Complexity Theory Update Meeting

IMSc, Chennai. 23-25 January 2025.

Long talks

1. Mrinal Kumar, TIFR
   Abstract: The talk will be based on the paper:
   Constant-Depth Arithmetic Circuits for Linear Algebra Problems by Robert Andrews, Avi Wigderson(FOCS 2024).

2. Amit Sinhababu, CMI
   Abstract: Multivariate polynomial factoring where the polynomial is given as an arithmetic circuit reduces to circuit PIT (KSS, CCC 2014). Even if the polynomial to be factored is simple such as sparse/constant depth circuit, the corresponding PIT instance comes from a significantly bigger class such as ABPs for which we do not know any nontrivial PIT. Some recent works have tried to bypass the various bottlenecks and got derandomization results in various special cases. Furthermore, better understanding of the derandomization challenges in multivariate factoring (and related problems) led to progress in derandomizing special cases of PIT. The talk will be based on recent results in multivariate polynomial factorization.

3. Anil Shukla, IIT Ropar
   Abstract: Proposition model counting #SAT is a well known computationally hard problem in the field of computational complexity. In fact Toda [1991] has shown that with a single #SAT oracle, any problem from the polynomial hierarchy can be solved in polynomial time. On the other hand, proof complexity studies of #SAT have been very recently started.

   In proof complexity, we study the hardness in finding the certificate of #SAT. That is, if the number of satisfying assignments (models) of a CNF formula F is k, then proof complexity studies various ways (proof systems) of proving the fact that the given CNF F has indeed exactly k models. At this moment, this study is in its initial stage. In the literature, there are only three non-trivial proof systems for #SAT:

   - Florent Capelli: Knowledge Compilation Languages as Proof Systems. SAT 2019: This paper introduces a static proof system for #SAT known as KCPS.
     DOI: `https://doi.org/10.1007/978-3-030-24258-9_6`
   - Olaf Beyersdorff, Tim Hoffmann, Luc Nicolas Spachmann: Proof Complexity of Propositional Model Counting. J. Satisf. Boolean Model. Comput. 15(1): 27-59 (2024): This paper introduces the MICE' proof system for #SAT.
     DOI: `https://doi.org/10.3233/SAT-231507`
   - Randal E. Bryant, Wojciech Nawrocki, Jeremy Avigad, Marijn J. H. Heule: Certified Knowledge Compilation with Application to Verified Model Counting. SAT 2023: 6:1-6:20: This paper introduces CPOG proof systems for #SAT.
     `DOI:https://doi.org/10.4230/LIPIcs.SAT.2023.6`
   - In this talk, I plan to discuss all the three proof systems and their simulations among themselves from the following paper:
     Olaf Beyersdorff, Johannes Klaus Fichte, Markus Hecher, Tim Hoffmann, Kaspar Kasche:

The Relative Strength of #SAT Proof Systems. SAT 2024: 5:1-5:19.
DOI: https://doi.org/10.4230/LIPIcs.SAT.2024.5

4. Nitin Saurabh, IIT Hyderabad
   Abstract: The talk will be based on the following papers:

   - Hard submatrices for non-negative rank and communication complexity by Pavel Hrubes(CCC 2024).
   - The Communication Complexity of Approximating Matrix Rank by Alexander A. Sherstov, Andrey A. Storozhenko(FOCS 2024).

5. Pushkar Joglekar, VIT-P.
   Abstract: The talk will survey polynomial factorization in the non-commutative setting.

6. Prahladh Harsha, TIFR
   Title: Recent Advances in List-Decoding Polynomial Codes Abstract: The field of list-decoding polynomial codes has seen a flurry of activity in the last 5-6 years. In particular, we have seen the following results:

   (a) resolution of the GM-MDS conjecture, higher-order MDS codes and combinatorial optimal list-decoding of the Reed-Solomon (RS) code
   (b) nearly linear-time list-decoding of folded RS and multiplicity codes and
   (c) optimal list-size bounds for FRS and multiplicity codes.

   In this talk, I will survey these results and then do a deep-dive into optimal list-size bounds (item (c) from above) due to Srivastava and Chen-Zhang.

   We will see detailed proofs from the following 3 papers in the second half of the talk.

