RESEARCH STATEMENT

NATHAN LINDZEY

I study the interplay between algebra, combinatorics, optimization, and their applications to problems in extremal combinatorics and theoretical computer science. My current research focuses on the use and development of *discrete harmonic analysis*, i.e., generalizations of discrete Fourier analysis, to solve problems in extremal combinatorics and complexity theory. Increasingly more problems in these areas call for such techniques, especially when they involve combinatorial objects with a more complicated algebraic structure that resist the traditional Fourier-analytical methods in theoretical computer science. A nascent theory has recently emerged to fill this void, and in this vein, my current research programme (with my supervisor Yuval Filmus) aims to generalize the classical theory of *Boolean functions* [1] to simplicial complexes and other domains with high combinatorial regularity [2, 3].

Below is an overview of some recent results that I have obtained in theoretical computer science and mathematics where discrete harmonic analysis and representation theory plays a central role.

Computational Complexity Theory. A cycle in an undirected graph is *Hamiltonian* if it visits every vertex. It is a classic hard (i.e., NP-complete) problem to decide if a graph has a Hamiltonian cycle, that is, one can efficiently reduce (i.e., in polynomial time) the problem of deciding whether a graph has a Hamiltonian cycle to deciding if a particular sentence of propositional logic written in conjunctive normal form (k-CNF) is a tautology. The *Strong Exponential Time Hypothesis (SETH)* asserts for any $\epsilon > 0$, there exists a $k \geq 3$ such that deciding if a k-CNF sentence on N variables is a tautology cannot be done in $O(2^{(1-\epsilon)N})$ time [4]. Studying computational complexity under this plausible but difficult to prove hypothesis has given rise to an exciting new area of theoretical computer science called *fine-grained complexity.*

An even harder problem of course is to *count* the number of Hamiltonian cycles in a graph. In light of the hardness of counting Hamiltonian cycles, computer scientists have designed clever *parameterized algorithms* where the number of steps taken by the algorithm can be analyzed in terms of various graph parameters that measure, for example, how "tree-like" or "path-like" the input graph is. In joint work with Radu Curticapean and Jesper Nederlof [5, 6] we give results on the fine-grained complexity of counting Hamiltonian cycles #HC. In particular, assuming SETH, we give a lower bound on #HC that matches the runtime of the best known parameterized algorithms for the problem up to polynomial factors (the asymptotic notation $O^*(\cdot)$ suppresses such factors).

Theorem 1. [5] *Assuming SETH, there is no $\epsilon > 0$ such that #HC can be solved in $O^*((6-\epsilon)^{\mathrm{pw}})$-time on graphs with a given path decomposition of width* pw.

In other words, algorithm designers need not look further for substantially more efficient algorithms for counting Hamiltonian cycles if they believe SETH, or on the contrary, that any constant-factor improvement in the base of the runtime would refute SETH. The proof proceeds via a long technical reduction that boils down to computing the rank of *the Hamiltonian cycle matrix* H_n, a binary matrix indexed by perfect matchings of K_{2n} and defined such that its ij-entry is 1 if $i \cup j$ is a Hamiltonian cycle and 0 otherwise. Using the representation theory of the symmetric group and enumerative combinatorics, we give a formula for the rank of H_n in terms of standard Young tableaux along with an asymptotic estimate of the rank of H_n that is tight up to polynomial factors.

Another way to prove conditional lower bounds on algorithmic problems in complexity theory is by studying the problem's *query complexity*, i.e., the number of calls (queries) that any algorithm must make to a given black-box routine (oracle) to correctly solve the problem. In the quantum world, one considers the *quantum query complexity* of the problem, where the oracle is a black-box unitary that can be queried in *superposition*.

A problem in quantum computing that has been studied intensely in this framework is the so-called *Index-Erasure problem*, which asks a quantum computer to prepare, for a given injective function $f : [n] \to [m]$ where $n < m$, the quantum state $(1/\sqrt{n}) \sum_{x=1}^{n} |f(x)\rangle$. Here, the oracle is a unitary matrix that sends $|x\rangle$ to $|f(x)\rangle$, i.e., the oracle answers $|f(x)\rangle$ when presented with the query $|x\rangle$. To generate quantum states such as this on a quantum computer, one often needs additional temporary storage (qubits) and we may either insist that these qubits be reset to a default state or be left in an arbitrary state once the algorithm terminates. The latter is called *non-coherent quantum state generation* and the *non-coherent quantum query complexity* of a problem is the least number of quantum oracle queries needed for a quantum algorithm to solve the problem non-coherently. With Ansis Rosmanis [7], we give a tight lower bound on the non-coherent quantum query complexity on the Index-Erasure problem, answering a question of Ambainis et al [8].

