEEE Symposium on Foundations of Computer Science*, pages 743–754, 2017.

[4] V. Guruswami, B. Lin, X. Ren, Y. Sun, and K. Wu. Parameterized Inapproximability Hypothesis under ETH. In *Proceedings of the 56th ACM Symposium on Theory of Computing*, pages 24–35, 2024.

[5] V. Guruswami, B. Lin, X. Ren, Y. Sun, and K. Wu. Almost Optimal Time Lower Bound for Approximating Parameterized Clique, CSP, and More, under ETH. *Electron. Colloquium Comput. Complex.* TR24-075, 2024.

[6] D. Lokshtanov, M. S. Ramanujan, S. Saurabh, and M. Zehavi. Parameterized complexity and approximability of directed odd cycle transversal. In *Proceedings of the ACM-SIAM Symposium on Discrete Algorithms*, pages 2181–2200. 2020.

Recent Developments in the Theory of Randomness Extractors

Xin Li

Randomness extractors are fundamental objects in the study of pseudorandomness. In short, a randomness extractor for a class C of weak random sources with support in $\{0,1\}^n$ is a function $Ext : \{0,1\}^n \to \{0,1\}^m$ such that for any weak source $X \in C$ with entropy $H_\infty(X) \geq k$ for some threshold k, the output distribution over $\{0,1\}^m$ is statistically close to the uniform distribution. Many models of randomness extractors have been studied over the past four decades.

A long line of work in the past two decades or so established close connections between several different randomness extractors and applications, including seeded or seedless non-malleable extractors, two source extractors, (bipartite) Ramsey graphs, privacy amplification protocols with an active adversary, non-malleable codes and many more. These connections essentially show that an asymptotically optimal construction of one central object will lead to asymptotically optimal solutions to all the others. However, despite considerable effort, previous works can get close but still lack one final step to achieve truly asymptotically optimal constructions.

In this talk we describe a recent work [1] that provides the last missing link, thus simultaneously achieving explicit, asymptotically optimal constructions and solutions for various well studied extractors and applications, that have been the subjects of long lines of research. These results include:

- Asymptotically optimal seeded non-malleable extractors, which in turn give two source extractors for asymptotically optimal min-entropy of $O(\log n)$, explicit constructions of K-Ramsey graphs on N vertices with $K = \log^{O(1)} N$, and truly optimal privacy amplification protocols with an active adversary.
- Two source non-malleable extractors and affine non-malleable extractors for some linear min-entropy with exponentially small error, which in turn give the first explicit construction of non-malleable codes against 2-split state tampering and affine tampering with constant rate and *exponentially* small error.
- Explicit extractors for affine sources, sumset sources, interleaved sources, and small space sources that achieve asymptotically optimal min-entropy of $O(\log n)$ or $2s + O(\log n)$ (for space s sources).
- An explicit function that requires strongly linear read once branching programs of size $2^{n-O(\log n)}$, which is optimal up to the constant in $O(\cdot)$. Previously, even for standard read once branching programs, the best known size lower bound for an explicit function is $2^{n-O(\log^2 n)}$.

The formal definitions of these objects and a history of related research can be found in [1]. At the core of the techniques, we show a general way to construct a *one-source* non-malleable condenser from any *multi-source* non-malleable extractor. This construction together with known constructions of multi-source non-malleable extractor with exponentially small error [5] is then used to achieve an asymptotically optimal seeded non-malleable extractor, which in turn gives the improvements of all the applications mentioned above, via various connections established in previous works [3, 6, 8, 4, 2].

There are still interesting and important open problems left. For example, one natural open question is to improve the output length and error of the seedless extractors constructed. Currently for asymptotically optimal entropy, the constructions can only output 1 bit (or a constant number of bits by the techniques in [7]) with constant error, while it is desirable to achieve negligible, or exponentially small error in cryptographic applications. Interestingly, improving the error may also lead to an improvement in output length by the techniques in [7]. As observed in previous works, one possible approach is to design t-non-malleable extractors with better dependence on t, which appears to be a challenging problem. One could also ask if we can construct explicit two-source extractors with entropy $\log n + O(1)$, which would give optimal Ramsey graphs. For non-malleable codes it would be interesting to improve the rates of our codes to optimal. Finally, it is always interesting to find other applications of the pseudorandom objects studied in this literature.