   (a) Itzhak Tamo, Tighter list-size bounds for list-decoding and recovery of folded Reed-Solomon and multiplicity codes. Ref: https://doi.org/10.1109/TIT.2024.3402171, http://arxiv.org/abs/2312.17097.
   (b) Shashank Srivastava. Improved list size for folded Reed-Solomon codes. Ref: https://doi.org/10.1137/1.9781611978322.64, http://arxiv.org/abs/2410.09031
   (c) Yeyuan Chen and Zihan Zhang. Explicit folded Reed-Solomon and multiplicity codes achieve relaxed generalized singleton bound, 2024. Ref: http://arxiv.org/abs/2408.15925

7. Jayalal Sarma M N, IITM
   Abstract: The talk will be based on the paper:
   Tree Evaluation is in Space $O(\log n \log\log n)$ by James Cook; Ian Mertz(STOC 2024).

8. Yadu Vasudev, IITM
   Abstract: The talk will be based on recent advances in Property Testing.

9. Chandra Kanata Mohapatra, CMI
   Abstract: The talk will be based on the paper:
   Power Series Composition in Near-Linear Time by Yasunori Kinoshita, Baitian Li(FOCS 2024)

Abstracts: Short talks

1. Title: One-way functions and Polynomial-time dimension
   Speaker: Akhil S (IIT K)
   Abstract: This work explores the connections between notions in cryptography (OWFs) with notions in algorithmic information theory(Polynomial-time dimension). Ref: `https://arxiv.org/pdf/2411.02392`.

   Polynomial time dimension is a quantification of the density of information present in an infinite binary string, as measured by polynomial time algorithms. Denoted cdim_{P}, it is measured using betting algorithms called s-gales. Formally, fixing $s \leq 1$, bets $(p_i, 1-p_i)$ are placed on the next bit $X[i]$ of string X, such that the payoff after the bet is $2^s.p_i$ or $2^s.(1-p_i)$. The betting algorithm (or the gale) wins on the sequence if an arbitrary amount of money can be procured. The information density is measured by making the betting environment more hostile by decreasing s, and finding the least value of s at which winning is still possible. In this approach, we quantify information density using the *predictability* of the next bit in the sequence.

   Analogously, a notion of information density can also be quantified using time-bounded Kolmogorov complexity. Formally, for a finite string x, we find the shortest description (or program) from which a polynomial time algorithm can recover the string. For an infinite string X, we consider its finite n-length prefixes, divide the time-bounded Kolmogorov complexity by the length of the string n and take its limiting values. The corresponding value is denoted as $\mathcal{K}_{\text{poly}}$. In this approach, we quantify information density using the *compressibility* of the finite prefixes of the sequence.

   In the unbounded time setting, these notions are shown to be equivalent [Mayordomo,Lutz 2002]. It has been a long standing open question [Hitchcock and Vinodchandran [2006] if the polynomial time notions, cdim_{P} and $\mathcal{K}_{\text{poly}}$ are equivalent. Recently, works by Pass and Liu [2021] have unearthed interesting connections between time bounded Kolmogorov complexity and the existence of One-way functions. In a similar spirit, we give a resolution to this open question, relating it with the existence of one-way functions.

   We show that the notions cdim_{P} and $\mathcal{K}_{\text{poly}}$ are unequal if One-way functions(OWFs) exist. Existence of OWFs and pseudo random generators (PRG) are known to be equivalent. The idea is that outputs of PRG by design have low $\mathcal{K}_{\text{poly}}$. Our proof involves new constructions that utilise s-gales that wins on outputs of PRG (which exist if the notions are equivalent) to come up with distinguishers that break the PRG. We also use some measure theoretic tools like the Borel-Cantelli Lemma, which is central in the analysis. We hope that our work sheds new light in the current line of research that explores connections between concepts in cryptography and meta-complexity.

2. Title: Fast list-decoding of univariate multiplicity codes
   Speaker: Ashutosh Shankar, TIFR
   Abstract: Univariate multiplicity codes are a generalization of Reed-Solomon codes and are among the first families of efficiency list-decodable codes all the way up to capacity (Guruswami-Wang and Kopparty). In this work, we show how these efficient list-decoders for univariate multiplicity codes can in fact be made to run in nearly linear time. Our results also hold for Folded Reed-Solomon codes. An important intermediate step in our nearly-linear

time decoding algorithm is obtaining a nearly-linear time solver for ordinary differential equations.

