Institute for Advanced Study
granha@ias.edu
https://granha.github.io/
Nationality: Brazilian

# Fernando Granha Jeronimo

## Research Statement

I am broadly interested in theoretical computer science and its mathematical foundations [Wig19]. More specifically, my research focuses on the still largely mysterious boundary between efficient and intractable computation. I am particularly attracted to mathematical structures and properties enabling efficient algorithms, and conversely, also to those underpinning hardness or obstructions for such algorithms. So far, my work has involved convex optimization, coding theory, expansion and quantum computing including their interactions. In this statement, I will first briefly describe the areas most relevant to my research until now indicating where my research fits in. Then, I will provide more details in a summary of my completed projects, almost all done in various collaborations. Finally, I will point some future directions.

**Optimization:** Convex optimization has played an important role in the design of efficient algorithms for combinatorial optimization problems [Vaz01, WS11, GW95]. Linear programming and semi-definite programming reshaped our understanding of efficient computation. A natural generalization of these powerful tools is embodied in the Sum-of-Square (SOS) semi-definite hierarchy [Las15, FKP19, Dar20c], which captures the state-of-the-art polynomial time guarantees for many combinatorial optimization problems [Rag08, ARV04, BRS11, GS11]. Given this success, SOS has a double role in the study of computation. On the positive side, it can serve as a powerful tool to help advance the frontiers of efficient algorithms, and alternatively, a hardness result against this hierarchy can serve as a proxy for hardness, particularly useful for average case problems [BHK+16, KMOW17, GJJ+20] for which the sophisticated PCP machinery, e.g., [ALM+98, Din06, Aro98], for NP-hardness is not readily available. As I will discuss in more detail shortly, my research and interests span both algorithms [AJT19, AJQ+20, JQST20] and lower bounds [GJJ+20] involving this hierarchy. I believe that one of my most important contributions so far is the introduction of new optimization based decoding algorithms for explicit near-optimal codes [TS17], namely, one based on the SOS hierarchy [JQST20] decoding these codes for the first time and another with faster running time based on a new weak regularity decomposition of *expanding* hypergraphs [JST20, Jer22].

**Codes:** Roughly speaking, coding theory is the study of properties and algorithms related to sets of strings (*codes*) over finite alphabets [GRS19, vL99, Dar20a]. Typically, to really "unlock" interesting properties of codes, one brings to bear way more structure such as algebraic properties of low degree polynomials or structural properties of expanders graphs (the latter playing an important role in my research [AJQ+20, JQST20, JST20, JMO+22, Jer22]). The quest towards optimal parameter trade-offs for codes is particularly important. For a concrete example, consider all the information communicated and stored in binary form. To protect it against corruptions, we might want to encode it using binary codes which are sufficiently robust to allow recovery from possible corruptions. Being able to encode with the least amount of redundancy while providing the desired robustness guarantees can have several benefits (e.g., reduced energy consumption, faster communication time, reduced storage requirement and less waste). Since coding theory is a reasonably mature field dating back to the seminal work of Shannon [Sha49] and Hamming [Ham50], one might expect that, by now, binary codes are thoroughly understood. Surprisingly, this is not at all the case and in several aspects binary codes (and sometimes even small constant size alphabet codes) are the elusive case compared to their much larger alphabet counterparts [Gur09, Gur10]. For instance, in the case of general adversarial corruptions, we know since the 1950's [Gil52, Var57] that random binary codes achieve near optimal redundancy (rate) versus robustness (distance) trade-off, the so-called Gilbert–Varshamov (GV) bound. However, it was only in a recent breakthrough work that the first **explicit** construction of very robust (i.e., large distance) **binary** codes with parameters near the GV bound were discovered by Ta-Shama [TS17]. Ta-Shma's construction relies on the pseudorandom properties of expander graphs and it was **not** known to be efficiently decodable. As mentioned above, in [JQST20], we used the SOS hierarchy to design the first polynomial time decoding algorithms for Ta-Shma's codes, and later near-linear time decoders for binary [JST20] and larger constant (prime) alphabets [Jer22].

**Expanders:** Expansion is a phenomenon at the core of a myriad of results in theoretical computer science. To give a few examples, there are several expander based code constructions [ABN$^+$92, SS96, GKO$^+$17, HRW17, TS17, DHK$^+$19], the combinatorial proof of the PCP Theorem [Din06] and agreement testers [DK17, DD19]. Roughly speaking, an expander graph is an explicit sparse but well-connected graph admitting a variety of pseudorandom properties [HLW06, Chu97]. Expander graphs and coding theory have a synergetic two way multi-faceted relationship. As a concrete example (and a connection appearing in my research [AJQ$^+$20, JQST20, JST20, JMRW22, Jer22]), expander graphs can be used to resource efficiently amplify the distance of a base code, or to construct codes from smaller ones [JMO$^+$22]. Now, we give a gist of how the expander properties may be useful in this process: (i) an expander being pseudorandom can imply large distance, (ii) an expander being sparse can imply lower redundancy, and (iii) an expander being explicit can imply explicit code. More recently, a systematic study of **hypergraph** expanders, the so-called high-dimensional expanders (see [Lub18, Dar20b]), has emerged. This brought a new set of questions ranging from coding theory to design of very efficient PCPs.

## Completed Research Projects

In the following, I give brief descriptions of my completed projects almost all done in various collaborations (please see my website for further details).