Theorem 2. [7] *The bounded-error quantum query complexity of Index-Erasure is $\Theta(\sqrt{n})$ in the non-coherent state generation regime, provided that $m \geq n^{3+\epsilon}$ for some $\epsilon > 0$.*

The proof uses discrete harmonic analysis over the set of injective functions $f : [n] \to [m]$ to solve an infinite family of *semidefinite programs* (SDPs) whose objective value captures the non-coherent quantum query complexity of the problem. Relatively little was known about the algebraic combinatorics of injective functions prior to this work, and it uncovered a remarkable connection between non-coherent quantum query complexity and the dual structure constants (so-called *Krein parameters*) of a commutative matrix algebra. The theory developed in [7] also led to new results in *coding theory* [9, 10].

Boolean Functions. The *analysis of Boolean functions* is the study of Boolean functions $f : \{0,1\}^n \to \{0,1\}$ on the hypercube $\{0,1\}^n$ from the perspective of Fourier analysis. This point of view has had a profound impact on theoretical computer science which has inspired a recent movement to extend classical results in this area to other discrete domains (see [11, 12, 13, 14], for example). But for these more complicated domains it is not at all obvious whether analogous theories exist. Indeed, a natural question is whether the classical *complexity measures* of Boolean functions on $\{0,1\}^n$ transfer to other domains, and whether they enjoy the same nice theoretical properties. To give an example of a complexity measure, for a given Boolean function f and input $x \in \{0,1\}^n$, let $s(f,x)$ be the number of coordinates i such that if we flip the ith coordinate of x, the value of the function changes, so that the *sensitivity* of f is $S(f) := \max_{x\in\{0,1\}^n} s(f,x)$. A recent breakthrough in this area was the proof of the *Sensitivity Conjecture* [15] which showed the *degree* $\deg(f)$ of a Boolean function f on the hypercube (as a multilinear polynomial) and its sensitivity are *polynomially related*, in particular, $S(f) \geq \sqrt{\deg(f)}$. With coauthors [2], we give natural generalizations of several classic complexity measures such as sensitivity to other domains (e.g., permutations, perfect matchings) and surprisingly show that these measures are in fact polynomially related.

Another obstacle to generalizing the theory of Boolean functions to other domains is that we are no longer guaranteed the existence of a unique multilinear polynomial representation of a Boolean function, a fact that is fundamental to many polynomial methods in theoretical computer science. With Yuval Filmus [3], we show that Boolean functions on other domains (e.g., perfect matchings) do in fact have a unique *harmonic* multilinear polynomial representation that enjoys many of the same spectral properties as the unique multilinear polynomial representation of Boolean functions on the hypercube.

In ongoing work with Yuval Filmus we are continuing this programme of extending fundamental results in the analysis of Boolean functions to other combinatorial domains. Many of the results obtained in [2, 3] draw from my work in algebraic and extremal combinatorics that I obtained in my doctoral dissertation, which I describe below.

Extremal Combinatorics. My contributions to extremal combinatorics are in the area of *Erdős-Ko-Rado (EKR) combinatorics* which studies how large families of discrete objects can be subject to the restriction that their members pairwise intersect, as well as the structure of the largest such families. The field's namesake comes from the following seminal result of Erdős, Ko, and Rado.

Theorem 3 (The Erdős–Ko–Rado Theorem)**.** *Let $k < n/2$ and let $\binom{[n]}{k}$ be the set of all k-element subsets of $[n] := \{1, 2, \cdots, n\}$. If $\mathcal{F}$ is intersecting, i.e., $S \cap T \neq \emptyset$ for all $S, T \in \mathcal{F}$, then*

$$|\mathcal{F}| \leq \binom{n-1}{k-1}.$$

Moreover, equality holds if and only if there exists an $i \in [n]$ such that $\mathcal{F} = \{S \in \binom{[n]}{k} : i \in S\}$.

There are many proofs of this theorem, and it has been generalized to many different combinatorial domains, e.g., words [16], subspaces [17], and permutations [18]. Algebraic techniques have played a distinguished role in EKR combinatorics, so much so that a textbook [19] has been written on the subject, wherein my early masters work [20] is referenced. With Yuval Filmus [21], we give short and purely spectral proofs of the Erdős–Ko–Rado theorem and some of its generalizations.