3. Title: On the Composition of the Complexity Measures of Boolean Functions
   Speaker: Chandrima Kayal, IMSc
   Abstract: We can compose two Boolean functions f and g to obtain a new function $f \circ g$, but what happens to the complexity measures? Can we express the complexity of the composed function in terms of the smaller functions (f and g) ? Precisely, the question is if the following holds: $M(f \circ g) = \Theta(M(f) \cdot M(g))$ for some particular complexity measure (of Boolean function) M. This is one of the fundamental questions in the area of Analysis of Boolean functions. Following a long line of work there are two big open problems in this area:

   (a) Does approximate degree compose?

   (b) Does randomized query complexity compose?

   Although these two measures are standard and well-studied, still it is not known if they behave nicely under composition or not. In these studies, we have explored two different directions and generalized the existing results, which gave an affirmative answer to both the problems for larger classes of functions. In this talk, we will describe some of the recent results and the related open problems.

   Talk is based on the two following works:

   - On the Composition of Randomized Query Complexity and Approximate Degree(joint work with Sourav Chakraborty, Rajat Mittal, Manaswi Parashaar, Swagato Sanyal, and Nitin Saurabh).
   - Approximate degree composition for recursive functions (joint work with Sourav Chakraborty, Rajat Mittal, Manaswi Parashaar, and Nitin Saurabh).

4. Title: Circuits, Proofs and Propositional Model Counting
   Speaker: Sravanthi Chede, IIT-Ropar
   Abstract: In this short talk, we present and discuss the new proof system CLIP (Circuit Linear Induction Proposition) for #SAT. CLIP efficiently simulates all the existing #SAT proof systems. Also, CLIP has an easy upper bound for a family of CNF formulas which are hard for other existing proof systems. Infact, proving lower bounds in the CLIP system is equivalent to solving major open problems in various fields of computational complexity.

   This is a joint work with Leroy Chew (TU Wien, Austria) and Anil Shukla (IIT Ropar). DOI: `https://doi.org/10.4230/LIPIcs.FSTTCS.2024.18`

5. Title: Fourier analysis of Boolean valued functions over finite Abelian groups.
   Speaker: Swarnalipa Dutta, ISI Kolkata.
   Abstract: A Boolean valued function is a function from some domain set $\mathcal{D}$ to a range set of cardinality two, for example $\{-1, +1\}$, $\{0, 1\}$ etc. These Boolean valued functions are an important topic in the field of theoretical computer science, additive combinatorics and many other areas. They also have immense importance in the study of algorithms and complexity, when the domain $\mathcal{D}$ is endowed with some nice algebraic structure, such as finite Abelian groups. It helps us to study the Fourier analysis of Boolean valued functions, understand various properties of the Fourier spectrum and structure of the Fourier coefficients.

Studies have mostly been done when the domain $\mathcal{D} = \mathbb{Z}_2^n$, that is binary strings of length n, on various measures of these functions. The question is, can these results be generalized for Boolean-valued functions over finite Abelian groups? This talk will cover the following problems that we have generalized for finite Abelian groups.

Granularity: Fourier sparsity is the number of nonzero Fourier coefficients of f. Let's say the Fourier sparsity of a Boolean valued function is small. What can one say about the size of the Fourier coefficients? Gopalan et. al, in the year 2011 showed that any nonzero Fourier coefficient of a Boolean function when the domain is $\mathbb{Z}_2^n$ is at least $\frac{1}{s_f}$ in its absolute value, where s_f is the size of the Fourier support, that is, the number of nonzero Fourier coefficients of f.

Upper bound on the Fourier dimension: Fourier dimension r_f is the dimension of the Fourier support of f. Sanyal in the year 2019 showed that $r_f = O(\sqrt{s_f} \log s_f)$, which was improved by Chakraborty et. al in the year 2020, they showed that $r_f = O(\sqrt{s_f \delta_f} \log s_f)$, where $\delta_f = \Pr_x[f(x) = -1]$. These results show that for a function with small sparsity, the Fourier dimension cannot be too big.