- **Decoding algorithms for near optimal codes:** In [JQST20], we give polynomial time *unique decoding*[1] algorithm for nearly optimal, in terms of redundancy (rate) versus robustness (distance) trade-off (i.e., near the so-called Gilbert–Varshamov bound [Gil52, Var57]), explicit **binary** codes of large distance. These codes are (essentially) those explicit binary codes of distance $1/2 - \varepsilon$ and rate $\Omega(\varepsilon^{2+o(1)})$ arising from the breakthrough construction of Ta-Shma [TS17]. Our algorithms are based on the Sum-of-Squares hierarchy and use as a starting point a decoding framework from our earlier work [AJQ$^+$20]. Our main contribution consists in overcoming the far from optimal rates from [AJQ$^+$20] to operate in this near optimal regime for unique decoding. This result can be seen as a step towards a better understanding of the elusive case of binary codes in the general adversarial error model of Hamming [Ham50]. These algorithms are just a proof of concept showing that polynomial

[1] In fact, we obtain list decoding algorithms from which unique decoding follows. In particular, we now know that list decoding radius $1/2 - \varepsilon^c$ with rate $\Omega(\varepsilon^{2+\beta})$ with constant $c = c(\beta)$ can be deduced from all our algorithms mentioned in this paragraph. Even a tighter analysis [RR22] of our Sum-of-Squares decoding algorithm achieves list decoding radius $1/2 - \sqrt{\varepsilon}$ with rate $\Omega(\varepsilon^{2+o(1)})$, namely, near the Johnson bound.

time algorithms exist in this previously unattained regime. This result opened avenues for our subsequent near-linear time unique algorithms [JST20] using a novel algorithmic weak regularity decomposition in the style of Frieze and Kannan [FK96] but for sparse tensors supported on expanding hypergraphs. In [Jer22], we extend the near-linear time decoder to larger constant (prime) alphabets by generalizing the weak algorithmic weak regularity decomposition. Despite much work in the case of larger constant alphabets with some algebraic geometry codes even beating the GV bound[2], decoding explicit codes near the optimal regime[3] of $q$-ary codes of distance $1 - 1/q - \varepsilon$ and rate $\Omega_q(\varepsilon^{2+o(1)})$ was also an open problem. We hope that these techniques can also open avenues to list decoding algorithms with near optimal parameters (i.e., list decoding radius $1/2 - \varepsilon$ and rate near $\Omega(\varepsilon^2)$ for binary codes), this being a major open problem in the field [Gur09, Gur10]. In fact, a recent work [RR22] tightening the analysis of the Sum-of-Squares decoding algorithm [JQST20] interestingly shows that list decoding radius $1/2 - \sqrt{\varepsilon}$ with rate $\Omega(\varepsilon^{2+o(1)})$ is attained for binary codes (i.e., near Johnson bound parameters).

- **List decoding framework for binary codes:** In [AJQ+20], we provide a *list decoding* framework for distance amplified codes based on expanding structures: high-dimensional expanders (as in Dinur and Kaufman definition [DK17]) and walks on expander graphs. Roughly, list decoding is a relaxed decoding model in which we double the unique decoding radius at the expense of possibly having a small list of codewords rather than at most one. We view the problem of *unique decoding* as solving a suitable Max $k$-CSP (Constraint Satisfaction Problem) instance, which can be solved using our earlier work [AJT19] based on the SOS hierarchy. To obtain the list decoding framework, we maximize an entropic proxy[4] while solving a $k$-CSP. This makes the SOS solution rich enough so that we can "recover" a list of all the desired codewords from it. A noteworthy novelty of this work is that this framework can decode distance amplified **binary** codes obtained from **binary** codes of smaller distance without any use of larger alphabet codes at intermediate steps. Although this gives a new "genuinely binary" algorithmic technique, our rates were very far from the state-of-the-art results which typically rely on large alphabet techniques. Despite this parameter shortcoming, this framework served as our starting point for *unique decoding* results of nearly optimal codes [JQST20] mentioned above.

- **What exactly are optimal binary codes? (Phase I):** A longstanding mystery about binary codes is that we still do not have a fine-grained understanding of the rate versus distance trade-offs they achieve. We know that random binary codes achieve great parameters, but we do not know whether this is best possible. For codes of distance $1/2 - \varepsilon$, a random code achieves rate $\Omega(\varepsilon^2)$ whereas the best upper bound (impossibility result) is $O(\varepsilon^2 \log(1/\varepsilon))$ (see [Del75, MRRW77, Lau07, NS09, Alo09, Val19] for some upper bound related results). Improving any of these bounds (if possible) would be wonderful. For now, we are trying to tighten the upper bound. The state-of-the-art upper bound is obtained via a theoretical analysis of linear programs of Delsarte in [MRRW77] giving rise to the LP bound[5]. It is known that if the LP bounds are not asymptotically tight (i.e., the true rate is $o(\varepsilon^2 \log(1/\varepsilon))$), we will need stronger methods than Delsarte's LPs. Surprisingly, for the important class of linear codes it is only known the same bounds of general codes. In [CJJ22], we introduce a

[2] When they beat the GV bound, this happens in very specific distance intervals and not in the entire GV curve.

[3] In the larger constant alphabet case, there are two near optimal regimes: (i) fixed $q$ and vanishing $\varepsilon$ with distance $1 - 1/q - \varepsilon$ and rate $\Omega_q(\varepsilon^{2+o(1)})$ and (ii) $q$ being a function of $1/\delta$ with codes of distance $1 - \delta$ and rate $\approx \delta$.

[4] This entropic idea was independently used for list decoding in the context of machine learning by Karmalkar, Klivans and Kothari [KKK19] and Raghavendra and Yau [RY19]. Our results deal with finite fields/alphabets whereas theirs deal with $\mathbb{R}$. Among others, this leads to a variety of technical differences.

[5] Actually, there are two LP bounds and two families of Delsarte's LPs used to obtain them.

new hierarchy of linear programs which is structurally similar to Delsarte's LPs and actually coincides with them at its first level, but it is proven to converge to the true size of a code for linear codes. In particular, this opens up a new avenue of attack on this problem for linear codes that is theoretically proven to be sufficient and may better connect with existing techniques. Subsequently in [CJJ23], we refine the understanding of this hierarchy by introducing a new description of it and showing that the convergence is exact and happens at a lower level. This new perspective allows us to obtain that a similar hierarchy [LL22] by Loyfer and Linial is also complete. See my website for a short course explaining the background material as well as the hierarchy introduced in our work.