References

[1] Xin Li. Two source extractors for asymptotically optimal entropy, and (many) more. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, 2023.

[2] Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pages 601–610, 2009.

[3] Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functions. *Annals of Mathematics*, 189:653–705, 2019.

[4] Mahdi Cheraghchi and Venkatesan Guruswami. Non-malleable coding against bit-wise and split-state tampering. In *TCC*, pages 440–464, 2014.

[5] Eshan Chattopadhyay and David Zuckerman. Non-malleable codes against constant split-state tampering. In *Proceedings of the 55th Annual IEEE Symposium on Foundations of Computer Science*, pages 306–315, 2014.

[6] Avraham Ben-Aroya, Dean Doron, and Amnon Ta-Shma. An efficient reduction from two-source to nonmalleable extractors: Achieving near-logarithmic min-entropy. *SIAM Journal on Computing*, 51(2):STOC17–31–STOC17–49, 2022.

[7] Xin Li. Improved two-source extractors, and affine extractors for polylogarithmic entropy. In *Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science*, 2016.

[8] Xin Li. Improved non-malleable extractors, non-malleable codes and independent source extractors. In *Proceedings of the 49th Annual ACM Symposium on Theory of Computing*, 2017.

Reporter: Rahul Ilango

Participants

Dr. Amir Abboud
Department of Mathematics
The Weizmann Institute of Science
P.O. Box 26
Rehovot 76 100
ISRAEL

Prof. Dr. Markus Bläser
Fachbereich Informatik
Universität des Saarlandes
Saarland Informatics Campus E1.3
66123 Saarbrücken
GERMANY

Prof. Dr. Peter Bürgisser
Institut für Mathematik
Technische Universität Berlin
Sekretariat MA 3-2
Straße des 17. Juni 136
10623 Berlin
GERMANY

Prof. Dr. Irit Dinur
Department of Computer Science
and Applied Mathematics
The Weizmann Institute of Science
P.O. Box 26
76100 Rehovot
ISRAEL

Dr. Pranjal Dutta
National University of Singapore
Innovation 4.0
NUS-NCS Joint Laboratory for
Cybersecurity, &
School of Computing
Singapore 117417
SINGAPORE

Prof. Dr. Cynthia Dwork
School of Engineering and Applied
Sciences
Harvard University
150 Western Avenue
Boston, MA 02134
UNITED STATES

Dr. Nick Fischer
Department of Computer Science
and Applied Mathematics
The Weizmann Institute of Science
P.O. Box 26
76100 Rehovot
ISRAEL

Prof. Dr. Oded Goldreich
Department of Computer Science
and Applied Mathematics
The Weizmann Institute of Science
P.O. Box 26
Rehovot 76100
ISRAEL

Prof. Dr. Shafi Goldwasser
UC Berkeley
Melvin Calvin Lab
Berkeley, CA 94720
UNITED STATES

Prof. Dr. Venkatesan Guruswami
Departments of EECS and Mathematics
Simons Institute for the Theory of
Computing
University of California, Berkeley
625 Soda Hall
Berkeley, CA 94720-1770
UNITED STATES

Prof. Dr. Johan Håstad
Department of Mathematics
KTH Royal Institute of Technology
100 44 Stockholm
SWEDEN

Prof. Dr. Shuichi Hirahara
National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku
Tokyo 101-8430
JAPAN

William Hoza
Department of Computer Science
The University of Chicago
5730 South Ellis Ave
Chicago, IL 60637
UNITED STATES

Dr. Christian Ikenmeyer
Mathematics Institute
University of Warwick
Coventry CV4 7AL
UNITED KINGDOM

Rahul Ilango
Department of Mathematics
Massachusetts Institute of
Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

Dr. Yael Tauman Kalai
Microsoft Research Laboratory
One Memorial Drive
Cambridge, MA 02142
UNITED STATES

Prof. Dr. Tali Kaufman-Halman
Department of Computer Science
Bar-Ilan University
Ramat-Gan 5290002
ISRAEL

