Mathematisches Forschungsinstitut Oberwolfach

Report No. 54/2021

DOI: 10.4171/OWR/2021/54

Complexity Theory (hybrid meeting)

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

14 November – 20 November 2021

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 interactive proof systems, quantum information and computation, algorithmic coding theory, arithmetic complexity, expansion of hypergraphs and simplicial complexes, Markov chain Monte Carlo, and pseudorandomness. Many of the developments are related to diverse mathematical fields such as algebraic geometry, extremal combinatorics, combinatorial number theory, probability theory, representation theory, and operator algebras.

Mathematics Subject Classification (2010): 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 November 11–20 2021 in hybrid format. It was attended by approximately 50 participants spanning a wide range of interests within the field of Computational Complexity. Among those, around 30 participated in person and the rest virtually. The plenary program featured twelve long lectures and two 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. The meeting usually features a couple of special focus topics which vary from meeting to meeting. The special focus topics of the current meeting were quantum computation and algorithmic aspects of error-correcting codes.

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.

Interactive proofs with quantum provers sharing entanglement. Thomas Vidick gave an overview of his spectacular 2020 breakthrough with Ji, Natarajan, Wright, and Yuen, which connects quantum computation, operator algebras and computational complexity. This was complemented by a plenary talk of his coauthor Henry Yuen on noncommutative property testing in which more details were provided.

A classic result due to Babai, Fortnow and Lund (1991) showed that any language in nondeterministic exponential time has a two-prover interactive (probabilistically checkable) proof, in short: $\mathsf{MIP} = \mathsf{NEXP}$. This early result and its method of proof (arithmetization) were influential for the discovery of the PCP theorem, another fundamental result characterizing the complexity class NP in terms of extremely efficient probabilistically checkable proofs.

One may wonder what are the changes when bringing in quantum computation into the game. In 2004 the quantum analogue MIP^* was introduced, which is characterized by a classical polynomial-time verifier interacting with multiple quantum provers *sharing entanglement.* Entanglement goes back to a famous paper by Einstein, Podolsky and Rosen, and for a long time, the correlations afforded by quantum mechanics were considered by most physicists as an oddity with little practical relevance. The situation changed drastically in the early 1990s with the discovery that entanglement could act as a resource for quantum information tasks. In the early 1980s Tsirelson wrote a series of papers laying out the mathematical formalism for the systematic study of the nonlocal properties of quantum mechanics. Tsirelson had stated an open problem that much later was realized to be essentially equivalent to Connes' embedding problem, a major question from the 1970s in the theory of operator algebras (von Neumann algebras).

A complete characterization of the class MIP^* was finally obtained in 2020, leading to an utterly surprising and counterintuitive answer: the class MIP^* coincides with the class of recursively enumerable languages: $\mathsf{MIP}^* = \mathsf{RE}$. In particular, MIP^* contains the (undecidable) Halting Problem! This has significant consequences in mathematics: it leads to a strict inclusion in Tsirelson's problem and provides a refutation of Connes' embedding conjecture from the theory of von Neumann algebras.

In his excellent talk, Thomas Vidick outlined the proof of this breakthrough result: a difficult task since the original paper is around 200 pages long. Thomas focused on the design of a "compression procedure" for multiprover interactive proofs and illuminated the differences between the classical and the quantum setting.

The talk by Henry Yuen followed up on this by explaining low degree tests with quantum functions. Essential features were illustrated by discussing the Magic Square Game in detail.

A breakthrough in locally testable codes. A (linear) error-correcting code is a linear subspace of n-bit strings that are pairwise far apart in Hamming distance. These strings can be used to encode messages so that even if a small fraction of the bits are flipped, there is a way to figure out what the original codeword has been and thus recover the original message. The theory of error-correcting codes is well developed with origins dating back to the works of Shannon and Hamming from the late 1940s and early 1950s. The two important parameters of an error-correcting code are the rate and the distance, and the golden standard of error-correcting codes requires both of these to be a constant multiple of the length n.

Local testability is a much newer notion that emerged from complexity works in the 1990s on probabilistically checkable proofs (PCPs) that have lead to the area of property testing. A locally testable code is a code that comes together with a property tester, namely, an algorithm that can check if a given codeword carries many errors by reading only a small number of bits. Constructions of locally testable code are typically based on low degree polynomial functions and codes such as the Reed–Muller code. These codes require significant redundancy to achieve the local testability property and therefore fell short of meeting the golden standard in terms of rate and distance.

The meeting featured two plenary talks on recent breakthroughs in this area. The first, by Irit Dinur, described a new construction of locally testable codes by her and coauthors that have the so-called c^3 *property*: they have constant relative distance, constant relative rate, and are testable with a constant number of queries. The codes are constructed similar in spirit to expander codes. Instead of an expander graph, one starts out with a new object called a left-right Cayley complex. This complex is a graph that, in addition to vertices and edges, also has squares. The bits are placed on the squares and the second level is somehow used for proving testability. The second talk, by Ryan O'Donnell, described a new work by Panteleev and Kalachev that was posted on arXiv just a couple of weeks before the meeting took place. This work achieves both c^3 LTCs as well as the first known quantum LDPC codes that are asymptotically good, namely have constant relative rate and distance. Quantum LDPC codes are given by two subspaces C_X, C_Z with the property that $C_X^\perp \subseteq C_Z$ and $C_Z^\perp \subseteq C_X$. The talk focused on describing the concrete construction through a highly symmetric chain of vertices edges and squares.

Superpolynomial lower bounds for low depth arithmetic circuits. The computational complexity of computing a polynomial over a field is defined as the minimum size of an arithmetic (or algebraic) circuit computing it. While it is well known that almost all polynomials have a complexity that is essentially its number of monomial terms, proving superpolynomial lower complexity bounds for specific polynomials (like the permanent) has remained elusive. Doing so would amount to proving the separation $\mathsf{VP} \neq \mathsf{VNP}$, which is an algebraic analogue of the famous $\mathsf{P} \neq \mathsf{NP}$ problem in the setting of Boolean functions.

Therefore, efforts have focused on restricted models of computation: a common assumption is to restrict the depth of the circuits. In fact, for constant-depth Boolean circuits, strong lower bounds have been known since the 1980s.

In her talk, Nutan Limaye presented her recent breakthrough result, where she and coauthors establish, for the first time, superpolynomial lower bounds for explicit polynomials in the model of constant-depth algebraic circuits over fields of characteristic 0. In fact, these bounds apply to iterated matrix multiplication, which is the problem of computing the trace of the product of d many $n \times n$ matrices, whose entries are different variables.

While the general pattern of the proof follows known strategies, several significant improvements are introduced. The first step is to focus on the more restricted model of set-linear circuits, which was introduced by Nisan and Wigderson in 1995. Limaye et al. managed to improve the lower bound techniques in the latter work. The second step is an improved conversion of constant-depth algebraic circuit to a constant-depth set-multilinear circuit.

Approximate counting, sampling and high dimensional expanders. Approximate counting is the problem of efficiently computing the approximate number of solutions to a given problem. For example, given a graph, count how many forests of size k there are in the graph. When $k = n - 1$, we are counting spanning trees, which can be calculated exactly in polynomial time using Kirchhoff's Matrix–Tree Theorem, but for smaller values of k, it was a long-standing open problem how to even approximately count forests in polynomial time. It is well known that such approximate counting problems are equivalent to sampling, the problem of generating a solution chosen almost uniformly at random from the set of solutions. A very successful approach to these questions is given by the Markov Chain Monte Carlo (MCMC) method. Devise a Markov chain that uses simple steps to move from solution to solution in a random way. If the Markov chain mixes sufficiently rapidly, the algorithm will quickly sample from (almost) the desired distribution.

In his talk, Shayan Oveis Gharan described a breakthrough work in which he and coauthors solved the problem of sampling a random basis of any given Matroid, including the case of forests of arbitrary size as a special case. He described a simple and natural Markov chain that randomly moves from one basis to another. The key idea is to understand and analyze this Markov chain by viewing it as a random walk on a high dimensional expander. From the matroid there is a simple way to construct a simplicial complex: the ground set is the ground set of the matroid, and the top faces (those with highest dimension) are the bases of the matroid. One then looks at the random walk from basis to basis as a walk on the top faces of the simplicial complex. The mixing time of this walk can be analyzed by analyzing the mixing time of the *links* of this complex, which have relatively simple structure.

Progress on the sunflower conjecture. This online talk by Shachar Lovett summarized the recent progress on the sunflower conjecture, which was led by Lovett and his coauthors. The sunflower conjecture is a famous conjecture in extremal combinatorics due to Erdös and Rado (1960). Let us fix a finite universe. A w-set system is a collection $\mathcal{F}$ of subsets of cardinality at most w. We are interested in subcollections $\{S_1, \ldots, S_r\}$ of $\mathcal{F}$ with the property that all its pairwise intersections are the same. Those are called r-sunflowers.

The talk started with Erdös and Rado's proof of the sunflower lemma, which states that $|\mathcal{F}| \geq w!(r-1)^w$ is enough to guarantee the existence of an r-sunflower in an w-set system $\mathcal{F}$. The sunflower conjecture essentially claims that $w!$ in this bound can be removed. More specifically, it claims that any w-set system $\mathcal{F}$ contains an r-sunflower, provided the cardinality of $\mathcal{F}$ exceeds $c(r)^w$, where $c(r)$ denotes a constant only depending on $r \geq 3$. The claimed bound is easily seen to be optimal. In the talk, also a related conjecture by Erdös and Szemeredi involving the size of the universe was discussed. All these results and conjectures found many applications in mathematics and theoretical computer science.

Lovett went on to outline in quite detail the proof of his new result, thereby focusing on the case $r = 3$ for simplicity. The new result states that any w-set system satisfying $|\mathcal{F}| \geq (\log w)^{O(w)}$ contains a 3-sunflower. The proof emphasized two general principles: on the one hand, structure versus randomness. On the other hand, it was relevant to think of set systems in terms of monotone disjunctive normal formulas, which are a standard object of study in computational complexity but lead to a new perspective on a classic pure combinatorics problem. Ihere are several follow-up works by combinatorialists and computer scientists which led to improvements, applications, and/or simplified proofs.

Recent Advances on Indistinguishability Obfuscation. Obfuscation aims to efficiently compile programs into "unintelligible ones" while preserving functionality. Obfuscators are a fascinating and powerful concept; if we could construct them, they would enable a vast array of new cryptographic tasks and beyond.

The specific notion of *indistinguishability obfuscation (iO)* was first proposed in a work by Barak et al., presented at 2000 Oberwolfach Meeting of Computational Complexity. The main result of Barak et al. was negative, showing that a stronger form of obfuscation is impossible to achieve, and for more than a decade, it was suspected that indistinguishability obfuscation would also be impossible. Starting in 2013, the cryptography research community became more optimistic about the existence of iO, and generated a wealth of proposals for constructing it. However, these proposals relied on heuristics or newly conjectured hardness assumptions whose correctness was difficult to assess (and were often refuted).

In her talk, Huijia Lin described a series of breakthrough constructions of iO where she and her coauthors rely only on well-known hardness assumptions that have already undergone significant scrutiny and thus are very plausible. These assumptions involve the hardness of (a) solving noisy linear equations over prime fields, (b) breaking pseudorandom generators in which every output bit depends on only a constant number of input bits, and (c) solving a decisional variant of the discrete logarithm problem in bilinear groups of prime order. Surprisingly, their construction makes no use of hardness assumptions involving high-dimensional lattices, which had been the basis of other powerful cryptographic primitives (like fully homomorphic encryption) and were used in prior constructions of iO.

Thresholds for random subspaces, aka LDPC codes achieve list-decoding capacity. Random linear codes and random *low-density parity-check* (LDPC) linear codes are two well-studied families of codes. The first is obtained by selecting a random matrix and the second is obtained by selecting a random *sparse* matrix. There are many algorithmic advantages to using random LDPC codes rather than random codes. The most obvious is that for a random code we expect the decoding complexity to be very high (super-polymomial), whereas random LDPC codes have very efficient decoding algorithms. On the other hand, many combinatorial properties are easier to prove for random codes because more randomness implies more probabilistic independence.

In her talk, Mary Wootters defined a collection of so-called local properties of codes. She showed that such properties can be transferred from the case of random codes to the case of random LDPC codes. The class of local properties is quite a rich class of properties that allows formulating many interesting features of error-correcting codes, including distance and list-decodability. Thus, an application of this result allowed proving, for the first time, that random LDPC codes are list-decodable up to list-decoding capacity.

Recent progress on derandomizing space-bounded computation. A central question in computational complexity is whether randomized algorithms can solve problems with significantly less resources (especially, time or space) than deterministic algorithms, or instead that all randomized algorithms can be *derandomized* with only a small loss in efficiency. Postdoctoral fellow William Hoza gave a beautiful survey talk on recent progress (by a variety of researchers, including Hoza) aimed at proving that BPL=L, which means that all randomized algorithms can be made deterministic with only a constant-factor increase in memory usage. Hoza's talk covered four themes, and the payoffs each has yielded (e.g. in derandomizing subclasses of space-bounded computation). The first theme was that of *iterated pseudorandom restrictions*, where portions of the algorithm's random bits are iteratively replaced with sequences of pseudorandom bits, which turns out to be an easier task than trying to generate all of the pseudorandom bits at once. The second was exploiting a connection between derandomizing space-bounded computation and approximately inverting directed Laplacian matrices. A third was error-reduction procedures for approximating the behavior of randomized space-bounded algorithms. The fourth was the use of expander graphs in constructing pseudorandom generators and related objects for space-bounded computation. One concrete consequence of some of these ideas is Hoza's own result that gave the first improvement in the derandomization of general space-bounded computation in over 25 years, namely that a randomized space S algorithm can be converted to a deterministic algorithm that uses space $O(S^{3/2}/\sqrt{\log S})$. (In 1995, Saks and Zhou gave the bound $O(S^{3/2})$, and it is conjectured that $O(S)$ is possible.)

Quantum information theory, tensors and algebraic complexity. Christandl's talk started with general comments on the connection of quantum states and tensors. He then moved on to explain the connection to algebraic complexity. For instance, the tensor $\langle 2,2,2\rangle$ of 2 by 2 matrix multiplication can be seen as the state of three qubits with pairwise EPR entanglement. In this context the notion of the asymptotic restriction of tensors, introduced by Volker Strassen in 1988, enters naturally. A tensor t' is called an *asymptotic restriction* of a tensor t, written $t \succeq t'$, if the n-fold tensor power $t'^{\otimes n}$ of t' can be obtained as a restriction of $t^{\otimes N_n}$, when N_n is not much larger than n, namely $\lim_{n\to\infty} N_n/n = 1$. This definition has a natural interpretation from an information-theoretic point of view when the tensors are interpreted as quantum states. The exponent of matrix multiplication equals 2 iff $\langle 4\rangle \succeq \langle 2,2,2\rangle$, where $\langle 4\rangle = \sum_{i=1}^{4} |iii\rangle$ denotes the unit tensor of dimension four. Strassen proved a fundamental duality theorem stating that $t \succeq t'$ iff $F(t) \geq F(t')$ for all functionals F on tensors that are additive (w.r.t. direct sum), multiplicative (w.r.t. tensor product), and monotone with respect to restriction. Moreover, for certain classes of tensors, Strassen described an explicit family F_θ of "support functionals", parameterized by $\theta_1, \theta_2, \theta_3 \geq 0$ such that $\theta_1 + \theta_2 + \theta_3 = 1$.

Christandl briefly outlined his recent work on *quantum functionals*, which, in characteristic zero, generalizes Strassen's support functionals to cover all tensors. Morevoer, the quantum functional $F_\theta(t)$ has a clean description in terms of the *moment polytope* $\Delta(t)$ of t. The value $\log F_\theta(t)$ is obtained by maximizing the convex combination of entropies $\theta_1 H(P_1) + \theta_2 H(P_2) + \theta_3 H(P_3)$ over all probability distributions P with support contained in $\Delta(t)$; here P_1, P_2, P_3 denote the three marginal distributions of P. The moment polytope is a fundamental concept at the crossroad of symplectic geometry and geometric invariant theory that enters here in an unexpected way.