- **Almost optimal expanders from arbitrary expanders via operator amplification[6]:** In the work [JMRW22], we give an efficient algorithm that transforms any bounded degree expander graph into another one that achieves almost optimal (namely, near-quadratic, $d \leq 1/\lambda^{2+o(1)}$) trade-off between (any desired) spectral expansion $\lambda$ and degree $d$. Furthermore, the algorithm is *local*: every vertex can compute its new neighbors as a subset of its original neighborhood of radius $O(\log(1/\lambda))$. The optimal quadratic trade-off is known as the Ramanujan bound, so our construction gives almost Ramanujan expanders from arbitrary expanders.

  The transformation preserves structural properties of the original graph, and thus has many consequences. Applied to Cayley graphs, our transformation shows that *any* expanding finite group has almost Ramanujan expanding generators. Similarly, one can obtain almost optimal explicit constructions of quantum expanders, dimension expanders, monotone expanders, etc., from existing (suboptimal) constructions of such objects. Another consequence is a "derandomized" random walk on the original (suboptimal) expander with almost optimal convergence rate. Our transformation also applies when the degree is not bounded or the expansion is not constant.

  We obtain our results by a generalization of Ta-Shma's technique in his breakthrough paper [TS17], used to obtain explicit almost optimal binary codes. Specifically, our spectral amplification extends Ta-Shma's analysis of bias amplification from scalars to matrices of arbitrary dimension in a very natural way. Curiously, while Ta-Shma's explicit bias amplification derandomizes a well-known probabilistic argument (underlying the Gilbert–Varshamov bound), there seems to be no known probabilistic (or other existential) way of achieving our explicit ("high-dimensional") spectral amplification.

  Due to the generality of this transformation with its many consequences improving our understanding of almost optimal spectral expansion, I believe that this is also one of my most important contributions so far (see my website for a video explaining this work).

- **Expanders with additional symmetries:** In [JMO+22], we construct explicit expander graphs with additional (Abelian) symmetry properties. These extra symmetries are crucial in some applications such as the construction of classical quasi-cyclic LDPC codes which are widely used in practice as they are part of the 5G mobile standard [LBM+18]. They were also crucial in the first construction of almost linear quantum codes [PK21] (subsequently improved in the breakthrough [PK22] to linear distance and rate). To construct these expanders we use the lifting technique of Bilu and Linial [BL06] and are able to get explicit expanders very close to the Ramanujan bound. For instance, we can construct explicit expanders of degree $d$ with (unnormalized) expansion $2\sqrt{d-1} + o(1)$ with very large (Abelian) symmetries (see [JMO+22] for more technical details and see my website for a video explaining the techniques).

[6] I am borrowing from the abstract of our paper [JMRW22] since it says more or less exactly what I want to say here

- **Tighter bounds for the Birkhoff graph:** In [CJ20], we provide tighter bounds for the independence number of the Birkhoff graph family. This is a family of Cayley graphs on the symmetric group $S_n$ encoding the skeleton of the so-called Birkhoff polytope of doubly stochastic matrices [Bir46, Bar02]. Our results are obtained by making the beautiful representation theoretic techniques of Kane, Lovett and Rao [KLR17] "higher-order" (by analyzing more irreducible representations) and using linear programming. In particular, this allows us to improve their upper bound from $O(n!/\sqrt{2}^n)$ to $O(n!/1.97^n)$. By known connections this readily implies stronger alphabet lower bounds for a family of codes for distributed storage [GHJY14, GHK$^+$17].

- **Approximating $k$-CSPs on expanding structures:** In [AJT19], we give polynomial time approximation algorithms for $k$-CSPs (Constraint Satisfaction Problems) on suitably [7] expanding hypergraphs, which is a class of structures containing high-dimensional expanders (as in Dinur and Kaufman definition [DK17]) as an important special case. Naturally, the quality of approximation crucially depends on the quality of expansion of these hypergraphs. Our algorithmic results are based on the SOS hierarchy and generalize the 2-CSPs results of [BRS11, GS11]. Our results can be seen as a step towards better understanding structural properties of hypergraphs making $k$-CSPs easy to approximate. On the flip side, this result can also better inform what particular conditions[8] to avoid when trying to design hard $k$-CSP instances using hypergraphs, say, when designing a PCP. Via known connections, our algorithms translate into approximation algorithms for quantum $k$-CSPs, the so-called $k$-local Quantum Hamiltonians. However, contrary to the classical case where PCP theorems are known, the Quantum PCP Hamiltonian Conjecture [AAV13a] is widely open. More recently in [Jer22], using weak regularity techniques we obtain near-linear time (in the number of constraints) approximation algorithms for several of these expanding $k$-CSPs. In this later work, we also explore the special structure of linear equations over a general finite group to obtain improved approximation guarantees via a new weak regularity for matrix valued functions.

- **SOS lower bounds for the Sherrington–Kirkpatrick model:** In [GJJ$^+$20], we show that even as many as $n^\delta$ levels[9] of the SOS hierarchy (subexponential running time) still fail to provide a tighter energy upper bounds on the Sherrington–Kirkpatrick (SK) Hamiltonian [SK75] than the trivial, and non-tight, spectral bound. The SK Hamiltonian is a widely studied fundamental model of spin-glass in statistical physics admitting surprising connections [Tal06, Pan14, MS16, KB19, Mon19, MRX20] (e.g., the max-cut value of a random $d$-regular graphs is "determined" by this model [DMS17]). Despite this mouthful description, the SK model simply consists in maximizing a familiar[10] quadratic form $x^t Mx$, with $x$ ranging in $\{\pm 1\}^n$ and the twist that $M$ is an $n \times n$ random symmetric matrix with independent Gaussian entries[11]. With high probability this quadratic form has value $\approx 1.5264 \cdot n^{3/2}$ whereas SOS thinks its value is $(2 + o(1)) \cdot n^{3/2}$ (the spectral bound). We actually obtain lower bounds for another natural problem by doing *Fourier analysis of random matrices* [AMP20], and then via known connections [MRX20] derive the SK lower bound.

- **The power of unentangled quantum proofs I:** Quantum states can exhibit a unique form of

[7] More precisely, we generalize to hypergraphs the notion of threshold rank of a graph [BRS11] which is a robust version of expansion tolerating a few,i.e., $O(1)$, large eigenvalues (the rank) in the adjacency matrix of a graph.