In this area, it is significantly more difficult to prove what are known as *t-intersecting* results, where the intersection of any two members in the family must now have size t or greater. Another challenging line of inquiry that is common in extremal combinatorics is to show *stability* results, e.g., that "large" intersecting families must be close in structure to the largest intersecting families. In my dissertation, I show how algebraic techniques can be used to solve these sorts of problems for *perfect matchings* of the complete graph K_{2n}, i.e., sets of n disjoint edges that cover all the vertices [22]. In particular, I answered an open question of Godsil and Meagher [19, Ch. 16] that can be seen as the non-bipartite analogue of the *Deza-Frankl Conjecture* proven by Ellis, Friedgut, and Pilpel [23], a seminal result in extremal combinatorics.

Theorem 4. [24] *Let $\mathcal{M}_{2n}$ be the collection of perfect matchings of K_{2n} and let $t \in \mathbb{N}$. If $\mathcal{F} \subseteq \mathcal{M}_{2n}$ is t-intersecting, i.e., $|m \cap m'| \geq t$ for all $m, m' \in \mathcal{F}$, then for sufficiently large n, we have*

$$|\mathcal{F}| \leq (2(n-t)-1)!!.$$

Moreover, equality holds if and only if $\mathcal{F} = \{m \in \mathcal{M}_{2n} : T \subseteq m\}$ for some set T of t disjoint edges.

The proof of this theorem can be understood in purely graph-theoretical terms. Let $G_{n,t}$ be the graph defined over $\mathcal{M}_{2n}$ such that $m, m' \in \mathcal{M}_{2n}$ are adjacent if $|m \cap m'| < t$. The *independent sets* of $G_{n,t}$, i.e., sets of vertices with no edges between them, correspond to t-intersecting families, thus we seek the size of a largest independent set in $G_{n,t}$. The latter is an NP-complete problem, but the well-known *Lovász theta function* $\vartheta(G_{n,t})$ provides an upper bound for this as the optimal value of a SDP. The proof of Theorem 4 uses discrete harmonic analysis on the space of perfect matchings to solve an infinite family of SDPs, i.e., that $\vartheta(G_{n,t}) = (2(n-t)-1)!!$ for all t and sufficiently large n.[1] The algebraic framework used in this proof and throughout my dissertation is the *theory of association schemes*, a generalization of finite group character theory to finite sets with high combinatorial regularity.

The characterization of the extremal families in Theorem 4 is deduced from a stability result for t-intersecting families that generalizes the following result that I also showed in my dissertation.

[1] This upper bound is easily seen to be tight.

Theorem 5. [25] *For any ϵ and $n > n(\epsilon)$, any intersecting family of $\mathcal{M}_{2n}$ of size greater than $(1-1/\sqrt{e}+\epsilon)(2n-3)!!$ is contained in an intersecting family of the form $\mathcal{F}_{ij} := \{m \in \mathcal{M}_{2n} : ij \in m\}$.*

Let $\mathcal{M}^k_{kn}$ be the collection of perfect matchings of the *complete k-uniform hypergraph* K^k_{kn} on kn vertices, i.e., pairwise disjoint sets of n hyperedges of size k that cover all the vertices. We say $\mathcal{F} \subseteq \mathcal{M}^k_{kn}$ is *partially 2-intersecting* if for any $m, m' \in \mathcal{F}$ there exist hyperedges $e \in m$ and $e' \in m$ such that $|e \cap e'| \geq 2$. With Yuval Filmus, we answer a conjecture [26, Conjecture 1] on the characterization of the largest partially 2-intersecting families of $\mathcal{M}^k_{kn}$.

Theorem 6. [21] *For all k and sufficiently large n, $\mathcal{F} \subseteq \mathcal{M}^k_{kn}$ is a largest partially 2-intersecting family if and only if $\mathcal{F} = \{m \in \mathcal{M}^k_{kn} : ij \subseteq e \text{ for some } e \in m\}$ for some 2-set ij.*

The techniques involved in this work are novel, as the algebraic combinatorics of $\mathcal{M}^k_{kn}$ for $k \geq 3$ confronts us with a non-commutative matrix algebra that we are still able to calculate within.