Connecting meta-complexity and crypto. Meta complexity is the study of computational problems that are themselves about complexity. Examples include the Minimum Circuit Size Problem (given a the truth table of a boolean function f, determine the size of the smallest boolean circuit computing f) and computing time-bounded versions of Kolmogorov Complexity. In this survey talk, Rahul Santhanam gave an overview of recent work on meta-complexity. In particular, Santhanam discussed the surprising recent result of Liu and Pass, which showed that the existence of one-way functions (the minimal assumption for complexity-based cryptography) is *equivalent* to the average-case hardness of computing the polynomial-time bounded analogue of Kolmogorov complexity. This constitutes a major advance on the long-running project of understanding the relationship between one-way functions and the average-case hardness of natural problems.

Brief Reports. In one plenary session, graduate student Yotam Dikstein and the postdoctoral fellow Visu Makam presented brief reports of their research agendas.

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:

- Average-case problems and the sum-of-squares hierarchy
- The complexity of matrix multiplication
- Pseudorandomness and derandomization of space-bounded computation
- Geometric complexity theory
- Threshold phenomena in random graph models
- Spectral graph theory
- Coding theory and fault tolerance
- Algorithmic fairness

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-1641185, "US Junior Oberwolfach Fellows".

Workshop (hybrid meeting): Complexity Theory

Table of Contents

Abstracts

Superpolynomial Lower Bounds against Low-Depth Algebraic Circuits

Nutan Limaye

(joint work with Srikanth Srinivasan, Sébastien Tavenas)

Algebraic circuits are algebraic algorithms for computational problems defined by multivariate polynomials. Given a (sequence of) polynomials $P_n(x_1, ..., x_n)$, the computational problem is to evaluate P_n at a given input point x. Many fundamental computational problems such as the determinant, the permanent, and matrix multiplication can be cast in this language.

An algebraic circuit is an algorithm that performs such a computation by constructing the formal polynomial P_n using algebraic operations (linear combinations and multiplications). The model is syntactic, as opposed to the general Boolean circuit model, which is only defined by a set of input-output behaviours. Lower bounds for this model should consequently be easier to prove.

Despite this, we did not have lower bounds against constant-depth algebraic circuits (while constant-depth Boolean circuit lower bounds were known since the 1980s). In recent work, we showed the first superpolynomial lower bounds for constant-depth algebraic circuits.

Our approach is surprisingly simple. We first prove superpolynomial lower bounds for constant-depth *Set-Multilinear* circuits. While strong lower bounds were already known against such circuits, most previous lower bounds were of the form $\Omega(f(d) \cdot \mathrm{poly}(N))$, where d denotes the degree of the polynomial. In analogy with Parameterized complexity, we call this an *FPT* lower bound. We extend a well-known technique of Nisan and Wigderson (FOCS 1995 [1]) to prove *non-FPT* lower bounds against constant-depth set-multilinear circuits computing the Iterated Matrix Multiplication polynomial $\mathrm{IMM}_{n,d}$ (which computes a fixed entry of the product of d $n \times n$ matrices). More precisely, we prove that any set-multilinear circuit of depth Δ computing $\mathrm{IMM}_{n,d}$ must have size at least $n^{d^{\exp(-O(\Delta))}}$. This result holds over any field, as long as $d = o(\log n)$.

We then show how to convert any constant-depth algebraic circuit of size s to a *constant-depth* set-multilinear circuit with a blow-up in size that is exponential in d but only polynomial in s over fields of characteristic 0. (For depths greater than 3, previous results of this form increased the depth of the resulting circuit to $\Omega(\log s)$.) This implies our constant-depth circuit lower bounds.

We can also use these lower bounds to prove a Depth Hierarchy theorem for constant-depth circuits. We show that for every depth Γ, there is an explicit polynomial which can be computed by a depth Γ circuit of size s, but requires circuits of size $s^{\omega(1)}$ if the depth is $\Gamma - 1$.

Finally, we observe that our superpolynomial lower bound for constant-depth circuits implies the first deterministic sub-exponential time algorithm for solving the Polynomial Identity Testing (PIT) problem for all small depth circuits using the known connection between algebraic hardness and randomness.

In this talk, we will discuss the background behind our results. We will then give details of the lower bound proof.

References

[1] N. Nisan, A. Wigderson *Lower bounds on arithmetic circuits via partial derivatives.*, Computational Complexity **6(3)**, 217–234, 1997.

MIP*=RE

Thomas Vidick

(joint work with Zhengfeng Ji, Anand Natarajan, John Wright, Henry Yuen)

The equality MIP*=RE characterizes the class of language that have two-prover interactive proofs with a classical polynomial-time verifier and two all-powerful quantum provers sharing entanglement as being equal to the class of recursively enumerable languages. The equality forms a surprising counterpart to the famous result MIP=NEXP by Babai, Fortnow and Lund and has consequences to long-standing open problems in the foundations of quantum mechanics (Tsirelson's problem) and the theory of von Neumann algebras (Connes' Embedding Problem).

In the talk we focused on the key step in the proof of MIP*=RE, which is the design of a "compression procedure" for multiprover interactive proofs with favorable properties. For simplicity we focus on two-prover one-round games:
Definition. A *two-player one-round game* G is specified by a tuple (X, Y, A, B, μ, D) where

(1) X and Y are finite sets (called the *question alphabets*),
(2) A and B are finite sets (called the *answer alphabets*),
(3) μ is a probability distribution over $X \times Y$ (called the *question distribution*), and
(4) $D : X \times Y \times A \times B \to \{0, 1\}$ is a function (called the *decision predicate*).

Let $\mathcal{C} \subseteq [0,1]^{X\times Y\times A\times B}$. Then to any game $G = (\mu, D)$ we can associate a *value* which is the largest achievable success probability when the provers' strategy is required to generate distributions that lie in $\mathcal{C}$:

$$\omega(G; \mathcal{C}) = \sup_{p\in\mathcal{C}} \sum_{x,\,y,\,a,\,b} \mu(x, y)\, D(x, y, a, b)\, p_{x,y,a,b}\ .$$

When $\mathcal{C}$ is the set of quantum correlations, i.e. those of the form $p_{x,y,a,b} = \langle\psi| A^x_a \otimes B^y_b |\psi\rangle$ for a state $|\psi\rangle$ and POVM $\{A^x_a\}$ and $\{B^y_b\}$ we simply write $\omega(G)$ for the associated value.

Say that a family of games $(G_n)_{n\geq 1}$ has a *succinct representation* if there is a polynomial-time computable map $\mathcal{G} : 1^n \mapsto G_n$, where G_n is represented by a pair of circuits for sampling from the distribution μ_n (given as input a uniformly random string) and computing the predicate D_n (given as input strings x, y, a, b) respectively.

Suppose that there is a polynomial-time computable function *Compress* that given as input a succinct representation for a family of games $(G_N)_{N\geq 1}$ returns a succinct representation for a family of games $(G'_n)_{n\geq 1}$ such that the following conditions hold for all $n \geq 1$ and $N = 2^n$:

(1) If $\omega(G_N) = 1$ then $\omega(G'_n) = 1$;

(2) The smallest dimension of an entangled state sufficient to succeed in G'_n with probability at least $\frac{1}{2}$ is at least the maximum of N and the smallest dimension of an entangled state sufficient to succeed in G_N with probability at least $\frac{1}{2}$.

In the talk we showed that, provided some additional technical conditions are satisfied, the existence of such a compression procedure leads through an (effective) fixed-point argument to a proof of the equality MIP*=RE. We then briefly sketched how the desired compression procedure could be designed by combining techniques from the classical theory of probabilistically checkable proofs with arguments on the rigidity of quantum entanglement, leading to methods for "compressing" the communication in an interactive proof with quantum provers.

References

[1] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP*= RE. *arXiv preprint arXiv:2001.04383*, 2020.

Tensors in Quantum Information Theory and their Relation to Algebraic Complexity

Matthias Christandl

(joint work with Peter Vrana and Jeroen Zuiddam)

The state of a system of several quantum particles is an element in the tensor product of Hilbert spaces. In certain situations, the inner product requirement can be relaxed. Quantum states then turn into tensors, and tools and intuition from quantum information and algebraic complexity can connect.

Motivated by the complexity of matrix multiplication, Strassen introduced the asymptotic restriction problem of tensors [1]. The problem is very natural also from a quantum information theoretic point of view, and has led us to the construction of a set of obstructions for asymptotic restriction, which we call the quantum functionals [2].

We will call elements of $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$ *tensors*. Given two tensors t and t', we will write $t \geq t'$ if there are matrices a, b and c s.th. $a \otimes b \otimes ct = t'$ and then say that *t restricts to t'*. Note that the notion of restriction is invariant under enlarging the spaces and also results in an equivalence relation. Special is the tensor $t = \alpha \otimes \beta \otimes \gamma$, which, when combined with the direct sum operations $\oplus$ (r times) allows to construct the *unit tensor* $\langle r \rangle = \sum_i e_i \otimes e_i \otimes e_i$ for a basis e_i of $\mathbb{C}^r$. One can also combine tensors with the Kronecker product $\otimes$, an operation which naturally leads to define *asymptotic restriction* $t \succsim t'$ by $t^{\otimes n+o(n)} \geq t'^{\otimes n}$. Interestingly, the exponent of matrix multiplication equals two if and only if $\langle 4 \rangle \succsim \langle 2,2,2 \rangle$, where $\langle 2,2,2 \rangle$ is the matrix multiplication tensor for multiplying 2-by-2 matrices. Obstructions to asymptotic restriction therefore correspond to lower bounds on algorithms (e.g. for matrix multiplication). Strassen showed that indeed there is a complete set of obstructions given by restriction-monotone, multiplicative, additive and normalised functionals on the set of tensors, but how to find those?

Given a tensor t, we can *flatten* it to a matrix $t_A \in \mathbb{C}^d \otimes (\mathbb{C}^d \otimes \mathbb{C}^d)$ and similarly for the other two options of grouping two spaces. Since matrix rank has all the required properties, rank t_A is an obstruction in Strassen's sense. In our work, we construct a family of functionals, the *quantum functionals* $F_\theta(t) := 2^{E_\theta(t)}$, which in a sense interpolate between the flattening ranks. They are defined for weights $\theta_A \geq 0, \theta_B \geq 0, \theta_C \geq 0 \sum_i \theta_i = 1$ as

$$E_\theta(t) := \sup_{t \geq t'} \left(\theta_A H(t'_A) + \theta_B H(t'_B) + \theta_B H(t'_C)\right),$$

where $H(t_A)$ is the Shannon entropy of the singular values squared of $t_A/||t||_2$. In quantum information language, $H(t_A)$ is the von Neumann entropy of the reduced density matrix (of particle A) of the quantum state $t/||t||_2$. Asymptotic restriction can be cast into the form of a distributed compression tasks for independent and identically prepared triples of quantum particles (the quantum analog of i.i.d. random variables). The proof of multiplicativity of F_θ is the most crucial one and uses a dual characterization of the moment polytope due to Brion for the action of $GL(d) \times GL(d) \times GL(d)$ on $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$.

References

[1] V.Strassen *The asymptotic spectrum of tensors* J. Reine Angew. Math., **384** (1988) 102–152.

[2] M. Christandl, J. Zuiddam, P. Vrana *Universal points in the asymptotic spectrum of tensors*, accepted for publication in Journal of the American Mathematical Society (2022).

New bounds for the sunflower lemma, and connections to complexity theory

Shachar Lovett

(joint work with Ryan Alweiss, Kewen Wu, Jiapeng Zhang)

1. Introduction

We start by defining the main object of interest for us: sunflowers.

Definition 1.1 (Sunflower). *A collection of sets $S_1, \ldots, S_r$ is called an r-*sunflower *if all their pairwise intersections are the same. Namely, if*

$$S_i \cap S_j = S_1 \cap \cdots \cap S_r \qquad \forall i \neq j.$$

We call $K = S_1 \cap \cdots \cap S_r$ the kernel *of the sunflower.*

Erdős and Rado [3] proved that large enough set systems must contain a sunflower. It is noteworthy that Erdős and Rado originally called sunflowers Δ-systems, but the term "sunflower" was coined by Deza and Frankl [2] and is now more widely used. To describe the lemma we need some notation: a w-set system is a family of sets, each of size at most w.

Lemma 1.2 (Sunflower lemma [3])**.** *Let $r \geq 3$ and $\mathcal{F}$ be a w-set system of size $|\mathcal{F}| \geq w! \cdot (r-1)^w$. Then $\mathcal{F}$ contains an r-sunflower.*

Erdős and Rado conjectured in the same paper that the bound in Lemma 1.2 can be drastically improved.

Conjecture 1.3 (Sunflower conjecture [3])**.** *Let $r \geq 3$. There exists $c = c(r)$ such that any w-set system $\mathcal{F}$ of size $|\mathcal{F}| \geq c^w$ contains an r-sunflower.*

The bound in Lemma 1.2 is of the form $w^{w(1+o(1))}$ where the $o(1)$ term depends on r. Despite nearly 60 years of research, the best known bounds were still of the form $w^{w(1-o(1))}$. In this work, we vastly improve the known bounds. We prove that any w-set system of size $(\log w)^{w(1+o(1))}$ must contain a sunflower. More precisely, we prove the following:

Theorem 1.4 (Main theorem, sunflowers)**.** *Let $r \geq 3$. Any w-set system $\mathcal{F}$ of size $|\mathcal{F}| \geq (\log w)^{w(1+o(1))} r^{O(w)}$ contains an r-sunflower.*

This bound has since been strengthened; see the subsequent works subsection for details.

1.1. **Robust sunflowers.** We consider a "robust" generalization of sunflowers, the study of which was initiated by Rossman [13], who was motivated by questions in complexity theory. Later, it was studied by Li, Lovett and Zhang [9] in the context of the sunflower conjecture.

Given a finite set X, we denote by $\mathcal{U}(X,p)$ the p-biased distribution over X; namely, the distribution over subsets $R \subset X$, where each element $x \in X$ is included in R independently with probability p.

Definition 1.5 (Satisfying set system)**.** *Let $0 < \alpha, \beta < 1$. A set system $\mathcal{F}$ on X is (α,β)-satisfying if*

$$\Pr_{R \sim \mathcal{U}(X,\alpha)}[\exists S \in \mathcal{F}, S \subset R] > 1 - \beta.$$

The explanation for the name "satisfying" is that if the set system is interpreted as a disjunctive normal form (DNF) formula, then this condition is that the formula has more than a $1-\beta$ probability of being satisfied on α-biased inputs; see [10]. We next use this to define *robust sunflowers.*

Definition 1.6 (Robust sunflower)**.** *Let $0 < \alpha, \beta < 1$, $\mathcal{F}$ be a set system, and let $K = \bigcap_{S \in \mathcal{F}} S$ be the common intersection of all sets in $\mathcal{F}$. $\mathcal{F}$ is an (α,β)-robust sunflower if (i) $K \notin \mathcal{F}$, and (ii) $\mathcal{F}_K$ is (α,β)-satisfying. We call K the* kernel*.*

As the name suggests, robust sunflowers indeed generalize sunflowers.

Lemma 1.7 ([10, Corollary 15])**.** *Any $(1/r, 1/r)$-robust sunflower contains an r-sunflower.*

Theorem 1.4 follows directly from the following theorem, which shows that any large enough set system must contain a robust sunflower.

Theorem 1.8 (Main theorem, robust sunflowers)**.** *Let $0 < \alpha, \beta < 1$. Any w-set system $\mathcal{F}$ of size $|\mathcal{F}| \geq \log(w)^{w(1+o(1))} \left(\log(1/\beta)/\alpha\right)^{O(w)}$ contains an (α, β)-robust sunflower.*

1.2. **Proof ideas.** Given a set system $\mathcal{F}$ on X and a set $T \subset X$, the *link* of $\mathcal{F}$ at T is

$$\mathcal{F}_T = \{S \setminus T : S \in \mathcal{F}, T \subset S\}.$$

We next use links to define *spread* set systems.