[8] Of course the connection of, say, high-dimensional expanders and CSPs can take many forms, see [DFHT20] for a variation that already yields SOS hard instances.

[9] Here, $\delta > 0$ is a universal constant.

[10] Note that when $M$ is a the Laplacian of a graph this maximization problem becomes the familiar MaxCut problem.

[11] More precisely, $M$ is from the Gaussian orthogonal ensemble GOE($n$) (see [Tao12]).

quantum correlation known as quantum entanglement which can be stronger than any classical correlation [HHHH09]. Entanglement is also a fundamental resource in quantum computation and information [NC10, Wat18], and it underpins much of the distinctive power of the quantum setting. Despite its important role, entanglement is far from well-understood. In this project, we take a computational lens approach to study entanglement by investigating the power of quantum proofs *without* entanglement, a wide open well-known question in quantum complexity. Understanding its power is closely related to the complexity of determining if a (classical description of) quantum state is entangled and to the hardness of a variety of optimization problems (e.g., polynomial optimization over the sphere).

While two NP proofs are equivalent to a single larger one, two unentangled proofs seem substantially more powerful than a single one. A beautiful early result in this direction shows that two quantum proofs of logarithmic size[12] are enough to decide the NP-complete problem of graph 3-coloring [BT09]. However, one shortcoming of known results is that the verifier has a tiny polynomially small probability of distinguishing 'yes' from 'no' instances. From these results, it is only possible to deduce hardness results within tiny polynomial error (rather than constant error), and it also prevents scaling up these results to NEXP in an interesting way since the distinguishing probability becomes exponentially small.

In [JW22][13], we consider the case of unentangled quantum proofs with non-negative amplitudes and dub the corresponding complexity class $\mathrm{QMA}^+(2)$ (in analogy with the known $\mathrm{QMA}(2)$). In this setting, we design "global" protocols with distinguishing probabilities (gap) that are universal constants independent of the size of the quantum proofs. In particular, we design global protocols for small set expansion (SSE), unique games and label cover. In particular, this establishes $\mathrm{NP} \subseteq \mathrm{QMA}^+_{\log}(2)$ with constant gap and logarithmic sized proofs. Thanks to this constant distinguishing probability, scaling up these ideas leads to the full characterization $\mathrm{QMA}^+(2) = \mathrm{NEXP}$.

## Future Directions

In this section, I will point some reasonably concrete near future directions and I stress that I am not claiming any progress, but I am just expressing some of my interests[14]. Most of these projects are being pursued in various collaborations. Some of these problems might be quite challenging in which case any improved understanding might already constitute a nice outcome. I hope to also inspire a new generation of graduate students in tackling some of these various research directions.

The following are some directions being actively pursued.

- **Explicit binary codes near *list decoding capacity*:** List decoding provides a candidate bridge to achieve the best parameters of the simpler error model of Shannon [Sha49] in the general adversarial error regime of Hamming [Ham50]. Finding explicit optimal binary codes admitting efficient list decoding algorithms is a major open problem in coding theory [Gur09, Gur10]. Prior to the work of Ta-Shma [TS17], we had no idea what **explicit** near optimal binary codes for unique decoding looked like. Now, we do and more recently obtained unique and list decoding algorithms for them [JQST20, JST20]. Recently, in [RR22], a tighter analysis of the Sum-of-Squares decoding algorithm [JQST20] was shown to achieve list decoding radius $1/2 - \sqrt{\varepsilon}$ and rate $\Omega(\varepsilon^{2+o(1)})$, which is quadratically off from the near optimal

[12] number of qubits

[13] We are currently polishing the manuscript.

[14] Moreover, sometimes I may omit any partial approaches and results that we may have.

$1/2 - \varepsilon$ and rate $\Omega(\varepsilon^{2+o(1)})$. Given the power of Sum-of-Squares, it is conceivable that this Sum-of-Squares based algorithm is all we need algorithmically, and the remaining obstacle lies in proving combinatorial bounds on the list sizes. More precisely, we can ask the information theoretic question of whether Ta-Shma's codes are *combinatorially list decodable*, i.e., all list sizes are small regardless of the computational cost to find them. Resolving this question seems to require a more sophisticated use of the pseudorandom properties of expander graphs than done in [TS17], and hopefully might deepen our understanding of the connection between expanders and codes. Currently, only random ensembles of binary codes are known to achieve (near) optimal list decoding radius versus rate trade-offs[15] [MRRZ+19, GR08, GRS19], so only randomized analyses are available.

- **What exactly are optimal binary codes? (Phase II):** We are working in the analysis of our linear programming hierarchy from [CJJ22] trying to obtain improved asymptotic bounds on the rate of binary linear codes. We know that some (modern) Fourier analytic techniques used to analyze Delsarte's linear program (the state-of-the-art approach) generalize to our hierarchy. Better bounds (if possible) seem to require knowledge of the asymptotics of various quantities related to the hierarchy as well as a clever use of these Fourier techniques. We are currently investigating these asymptotic quantities and how to best use these techniques.

- **Quest for a second generation of near optimal explicit codes:** Ta-Shma's construction of explicit binary codes of distance $1/2 - \varepsilon$ and rate $\Omega(\varepsilon^{2+o(1)})$ was a tremendous breakthrough explicitly achieving distance versus rate trade-offs near probabilistic constructions from 1950's that gave rise to the GV bound. Nonetheless, there is still great interest in improving the rate all the way to the one of the probabilistic construction which is $\Omega(\varepsilon^2)$ for large distances (or even more ambitiously to stay close to the GV bound for every distance). Such a quest for even better codes may be very interesting and introduce even more techniques to the field.