Prof. Dr. Pravesh K. Kothari
Department of Computer Sciences
Carnegie Mellon University
&
Department of Computer Science
Princeton University
Pittsburgh, PA 15213-3890
UNITED STATES

Prof. Dr. Xin Li
Department of Computer Science
Johns Hopkins University
3400 N. Charles St.
Baltimore, MD 21218
UNITED STATES

Dr. Nutan Limaye
Department of Computer Science
ITU Copenhagen
2300 København
DENMARK

Prof. Dr. Huijia (Rachel) Lin
Paul G. Allen School of Computer
Science
& Engineering
University of Washington
Box 352350
Seattle, WA 98195-2350
UNITED STATES

Kuikui Liu
Department of Electrical Engineering
and Computer Science
Massachusetts Institute of
Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

Dr. Raghu R. Meka
Department of Computer Science
University of California, Los Angeles
3732 H. Boelter Hall
Los Angeles, CA 90095
UNITED STATES

Dor Minzer
Department of Mathematics
Massachusetts Institute of
Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

Dr. Sidhanth Mohanty
MIT CSAIL
The Stata Center
32 Vassar Street
Cambridge, MA 02139
UNITED STATES

Prof. Dr. Ryan O'Donnell
School of Computer Science
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213-3890
UNITED STATES

Dr. Jinyoung Park
Courant Institute of
Mathematical Sciences
New York University
251, Mercer Street
New York, NY 10012-1110
UNITED STATES

Prof. Dr. Toniann Pitassi
Columbia University
New York, NY 10027
UNITED STATES

Prof. Dr. Omer Reingold
Gates Computer Science Building
Stanford University
353 Serra Mall
Stanford, CA 94305
UNITED STATES

Prof. Dr. Guy Rothblum
Department of Computer Science
and Applied Mathematics
The Weizmann Institute of Science
P.O. Box 26
Rehovot 76100
ISRAEL

Prof. Dr. Ron Rothblum
Technion
Haifa 32000
ISRAEL

Dr. Shubhangi Saraf
Department of Mathematics
University of Toronto
40 St. George Street
Toronto ON M5S 2E4
CANADA

Dr. Srikanth Srinivasan
Department of Computer Science
Aarhus University
IT-Parken, Aabogade 34
8200 Aarhus N
DENMARK

Prof. Dr. Madhu Sudan
John A. Paulson School of Engineering
and Applied Sciences
Harvard University
150 Western Avenue, SEC 3.434
Boston, MA 02134
UNITED STATES

Dr. Avishay Tal
EECS Department
University of California, Berkeley
Soda Hall
Berkeley, CA 94720-1776
UNITED STATES

Prof. Dr. Amnon Ta-Shma
Department of Computer Science
Tel Aviv University
Tel Aviv 69978
ISRAEL

Sébastien Tavenas
CNRS
Université Savoie Mont Blanc
LAMA
73376 Le Bourget-du-Lac Cedex
FRANCE

Prof. Dr. Chris Umans
Department of Computer Science
California Institute of Technology
MC 305-16, Annenberg 311
1200 E. California Boulevard
Pasadena, CA 91125-5000
UNITED STATES

Prof. Dr. Salil Vadhan
Science and Engineering Complex
School of Engineering and Applied Sciences
Harvard University
150 Western Avenue
Cambridge, Boston, MA 02134
UNITED STATES

Prof. Dr. Virginia Vassilevska Williams
Department of Engineering and Computer Science
MIT
32 Vassar Street, 32-G640
Cambridge, MA 02139
UNITED STATES

Prof. Dr. Avi Wigderson
School of Mathematics
Institute for Advanced Study
1 Einstein Drive
Princeton, NJ 08540
UNITED STATES

Prof. Dr. Ryan Williams
Department of Electrical Engineering and Computer Science
MIT CSAIL
32 Vassar Street
Cambridge, MA 02139
UNITED STATES

Prof. Dr. David Zuckerman
Department of Computer Science
University of Texas at Austin
2317 Speedway, Stop D9500
Austin, TX 78712
UNITED STATES

Dr. Jeroen Zuiddam
Korteweg-de Vries Institute for Mathematics
University of Amsterdam
Science Park 105-107
P.O. Box 94248
1090 GE Amsterdam
NETHERLANDS