Algebraic Graph Theory. One of the most important objects in algebraic combinatorics is the *Kneser graph*, a graph defined over all k-sets of an n-element set such that two k-sets are adjacent if they have no element in common. A classic result of Lovász is that the eigenvalues η^j of this graph are simply binomial coefficients of the form $\eta^j = (-1)^j \binom{n-k}{k-j}$ for all $j = 0, 1, \ldots, k$.

There are many natural analogues of the Kneser graph for other combinatorial objects, and over the years their eigenvalues too are now well-understood with two notable exceptions: the *permutation* and *perfect matching analogues of the Kneser graph*. These are graphs defined over the set of all perfect matchings of $K_{n,n}$ (i.e., permutations) and K_{2n} respectively such that two perfect matchings are adjacent if they have no edge in common.

A long-standing open question in algebraic graph theory is whether an analogue of Lovász's result exists for the eigenvalues η^λ_1, η^λ_2 permutation and perfect matching analogues of the Kneser graph, i.e., an elegant combinatorial formula. Very recently, I answered this question affirmately by showing that the eigenvalues of these graphs count a basic new combinatorial object associated with an integer partition $\lambda = (\lambda_1, \cdots, \lambda_\ell) \vdash n$ called *λ-colored (perfect matching) derangements* [27].

Theorem 7 (L. 22+)**.** *Let η^λ_1 and η^λ_2 be the λ-eigenvalue of the permutation and perfect matching analogues of the Kneser graph. Then $\eta^\lambda_1 = (-1)^{n-\lambda_1} D^\lambda_1$ and $\eta^\lambda_2 = (-1)^{n-\lambda_1} D^\lambda_2$ where D^λ_1 and D^λ_2 are the number of λ-colored derangements of K_{λ_1,λ_1} and $K_{2\lambda_1}$, respectively.*

The proof crucially uses combinatorial identities connected to classical invariant theory that were discovered in the TCS-driven work on harmonic analysis over the space of perfect matchings [3].

Previous Research. Below is a brief sample of my earlier work in algorithmic graph theory and combinatorial optimization, which has taken a back seat to my recent research interests.

A binary matrix has the *consecutive-ones property* if there exists a permutation of its columns such that the 1's appear consecutively in each row. In joint work with Ross McConnell [28], we give a linear-time algorithm for certifying that a binary matrix does not have the consecutive-ones property, and also for certifying whether a graph is an *interval graph*, i.e., the intersection graph of a family of intervals on the real line. The latter graph class is particularly well-studied in algorithms and has spawned many interesting generalizations of interest to the algorithms community. One such generalization is the class of *co-TT* graphs introduced by Reed, Trotter, and Monma, who also proposed a $O(n^4)$-time algorithm for deciding if a graph on n vertices is co-TT [29]. With co-authors, we improve on this result by giving a faster $O(n^2)$-time algorithm for deciding if a graph on n vertices is co-TT [30].

References

[1] Ryan O'Donnell. *Analysis of Boolean Functions.* Cambridge University Press, 2014.

[2] Neta Dafni, Yuval Filmus, Noam Lifshitz, Nathan Lindzey, and Marc Vinyals. Complexity measures on the symmetric group and beyond (extended abstract). In James R. Lee, editor, *12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference*, volume 185 of *LIPIcs*, pages 87:1–87:5. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.

[3] Yuval Filmus and Nathan Lindzey. Harmonic polynomials on perfect matchings (extended abstract). In *Proceedings of the 34th International Conference on"Formal Power Series and Algebraic Combinatorics"*, FPSAC '22, 2022.

[4] Russell Impagliazzo and Ramamohan Paturi. The complexity of k-SAT. In *Proceedings of the Fourteenth Annual IEEE Conference on Computational Complexity*, COCO '99, page 237, USA, 1999. IEEE Computer Society.

[5] Radu Curticapean, Nathan Lindzey, and Jesper Nederlof. A tight lower bound for counting Hamiltonian cycles via matrix rank. In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '18, pages 1080–1099, Philadelphia, PA, USA, 2018. Society for Industrial and Applied Mathematics.

[6] Radu Curticapean, Nathan Lindzey, and Jesper Nederlof. A Tight Lower Bound for Counting Hamiltonian Cycles via Matrix Rank. In *3rd Highlights of Algorithms (HALG 2018), Amsterdam, Netherlands*, June 2018.

[7] Nathan Lindzey and Ansis Rosmanis. A Tight Lower Bound For Non-Coherent Index Erasure. In Thomas Vidick, editor, *11th Innovations in Theoretical Computer Science Conference (ITCS 2020)*, volume 151 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 59:1–59:37, 2020.