- **The power of unentangled proofs II:** In the first phase, we developed some "global" protocols with constant distinguishing probability (gap) where the quantum proofs are assumed to have non-negative amplitudes. Starting from these protocols, the goal of the second phase is to try to handle (if possible) arbitrary quantum proofs with protocols of constant gap. Using small set expansion or unique games might give us some leverage due to the extra structure of these problems. If this phase succeeds, we might be able to obtain several improved hardness results (e.g., polynomial optimization over the sphere and several tensor problems) from the characterization $\mathrm{QMA}_{\log}(2) = \mathrm{NP}$ (with constant gap) and possibly also the characterization $\mathrm{QMA}(2) = \mathrm{NEXP}$. Currently, only trivial bounds on $\mathrm{QMA}(2)$ are known (i.e., $\mathrm{QMA} \subseteq \mathrm{QMA}(2) \subseteq \mathrm{NEXP}$).

- **Mixing properties of Markov chains for combinatorial problems:** Investigating expansion properties of Markov chains can be particularly useful in the study of sampling[16] combinatorial objects. One elusive such case is in sampling an approximately uniform proper coloring of a graph [FV07]. More precisely, given a graph of maximum degree $\Delta$ as input, can we efficiently sample an approximately uniform coloring using $q \geq \Delta + 2$ colors? The number of proper colorings of a graph is typically very large (exponential large[17]), so it is convenient to define a Markov chain that moves from a proper coloring to another only using local update rules (e.g., Glauber dynamics). If such a coloring Markov chain can be shown to be sufficiently expanding, then sampling amounts to start from an arbitrary proper coloring and

[15] These random ensembles actually achieve optimal list decoding radius versus rate trade-offs.

[16] in an approximate way

[17] in the number of vertices of the input graph.

then take polynomially many random steps in this chain to get an approximately uniform proper coloring. In this project, we are trying to better understand natural assumptions on the input graph that implies fast mixing.

The following directions are being cautiously and less actively pursued for now.

- **Derandomization of probabilistic log space:** one model at the frontier of our understanding of derandomization is probabilistic log space (e.g., the RL equals to L question). Understanding fine grained versions of operator amplification may be very useful in making progress on this question.

- **Quantum PCP conjecture:** The local Hamiltonian is the quantum analogue of classical constraint satisfaction problems (CSPs). One version of the classical PCP theorem asserts that deciding whether a CSP is fully satisfiable or far from satisfiable[18] is NP-hard in general. The quantum PCP conjecture [AAV13b] postulates that a similar phenomenon occurs in the quantum setting, namely, that approximating the "value" of a local Hamiltonian within a constant error is QMA-hard. The recent progress on quantum codes (with good quantum LDPC codes [PK22]) and the confirmation of the NLTS conjecture [ABN22] implied by the quantum PCP conjecture suggests that we are getting closer to understanding this latter conjecture.

- **Ramanujan graphs of every degree:** Ramanujan graphs were independently discovered by Lubotzky, Phillips and Sarnak [LPS88] and Margulis [Mar88]. Their constructions were based on number theoretic results and only some specific values of vertex degree were obtained. More recently, Marcus, Spielman and Srivastava [MSS15a] showed that *bipartite* Ramanujan graphs of every degree exist using a lift based construction. Nonetheless, it is still unknown whether general Ramanujan graphs of every possible degree exist. Since the Ramanujan bound represents the optimal degree versus expansion trade-offs, tackling this problem may lead to interesting new techniques as there is no margin for small errors (e.g., the solution to the Kadison–Singer problem [MSS15b] came as a byproduct of [MSS15a]).

- **Towards a systematic theory of average case hardness:** Currently, to understand the average case hardness of a computational problem, we do not have at our disposal the sophisticated PCP machinery of the worst case NP-hardness. As mentioned above, lower bounds against the powerful Sum-of-Squares hierarchy can be used as a hardness proxy for these problems. However, these lower bounds results are often very problem dependent and very technical. This ad-hoc nature is not conductive to a more systematic understanding of average case hardness. It is conjectured that simple general properties should be sufficient to determine the average hardness of several problems. Can we provide general Sum-of-Squares lower bounds based on these simple general conditions?

- **Subexponential time guarantees for MaxCut:** What are the best approximation guarantees for the MaxCut problem in the $1-\varepsilon$ regime that can obtained with subexponential time Sum-of-Squares (i.e., using $o(n)$ levels)? Can this be done by a geometric rounding scheme using the large number of vectors that Sum-of-Squares can provide in this case?

- **Combinatorial approach to the unique games conjecture:** Combinatorial ideas gave us a good control in the construction of expanders graphs, as in the zig-zag product of [RVW00], and the PCP Theorem by gap amplification of [Din06] (providing alternatives to the previous more algebraic approaches), I wonder whether the Unique Games Conjecture [Kho10] can be tackled using combinatorial ideas.

[18] A constant fraction of constraints is violated.

## Long Term Views

As theoretical computer science experiences a revolution in terms of its increased diversity, depth and impact to other sciences, I hope to contribute to this multidisciplinary effort by establishing bridges among its various (and constantly emerging) ramifications as well as by deepening its connection to mathematics. I am certain that convex optimization, coding theory, expansion and quantum computing will be part of my future explorations, but I want to keep an evergrowing horizon.

# References

[AAV13a] Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: The quantum PCP conjecture. *SIGACT News*, 44(2), June 2013. 5

[AAV13b] Dorit Aharonov, Itai Arad, and Thomas Vidick. The quantum pcp conjecture. *SIGACT News*, 2013. 8

[ABN$^+$92] N. Alon, J. Bruck, J. Naor, M. Naor, and R. Roth. Construction of asymptotically good, low-rate error-correcting codes through pseudo-random graphs. *IEEE Transactions on Information Theory*, 28:509–516, 1992. 2

[ABN22] Anurag Anshu, Nikolas P. Breuckmann, and Chinmay Nirkhe. Nlts hamiltonians from good quantum codes, 2022. 8

[AJQ$^+$20] Vedat Levi Alev, Fernando Granha Jeronimo, Dylan Quintana, Shashank Srivastava, and Madhur Tulsiani. List decoding of direct sum codes. In *Proceedings of the 31st ACM-SIAM Symposium on Discrete Algorithms*, pages 1412–1425. SIAM, 2020. 1, 2, 3