Definition 1.9 (Spread set systems, [10])**.** *We say that a w-set system $\mathcal{F}$ is κ-*spread *if $|\mathcal{F}| \geq \kappa^w$ and $|\mathcal{F}_T| \leq \kappa^{-|T|}|\mathcal{F}|$ for all non-empty T, where $|\mathcal{F}_T|$ is the size of the link at T.*

Say $\mathcal{F}$ is a w-set system of size $|\mathcal{F}| \geq \kappa^w$ on a ground set X. Then either $\mathcal{F}$ is κ-spread, or there is a link $\mathcal{F}_T$ of size $|\mathcal{F}_T| \geq \kappa^{w-|T|}$. In the latter "structured" case, we can simply pass to the link and apply induction, much like in the original proof of Erdős and Rado [3].

Thus, it suffices to consider the "pseudorandom" case of w-set systems which are κ-spread. In [9, 10], it was conjectured that for $\kappa = (\log w)^{O(1)}$, any κ-spread set system is also $(1/3, 1/3)$-satisfying. We show that in fact that is true for $\kappa = (\log w)^{1+o(1)}$ and that this value is tight, up to the $o(1)$ term in the exponent.

We next outline how we obtain the bound on κ. We will prove that a κ-spread w-set system is (α, β)-satisfying for appropriate κ, w, α, β through a series of reductions.

Let $\mathcal{F}$ be a w-set system which is κ-spread. Sample $W \sim \mathcal{U}(X, p)$ for some $p = O(1/\log w)$. We show that with high probability over the choice of W, for almost all sets $S \in \mathcal{F}$, there exists a set $S' \in \mathcal{F}$ such that: (i) $S' \setminus W \subset S \setminus W$; and (ii) $|S' \setminus W| \leq w'$, for some w' which we will take to be $w(1-\varepsilon)$ for a small ε. We throw out sets S that do not satisfy this property (which we call the *bad* sets for W), and replace any S that does with $S' \setminus W$ (we call these the *good* sets for W). This yields a w'-set system $\mathcal{F}'$ which has almost as many sets as the original $\mathcal{F}$, and therefore will have almost the same spreadness. We continue in this manner $O(\log w)$ steps until we reach a set system of sizes of constant size, where we can apply standard probabilistic techniques to finish the proof.

In the language of DNFs, the width reduction step is to take a random restriction of a pseudorandom DNF and approximate the result by a smaller width DNF whose clauses come from removing some variables from clauses of the original DNF. The main idea to prove it is to use an encoding argument, inspired by Razborov's proof of Håstad's switching lemma [6, 12]. We show that pairs (W, S) for which S is bad for W can be efficiently encoded, crucially relying on the spreadness condition. This allows to show that for a random W it is very unlikely that there will be many bad sets.

1.3. **Subsequent works.** After the current work was made available on the ArXiv, Rao [11] simplified the proof using information theoretic techniques. Furthermore, following the initial release of this work, the technique developed in this paper has been used by Frankston, Kahn, Narayanan, and Park [4] to resolve a conjecture of Talagrand in random graph theory. Rao then used their refinements to further improve the bound in Theorem 1.8 to $((C/\alpha)\log(w/\beta))^w$ and the bound in Theorem 1.4 to $(Cr\log(wr))^w$. Bell, Chueluecha, and Warnke [1] observed that a small modification of the argument improves the bound in Theorem 1.4 further to $(Cr\log(w))^w$. Following Rao's proof using information theory, two more proofs using information theory were given (in blogs) by Tao [14] and by Hu [7].

References

[1] T. Bell, S. Chueluecha, and L. Warnke. Note on sunflowers. *Discrete Mathematics*, 344(7):112367, 2021.

[2] M. Deza and P. Frankl. Every large set of equidistant $(0,+1,-1)$-vectors forms a sunflower. *Combinatorica*, 1(3):225–231, 1981.

[3] P. Erdős and R. Rado. Intersection theorems for systems of sets. *Journal of the London Mathematical Society*, 35(1):85–90, 1960.

[4] K. Frankston, J. Kahn, B. Narayanan, and J. Park. Thresholds versus fractional expectation-thresholds. *Annals of Mathematics*, 194(2):475–495, 2021.

[5] J. Fukuyama. Improved bound on sets including no sunflower with three petals. *arXiv preprint arXiv:1809.10318*, 2018.

[6] J. Håstad. *Computational limitations of small-depth circuits.* MIT Press, Cambridge, MA, USA, 1987.

[7] L. Hu. Entropy estimation via two chains: Streamlining the proof of the sunflower lemma. `http://theorydish.blog/2021/05/19/entropy-estimation-via-two-chains-streamlining-the-proof-of-the-sunflower-lemma`, 2021.

[8] A. Kostochka. A bound of the cardinality of families not containing Δ-systems. In *The Mathematics of Paul Erdős II*, pages 229–235. Springer, 1997.

[9] X. Li, S. Lovett, and J. Zhang. Sunflowers and quasi-sunflowers from randomness extractors. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2018).* Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

[10] S. Lovett, N. Solomon, and J. Zhang. From DNF compression to sunflower theorems via regularity. In *34th Computational Complexity Conference, CCC 2019, July 18-20, 2019, New Brunswick, NJ, USA.*, pages 5:1–5:14, 2019.

[11] A. Rao. Coding for sunflowers. *Discrete Analysis*, 2020.

[12] A. A. Razborov. Bounded arithmetic and lower bounds in boolean complexity. In *Feasible Mathematics II*, pages 344–386. Springer, 1995.

[13] B. Rossman. The monotone complexity of k-clique on random graphs. *SIAM J. Comput.*, 43(1):256–279, 2014.

[14] T. Tao. The sunflower lemma via shannon entropy. `http://terrytao.wordpress.com/2020/07/20/the-sunflower-lemma-via-shannon-entropy`, 2020.

Noncommutative Property Testing

Henry Yuen

In the standard setting of property testing, a randomized algorithm (called a *tester*) is given query access to a black box that responds with deterministic evaluations of an unknown function $f : \mathcal{X} \to \mathcal{A}$. The goal of the the algorithm is to determine whether the function f has some property P or is far from having it, where we measure the distance of f from P to be the minimum fraction of values $f(x)$ over $x \in \mathcal{X}$ that have to be changed in order for f to have property P.

Recall one of the most important topics in property testing: testing linear functions. The famous Blum-Luby-Rubinfeld (BLR) test queries an unknown function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ at x, y, and $x + y$ for uniformly random $x, y \in \mathbb{F}_2^n$ and checks if $f(x)+f(y) = f(x+y)$. Blum, Luby and Rubinfeld [1] showed that any function f accepted by the BLR test with probability $1-\epsilon$ must be $O(\epsilon)$-close to a linear function (i.e. a function that satisfies the linearity condition $f(x)+f(y) = f(x+y)$ for *all* pairs (x, y)). Thus, the linearity property has strong *local-to-global* features: approximately satisfying linearity *locally* is enough to constrain the function to approximately satisfying linearity *globally*.

We consider generalizing the model of property testing to more general models of black boxes that the tester may have access to. What if we consider *probabilistic* boxes? That is, whenever the tester algorithm makes a query $x \in \mathcal{X}$ to the box, there is some probabilistic process that generates an output $a \in \mathcal{A}$; in the most general scenario, these probabilistic processes don't necessarily have to be independent of the previous queries and outputs! Guided by physical principles, we can imagine that a reasonable model would be a box whose internal processes are described by *quantum mechanics*.

We formalize a model of quantum mechanical boxes via the notion of *quantum functions*. A quantum function F with input set $\mathcal{X}$ and output set $\mathcal{A}$ is specified by the following data:

(1) A dimension $d \in \mathbb{N}$,
(2) For all $x \in \mathcal{X}$, a set of *measurements* A_x, which itself is a set of positive semidefinite $d \times d$ matrices $\{A_{a|x}\}_{a\in\mathcal{A}}$ satisfying $\sum_{a\in\mathcal{A}} A_{a|x}^2 = I$.

Querying a quantum function F with sequence of queries $(x_1, \ldots, x_q) \in \mathcal{X}^q$ yields a sequence of outputs $(a_1, \ldots, a_q) \in \mathcal{A}^q$ with probability

$$p(a_1, \ldots, a_q \mid x_1, \ldots, x_q) = \|A_{a_1|x_1} \cdot A_{a_2|x_2} \cdots A_{a_q|x_q}\|_\tau^2$$

where $\|X\|_\tau = \sqrt{\frac{1}{d}\mathrm{Tr}(XX^*)}$ denotes the *normalized Frobenius norm* of a matrix X (with $\mathrm{Tr}(\cdot)$ denoting the matrix trace and X^* denoting the adjoint of X). We call this function p the *q'th moment of F*. It is easy to verify that $p(a_1, \ldots, a_q \mid x_1, \ldots, x_q)$ is a valid probability distribution over $\mathcal{A}^q$. This formula for p_F is motivated by quantum mechanics; it corresponds to the probability of sequentially performing measurements $A_{x_1}, A_{x_2}, \ldots, A_{x_q}$ on a certain quantum state known as the *maximally entangled state* and obtaining outcomes $(a_1, a_2, \ldots, a_q)$.

An important aspect of quantum functions is that the output probabilities *depend on the order of queries*. This is because the measurement operators $A_{a|x}$ and $A_{b|y}$ need not *commute* (i.e., in general $A_{a|x}A_{b|y} \neq A_{b|y}A_{a|x}$). When the measurement operators all commute, then this model essentially reduces to the classical setting. This is formalized by the following:

Theorem 1.1. *Let F be a quantum function where all measurements commute. Then there exists a finite set Λ, a probability distribution μ over Λ, and a set* *of (classical) functions* $\{f_\lambda : \mathcal{X} \to \mathcal{A}\}_{\lambda \in \Lambda}$ *such that for all* $q \in \mathbb{N}$*, the q'th moment of* F *is distributed the same as first sampling* $\lambda \sim \mu$*, and then outputting* $(f_\lambda(x_1), \ldots, f_\lambda(x_q))$*.*

In other words, querying a commutative quantum function F is essentially the same as querying a classical box that first samples a function f_λ from some distribution, and then deterministically responds according to f_λ.

Things get much more interesting when the measurements don't commute. This gives rise to *noncommutative property testing*, in which tester algorithms are given query access to an arbitrary quantum function F, and the goal is to deduce whether F satisfies some global property or is far from satisfying it. A number of questions immediately come to mind. What kinds of noncommutative properties are there? How does one measure a quantum function's distance to a noncommutative property? What properties of quantum functions can be tested using few queries?

Let's revisit linearity testing. Suppose we run the BLR test with a quantum function $F : \mathbb{F}_2^n \to \mathbb{F}_2$, where now we pay attention to the fact that the tester has to specify an order to the queries. If the test passes with probability $1 - \epsilon$, can we deduce anything about the structure of F? The next theorem is shows that we have guarantees analogous to that in the classical (i.e. deterministic) setting:

Theorem 1.2. *Let* F *be a quantum function that passes the BLR test with probability* $1 - \epsilon$*. Then there exists a* commuting *quantum function* G *that passes the BLR test with probability* 1 *and* F *is* $O(\sqrt{\epsilon})$*-close to* G*.*

For lack of space we omit a precise definition of closeness between quantum functions here; however it suffices to think of it as measuring how close the measurement operators of the two quantum functions are. Keep in mind that the quantum function F could have, *a priori*, extremely complicated measurements in enormous dimension. However Theorem 1.2 shows that these measurements must be close (in the appropriate sense) to being commutative, and thus the function F must be close to being a convex combination of deterministic functions (by Theorem 1.1).

Let's turn to an example where noncommutative behavior is *necessary.* Consider the following constraint satisfaction problem called the *Magic Square CSP.* There are 9 variables $u_1, \ldots, u_9 \in \{\pm 1\}$ arranged in a 3×3 grid. Each row of variables must multiply to $+1$ and each column of variables must multiply to -1. This is clearly an unsatisfiable CSP. Consider the following tester (called the *Magic Square test*) that is given query access to a function $f : [9] \to \{\pm 1\}$. It chooses a row or column of the grid at random, and then queries the function f at the corresponding cells, and checks whether the corresponding constraint is satisfied. Since the CSP is unsatisfiable, all functions f must fail with some positive probability.

On the other hand, there exists a *quantum function* F that passes the Magic Square test with probability 1! By the foregoing discussion and Theorem 1.1, it must be that F is noncommutative and in particular the dimension of F must be greater than 1 (in fact, the minimum dimension of any quantum function F that passes perfectly is 4). This is a rather remarkable conclusion; the dimension of a quantum function F is not something that is directly accessible via queries.

What about tests for larger dimensions? Are there tradeoffs between the dimension guarantee, the complexity of the test, and the test's robustness? The quantum complexity theory result MIP* = RE [3], viewed as a result about noncommutative property testing, implies that there are *no* tradeoffs necessary:

Theorem 1.3 (Corollary of MIP* = RE)**.** *There exist finite sets $\mathcal{X}, \mathcal{A}$ and a test T for quantum functions $F : \mathcal{X} \to \mathcal{A}$ such that (1) the test T makes only two queries to F, (2) if a quantum function F is finite dimensional, then* $\Pr[T \textit{ accepts } F] \leq \frac{1}{2}$*, (3) there exists a quantum function F such that*

$$\Pr[T \textit{ accepts } F] = 1.$$

Clearly, the function F that is accepted by the test T with certainty must have *infinite* dimension. Furthermore, by the guarantees of the test T, it cannot be approximated arbitrarily well by finite-dimensional quantum functions; thus T is a *robust* test for infinite-dimensionality. This also has surprising consequences for pure mathematics; the existence of such an inapproximable infinite-dimensional quantum function F directly gives a negative answer to something known as Connes' embedding problem, which was a long-standing question in the study of von Neumann algebras [5].

At the heart of the construction of the test T from MIP* = RE is the analysis of the *low degree test* with quantum functions. Low-degree testing is a generalization of linearity testing where instead of checking that a function is linear, one checks that local "sections" of the function are consistent with a low-degree polynomial [6]. Just as low-degree testing was one of the key drivers of the original proofs of the PCP Theorem, it plays a similarly central role in the construction of the test T [2, 4].

The MIP* = RE result, when formulated in this way, illustrates the depth and richness of the noncommutative property testing framework. There are many interesting questions and avenues to explore in this subject. For example, is there a characterization of when a test forces a quantum function to be commutative? What happens if we try to test *graph properties* with quantum functions? Beyond testing dimension, can one design tests that force a quantum function's measurements to generate a specific *algebra*? Are there applications of noncommutative property testing to algorithms, complexity theory, or cryptography?

References

[1] M. Blum, M. Luby, R. Rubinfeld. *Self-testing/correcting with applications to numerical problems.* Journal of Computer and System Sciences, 47(3), 549-595. (1993)

[2] T. Ito and T. Vidick. *A multi-prover interactive proof for NEXP sound against entangled provers.* IEEE 53rd Annual Symposium on Foundations of Computer Science. (2012)

[3] Z. Ji, A. Natarajan, T. Vidick, J. Wright, H. Yuen. *MIP* = RE.* arXiv preprint arXiv:2001.04383. (2020)

[4] Z. Ji, A. Natarajan, T. Vidick, J. Wright, H. Yuen. *Quantum soundness of the classical low individual degree test.*. arXiv preprint arXiv:2009.12982. (2020)

[5] N. Ozawa. *About the Connes embedding conjecture.* Japanese Journal of Mathematics 8.1: 147-183. (2013)

[6] R. Rubinfeld and M. Sudan. *Self-testing polynomial functions efficiently and over rational domains.* In SODA, pages 23–32. (1992)

Approximate Counting & Sampling using HDX

Shayan Oveis Gharan

(joint work with Dorna Abdolazimi, Nima Anari, Kuikui Liu, Cynthia Vinzant)

Let U be a ground set of elements and $n \geq 1$ be an integer. Given a weight function $w : \binom{U}{n} \to \mathbb{R}_{\geq 0}$ we consider the following tasks:

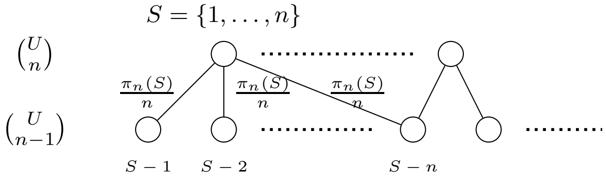
- Sample a set $S \in \binom{U}{n}$ with probability proportional to $w(S)$
- Compute the "normalizing constant" of this distribution, namely $\sum_{S\in\binom{U}{n}} w(S)$.