[8] Andris Ambainis, Loïck Magnin, Martin Roetteler, and Jeremie Roland. Symmetry-assisted adversaries for quantum state generation. In *Proceedings of the 2011 IEEE 26th Annual Conference on Computational Complexity*, CCC '11, pages 167–177, Washington, DC, USA, 2011. IEEE Computer Society.

[9] Peter Dukes, Ferdinand Ihringer, and Nathan Lindzey. On the algebraic combinatorics of injections (extended abstract). In *Proceedings of the 32nd International Conference on"Formal Power Series and Algebraic Combinatorics"*, FPSAC '20, 2020.

[10] P. J. Dukes, F. Ihringer, and N. Lindzey. On the algebraic combinatorics of injections and its applications to injection codes. *IEEE Transactions on Information Theory*, pages 1–1, 2020.

[11] Yuval Filmus. Friedgut-Kalai-Naor theorem for slices of the boolean cube. *Chic. J. Theor. Comput. Sci.*, 2016, 2016.

[12] Yuval Filmus, Ryan O'Donnell, and Xinyu Wu. A log-Sobolev inequality for the multislice, with applications. In Avrim Blum, editor, *10th Innovations in Theoretical Computer Science Conference, ITCS 2019, January 10-12, 2019, San Diego, California, USA*, volume 124 of *LIPIcs*, pages 34:1–34:12. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[13] Yuval Filmus, Guy Kindler, Elchanan Mossel, and Karl Wimmer. Invariance principle on the slice. *ACM Trans. Comput. Theory*, 10(3):11:1–11:37, 2018.

[14] Yuval Filmus. FKN theorem for the multislice, with applications. *Comb. Probab. Comput.*, 29(2):200–212, 2020.

[15] Hao Huang. Induced subgraphs of hypercubes and a proof of the sensitivity conjecture. *Annals of Mathematics*, 190(3):949–955, 2019.

[16] Aeryung Moon. An analogue of the Erdős–Ko–Rado theorem for the Hamming schemes $H(n,q)$. *J. Comb. Theory, Ser. A*, 32(3):386–390, 1982.

[17] P. Frankl and R.M. Wilson. The Erdős–Ko–Rado theorem for vector spaces. *Journal of Combinatorial Theory, Series A*, 43(2):228 – 236, 1986.

[18] Peter J. Cameron and C.Y. Ku. Intersecting families of permutations. *European Journal of Combinatorics*, 24(7):881 – 890, 2003.

[19] C. Godsil and K. Meagher. *Erdős–Ko–Rado Theorems: Algebraic Approaches.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2015.

[20] Nathan Lindzey. Erdös–Ko–Rado for perfect matchings. *European Journal of Combinatorics*, 65:130 – 142, 2017.

[21] Yuval Filmus and Nathan Lindzey. Simple algebraic proofs of uniqueness for Erdős–Ko–Rado theorems, 2022.

[22] Nathan Lindzey. *Matchings and Representation Theory.* PhD thesis, University of Waterloo, 2018.

[23] D. Ellis, E. Friedgut, and H. Pilpel. Intersecting families of permutations. *J. Amer. Math. Soc.*, 24:649–682, 2011.

[24] Nathan Lindzey. Intersecting families of perfect matchings (arXiv: 1811.06160).

[25] Nathan Lindzey. Stability for 1-intersecting families of perfect matchings. *European Journal of Combinatorics*, 86:103091, 2020.

[26] Karen Meagher, Mahsa N. Shirazi, and Brett Stevens. An extension of the Erdős-Ko-Rado theorem to uniform set partitions (arxiv pre-print), 2021.

[27] Nathan Lindzey. Jack derangements. *(Submitted)*, 2022.

[28] Nathan Lindzey and Ross M. McConnell. Linear-time algorithms for finding Tucker submatrices and Lekkerkerker-Boland subgraphs. *SIAM J. Discret. Math.*, 30(1):43–69, 2016.

[29] Clyde L. Monma, Bruce Reed, and William T. Trotter. Threshold tolerance graphs. *Journal of Graph Theory*, 12(3):343–362, 1988.

[30] Petr A. Golovach, Pinar Heggernes, Nathan Lindzey, Ross M. McConnell, Vinícius Fernandes dos Santos, Jeremy P. Spinrad, and Jayme Luiz Szwarcfiter. On recognition of threshold tolerance graphs and their complements. *Discret. Appl. Math.*, 216:171–180, 2017.