[AJT19] Vedat Levi Alev, Fernando Granha Jeronimo, and Madhur Tulsiani. Approximating constraint satisfaction problems on high-dimensional expanders. In *Proceedings of the 60th IEEE Symposium on Foundations of Computer Science*, pages 180–201, 2019. 1, 3, 5

[ALM$^+$98] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and hardness of approximation problems. *Journal of the ACM*, 45(3):501–555, 1998. Preliminary version in *Proc. of FOCS'92*. 1

[Alo09] Noga Alon. Perturbed identity matrices have high rank: Proof and applications. *Comb. Probab. Comput.*, 18(1-2):3–15, 2009. 3

[AMP20] Kwangjun Ahn, Dhruv Medarametla, and Aaron Potechin. Graph matrices: Norm bounds and applications. abs/1604.03423, 2020. URL: `https://arxiv.org/abs/1604.03423`, `arXiv:1604.03423`. 5

[Aro98] S. Arora. The approximability of NP-hard problems. In *Proceedings of the 30th ACM Symposium on Theory of Computing*, pages 337–348, 1998. 1

[ARV04] Sanjeev Arora, Satish Rao, and Umesh Vazirani. Expander flows and a $\sqrt{\log n}$-approximation to sparsest cut. In *Proceedings of the 36th ACM Symposium on Theory of Computing*, 2004. 1

[Bar02] A. Barvinok. *A Course in Convexity*. Graduate Studies in Mathematics. American Mathematical Society, 2002. 5

[BHK$^+$16] B. Barak, S. B. Hopkins, J. Kelner, P. Kothari, A. Moitra, and A. Potechin. A nearly tight sum-of-squares lower bound for the planted clique problem, 2016. 1

[Bir46] G. Birkhoff. Tres observaciones sobre el algebra lineal. *Universidad Nacional de Tucuman, Revista. Serie A*, 5, 1946. 5

[BL06] Yonatan Bilu and Nathan Linial. Lifts, discrepancy and nearly optimal spectral gap. *Combinatorica*, 26(5):495–519, October 2006. 4

[BRS11] Boaz Barak, Prasad Raghavendra, and David Steurer. Rounding semidefinite programming hierarchies via global correlation. In *Proceedings of the 52nd IEEE Symposium on Foundations of Computer Science*, pages 472–481, 2011. 1, 5

[BT09] Hugue Blier and Alain Tapp. All languages in NP have very short quantum proofs. In *2009 Third International Conference on Quantum, Nano and Micro Technologies*, 2009. 6

[Chu97] F. R. K. Chung. *Spectral Graph Theory*. American Mathematical Society, 1997. 2

[CJ20] Leonardo Nagami Coregliano and Fernando Granha Jeronimo. Tighter Bounds on the Independence Number of the Birkhoff Graph, 2020. arXiv:2007.05841. 5

[CJJ22] Leonardo Nagami Coregliano, Fernando Granha Jeronimo, and Chris Jones. A complete linear programming hierarchy for linear codes. In *ITCS*, volume 215, 2022. 3, 7

[CJJ23] Leonardo Nagami Coregliano, Fernando Granha Jeronimo, and Chris Jones. Exact completeness of lp hierarchies for linear codes. In *ITCS (to appear)*, 2023. 4

[Dar20a] Darintuga. Reading list on coding theory, 2020. URL: https://darintuga.github.io/doc/codes_reading.pdf. 1

[Dar20b] Darintuga. Reading list on high-dimensional expanders, 2020. URL: https://darintuga.github.io/doc/hdx_group.pdf. 2

[Dar20c] Darintuga. Reading list on the sum-of-squares hierarchy, 2020. URL: https://darintuga.github.io/doc/sos_reading.pdf. 1

[DD19] Yotam Dikstein and Irit Dinur. Agreement testing theorems on layered set systems. In *Proceedings of the 60th IEEE Symposium on Foundations of Computer Science*, 2019. 2

[Del75] P. Delsarte. The association schemes of coding theory. In *Combinatorics*, pages 143–161. Springer Netherlands, 1975. 3

[DFHT20] Irit Dinur, Yuval Filmus, Prahladh Harsha, and Madhur Tulsiani. Explicit sos lower bounds from high-dimensional expanders, 2020. arXiv:2009.05218. 5

[DHK$^+$19] Irit Dinur, Prahladh Harsha, Tali Kaufman, Inbal Livni Navon, and Amnon Ta-Shma. List decoding with double samplers. In *Proceedings of the 30th ACM-SIAM Symposium on Discrete Algorithms*, pages 2134–2153, 2019. 2

[Din06] Irit Dinur. The PCP theorem by gap amplification. In *Proc. 38th ACM Symp. on Theory of Computing*, pages 241–250, 2006. 1, 2, 8

[DK17] Irit Dinur and Tali Kaufman. High dimensional expanders imply agreement expanders. In *Proceedings of the 58th IEEE Symposium on Foundations of Computer Science*, pages 974–985, 2017. 2, 3, 5

[DMS17] Amir Dembo, Andrea Montanari, and Subhabrata Sen. Extremal cuts of sparse random graphs. *Ann. Probab.*, 45(2):1190–1217, 03 2017. 5

[FK96] A. Frieze and R. Kannan. The regularity lemma and approximation schemes for dense problems. In *Proceedings of the 37th IEEE Symposium on Foundations of Computer Science*, 1996. 3

[FKP19] N. Fleming, P. Kothari, and T. Pitassi. *Semialgebraic Proofs and Efficient Algorithm Design*. 2019. 1

[FV07] Alan Frieze and Eric Vigoda. 53a survey on the use of markov chains to randomly sample colourings. In *Combinatorics, Complexity, and Chance: A Tribute to Dominic Welsh*. Oxford University Press, 01 2007. 7

[GHJY14] P. Gopalan, C. Huang, B. Jenkins, and S. Yekhanin. Explicit maximally recoverable codes with locality. *IEEE Transactions on Information Theory*, 60(9):5245–5256, Sep. 2014. 5