It follows by a classic result of Jerrum, Valiant and Vazirani [9] that the above two problems are equivalent for most interesting probability distributions and more generally even the approximate versions of these problems are equivalent.

So, in this extended abstract we will mainly address the sampling problem. Broder [4] in his influential paper proposed to design a Markov chain with stationary distribution $\pi_n(S) := \frac{w(S)}{\sum_{T\in\binom{U}{n}} w(T)}$ and then bound the *mixing time* of the chain. Recall that for a Markov chain with transition probability matrix P the mixing time is

$$\tau_{\text{mix}} = \max_{S\in\binom{U}{n}} \min\{t : \left\|P^t(S,.) - \pi_n\right\|_1 \leq 1/4\},$$

where $P^t(S,.)$ is the distribution of the chain started at S after t steps. In this extended abstract we will study the following Markov chain to sample from π_n: Given a state S, first we delete a uniformly random element from S, say i and we go to $S - \{i\}$. Then, from all the sets T that contain $S - \{i\}$ we choose one with probability proportional to $\pi_n(T)$. In other words, consider a weighted bipartite graph $G = (\binom{U}{n}, \binom{U}{n-1}, E)$ where a set $S \in \binom{U}{n}$ is connected to $T \in \binom{U}{n-1}$ iff $T \subseteq S$ and the weight of that edge is equal to $\frac{\pi_n(S)}{n}$. The aforementioned chain is the same as running a simple random walk on this bipartite graph where from each vertex we jump to a neighbor with probability proportional to the weight edge connecting to the neighbor. Since the (weighted) degree of every vertex $S \in \binom{U}{n}$ is exactly $\pi_n(S)$, the stationary distribution on the top vertices is exactly $\pi_n(.)$. See the following diagram for an example. This walk is known as the down-up walk in the high-dimensional expander language [10], the Glauber dynamics in statistical physics and basis exchange walk in the matroid language. For a concerete example, let $G = (V, E)$ be a graph with $n := |V|$ vertices that we want to uniformly randomly color with q colors. We define U to be the set of all vertex-color pairs, (v, c), $v \in V, c \in [q]$. A set $S \in \binom{U}{n}$ is in support if π_n if it corresponds to a valid proper color of G and π_n is simply the uniform distribution over all such sets. In such a



case the down-up walk corresponds to first choosing a u.r. vertex of G, v; then "un-color" v. Finally, among all valid colors we can assign to v, choose one u.a.r.

Classical Techniques: Classically there are two well-known methods to study mixing time of random walks.

- **Canonical Path Method:** This method was proposed in the influential work of Jerrum and Sinclair [7]. The high-level idea is to construct a multi-commodity flow on the graph of the Markov chain between each pair of states and then use the connection to the sparsest cut problem to bound the spectral gap of the chain. This method is most famously used to sample a uniformly random perfect matching from a bipartite graph [8]. Unfortunatley, most applications of this method is limited to problems related to matchings.
- **Path Coupling:** In this method, one would directly bound the mixing time by designing a "Markovian coupling" between the distribution of the chain and the stationary distribution. This method is widely used in theory but often it does not give the optimal result.

Write $P_n^{\vee}$ to denote the transition probability matrix of the down-up walk we defined above. In this extended abstract we explain a new technique to analyze the mixing time of these family of walks called the *spectral independence.*

Definition 1.1. *Given a probability distribution π_n on $\binom{U}{n}$, define a matrix $\Psi \in \mathbb{R}^{U \times U}$ where for any $i, j \in U$,*

$$\Psi_{\pi_n}(i,j) = \mathbb{P}_{S\sim\pi_n}\left[j \in S | i \in S\right] - \mathbb{P}_{S\sim\pi_n}\left[j \in S\right].$$

We say π_n is η-spectrally independent if $\lambda_{\max}(\Psi_{\pi_n}) \leq \eta$. We say π_n is η^*-spectrally independent if for any sequence $i_1, \ldots, i_{n-2} \in U$, $(\pi_n), (\pi_n | i_1), (\pi_n | i_1, i_2), \ldots,$ $(\pi_n | i_1, \ldots, i_n)$ are η-spectrally independent.

For example, suppose π_n is a product distribution. In that case for any $i, j \in U$, $\mathbb{P}[j|i] = \mathbb{P}[j]$. Therefore, all off-diagonal entries of Ψ_{π_n} are zero; since the diagonal entries are at most 1, π_n is 1-spectrally independent. For another example, if π_n is a *negatively correlated* distribution, namely for any $i, j \in U$, $\mathbb{P}[j|i] \leq \mathbb{P}[j]$, then all off-diagonal entries of Ψ_{π_n} are non-positive and their sum in every row is exactly -1. It follows that π_n is 2-spectrally independent. Lastly, for a bad example, suppose there are only two sets in the support of π_n; namely $\pi_n(\{1, \ldots, n\}) = \pi_n(\{n+1, \ldots, 2n\} = 1/2$. In this case the distribution is very positively correlated (and in fact the down-up walk explained before is not even connected). It follows that $\Psi_{\pi_n} = \frac{1}{2}\begin{pmatrix} J_n & -J_n \\ -J_n & J_n \end{pmatrix}$. So, π_n is n-spectrally independent.

The following "local-to-global" theorem follows from a long line of works in theory of high dimensional expanders and extensions to the field of analysis of random walks:

Theorem 1.2 ([6, 11, 1, 2])**.** *If π_n is η^* spectrally independent then the down-up walk $P_n^\vee$ has spectral gap at least $\frac{1}{O(n^{1+\eta})}$ and thus it mixes in polynomial time, assuming $\eta \leq O(1)$.*

In other words, the above theorem shows that even if π_n is positively correlated, but the positive correlations are "limited" then still the simple down-up walk mixes rapidly. Building on the above theorem over the last couple of years it was shown that a number of well-known probability distributions are indeed spectrally independent; this has lead to the resolution of several long standing open problems (see below).

Sampling Bases of Matroids: Given a matroid M of rank n, defined on the ground set of elements U, let π_n be the uniform distribution over the bases of M. In [3] it was shown that such a distribution is 2-spectrally independent therefore the down-up walk gives a fast algorithm to sample bases of matroids. As a consequence this work gave the first efficient algorithm to sample forests of a given graph or to sample from the "reliability polynomial" of matroids.

Sampling from the Hard-core Distribution: Given a graph $G = (V, E)$ with n vertices, a set $S \subseteq V$ is an independent set if there are no edges of E connecting vertices of S. Define U to be the set of $(v, \text{in}), (v, \text{out})$ for any $v \in V$. Given an "activity threshold" $\lambda > 0$, let π_n be the distribution over $\binom{U}{n}$ where a set $S \in \binom{U}{n}$ is in the support of π_n if every vertex is either in or out and the set of in vertices form an independent set of G. In such a case we define $\pi_n(S) = \lambda^{\#\text{in vertices}}$. This probability distribution is called the hard-core model and it is of utmost importance in statistical physiscs to design efficient algorithm to sample from π_n for the largest possible value of λ. In sequence of works [2, 5] it was shown for the first time that π_n is η^* independent from $\eta \leq O(1)$ when $\lambda \leq \lambda^*(\Delta)$, the tree uniqueness threshold above which it is NP-hard to sample from π_n. Here Δ is the maximum degree of graph G.

Open Problem. It remains an open problem to relate the canonical path method to the spectral independence technique. Such a result could have an abundance of applications in the field of approximate counting and sampling most notably in sampling perfect matchings in non-bipartite graphs.

References

[1] V. L. Alev, L. C. Lau, *Improved analysis of higher order random walks and applications*, STOC (2020), pages 1198-1211.

[2] N. Anari, K. Liu, S. Oveis Gharan, *Spectral Independence in High-Dimensional Expanders and Applications to the Hardcore Model*, SIAM Journal on Computing, FOCS20-1-FOCS20-37 (2021).

[3] N. Anari, K. Liu, S. Oveis Gharan, C. Vinzant, *Log-concave polynomials II: high-dimensional walks and an FPRAS for counting bases of a matroid*, STOC (2019), pages 1-12.

[4] A. Z. Broder, *How hard is it to marry at random?(On the approximation of the permanent)*, STOC 1986, pp. 50-58.

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

[6] I. Dinur, T. Kaufman, *High Dimensional Expanders Imply Agreement Expanders*, FOCS (2017), pages 974-985.

[7] M. Jerrum, A. Sinclair, *Approximating the Permanent*, Siam J. of Computing, **18(6)** (1989), pages 1149-1178.

[8] M. Jerrum, A. Sinclair, E. Vigoda, *A polynomial-time approximation algorithm for the permanent of a matrix with nonnegative entries*, Journal of the ACM, **51 (4)** (2004), pages 671–697.

[9] M. Jerrum, L. Valiant, V. Vazirani, *Random Generation of Combinatorial Structures from a Uniform Distribution*, Theoretical Computer Science, **43** (1986), 168-188.

[10] T. Kaufman, D. Mass, *High dimensional random walks and colorful expansion*, ITCS (2017), pages 4:1–4:27.

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

Locally Testable Codes with constant rate, distance, and locality

Irit Dinur

(joint work with Shai Evra, Ron Livne, Alexander Lubotzky, Shahar Mozes)

A locally testable code (LTC) is an error correcting code that has a property-tester. The tester reads q bits (randomly - but not necessarily uniformly - chosen) from a given word, and rejects words with probability proportional to their distance from the code. The parameter q is called the locality of the tester.

A random error-correcting code has, with high probability, constant rate and distance, but locality that is proportional to the length. This is true even for random LDPC codes [7], and a priori the mere existence of codes with constant locality is not obvious. The first LTCs appear implicitly in works on program checking [8] and on probabilistically checkable proofs (PCPs) [4, 21, 5, 3, 1]. A formal definition of an LTC appeared simultaneously in several places [5, 23, 15, 2] (see [18] for a detailed history). Spielman, in his PhD thesis [24], discusses the possibility of having an error-correcting code that is locally testable (he uses the term 'checkable code') and explains its potential applicability: *"A checker would be able to read only a constant number of bits of a received signal and then estimate the chance that a decoder will be able to correct the errors, then the checker can instantly request a retransmission of that block, before the decoder has* *wasted its time trying to decode the message. Unfortunately all known codes with local-checkers have rate approaching zero."*

Goldreich and Sudan [19] initiated a systematic study of LTCs as objects of interest in their own right. Over the years better and better LTCs were constructed [22, 19, 11, 6, 9, 13, 20, 16], but, nevertheless, experts went back and forth on whether "c^3-LTCs" (namely, LTCs with **c**onstant rate, **c**onstant distance, and **c**onstant locality) are likely to exist, compare [17] with [18, Section 3.3.2].

An outstanding open question has been whether there exist "c^3-LTCs", namely LTCs with **c**onstant rate, **c**onstant distance, and **c**onstant locality. We construct the first such family of LTCs,

Theorem. *For all $0 < r < 1$, there exist $\delta, \kappa > 0$ and $q \in \mathbb{N}$ and a polynomial-time construction of an infinite family of error-correcting codes $\{C_n\}$ with rate r and distance δ, such that for all n, C_n is κ-locally testable with q queries.*

Namely, every code C_n comes with a randomized local tester that reads at most q bits from a given word w and then accepts or rejects, such that

- *For all $w \in C_n$, $\Pr[accept] = 1$.*
- *For all $w \notin C_n$, $\Pr[reject] \geq \kappa \cdot \mathrm{dist}(w, C_n)$.*

We remark that [20, 16] have shown (see [16, Section 1.2]) how to take an LTC with rate arbitrarily close to 1 and with constant distance, and construct a new LTC with rate and distance approaching the Gilbert-Varshamov bound, and only a constant overhead in the locality q. So the theorem above holds for all $r, \delta > 0$ that satisfy $r + h(\delta) < 1$ where $h(\cdot)$ is the binary entropy function.

Expander codes, one dimension up. The celebrated expander-codes of Sipser and Spielman [25] are a family of error-correcting codes constructed from a single base code $C_0 \subseteq \mathbb{F}_2^d$ and a family of d-regular expander graphs $G_n = (V_n, E_n)$ such that the code corresponding to G_n consists of functions on E_n such that for every vertex in V_n, the local view from the neighboring edges (assuming some arbitrary fixed ordering) is itself in the base code C_0,

$$C = \left\{ f : E_n \to \mathbb{F}_2 \,\middle|\, \forall v \in V_n, f|_{edges(v)} \in C_0 \right\}.$$

Similarly, our codes will also be defined via a fixed base-code and an infinite family of expander graphs. Our graphs will have, in addition to vertices and edges, also two-dimensional faces, called squares, where each square touches four edges and four vertices.

Our codewords are functions *on the squares* such that for every edge, the bits on the neighboring squares form a codeword in the base code. It is natural to view our code as a Tanner code [26] with bits on the squares and constraints on the edges; whereas the expander-codes have bits on the edges and constraints on the vertices.

Inspecting our code on the set of squares neighboring a fixed vertex, we see an intermediate code, whose constraints come from the edges neighboring that vertex.

We thus have three codes for the three dimensions of links: the base code C_1 at the link of an edge, the intermediate code C_0 at the link of a vertex, and the global code C at the link of the empty face which is the set of all squares.

Left-Right Cayley Complex. Let us describe our construction of a graph-with-squares, namely a square complex. Let G be a finite group with two sets of generators A, B. We define the left-right Cayley complex $X = Cay^2(A, G, B)$ as follows

- The vertices are $X(0) = G$.
- The edges are $X(1) = X^A(1) \sqcup X^B(1)$ where

$$X^A(1) = \{\{g, ag\} \mid \ g \in G, a \in A\}, \qquad X^B(1) = \{\{g, gb\} \mid \ g \in G, b \in B\}.$$

The fact that with A we multiply on the left, and with B we multiply on the right, gives a local commutativity which generates many four-cycles, namely, squares. Indeed for every a, g, b the graph has a cycle of length 4 with alternating A and B edges, given by the walk g, gb, agb, ag, g. We place a square for each of these four-cycles.

- The squares are a set of the following four-cycles in the graph,

$$X(2) = \{(g, gb, agb, ag, g) \mid \ g \in G, a \in A, b \in B\}.$$

We denote by $[a, g, b]$ the square containing the edges $\{g, ag\}$ and $\{g, gb\}$. By changing the 'root' of the square we get $[a, g, b] = [a^{-1}, ag, b] = [a^{-1}, ab, b^{-1}] = [a, gb, b^{-1}]$.

The Code. Fix a left-right Cayley complex $X = Cay^2(A, G, B)$, and fix a pair of base codes $C_A \subseteq \mathbb{F}_2^A$ and $C_B \subseteq \mathbb{F}_2^B$ (assuming $|A| = |B| = d$ we can take both to be isomorphic to some $C_1 \subseteq \mathbb{F}_2^d$). Our code is defined to be

$$C[A, G, B, C_A, C_B] =$$
$$\{f : X(2) \to \mathbb{F}_2 \mid \ \forall a, g, b, \ f([\cdot, g, b]) \in C_A, \text{ and } f([a, g, \cdot]) \in C_B\}.$$

Observe that for a codeword $f \in C$ and a fixed vertex $g \in G$, the restriction of f to the squares touching g is $f([\cdot, g, \cdot])$. It is not difficult to check that this word necessarily belongs to the tensor code $C_A \otimes C_B$. Thus, by putting the constraints around each edge, we get an intermediate code on the squares touching a vertex, which turns out to be a tensor code! Tensor codes have non-trivial dependencies among the constraints defining them. This often implies local testability of tensor codes [10, 14, 12], and turns out important for showing that our code can be locally tested by the following simple test:

Local test: Choose a random vertex g, and accept iff $f([\cdot, g, \cdot]) \in C_A \otimes C_B$.