Linear Isomorphism testing: The Linear Isomorphism testing for Boolean functions over $\mathbb{Z}_2^n$ is also an important problem to study. For $A \in \mathbb{Z}_2^{n \times n}$, let $f \circ A : \mathbb{Z}_2^n \to \{-1, 1\}$ be the function $f \circ A(x) = f(Ax)$ for all $x \in \mathbb{Z}_2^n$. The Linear Isomorphism Distance between $f : \mathbb{Z}_2^n \to \{-1, 1\}$ and $g : \mathbb{Z}_2^n \to \{-1, 1\}$ is defined as $dist_{\mathbb{Z}_2^n}(f, g) = \min_{A \in \mathbb{Z}_2^{n \times n} : A \text{ is non-singular}} \delta(f \circ A, g)$. Assume that f and g satisfy the promise that either $dist_{\mathbb{Z}_2^n}(f, g) = 0$ or $dist_{\mathbb{Z}_2^n}(f, g) \geq \epsilon$, the question of Linear Isomorphism testing is that of deciding which is the case.

Studies have also been made on the approximate degree of a Boolean function, pseudorandom generators, and many more.

An important point to note here is that an Abelian group is not a vector space in general. So most of the results in $\mathbb{Z}_2^n$ cannot be directly extended for finite Abelian groups as the properties of a vector space do not hold in this case. The major drawbacks of generalizing the results to finite Abelian groups will be discussed in this talk.

6. Title: Inclusion matrices and polynomial approximations
Speaker: Vaibhav Krishan, IMSc
Abstract: Inclusion matrices are widely studied objects, especially in combinatorial design theory, with notable contributions from Gottlieb (Proc. Amer. Math. Soc. 1966), Wilson (Util. Math. 1973), Bapat (Linear Algebra Appl. 2000), and countless others. Several works have studied various properties of these matrices, such as their eigenvalues, pseudo-inverses, etc. Many of these properties are useful in constructing designs.

Polynomial approximations are useful in combinatorics as well as computer science. Various models of polynomial approximations have applications in learning theory, Boolean circuit lower bounds, query/communication complexity, quantum query/communication complexity, secret-sharing schemes, and many more.

We will focus on a recently proposed model of polynomial approximations, called torus polynomials. Torus polynomials arise out of higher order Fourier analysis, proposed by Bhrushundi, Hosseini, Lovett and Rao (ITCS 2019) as a method to prove a long-standing conjecture about Boolean circuits.

In this talk, we will describe how inclusion matrices are intricately connected to polynomial approximations. We will discuss some results about torus polynomials, and some future work, both based on the study of inclusion matrices. In fact, we are able to prove a nearly tight result about torus polynomials, whereas no lower bounds were known prior to our work.

This is a joint work with S. Vishwanathan at CSE, IITB.

7. Title: Towards Deterministic Algorithms for Constant-Depth Factors of Constant-Depth Circuits
   Speaker: Varun Ramanathan, TIFR.
   Abstract: Multivariate polynomial factorization is a natural algebraic problem with a lot of applications. von zur Gathen, Kaltofen, Trager et al gave us randomized algorithms for factoring black-box polynomials as well as polynomials given as explicit arithmetic circuits. Derandomization of factorization is connected to the derandomization of polynomial identity testing by a line of beautiful results; some are general and some are specific to constant-depth circuits. Yet, recent breakthroughs in deterministic PIT for constant-depth circuits have not immediately led to improvements in deterministic factorization of constant-depth circuits.

   In this talk, we will see an algorithm that makes some modest progress towards this problem. In particular, we will see a deterministic subexponential time algorithm that takes as input a multivariate polynomial f computed by a constant-depth circuit over rational numbers, and outputs a list L of circuits (of unbounded depth and possibly with division gates) that contains all irreducible factors of f computable by constant-depth circuits. This list L might also include circuits that are spurious: they either do not correspond to factors of f or are not even well-defined, e.g. the input to a division gate is a sub-circuit that computes the identically zero polynomial.

   The key technical ingredient of our algorithm is a notion of the pseudo-resultant of f and a factor g, which serves as a proxy for the resultant of g and f/g, with the advantage that the circuit complexity of the pseudo-resultant is comparable to that of the circuit complexity of f and g. This notion, which might be of independent interest, together with the recent results of Limaye, Srinivasan and Tavenas, helps us derandomize one key step of multivariate polynomial factorization algorithms - that of deterministically finding a good starting point for Newton Iteration for the case when the input polynomial as well as the irreducible factor of interest have small constant-depth circuits.

   This is joint work with Mrinal Kumar, Ramprasad Saptharishi and Ben Lee Volk.