[GHK$^+$17] P. Gopalan, G. Hu, S. Kopparty, S. Saraf, C. Wang, and S. Yekhanin. Maximally recoverable codes for grid-like topologies. In *Proceedings of the 28th ACM-SIAM Symposium on Discrete Algorithms*, 2017. 5

[Gil52] E.N. Gilbert. A comparison of signalling alphabets. *Bell System Technical Journal*, 31:504–522, 1952. 2

[GJJ$^+$20] Mrinalkanti Ghosh, Fernando Granha Jeronimo, Chris Jones, Aaron Potechin, and Goutham Rajendran. Sum-of-Squares Lower Bounds for Sherrington-Kirkpatrick via Planted Affine Planes. In *Proceedings of the 61st IEEE Symposium on Foundations of Computer Science*, 2020. 1, 5

[GKO$^+$17] Sivakanth Gopi, Swastik Kopparty, Rafael Oliveira, Noga Ron-Zewi, and Shubhangi Saraf. Locally testable and locally correctable codes approaching the Gilbert-Varshamov bound. In *Proceedings of the 28th ACM-SIAM Symposium on Discrete Algorithms*, SODA '17, pages 2073–2091, 2017. 2

[GR08] Venkatesan Guruswami and Atri Rudra. Concatenated codes can achieve list-decoding capacity. In *Proceedings of the 19th ACM-SIAM Symposium on Discrete Algorithms*, SODA '08, pages 258–267, 2008. 7

[GRS19] Venkatesan Guruswami, Atri Rudra, and Madhu Sudan. Essential coding theory. Available at `https://cse.buffalo.edu/faculty/atri/courses/coding-theory/book/index.html`, 2019. 1, 7

[GS11] Venkatesan Guruswami and Ali Kemal Sinop. Lasserre hierarchy, higher eigenvalues, and approximation schemes for graph partitioning and quadratic integer programming with psd objectives. In *Proceedings of the 52nd IEEE Symposium on Foundations of Computer Science*, pages 482–491, 2011. 1, 5

[Gur09] Venkatesan Guruswami. List decoding of binary codes–a brief survey of some recent results. In *Coding and Cryptology*, pages 97–106. Springer Berlin Heidelberg, 2009. 2, 3, 6

[Gur10] Venkatesan Guruswami. Bridging Shannon and Hamming: List error-correction with optimal rate. In *ICM*, 2010. 2, 3, 6

[GW95] M.X. Goemans and D.P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *Journal of the ACM*, 42(6):1115–1145, 1995. Preliminary version in *Proc. of STOC'94*. 1

[Ham50] Richard Hamming. Error detecting and error correcting codes. *Bell System Technical Journal*, 29:147–160, 1950. 2, 6

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, Jun 2009. 6

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc.*, 43(04):439–562, August 2006. 2

[HRW17] B. Hemenway, N. Ron-Zewi, and M. Wootters. Local list recovery of high-rate tensor codes applications. In *Proceedings of the 58th IEEE Symposium on Foundations of Computer Science*, pages 204–215, Oct 2017. 2

[Jer22] Fernando Granha Jeronimo. Fast decoding of explicit almost optimal $\varepsilon$-balanced $q$-ary codes and fast approximation of expanding $k$-csps. Manuscript available at https://granha.github.io/, 2022. 1, 2, 3, 5

[JMO$^+$22] Fernando Granha Jeronimo, Tushant Mittal, Ryan O'Donnell, Pedro Paredes, and Madhur Tulsiani. Explicit abelian lifts and quantum LDPC codes. In *ITCS*, volume 215, 2022. 1, 2, 4

[JMRW22] Fernando Granha Jeronimo, Tushant Mittal, Sourya Roy, and Avi Wigderson. Almost ramanujan expanders from arbitrary expanders via operator amplification. In *Proceedings of the 61st IEEE Symposium on Foundations of Computer Science*, 2022. 2, 4

[JQST20] Fernando Granha Jeronimo, Dylan Quintana, Shashank Srivastava, and Madhur Tulsiani. Unique Decoding of Explicit $\varepsilon$-balanced Codes Near the Gilbert–Varshamov Bound. In *Proceedings of the 61st IEEE Symposium on Foundations of Computer Science*, 2020. 1, 2, 3, 6

[JST20] Fernando Granha Jeronimo, Shashank Srivastava, and Madhur Tulsiani. Near-linear Time Decoding of Ta-Shma's Codes via Splittable Regularity. Manuscript, 2020. 1, 2, 3, 6

[JW22] Fernando Granha Jeronimo and Pei Wu. The power of unentangled quantum proofs with non-negative amplitudes. Manuscript available at https://granha.github.io/doc/gma2_plus.pdf, 2022. 6

[KB19] Dmitriy Kunisky and Afonso S. Bandeira. A tight degree 4 sum-of-squares lower bound for the sherrington-kirkpatrick hamiltonian. abs/1907.11686, 2019. URL: https://arxiv.org/abs/1907.11686, arXiv:1907.11686. 5

[Kho10] S. Khot. On the unique games conjecture (invited survey). In *2010 IEEE 25th Annual Conference on Computational Complexity*, pages 99–121, 2010. 8

[KKK19] Sushrut Karmalkar, Adam R. Klivans, and Pravesh K. Kothari. List-decodable linear regression. *CoRR*, abs/1905.05679, 2019. URL: http://arxiv.org/abs/1905.05679, arXiv:1905.05679. 3

[KLR17] D. Kane, S. Lovett, and S. Rao. The independence number of the birkhoff polytope graph, and applications to maximally recoverable codes. In *Proceedings of the 58th IEEE Symposium on Foundations of Computer Science*, pages 252–259, 2017. 5

[KMOW17] Pravesh Kothari, Ryuhei Mori, Ryan O'Donnell, and David Witmer. Sum of squares lower bounds for refuting any CSP. In *Proceedings of the 49th ACM Symposium on Theory of Computing*, 2017. 1

[Las15] Jean Bernard Lasserre. *An Introduction to Polynomial and Semi-Algebraic Optimization*. Cambridge Texts in Applied Mathematics. Cambridge University Press, 2015. doi:10.1017/CBO9781107447226. 1