Analysis. The lower bound on the rate and distance of our codes is proven similarly to the case of expander codes. Local testability is also shown via expansion of the underlying complex. We show that if a received word violates only a small amount of constraints, then locally it can be corrected, as long as the intermediate code $C_A \otimes C_B$ is itself *robustly locally testable.* We describe an iterative decoding algorithm and prove that it converges thanks to sufficient expansion of certain edge-to-edge random walks on our square complex. Conceptually, local local-testability (of the intermediate code $C_A \otimes C_B$), implies global local-testability (of the entire code), through expansion.

References

[1] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and intractability of approximation problems. *Journal of the ACM*, 45(3):501–555, 1998.

[2] S. Arora. *Probabilistic checking of proofs and the hardness of approximation problems.* PhD thesis, U.C. Berkeley, 1994. Available via anonymous ftp as Princeton TR94-476.

[3] S. Arora and S. Safra. Probabilistic checking of proofs: A new characterization of NP. *Journal of the ACM*, 45(1):70–122, 1998.

[4] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1:3–40, 1991.

[5] L. Babai, L. Fortnow, L. Levin, and M. Szegedy. Checking computations in polylogarithmic time. In *Proc. 23rd ACM Symp. on Theory of Computing*, pages 21–31, 1991.

[6] Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, and Salil Vadhan. Robust PCPs of proximity, shorter PCPs and applications to coding. *SIAM Journal on Computing*, 36(4):889–974, 2006. In special issue on Randomness and Computation.

[7] Eli Ben-Sasson, Prahladh Harsha, and Sofya Raskhodnikova. Some 3CNF properties are hard to test. *SIAM J. Comput.*, 35(1):1–21, 2005.

[8] M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. In *Proc. 22nd ACM Symp. on Theory of Computing*, pages 73–83, 1990.

[9] Eli Ben-Sasson and Madhu Sudan. Simple PCPs with poly-log rate and query complexity. In *Proc. 37th ACM Symp. on Theory of Computing*, pages 266–275, 2005.

[10] Eli Ben-Sasson and Madhu Sudan. Robust locally testable codes and products of codes. *Random Structures & Algorithms*, 28(4):387–402, 2006.

[11] Eli Ben-Sasson, Madhu Sudan, Salil P. Vadhan, and Avi Wigderson. Randomness-efficient low degree tests and short PCPs via epsilon-biased sets. In *Proc. 35th ACM Symp. on Theory of Computing*, pages 612–621, 2003.

[12] Eli Ben-Sasson and Michael Viderman. Tensor products of weakly smooth codes are robust. *Theory of Computing*, 5(12):239–255, 2009.

[13] Irit Dinur. The PCP theorem by gap amplification. *Journal of the ACM*, 54(3), 2007.

[14] Irit Dinur, Madhu Sudan, and Avi Wigderson. Robust local testability of tensor products of LDPC codes. In *Proc. 10th International Workshop on Randomization and Computation (RANDOM)*, 2006.

[15] Katalin Friedl and Madhu Sudan. Some improvements to total degree tests. *CoRR*, abs/1307.3975, 2013.

[16] Sivakanth Gopi, Swastik Kopparty, Rafael Mendes de Oliveira, Noga Ron-Zewi, and Shubhangi Saraf. Locally testable and locally correctable codes approaching the gilbert-varshamov bound. *IEEE Trans. Inf. Theory*, 64(8):5813–5831, 2018.

[17] Oded Goldreich. Short locally testable codes and proofs (survey). ECCC Technical Report TR05-014, 2005.

[18] Oded Goldreich. *Short Locally Testable Codes and Proofs: A Survey in Two Parts*, pages 65–104. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[19] Oded Goldreich and Madhu Sudan. Locally testable codes and PCPs of almost-linear length. *J. of the ACM*, 53(4):558–655, 2006.

[20] Swastik Kopparty, Or Meir, Noga Ron-Zewi, and Shubhangi Saraf. High-rate locally correctable and locally testable codes with sub-polynomial query complexity. *J. ACM*, 64(2):11:1–11:42, 2017.

[21] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, October 1992.

[22] A. Polishchuk and D. Spielman. Nearly linear size holographic proofs. In *Proc. 26th ACM Symp. on Theory of Computing*, pages 194–203, 1994.

[23] Ronitt Rubinfeld and Madhu Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM J. Comput.*, 25(2):252–271, 1996.

[24] Daniel A. Spielman. Linear-time encodable and decodable error-correcting codes. *IEEE Trans. Inform. Theory*, 42(6, part 1):1723–1731, 1996. Codes and complexity.

[25] Michael Sipser and Daniel A. Spielman. Expander codes. *IEEE Trans. Inform. Theory*, 42(6, part 1):1710–1722, 1996. Codes and complexity.

[26] R.M̃. Tanner. A recursive approach to low complexity codes. *IEEE Trans. Inform. Theory*, Vol. IT-27,(5):533–547, 1981.

Recent Advances on Foundations of Indistinguishability Obfuscation

Huijia Lin
(joint work with Aayush Jain, Amit Sahai)

Indistinguishability obfuscation (iO) for general programs computable in polynomial time [9] enables us to hide all implementation-specific details about any program while preserving its functionality. iO is a fundamental and powerful primitive, with a plethora of applications in cryptography and beyond. It is hence extremely important to investigate how to build iO, based on as *minimal assumptions* as possible, and via as *simple constructions* as possible. Advances on understanding what assumptions imply iO and simplification of iO constructions have immediate implications on the rest of cryptography through the many applications of iO.

The mathematical formalization of iO is as follows:

Definition 1.1 (Indistinguishability Obfuscator (iO) for Circuits [9])**.** *A probabilistic polynomial-time algorithm* iO *is called a secure indistinguishability obfuscator for polynomial-sized circuits if the following holds:*

- ***Completeness:*** *For every $\lambda \in \mathbb{N}$, every circuit C with input length n, every input $x \in \{0,1\}^n$, we have that*
$$\Pr\left[\tilde{C}(x) = C(x) \ : \ \tilde{C} \leftarrow i\mathrm{O}(1^\lambda, C)\right] = 1 \ .$$
- ***Indistinguishability:*** *For every two ensembles $\{C_{0,\lambda}\}_{\lambda\in\mathbb{Z}^+}$ and $\{C_{1,\lambda}\}_{\lambda\in\mathbb{Z}^+}$ of polynomial-sized circuits that have the same size, input length, and output length, and are functionally equivalent, that is, $\forall\lambda \in \mathbb{Z}^+$, $C_{0,\lambda}(x) = C_{1,\lambda}(x)$ for every input x, the distributions $i\mathrm{O}(1^\lambda, C_{0,\lambda})$ and $i\mathrm{O}(1^\lambda, C_{1,\lambda})$ are computationally indistinguishable: that is, for every efficient polynomial-time algorithm D, for every constant $c > 0$, there exists a constant $\lambda_0 \in \mathbb{Z}^+$, such that for all $\lambda > \lambda_0$, we have:*
$$\left|\Pr\left[D(i\mathrm{O}(1^\lambda, C_{0,\lambda}) = 1\right] - \Pr\left[D(i\mathrm{O}(1^\lambda, C_{1,\lambda}) = 1\right]\right| \le \frac{1}{\lambda^c}$$

So far, through the accumulation of extensive research by a large community since the first mathematical candidate iO proposal by [20] (see the survey in [21] and references therein), We recently gave the first construction of iO [29] based on four well-studied assumptions: Learning With Errors (LWE) [34], Decisional Linear assumption (DLIN) [8] over bilinear groups, Learning Parity with Noise over $\mathbb{F}_p$ [27], and Pseudo-Random Generators in NC^0 [23]. More recently, we further improved the construction by removing the reliance on LWE [28], obtaining the following theorem:

Theorem 1.2 (Informal)**.** Assume sub-exponential security of the following assumptions:

- the Learning Parity with Noise (LPN) assumption over general prime fields $\mathbb{F}_p$ with polynomially many LPN samples and error rate $1/k^\delta$, where k is the dimension of the LPN secret, and $\delta > 0$ is any constant;
- the existence of a Boolean Pseudo-Random Generator (PRG) in NC^0 with stretch $n^{1+\tau}$, where n is the length of the PRG seed, and $\tau > 0$ is any constant;
- the Decision Linear (DLIN) assumption on symmetric bilinear groups of prime order.

Then, (subexponentially secure) indistinguishability obfuscation for all polynomial-size circuits exists. Assuming only polynomial security of the assumptions above yields polynomially secure functional encryption for all polynomial-size circuits.

We now describe each of the assumptions we need in more detail and briefly survey their history.

The DLIN Assumption: The Decisional Linear assumption (DLIN) is stated as follows: For an appropriate λ-bit prime p, two groups $\mathbb{G}$ and $\mathbb{G}_T$ are chosen of order p such that there exists an efficiently computable nontrivial symmetric bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. A canonical generator g for $\mathbb{G}$ is also computed. Following the tradition of cryptography, we describe the groups above using multiplicative notation, even though they are cyclic. The DLIN assumption requires that the following computational indistinguishability holds:

$$\begin{gathered}\left\{\left(g^x, g^y, g^{xr}, g^{ys}, g^{r+s}\right) \mid x, y, r, s \leftarrow \mathcal{Z}_p\right\} \\ \approx_c \left\{\left(g^x, g^y, g^{xr}, g^{ys}, g^{z}\right) \mid x, y, r, s, z \leftarrow \mathcal{Z}_p\right\}\end{gathered}$$

This assumption was first introduced in the 2004 work of Boneh, Boyen, and Shacham [13], and instantiated using appropriate elliptic curves. Since then DLIN and assumptions implied by DLIN have seen extensive use in a wide variety of applications throughout cryptography, such as Identity-Based Encryption, Attribute-Based Encryption, Functional Encryption for degree 2 polynomials, Non-Interactive Zero Knowledge, etc. (See, e.g. [24, 16, 33, 10]).

The existence of PRGs in NC^0: The assumption of the existence of a Boolean Pseudo-Random Generator PRG in NC^0 states that there exists a Boolean function $\mathsf{G} : \{0,1\}^n \to \{0,1\}^m$ where $m = n^{1+\tau}$ for some constant $\tau > 0$, and where each output bit computed by G depends on a constant number of input bits, such that the following computational indistinguishability holds:

$$\{\mathsf{G}(\boldsymbol{\sigma}) \mid \boldsymbol{\sigma} \leftarrow \{0,1\}^n\} \approx_c \{\boldsymbol{y} \mid \boldsymbol{y} \leftarrow \{0,1\}^m\}$$

Pseudorandom generators are a fundamental primitive in their own right, and have vast applications throughout cryptography. PRGs in NC^0 are tightly connected to the fundamental topic of Constraint Satisfaction Problems (CSPs) in complexity theory, and were first proposed for cryptographic use by Goldreich [23, 19, 25] 20 years ago. The complexity theory and cryptography communities have jointly developed a rich body of literature on the cryptanalysis and theory of constant-locality Boolean PRGs [23, 19, 31, 17, 4, 5, 12, 2, 32, 7, 30, 18, 6].

LPN over large fields: The Learning Parity with Noise LPN assumption over finite fields $\mathcal{Z}_p$ is a decoding problem. The standard LPN assumption with respect to subexponential-size modulus p, dimension ℓ, sample complexity n, and a noise rate $r = 1/\ell^{\delta}$ for some $\delta \in (0,1)$, states that the following computational indistinguishability holds:

$$\begin{aligned} &\{\boldsymbol{A}, \boldsymbol{s}\cdot\boldsymbol{A}+\boldsymbol{e} \bmod p \ \mid\ \boldsymbol{A} \leftarrow \mathcal{Z}_p^{\ell\times n},\ \boldsymbol{s} \leftarrow \mathcal{Z}_p^{1\times\ell},\ \boldsymbol{e} \leftarrow \mathcal{D}_r^{1\times n}\} \\ \approx_c\ &\{\boldsymbol{A}, \boldsymbol{u} \ \mid\ \boldsymbol{A} \leftarrow \mathcal{Z}_p^{\ell\times n},\ \boldsymbol{u} \leftarrow \mathcal{Z}_p^{1\times n}\}. \end{aligned}$$

Above $e \leftarrow \mathcal{D}_r$ is a generalized Bernoulli distribution, *i.e.* e is sampled randomly from $\mathcal{Z}_p$ with probability $1/\ell^{\delta}$ and set to be 0 with probability $1-1/\ell^{\delta}$. We consider polynomial sample complexity $n(\ell)$, and the modulus p is an arbitrary subexponential function in ℓ.

The origins of the LPN assumption date all the way back to the 1950s: the works of Gilbert [22] and Varshamov [36] showed that random linear codes possessed remarkably strong minimum distance properties. However, since then, very little progress has been made in efficiently decoding random linear codes under random errors. The LPN over fields assumption above formalizes this, and was introduced over $\mathbb{Z}_2$ for cryptographic uses in 1994 [11], and formally defined for general finite fields and parameters in 2009 [26], under the name "Assumption 2".

While in [26], the assumption was used when the error rate was assumed to be a constant, in fact, polynomially low error (in fact $\delta = 1/2$) has an even longer history in the LPN literature: it was used by Alekhnovitch in 2003 [1] to construct public-key encryption with the field $\mathcal{Z}_2$, and used to build public-key encryption over $\mathcal{Z}_p$ in 2015 [3]. The exact parameter settings that we describe above, with both general fields and inverse polynomial error rate corresponding to an arbitrarily small constant $\delta > 0$ was explicitly posed by [15], in the context of building efficient secure two-party and multi-party protocols for arithmetic computations.

A comprehensive review of known attacks on LPN over large fields, for the parameter settings we are interested in, was given in [15, 14]. For our parameter setting, the running time of all known attacks is $\Omega(2^{\ell^{1-\delta}})$, for any choice of the constant $\delta \in (0,1)$ and for any polynomial number of samples $n(\ell)$.

Lattice v.s. (pairing + LPN over $\mathbb{F}_p$ + PRG in NC^0). An immediate consequence of our theorem is that the combination of bilinear pairing, LPN over $\mathbb{F}_p$, and constant-locality PRG is sufficient for building all the primitives that are implied by iO or Functional Encryption (FE) (and other assumptions that are implied by one of the three assumptions). This, somewhat surprisingly, includes *Fully Homomorphic Encryption (FHE)* that support homomorphic evaluation of (unbounded) polynomial-size circuits, as well as Attribute Based Encryption (ABE) that support policies represented by (unbounded) polynomial-size circuits. To this day, the only known constructions of FHE and ABE for circuits are based on the hardness of lattice-type problems – either directly from problems like LWE or Ring LWE, or slightly indirectly via problems such as the approximate GCD problem [35]. Our work hence yields the first alternative pathways towards these remarkable primitives.

References

[1] Michael Alekhnovich. More on average case vs approximation complexity. In *44th FOCS*, pages 298–307. IEEE Computer Society Press, October 2003.

[2] Benny Applebaum. Pseudorandom generators with long stretch and low locality from random local one-way functions. *SIAM J. Comput.*, 42(5):2008–2037, 2013.

[3] Benny Applebaum, Jonathan Avron, and Christina Brzuska. Arithmetic cryptography: Extended abstract. In Tim Roughgarden, editor, *ITCS 2015*, pages 143–151. ACM, January 2015.

[4] Benny Applebaum, Boaz Barak, and Avi Wigderson. Public-key cryptography from different assumptions. In Leonard J. Schulman, editor, *42nd ACM STOC*, pages 171–180. ACM Press, June 2010.

[5] Benny Applebaum, Andrej Bogdanov, and Alon Rosen. A dichotomy for local small-bias generators. In Ronald Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 600–617. Springer, Heidelberg, March 2012.

[6] Benny Applebaum and Eliran Kachlon. Sampling graphs without forbidden subgraphs and unbalanced expanders with negligible error. In David Zuckerman, editor, *60th FOCS*, pages 171–179. IEEE Computer Society Press, November 2019.