[Lau07] Monique Laurent. Strengthened semidefinite programming bounds for codes. *Math. Program.*, 109(2-3):239–261, March 2007. 3

[LBM$^+$18] Huaan Li, Baoming Bai, Xijin Mu, Ji Zhang, and Hengzhou Xu. Algebra-assisted construction of quasi-cyclic LDPC codes for 5G new radio. *IEEE Access*, 6:50229–50244, 2018. doi:10.1109/ACCESS.2018.2868963. 4

[LL22] Elyassaf Loyfer and Nati Linial. New LP-based Upper Bounds in the Rate-vs.-Distance Problem for Linear Codes, 2022. 4

[LPS88] Alexander Lubotzky, R. Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8:261–277, 1988. 8

[Lub18] Alexander Lubotzky. High dimensional expanders. In *ICM*, 2018. 2

[Mar88] G. A. Margulis. Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators. 1988. 8

[Mon19] A. Montanari. Optimization of the sherrington-kirkpatrick hamiltonian. In *Proceedings of the 60th IEEE Symposium on Foundations of Computer Science*, pages 1417–1433, 2019. 5

[MRRW77] R. McEliece, E. Rodemich, H. Rumsey, and L. Welch. New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities. *IEEE Transactions on Information Theory*, 23(2):157–166, 1977. 3

[MRRZ$^+$19] Jonathan Mosheiff, Nicolas Resch, Noga Ron-Zewi, Shashwat Silas, and Mary Wootters. LDPC codes achieve list decoding capacity. In *Proceedings of the 61st IEEE Symposium on Foundations of Computer Science*, 2019. 7

[MRX20] Sidhanth Mohanty, Prasad Raghavendra, and Jeff Xu. Lifting sum-of-squares lower bounds: Degree-2 to degree-4. In *Proceedings of the 52nd ACM Symposium on Theory of Computing*, 2020. 5

[MS16] Andrea Montanari and Subhabrata Sen. Semidefinite programs on sparse random graphs and their application to community detection. In *Proceedings of the 48th ACM Symposium on Theory of Computing*, pages 814–827, 2016. 5

[MSS15a] Adam Marcus, Daniel Spielman, and Nikhil Srivastava. Interlacing families i: Bipartite Ramanujan graphs of all degrees. *Annals of Mathematics*, 2015. 8

[MSS15b] Adam Marcus, Daniel Spielman, and Nikhil Srivastava. Interlacing families ii: Mixed characteristic polynomials and the kadison–singer problem. *Annals of Mathematics*, 2015. 8

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. 6

[NS09] Michael Navon and Alex Samorodnitsky. Linear programming bounds for codes via a covering argument. *Discrete Comput. Geom.*, 41(2):199–207, March 2009. 3

[Pan14] Dmitry Panchenko. The parisi formula for mixed $p$-spin models. *Ann. Probab.*, 42(3):946–958, 05 2014. 5

[PK21] Pavel Panteleev and Gleb Kalachev. Quantum LDPC Codes with Almost Linear Minimum Distance. *IEEE Transactions on Information Theory*, 2021. 4

[PK22] Pavel Panteleev and Gleb Kalachev. Asymptotically good quantum and locally testable classical ldpc codes. In *Proceedings of the 52nd ACM Symposium on Theory of Computing*, 2022. 4, 8

[Rag08] Prasad Raghavendra. Optimal algorithms and inapproximability results for every CSP? In *Proceedings of the 40th ACM Symposium on Theory of Computing*, pages 245–254, 2008. 1

[RR22] Silas Richelson and Sourya Roy. List-decoding random walk XOR codes near the johnson bound. *Electron. Colloquium Comput. Complex.*, TR22-069, 2022. 2, 3, 6

[RVW00] O. Reingold, S. Vadhan, and A. Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors. In *Proceedings of the 41st IEEE Symposium on Foundations of Computer Science*, 2000. 8

[RY19] Prasad Raghavendra and Morris Yau. List decodable learning via sum of squares. *CoRR*, abs/1905.04660, 2019. URL: `http://arxiv.org/abs/1905.04660`, `arXiv:1905.04660`. 3

[Sha49] Claude Shannon. The synthesis of two-terminal switching circuits. *Bell System Technical Journal*, 28:59–98, 1949. 2, 6

[SK75] David Sherrington and Scott Kirkpatrick. Solvable model of a spin-glass. *Phys. Rev. Lett.*, 35:1792–1796, Dec 1975. 5

[SS96] M. Sipser and D. Spielman. Expander codes. *IEEE Transactions on Information Theory*, 42(6):1710–1722, 1996. Preliminary version in *Proc. of FOCS'94*. 2

[Tal06] Michel Talagrand. The parisi formula. *Annals of mathematics*, pages 221–263, 2006. 5

[Tao12] Terence Tao. *Topics in Random Matrix Theory*. Graduate Studies in Mathematics. American Mathematical Society, 2012. 5

[TS17] Amnon Ta-Shma. Explicit, almost optimal, epsilon-balanced codes. In *Proceedings of the 49th ACM Symposium on Theory of Computing*, STOC 2017, pages 238–251, New York, NY, USA, 2017. ACM. 1, 2, 4, 6, 7

[Val19] Frank Vallentin. Semidefinite programming bounds for error-correcting codes. *ArXiv*, abs/1902.01253, 2019. 3

[Var57] R.R. Varshamov. Estimate of the number of signals in error correcting codes. *Doklady Akademii Nauk SSSR*, 117:739–741, 1957. 2

[Vaz01] Vijay V. Vazirani. *Approximation Algorithms*. Springer-Verlag, Berlin, Heidelberg, 2001. 1

[vL99] Jacobus H. van Lint. *Introduction to Coding Theory*. Springer-Verlag, 1999. 1

[Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018. 6

[Wig19] Avi Wigderson. *Mathematics and Computation: A Theory Revolutionizing Technology and Science*. Princeton University Press, 2019. 1

[WS11] David P. Williamson and David B. Shmoys. *The Design of Approximation Algorithms*. Cambridge University Press, USA, 1st edition, 2011. 1