[7] Benny Applebaum and Shachar Lovett. Algebraic attacks against random local functions and their countermeasures. In Daniel Wichs and Yishay Mansour, editors, *48th ACM STOC*, pages 1087–1100. ACM Press, June 2016.

[8] Lucas Ballard, Matthew Green, Breno de Medeiros, and Fabian Monrose. Correlation-resistant storage via keyword-searchable encryption. Cryptology ePrint Archive, Report 2005/417, 2005. `http://eprint.iacr.org/2005/417`.

[9] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil P. Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. In Joe Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 1–18. Springer, Heidelberg, August 2001.

[10] Allison Bishop, Abhishek Jain, and Lucas Kowalczyk. Function-hiding inner product encryption. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 470–491. Springer, Heidelberg, November / December 2015.

[11] Avrim Blum, Merrick L. Furst, Michael J. Kearns, and Richard J. Lipton. Cryptographic primitives based on hard learning problems. In Douglas R. Stinson, editor, *CRYPTO'93*, volume 773 of *LNCS*, pages 278–291. Springer, Heidelberg, August 1994.

[12] Andrej Bogdanov and Youming Qiao. On the security of goldreich's one-way function. *Comput. Complex.*, 21(1):83–127, 2012.

[13] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 41–55. Springer, Heidelberg, August 2004.

[14] Elette Boyle, Geffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. Snargs for bounded depth computations and PPAD hardness from sub-exponential LWE. *FOCS*, 2020.

[15] Elette Boyle, Geoffroy Couteau, Niv Gilboa, and Yuval Ishai. Compressing vector OLE. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *ACM CCS 2018*, pages 896–912. ACM Press, October 2018.

[16] Zvika Brakerski, Yael Tauman Kalai, Jonathan Katz, and Vinod Vaikuntanathan. Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage. In *51st FOCS*, pages 501–510. IEEE Computer Society Press, October 2010.

[17] James Cook, Omid Etesami, Rachel Miller, and Luca Trevisan. Goldreich's one-way function candidate and myopic backtracking algorithms. In Omer Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 521–538. Springer, Heidelberg, March 2009.

[18] Geoffroy Couteau, Aurélien Dupin, Pierrick Méaux, Mélissa Rossi, and Yann Rotella. On the concrete security of Goldreich's pseudorandom generator. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 96–124. Springer, Heidelberg, December 2018.

[19] Mary Cryan and Peter Bro Miltersen. On pseudorandom generators in NC. In *MFCS 2001*, volume 2136 of *LNCS*, pages 272–284. Springer, 2001.

[20] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *54th FOCS*, pages 40–49. IEEE Computer Society Press, October 2013.

[21] Romain Gay, Aayush Jain, Huijia Lin, and Amit Sahai. Indistinguishability obfuscation from simple-to-state hard problems: New assumptions, new techniques, and simplification. In *EUROCRYPT 2021*, volume 12698 of *LNCS*, pages 97–126. Springer, 2021.

[22] E. N. Gilbert. A comparison of signalling alphabets. *The Bell System Technical Journal*, 31(3):504–522, 1952.

[23] Oded Goldreich. Candidate one-way functions based on expander graphs. *Electronic Colloquium on Computational Complexity (ECCC)*, 7(90), 2000.

[24] Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 415–432. Springer, Heidelberg, April 2008.

[25] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. Cryptography with constant computational overhead. In Richard E. Ladner and Cynthia Dwork, editors, *40th ACM STOC*, pages 433–442. ACM Press, May 2008.

[26] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Founding cryptography on oblivious transfer - efficiently. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 572–591. Springer, Heidelberg, August 2008.

[27] Yuval Ishai, Manoj Prabhakaran, and Amit Sahai. Secure arithmetic computation with no honest majority. In *TCC Conference, TCC 2009, San Francisco, CA, USA, March 15-17, 2009. Proceedings*, pages 294–314, 2009.

[28] Aayush Jain, Huijia Lin, and Amit Sahai. Indistinguishability obfuscation from LPN over F_p, DLin, and PRGs in NC^0. Cryptology ePrint Archive, Report 2021/1334, 2021. `https://ia.cr/2021/1334`.

[29] Aayush Jain, Huijia Lin, and Amit Sahai. Indistinguishability obfuscation from well-founded assumptions. In Samir Khuller and Virginia Vassilevska Williams, editors, *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, pages 60–73. ACM, 2021.

[30] Pravesh K. Kothari, Ryuhei Mori, Ryan O'Donnell, and David Witmer. Sum of squares lower bounds for refuting any CSP. In Hamed Hatami, Pierre McKenzie, and Valerie King, editors, *49th ACM STOC*, pages 132–145. ACM Press, June 2017.

[31] Elchanan Mossel, Amir Shpilka, and Luca Trevisan. On e-biased generators in NC0. In *44th FOCS*, pages 136–145. IEEE Computer Society Press, October 2003.

[32] Ryan O'Donnell and David Witmer. Goldreich's PRG: evidence for near-optimal polynomial stretch. In *IEEE 29th Conference on Computational Complexity, CCC 2014, Vancouver, BC, Canada, June 11-13, 2014*, pages 1–12. IEEE Computer Society, 2014.

[33] Tatsuaki Okamoto and Katsuyuki Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 191–208. Springer, Heidelberg, August 2010.

[34] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005.

[35] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In Henri Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 24–43. Springer, Heidelberg, May / June 2010.

[36] Rom Varshamov. Estimate of the number of signals in error correcting codes. *Dokl. Akad. Nauk SSSR*, 1957.

Recent progress on derandomizing space-bounded computation

William Hoza

It is a long-standing open problem to prove that **L** = **BPL**, i.e., randomness is unnecessary for space-efficient computation. Over the past several decades, there has been a steady stream of exciting developments on this problem, and there is a feeling that perhaps it will be easier to resolve than **P** vs. **BPP** and other major problems in complexity theory. In this talk, we survey the developments of the past few years. We organize our discussion around four recurring themes.

Theme 1: Iterated pseudorandom restrictions. To prove **L** = **BPL**, it would suffice to design an explicit pseudorandom generator (PRG) with seed length $O(\log n)$ that fools polynomial-width read-once branching programs (ROBPs) that read the input variables in order (first x_1, then x_2, etc.) The best explicit PRG known for this model, by Nisan, has seed length $O(\log^2 n)$ [1]. In the past decade, a line of work has studied the more general model of *arbitrary-order* ROBPs, meaning that the variables are arbitrarily permuted. Forbes and Kelley gave a PRG for arbitrary-order ROBPs where the seed length is $O(\log^3 n)$ in the polynomial-width case and $\widetilde{O}(\log^2 n)$ in the constant-width case [2].

The Forbes-Kelley PRG is based on Ajtai and Wigderson's paradigm of *iterated pseudorandom restrictions* [3]. Forbes and Kelley showed how to sample a pseudorandom restriction $X \in \{0, 1, \star\}^n$ such that for every arbitrary-order ROBP f, we have $\mathbb{E}[f|_X(U_n)] \approx \mathbb{E}[f]$. For constant-width programs, X costs only $\widetilde{O}(\log n)$ truly random bits and assigns values to roughly half the input variables. From here, our remaining job is to fool the restricted function $f|_X$, so we can iterate the process, assigning values to more and more input variables.

For some subclasses of ROBPs, one can improve the seed length using an *early termination* approach introduced by Gopalan, Meka, Reingold, Trevisan, and Vadhan [4]. The idea is to show that f *simplifies* after a few pseudorandom restrictions, which makes it easier to assign values to the remaining variables. Doron, Meka, Reingold, Tal, and Vadhan used this approach to design a near-optimal PRG for constant-width *monotone* ROBPs [5] (i.e., each transition is monotone as a function of the state). Such programs can compute read-once $\mathbf{AC}^0$ and more.

Theme 2: The inverse Laplacian perspective. Ahmadinejad, Kelner, Murtagh, Peebles, Sidford, and Vadhan recently introduced an intriguing new viewpoint on **L** vs. **BPL** [6]. Let f be a given width-w length-n ROBP, and let $N = w \cdot (n + 1)$. We would like to compute the matrix $P \in \mathbb{R}^{N \times N}$ consisting of the expectations of all subprograms $f_{u \to v}$. We can start by computing the random walk matrix $W \in \mathbb{R}^{N \times N}$. One can show $P = W^0 + W^1 + \cdots + W^n$, which simplifies to $P = L^{-1}$, where $L = I - W$. Thus, to simulate **BPL**, it suffices to approximately invert the "Laplacian matrix" L.

One benefit of this perspective is that it suggests a new way of thinking about error. Given a candidate approximation $\widehat{P}$ to P, instead of measuring the error by looking at $P - \widehat{P}$, we can define the alternative error matrix $E = I - \widehat{P}L$. One can show that E is the matrix of "local consistency errors," meaning that we compare each entry $\widehat{P}_{u,v}$ with the value one would expect based on the entries $\widehat{P}_{u,s}$ for edges (s, v) leading into v. Cheng and Hoza used the concept of local consistency errors to show that optimal hitting set generators (HSGs) for ROBPs would imply $\mathbf{L} = \mathbf{BPL}$, not just $\mathbf{L} = \mathbf{RL}$ [7].

Theme 3: Error reduction. Preconditioned Richardson iteration is a method of converting a moderate-error matrix inverse into a low-error matrix inverse. Let f be a given width-n length-n ROBP, and assume that we can deterministically compute $\mathbb{E}[f] \pm 1/\mathrm{poly}(n)$ in space $S(n)$. Ahmadinejad, Kelner, Murtagh, Peebles, Sidford, and Vadhan showed that preconditioned Richardson iteration can be used in this setting, and consequently, for any $\varepsilon > 0$, we can deterministically compute $\mathbb{E}[f] \pm \varepsilon$ in space $O(S(n) + \log n \cdot \log\log_n(1/\varepsilon))$ [6].

Error reduction has also been explored in black-box settings. A few years ago, Braverman, Cohen, and Garg introduced the notion of a *weighted PRG* (WPRG, aka pseudorandom pseudodistribution generator) [8], which is a pair (G, ρ), where $G\colon \{0,1\}^s \to \{0,1\}^n$ and $\rho\colon \{0,1\}^s \to \mathbb{R}$, such that for every function f that we are interested in, we have $|\mathbb{E}_x[f(G(x)) \cdot \rho(x)] - \mathbb{E}[f]| \leq \varepsilon$. Braverman, Cohen, and Garg constructed a WPRG for ROBPs with a better dependence on ε [8] compared to Nisan's PRG [1]. Several follow-up works gave improved constructions [9, 10, 11, 12], and now we have explicit WPRGs for polynomial-width ROBPs with seed length $O(\log^2 n + \log(1/\varepsilon))$ [12]. The WPRG construction comes from an error reduction procedure that is once again based on preconditioned Richardson iteration. The insight that preconditioned Richardson iteration can be adapted to the WPRG setting is due to Cohen, Doron, Renard, Sberlo, and Ta-Shma [10] and, independently, Pyne and Vadhan [11]. Hoza recently showed that as a consequence of this line of work, we have $\mathbf{BPSPACE}(S) \subseteq \mathbf{DSPACE}(S^{3/2}/\sqrt{\log S})$ [12], a slight improvement over Saks and Zhou's $O(S^{3/2})$ bound [13].

Theme 4: Expander graphs. Let u and v be vertices in a directed graph G, and let $k \in \mathbb{N}$. To simulate **BPL**, it suffices to estimate the probability that a length-k random walk from u ends at v, given (G, u, v, k). Ahmadinejad, Kelner, Murtagh, Peebles, Sidford, and Vadhan gave a deterministic near-logarithmic-space algorithm for the special case that G is *undirected* or Eulerian [6]. Their algorithm uses the *derandomized square* operation of Rozenman and Vadhan [14], along with the inverse Laplacian perspective, error reduction techniques, and other tools. The derandomized square of a graph G sparsifies G^2 using *expander graphs*.

The derandomized square operation is closely related to the classic Impagliazzo-Nisan-Wigderson (INW) PRG [15]. In the past decade, a line of work has used the INW generator and other tools to design improved generators for so-called regular and permutation ROBPs. Pyne and Vadhan recently designed a WPRG for permutation ROBPs that beats Nisan's seed length in essentially all parameter regimes [11], and meanwhile, for regular ROBPs with a single accept vertex, Bogdanov, Hoza, Prakriya, and Pyne designed HSGs that beat Nisan's seed length in all parameter regimes except $\log w = \Theta(\log(1/\varepsilon)) = \Omega(\log n)$ [16].

Permutation ROBPs can be considered a kind of "opposite" to monotone ROBPs. Meka, Reingold, and Tal managed to combine iterated restrictions (which work well for monotone ROBPs) with the INW generator (which works well for permutation ROBPs) to fool width-3 ROBPs with seed length $\widetilde{O}(\log n)$ [17]. How far these techniques can be extended remains to be seen.

References

[1] N. Nisan, "Pseudorandom generators for space-bounded computation," *Combinatorica*, vol. 12, no. 4, pp. 449–461, 1992.

[2] M. A. Forbes and Z. Kelley, "Pseudorandom generators for read-once branching programs, in any order," in *Proc. 59th Symposium on Foundations of Computer Science (FOCS)*, pp. 946–955, 2018.

[3] M. Ajtai and A. Wigderson, "Deterministic simulation of probabilistic constant-depth circuits," *Advances in Computing Research – Randomness and Computation*, vol. 5, pp. 199–23, 1989.

[4] P. Gopalan, R. Meka, O. Reingold, L. Trevisan, and S. Vadhan, "Better pseudorandom generators from milder pseudorandom restrictions," in *Proc. 53rd Symposium on Foundations of Computer Science (FOCS)*, pp. 120–129, 2012.

[5] D. Doron, R. Meka, O. Reingold, A. Tal, and S. Vadhan, "Pseudorandom Generators for Read-Once Monotone Branching Programs," in *Proc. 25th International Conference on Randomization and Computation (RANDOM)*, pp. 58:1–58:21, 2021.

[6] A. Ahmadinejad, J. Kelner, J. Murtagh, J. Peebles, A. Sidford, and S. Vadhan, "High-precision estimation of random walks in small space," in *Proc. 61st Symposium on Foundations of Computer Science (FOCS)*, pp. 1295–1306, 2020.

[7] K. Cheng and W. M. Hoza, "Hitting Sets Give Two-Sided Derandomization of Small Space," in *Proc. 35th Computational Complexity Conference (CCC)*, pp. 10:1–10:25, 2020.

[8] M. Braverman, G. Cohen, and S. Garg, "Pseudorandom pseudo-distributions with near-optimal error for read-once branching programs," *SIAM Journal on Computing*, vol. 49, no. 5, pp. STOC18–242–STOC18–299, 2020.

[9] E. Chattopadhyay and J.-J. Liao, "Optimal Error Pseudodistributions for Read-Once Branching Programs," in *Proc. 35th Computational Complexity Conference (CCC)*, pp. 25:1–25:27, 2020.

[10] G. Cohen, D. Doron, O. Renard, O. Sberlo, and A. Ta-Shma, "Error Reduction for Weighted PRGs Against Read Once Branching Programs," in *Proc. 36th Computational Complexity Conference (CCC)*, pp. 22:1–22:17, 2021.

[11] E. Pyne and S. Vadhan, "Pseudodistributions That Beat All Pseudorandom Generators (Extended Abstract)," in *Proc. 36th Computational Complexity Conference (CCC)*, pp. 33:1–33:15, 2021.

[12] W. M. Hoza, "Better Pseudodistributions and Derandomization for Space-Bounded Computation," in *Proc. 25th International Conference on Randomization and Computation (RANDOM)*, pp. 28:1–28:23, 2021.

[13] M. Saks and S. Zhou, "$\mathrm{BP_HSPACE}(S) \subseteq \mathrm{DSPACE}(S^{3/2})$," *J. Comput. System Sci.*, vol. 58, no. 2, pp. 376–403, 1999.

[14] E. Rozenman and S. Vadhan, "Derandomized squaring of graphs," in *Proc. 9th International Workshop on Randomization and Computation (RANDOM)*, pp. 436–447, 2005.

[15] R. Impagliazzo, N. Nisan, and A. Wigderson, "Pseudorandomness for network algorithms," in *Proc. 26th Symposium on Theory of Computing (STOC)*, pp. 356–364, 1994.

[16] A. Bogdanov, W. M. Hoza, G. Prakriya, and E. Pyne, "Hitting sets for regular branching programs," 2021. ECCC preprint TR21-143.

[17] R. Meka, O. Reingold, and A. Tal, "Pseudorandom generators for width-3 branching programs," in *Proc. 51st Symposium on Theory of Computing (STOC)*, pp. 626–637, 2019.

Panteleev–Kalachev codes

Ryan O'Donnell

In this talk I outlined the very recent (November 2021) work of Pavel Panteleev and Gleb Kalachev [1], which achieved two breakthroughs on longstanding problems in the theory of error-correcting codes:

- Asymptotically good quantum LDPC codes, meaning CSS codes of constant relative distance, constant rate, and constant locality of checks.
- Asymptotically good locally testable (classical) codes, meaning classical codes with the above properties, as well as the following local testability condition: given any received word x, the fraction of parity checks (from the low-density parity check matrix) that x violates is at least a constant fraction of x's relative distance from the code.

The second breakthrough here, asymptotically good LTCs, was independently obtained by Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, and Shahar Mozes [2], with a similar construction and one slightly better parameter (rate arbitrarily close to 1, whereas the Panteleev–Kalachev classical LTCs have rate only arbitrarily close to 1/2).

To briefly recap the prior status of these important problems:

- In 1997, Kitaev introduced the toric quantum LDPC code, which has distance $\Theta(\sqrt{n})$ and dimension 2 (i.e., rate $2/n$). A code with distance $\Theta(\sqrt{n})$ and dimension $\Theta(n)$ was given by Tillich and Zémor in 2009, but as late as 2020 the largest known distance was only $\sqrt{n}\mathrm{polylog}n$. In 2020, Panteleev and Kalachev themselves gave quantum LDPC codes of distance $\Theta(n^{1-\epsilon/2}/\log n)$ and dimension $\Theta(n^{\epsilon}\log n)$ (for any $0 \leq \varepsilon < 1$), but even after this result, achieving constant relative distance and rate would still be considered remarkable.
- Classical LTCs were defined at least 15 years ago, and have tended to go hand in hand with constructions of probabilistically checkable proofs (PCPs). The best known LTCs prior to this work, constructed by Ben-Sasson–Sudan and Dinur around 2007, were LDPC codes with constant relative distance but dimension only $\Theta(n/\mathrm{polylog}n)$. Expert speculation on whether asymptotically good LTCs even exist was mixed.

The Panteleev–Kalachev paper [1] that was presented achieves the new asymptotically good quantum LDPC codes, and asymptotically good classical LTCs, via essentially the same construction. Roughly speaking, the construction is a pair of Tanner codes with several additional properties: first, the incidence structure of the checks and bits can be thought of as a 2-dimensional chain complex, with "vertices", "edges", and "squares"; second, this incidence structure is based on the a kind of product of an expanding Cayley graph with itself; third, the "small codes" used in the Tanner construction must have certain properties resembling robustness of tensor product codes. At a high level, these features are also all present in the [2] paper, though in the [1] paper the quantum code construction needs to be "very symmetric" between the checks imposed by squares on edges and the checks imposed by vertices on edges.

Major obvious open questions that remain are to construct asymptotically good, locally testable *quantum* LDPC codes, and to construct PCPs of linear rate.

References

[1] Pavel Panteleev and Gleb Kalachev. Asymptotically good quantum and locally testable classical LDPC codes. arXiv:2111.03654v1

[2] Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky and Shahar Mozes. Locally testable codes with constant rate, distance, and locality. arXiv:2111.04808

Thresholds for Random Subspaces, aka LDPC Codes Achieve List-Decoding Capacity

Mary Wootters

(joint work with Jonathan Mosheiff, Noga Ron-Zewi, Nicolas Resch, Shashwat Silas)

1. Introduction

What combinatorial properties are likely to be satisfied by a random linear subspace C of dimension k over a finite field $\mathbb{F}_q$? For example, is it likely that not too many points of C lie in any Hamming ball of fixed radius? What about any combinatorial rectangle of fixed side length? In this work, we give a simple characterization of the threshold on k/n below which this is very likely and above which this is very unlikely.

Our motivation comes from error correcting codes. In coding theoretic language, a random linear subspace C of dimension k in $\mathbb{F}_q^n$ is a *random linear code* of *rate* $R = k/n$. Our characterization can be used to *transfer* results about what properties are likely to be satisfied by C to analogous results about much more structured random ensembles of codes. In this work, our motivation is random Low Density Parity-Check (LDPC) codes, more precisely, Gallager's ensemble [1]. We use our characterization to show that these codes are list-decodable up to list-decoding capacity.

2. Local Properties

Let $C \subseteq \mathbb{F}_q^n$ be a linear code. We consider the class of *local* properties of such codes. Informally, a local property is one that is defined by the exclusion of a coordinate-permutation-invariant family of constant-sized "bad" sets. That is, let $\mathcal{B} \subseteq 2^{\mathbb{F}_q^n}$ be a collection of subsets of $\mathbb{F}_q^n$. Suppose that $\mathcal{B}$ is invariant under coordinate permutations, in the sense that if $B \in \mathcal{B}$, then $\{\pi(b) : b \in B\} \in \mathcal{B}$ for any coordinate permutation $\pi \in S_n$. Moreover, suppose that $|B| \leq \ell$ for all $B \in \mathcal{B}$, for some parameter ℓ (that is independent of n). We say that a subspace $C \subseteq \mathbb{F}_q^n$ satisfies the property $P_{\mathcal{B}}$ if there is no $B \in \mathcal{B}$ so that $B \subset C$. The property $P_{\mathcal{B}}$ is called an *ℓ-local property.*

Some ℓ-local properties of note in coding theory include:

- Distance: A code C has *distance* at least d if any pair of distinct codewords $c, c' \in C$ have $\Delta(c, c') \geq d$, where Δ denotes Hamming distance.
- List-Decoding: A code C is *(p, L)-list-decodable* if for any $z \in \mathbb{F}_q^n$, the number of codewords $c \in C$ so that $\Delta(z, c) \leq pn$ is strictly less than L.
- List-Recovery: A code C is *(ℓ, L)-(zero-error)-list-recoverable* if for any $S_1, \ldots, S_n \subset \mathbb{F}_q$ of size ℓ, the number of codewords $c \in C$ so that $c_i \in S_i$ for all $i \in [n]$ is strictly less than L.

3. Characterization of Threshold

Let $P_{\mathcal{B}}$ be a local property. Our main result is a simple characterization (in terms of $\mathcal{B}$) of a threshold R^* so that for any $\epsilon > 0$:

- If $R < R^* - \epsilon$, then with probability $1 - o(1)$, a random linear code C of rate R satisfies $P_{\mathcal{B}}$.
- If $R > R^* + \epsilon$, then with probability $1 - o(1)$, a random linear code C of rate R does not satisfy $P_{\mathcal{B}}$.

Our characterization is easiest to understand in the case when $\mathcal{B}$ consists of a single orbit under coordinate permuation. Let $B \in \mathcal{B}$, and suppose that $\mathcal{B}$ is generated by all coordinate permutations of B.

Let $R^{\mathbb{E}}(\mathcal{B})$ be the rate at which the *expected* number of bad sets is contained in a random subspace of dimension $R^{\mathbb{E}}(\mathcal{B})$. Call this the *expectation threshold* for $\mathcal{B}$. This quantity is easy to compute in terms of the size of $\mathcal{B}$, using linearity of expectation.

It would be quite nice if $R^*(\mathcal{B}) = R^{\mathbb{E}}(\mathcal{B})$. Unfortunately, while we always have

$$R^{\mathbb{E}}(\mathcal{B}) \leq R^*(\mathcal{B}),$$

(this follows from Markov's inequality), there are simple examples that show that they are not always equal. However, we show that it is *almost* the case. More precisely, consider a class $\mathcal{B}'$ obtained by a linear projection of $\mathcal{B}$. That is, $\mathcal{B}'$ is the class generated by coordinate permutations of $\{Ab : b \in B\}$ for some matrix $A \in \mathbb{F}^{\ell' \times \ell}$ for some $\ell' < \ell$. It is not hard to see that

$$R^{\mathbb{E}}(\mathcal{B}') \leq R^*(\mathcal{B}') \leq R^*(\mathcal{B}).$$

It turns out that this lower bound *is* tight, at least for some A. Our main theorem says that

$$R^*(\mathcal{B}) = \max_A R^{\mathbb{E}}(A\mathcal{B}),$$

where $A\mathcal{B}$ represents the projection $\mathcal{B}'$ of $\mathcal{B}$ under A as discussed above.

When $\mathcal{B}$ is comprised of multiple orbits under coordinate permutation, a similar characterization holds; one simply takes the minimum over all of the orbits.

4. Applications to LDPC Codes

The formulation above can be used to transfer any (positive) results that hold for random linear codes to random LDPC codes in a black-box way. The idea is as follows.

Let C' be a random code according to some other random ensemble; in our case, a random LDPC code according to Gallager's ensemble. Let C be a random linear code of approximately the same rate as C'. Since the above characterizion only relies on first-moment computations (that is, the computation of $R^{\mathbb{E}}$), if C' shares first-moment properties with C (that is, if the probability that a fixed bad set B is contained in C or C' is roughly the same), then C' should satisfy $P_{\mathcal{B}}$ with high probability if C does.

It turns out that this can be made precise, and in fact applies to random LDPC codes. This implies that Gallager's ensemble of LDPC codes are list-decodable to capacity, following a long line of work that established this for random linear codes.

5. Open Questions

Our main open question is to find other applications of this characterization; a few have already been found [3, 2]. A second open question, about LDPC codes in particular, is whether we can *efficiently* achieve list-decoding capacity for LDPC codes, as the result described above is combinatorial.

References

[1] R. Gallager. *Low-Density Parity-Check Codes.* IRS Transactions on Information Theory, 1962.

[2] V. Guruswami and J. Mosheiff. *Punctured Large Distance Codes, and Many Reed-Solomon Codes, Achieve List-Decoding Capacity.* arXiv preprint arXiv:2109.11725, 2021.

[3] V. Guruswami, R. Li, J. Mosheiff, N. Resch, S. Silas and M. Wootters. *Bounds for list-decoding and list-recovery of random linear codes.* IEEE Transactions on Information Theory, 2021.

Connecting Meta-Complexity and Crypto

Rahul Santhanam

"Meta-complexity" refers to the computational complexity of problems that are themselves about complexity, eg., the Minimum Circuit Size Problem MCSP and the problem $\mathsf{K}^{\mathsf{poly}}$ of computing the polynomial-time bounded Kolmogorov complexity of a string. Meta-complexity is central to many areas of theoretical computer science, including circuit complexity, proof complexity, pseudorandomness, average-case complexity, cryptography and learning.

In this plenary talk, I gave a brief overview of recent work on meta-complexity, with an emphasis on characterizations of one-way functions by average-case hardness of various meta-complexity problems [2, 4, 3, 1], including MCSP, $\mathsf{K}^{\mathsf{poly}}$ and the (uncomputable) problem of computing Kolmogorov complexity.

The relevant characterizations are:

(1) The breakthrough in [2] where the first characterization of one-way functions by average-case hardness of a natural problem is given. They show that one-way functions exist if and only if $\mathsf{K}^{\mathsf{poly}}$ is mildly hard on average over the uniform distribution.

(2) The surprising phenomenon uncovered by [2] and [4], where one-way functions can be characterized by the (bounded-error) average-case hardness of a meta-computational problem, namely the problem of computing the Levin time-bounded Kolmogorov complexity of a string, that is complete for exponential time. As shown in [2], the zero-error average-case hardness of this problem is equivalent to the worst-case hardness of exponential time with respect to probabilistic poly-time algorithms.

(3) The characterization in [4] of *parallel* cryptography (i.e., one way functions computable in NC^1) by the average-case hardness of the KT problem over the uniform distribution..

(4) The characterization in [1] of one-way functions by average-case hardness over *any* samplable distribution of a gap version of the problem of computing Kolmogorov complexity, and also by average-case hardness over *any* locally samplable distribution of a gap version of MCSP.

References

[1] R. Ilango, H. Ren and R. Santhanam, *Hardness on Any Samplable Distribution Suffices: New Characterizations of One-Way Functions by Meta-Complexity*, Electronic Colloquium on Computational Complexity (2021), 28(82)

[2] Y. Liu and R. Pass, *On One-Way Functions and Kolmogorov Complexity.* Proceedings of 61st Annual IEEE Symposium on Foundations of Computer Science (2020): 1243–1254

[3] Y. Liu and R. Pass, *On the Possibility of Basing Cryptography on EXP != BPP*, Proceedings of 41st Annual International Cryptology Conference (2021): 11–40

[4] H. Ren and R. Santhanam, *Hardness of KT Characterizes Parallel Cryptography*, Proceedings of 36th Computational Complexity Conference (2021): 35:1–35:58

Other Informal Talks

Testing thresholds for geometric random graphs

Tselil Schramm

(joint work with Siqi Liu, Sidhanth Mohanty, and Elizabeth Yang)

In the geometric random graph model $G(d, n, p)$, we sample an n-vertex graph by choosing n vectors uniformly at random from the sphere S^{d-1} in d dimensions, and then connecting pairs of points corresponding to vectors v_i, v_j which are sufficiently close, satisfying $\langle v_i, v_j \rangle \geq \tau(p)$ for $\tau(p)$ chosen so that the marginal probability of each edge is p. Though this model is well-studied in low-dimensions (where d is held fixed while $n \to \infty$), the high-dimensional case, in which $d \to \infty$ as a function of n, has received relatively little attention. In this talk, we address the following basic question: for which dimensions d is a graph G sampled from $G(d, n, p)$ recognizable as a geometric random graph, and for which d is it indistinguishable from a graph from the distribution $G(n, p)$ in which each edge is sampled independently? We show that when the average degree is constant, the total variation distance between $G(n, p)$ and $G(d, n, p)$ goes to zero when $d = \Omega(\text{polylog}(n))$, resolving a conjecture of Bubeck, Ding, Eldan, and Rácz [1] up to logarithmic factors.

Generalizing Strassen's 3n/2 border rank lower bound

Pascal Koiran

I gave a proof sketch of Strassen's $3n/2$ border rank lower bound, and suggested some directions for possible generalizations. One compelling reason to look again at Strassen's proof is that it is not a "rank method." It is therefore not subject to the barrier results obtained by Efremenko, Garg, Oliveira and Wigderson [2] (these barrier results show that one cannot obtain superlinear lower bounds on the rank of order 3 tensors using rank methods).

Quantum linearity and low-degree tests

Thomas Vidick

(joint work with Zhengfeng Ji, Anand Natarajan, John Wright, and Henry Yuen)

I first described the soundness analysis of the BLR linearity test when executed with quantum provers. I then explained the construction of the quantum linearity test, which combines two executions of the BLR linearity test, in two conjugate bases, with the Magic Square game to check that the bases used by the provers are indeed conjugate. I stated the main theorem on soundness of this test, which informally guarantees that successful provers must reply to the verifier's queries according to a (near-)uniform distribution over linear functions. We briefly discussed improvements provided by the quantum low-degree test. [3]

Algorithms for Fermionic Hamiltonians

Ryan O'Donnell
(joint work with Matthew B. Hastings)

Perhaps the most fundamental problem in computational quantum chemistry is the following matrix analogue of the weighted 4XOR CSP: Compute (or approximate) the maximum eigenvalue of $h = \sum_{S=(j1<j2<j3<j4)} a_S X_{j1} X_{j2} X_{j3} X_{j4}$ over all assignments of $D \times D$ matrices to $X_1, ..., X_n$ that satisfy $X_j* = X_j, X_j^2 = 1$ (the identity matrix), and $X_j X_k = -X_k X_j$ (for all distinct X_j and X_k). The average-case version of this problem, where the a_S's are independent Gaussian random variables with variance $1/\binom{n}{4}$, is known as the SYK Model. Physicists conjecture that the optimum value for SYK is $\Theta(sqrt(n))$ with high probability, and we verify this via efficient algorithms: we show that degree-6 SOS certifies that the optimum is $O(sqrt(n))$, and we give an efficient quantum algorithm that finds a state certifying that the optimum is $\Omega(sqrt(n))$. [4]

Circuits Resilient to Short-Circuit Errors

Yael Kalai
(joint work with Klim Efremenko, Bernhard Haeupler, Pritish Kamath, Gillat Kol, Nicolas Resch, and Raghuvansh Saxena)

Given a Boolean circuit C, we wish to convert it to a circuit C' that computes the same function as C even if some of its gates suffer from adversarial short circuit errors, i.e., their output is replaced by the value of one of their inputs [5]. Can we design such a resilient circuit C' whose size is roughly comparable to that of C? Prior work gave a positive answer for the special case where C is a formula.

We study the general case and show that any Boolean circuit C of size s can be converted to a new circuit C' of quasi-polynomial size $s^{O(\log s)}$ that computes the same function as C even if a $1/51$ fraction of the gates on any root-to-leaf path in C' are short circuited. Moreover, if the original circuit C is a formula, the resilient circuit C' is of near-linear size $s^{1+\epsilon}$. The construction of our resilient circuits utilizes the connection between circuits and DAG-like communication protocols [Raz95, Pud10, Sok17], originally introduced in the context of proof complexity.

On the Complexity of Evaluating Highest Weight Vectors

Markus Bläser
(joint work with Julian Dörfler, and Christian Ikenmeyer)

Geometric complexity theory (GCT) is an approach towards separating algebraic complexity classes through algebraic geometry and representation theory. Originally Mulmuley and Sohoni proposed (SIAM J Comput 2001, 2008) to use occurrence obstructions to prove Valiant's determinant vs permanent conjecture, but recently Bürgisser, Ikenmeyer, and Panova (Journal of the AMS 2019) proved this impossible. However, fundamental theorems of algebraic geometry and representation theory grant that every lower bound in GCT can be proved by the use of so-called highest weight vectors (HWVs). In the setting of interest in GCT (namely in the setting of polynomials) we prove the NP-hardness of the evaluation of HWVs in general, and we give efficient algorithms if the treewidth of the corresponding Young-tableau is small, where the point of evaluation is concisely encoded as a noncommutative algebraic branching program! In particular, this gives a large new class of separating functions that can be efficiently evaluated at points with low (border) Waring rank. As a structural side result we prove that border Waring rank is bounded from above by the ABP width complexity. [6].

Dense subsets of VNP - beyond border complexity

Christian Ikenmeyer

(joint work with Abhiroop Sanyal)

The classes $\underline{\mathrm{VF}}$, $\underline{\mathrm{VBP}}$, and $\underline{\mathrm{VP}}$ of polynomially bounded border formula complexity, polynomially bounded border algebaic branching program size, and polynomially bounded border circuit size are currently of high interest due to their fundamental connection to geometric complexity theory and all geometric methods for resolving the VP vs VNP and related questions. We introduce a topology on the space of sequences of polynomials with the property that the closure of VP is precisely $\underline{\mathrm{VP}}$, and analogously for VF and VBP. This topology is a box topology and not sequential, which means that the notion of limits of sets must be replaced by limits of nets. The notation $\overline{\mathrm{VP}}$ that is commonly used nowadays instead of $\underline{\mathrm{VP}}$ is therefore now finally justified. [7].

The Space Complexity of Sampling

David Zuckerman

(joint work with Eshan Chattopadhyay, and Jesse Goodman)

Recently, there has been exciting progress in understanding the complexity of distributions. Here, the goal is to quantify the resources required to generate (or sample) a distribution. Proving lower bounds in this new setting is more challenging than in the classical setting, and has yielded interesting new techniques and surprising applications. In this work, we initiate a study of the complexity of sampling with limited memory, and obtain the first nontrivial sampling lower bounds against oblivious read-once branching programs (ROBPs). In our first main result, we show a lower bound on the space to even weakly approximately sample the uniform distribution on a good code. In our second main result, we give a direct product theorem.

Hitting Sets for Regular Branching Programs

William Hoza
(joint work with Andrej Bogdanov, Gautam Prakriya, and Edward Pyne)

In this short informal talk, we discuss two constructions of improved hitting set generators for regular read-once branching programs (ROBPs). We focus on a lemma that is used in the analysis of both generators. The lemma says that any pseudorandom generator for regular ROBPs also fools a more general model called regular "unanimity programs." A unanimity program is defined like an ROBP, except that every vertex (not just those in the last layer) is labeled as either accepting or rejecting; the program accepts an input if every vertex visited on that input is an accepting vertex.

Asymptotic spectra: Theory, applications and extensions

Jeroen Zuiddam
(joint work with Avi Wigderson)

In 1969, Strassen shocked the computational world with his subcubic algorithm for multiplying matrices. Attempting to understand the best possible algorithm for this problem, Strassen went on to develop his magnificent theory of *asymptotic spectra* in three papers between 1986–1991 [9, 10, 8]. Expressed in the great generality of partially ordered semirings, the centerpiece of this theory is a *duality* theorem between the asymptotic "rank" of elements, and a topological space which is called asymptotic spectrum. This duality theorem is a vast generalization of linear programming duality (in which we have a semigroup rather than a semiring), and indeed also of certain versions of the Positivstellensatz, the duality theorem of polynomial inequalities over the Reals. Focusing on understanding the structure of the asymptotic spectrum of matrix multiplication, the theory has provided surprising *connectivity* and *convexity* theorems for it. Strassen's theory has led to many subsequent results, especially new algorithmic, structural and barrier results on matrix multiplication, and more generally for the semiring of tensors (which includes the matrix multiplication tensors). Perhaps even more impressively, the generality of Strassen's theory has been applied recently to the study of a variety of very different settings and parameters, in diverse fields including communication theory, graph theory, probability theory, quantum information theory and computational complexity. We feel that these developments call for an exposition of this growing field. Our paper [11] provides a comprehensive, self-contained, modern survey of Strassen's theory of asymptotic spectra and its various old and new application areas. In this talk I gave a brief overview of our paper, highlighting several important components and theorems.

Rigid Continuation Paths II: Structured Polynomial Systems

Peter Bürgisser
(joint work with Felipe Cucker and Pierre Lairez)

We study the average complexity of solving structured polynomial systems that are characterised by a low evaluation cost, as opposed to the dense random model previously used. Firstly, we design a continuation algorithm that computes, with high probability, an approximate zero of a polynomial system given only as black-box evaluation program. Secondly, we introduce a universal model of random polynomial systems with prescribed evaluation complexity L. Combining both, we show that we can compute an approximate zero of a random structured polynomial system with n equations of degree at most d in n variables with only $\mathrm{poly}(n, d)L$ operations with high probability. This exceeds the expectations implicit in Smale's 17th problem. The preprint is at [12].

Pseudorandom Generators for Read-Once Monotone Branching Programs

Avishay Tal
(joint work with Dean Doron, Raghu Meka, Omer Reingold, and Salil Vadhan)

Motivated by the derandomization of space-bounded computation, a long line of work constructed pseudorandom generators (PRGs) against various forms of read-once branching programs (ROBPs), with a goal of improving the $O(log^2(n))$ seed length of Nisan's classic construction [13] to the optimal $O(logn)$. In this work, we construct an explicit PRG with seed length $\tilde{O}(logn)$ against constant-width ROBPs that are monotone, in the sense that the transition function from one layer to the next is a monotone function of the state. Our PRG also works against monotone ROBPs that can read the input bits in any order, which are strictly more powerful than read-once AC0. Thus, we provide state-of-the-art PRGs for the latter class as well, improving upon [15].

References

[1] Bubeck, Sébastien and Ding, Jian and Eldan, Ronen and Rácz, Miklós Z *Testing for high-dimensional geometry in random graphs*. Random Structures & Algorithms, 2016.

[2] Klim Efremenko, Ankit Garg, Rafael Oliveira, and Avi Wigderson. *Barriers for rank methods in arithmetic complexity*. In Proc. of the 9th Innovations in Theoretical Computer Science (ITCS)Conference, 2018.

[3] Natarajan, Anand and Vidick, Thomas. *A quantum linearity test for robustly verifying entanglement*. In Proc. of the 49th Annual ACM SIGACT Symposium on Theory of Computing, 2017.

[4] Hastings, Matthew and O'Donnell, Ryan. *Optimizing Strongly Interacting Fermionic Hamiltonians*. 2021.

[5] Daniel J. Kleitman, Frank Thomson Leighton, and Yuan Ma. On the design of reliable boolean circuits that contain partially unreliable gates. Journal of Computer and System Sciences, 1997.

[6] Bläser, Markus and Dörfler, Julian and Ikenmeyer, Christian. *On the Complexity of Evaluating Highest Weight Vectors*. In Proc. of the 36th Computational Complexity Conference. 2021.

[7] Christian Ikenmeyer and Abhiroop Sanyal. *A note on VNP-completeness and border complexity*. 2021.

[8] Strassen, Volker, *Degeneration and complexity of bilinear maps: some asymptotic spectra*. Journal für die Reine und Angewandte Mathematik. [Crelle's Journal]. 1991.

[9] Strassen, Volker, *Relative bilinear complexity and matrix multiplication*. Journal für die Reine und Angewandte Mathematik. [Crelle's Journal]. 1987.

[10] Strassen, Volker, *The asymptotic spectrum of tensors*. Journal für die Reine und Angewandte Mathematik. [Crelle's Journal]. 1988.

[11] Avi Wigderson and Jeroen Zuiddam *Asymptotic spectra: Theory, applications and extensions*. 2021.

[12] Peter Bürgisser, Felipe Cucker and Pierre Lairez Rigid continuation paths II. Structured polynomial systems. *arXiv preprint arXiv:2010.10997*, 2020.

[13] Noam Nisan. *Pseudorandom generators for space-bounded computation*. Comb. 1992.

[14] Dean Doron and Raghu Meka and Omer Reingold and Avishay Tal and Salil P. Vadhan. *Pseudorandom Generators for Read-Once Monotone Branching Programs*. APPROX-RANDOM. 2021.

[15] Dean Doron and Pooya Hatami and William M. Hoza. *Near-Optimal Pseudorandom Generators for Constant-Depth Read-Once Formulas*. Computational Complexity Conference. 2021.

Reporter: Yotam Dikstein

Participants

Dr. Boaz Barak
Harvard John A. Paulson
School of Engineering and Applied
Sciences
29 Oxford Street
Cambridge MA 02138
UNITED STATES

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

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

Prof. Dr. Karl Bringmann
Saarland University
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

Dr. Lijie Chen
Department of Mathematics
Massachusetts Institute of
Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

Prof. Dr. Matthias Christandl
Department of Mathematical Sciences
University of Copenhagen
Universitetsparken 5
2100 København
DENMARK

Yotam Dikstein
Department of Mathematics
The Weizmann Institute of Science
P.O. Box 26
76100 Rehovot
ISRAEL

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

Prof. Dr. Zeev Dvir
Department of Computer Science
Princeton University
35 Olden Street
Princeton, NJ 08544-5233
UNITED STATES

Dr. Ankit Garg
Microsoft Research Bangalore
Vigyan Building
No. 9 Lavelle Road
Bangalore, Bengaluru, Karnataka 560
001
INDIA

Dr. Sumegha Garg
Department of Mathematics
Harvard University
Science Center
One Oxford Street
Cambridge MA 02138-2901
UNITED STATES

Prof. Dr. Shafi Goldwasser
UC Berkeley
Melvin Calvin Lab
04729 Berkeley CA 94720
UNITED STATES

Dr. Mika Göös
Ecole Polytechnique Fédérale de
Lausanne
EPFL IC THL5
Station 14
1015 Lausanne
SWITZERLAND

Prof. Dr. Venkatesan Guruswami
Computer Science Department
Carnegie Mellon University
GHC 7211
5000 Forbes Avenue
Pittsburgh PA 15213-3890
UNITED STATES

Prof. Dr. Prahladh Harsha
Department of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road, Colaba
400 005 Mumbai
INDIA

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

William Hoza
Simons Institute for the Theory of
Computing
University of California, Berkeley
Melvin Calvin Laboratory
Berkeley, CA 94720
UNITED STATES

Dr. Christian Ikenmeyer
Department of Computer Science
University of Liverpool
Ashton Building, Rm. 311
Ashton Street
Liverpool L69 3BX
UNITED KINGDOM

Dr. Yael Tauman Kalai
Microsoft Research Laboratory
Office 14063
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. Pascal Koiran
L I P
École Normale Supérieure de Lyon
46, Allée d'Italie
69364 Lyon Cedex 07
FRANCE

Prof. Dr. Swastik Kopparty
Department of Mathematics
University of Toronto
40 St. George Street
Toronto ON M5S 2E4
CANADA

Dr. Lap-Chi Lau
Algorithms and Complexity Group
Cheriton School of Computer Science
University of Waterloo
Waterloo ON N2L 3G1
CANADA

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

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

Prof. Dr. Shachar Lovett
Department of Mathematics
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0112
UNITED STATES

Dr. Urmila Mahadev
Department of Mathematics
California Institute of Technology
Pasadena, CA 91125
UNITED STATES

Dr. Visu Makam
School of Mathematics
Institute for Advanced Study
1 Einstein Drive
Princeton, NJ 08540
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 Y. Minzer
Department of Mathematics
Massachusetts Institute of
Technology
77 Massachusetts Avenue
Cambridge, MA 02139-4307
UNITED STATES

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

Shayan Oveis Gharan
Paul Allen School of Computer Science
and Engineering
University of Washington
P.O. Box 352350
Seattle WA 98195
UNITED STATES

Prof. Dr. Toniann Pitassi
Department of Computer Science
University of Toronto
10 King's College Road
Toronto ONT M5S 3G4
CANADA

Prof. Dr. Ran Raz
School of Engineering and Applied Science
Princeton University
35 Olden Street
Princeton, NJ 08544-5233
UNITED STATES

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

Prof. Dr. Rahul Santhanam
Department of Computer Science
Oxford University
Wolfson Building
Parks Road
Oxford OX1 3QD
UNITED KINGDOM

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

Dr. Tselil Schramm
Department of Statistics
Stanford University
Sequoia Hall
Stanford CA 94305-4065
UNITED STATES

Dr. Amir Shpilka
Department of Computer Science
Tel Aviv University
Tel Aviv 69978
ISRAEL

Dr. Nikhil Srivastava
Department of Mathematics
University of California, Berkeley
1035 Evans Hall
Berkeley CA 94720-3840
UNITED STATES

Prof. Dr. David Steurer
Department of Computer Science
ETH Zürich
Universitätsstrasse 6
8092 Zürich
SWITZERLAND

Prof. Dr. Madhu Sudan
John A. Paulson School of Engineering and Applied Sciences
Harvard University
33 Oxford Street
Cambridge MA 02138
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
Ramat Aviv
Tel Aviv 69978
ISRAEL

Prof. Dr. Luca Trevisan
Department of Decision Sciences
Bocconi University
Via Roentgen 1
20136 Milano
ITALY

Dr. Madhur Tulsiani
Toyota Technological Institute
at Chicago
6045 S Kenwood Av
Chicago, IL 60637
UNITED STATES

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
Boston, MA 02134
UNITED STATES

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

Prof. Dr. Thomas Vidick
Department of Computing and
Mathematical Sciences
California Institute of Technology
Annenberg 207
1200 E. California Boulevard
Pasadena, CA 91125-5000
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

Dr. Mary Wootters
Departments of Computer Science and
Electrical Engineering
Stanford University
1455 California Ave
94304 Palo Alto
UNITED STATES

Dr. Henry Yuen
School of Engineering and Applied Sciences
Columbia University
500 West 120 Street
New York, NY 10027
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