Certifying Solution Geometry in Random CSPs: Counts, Clusters and Balance

Jun-Ting Hsieh
Carnegie Mellon University, Pittsburgh, PA, USA

Sidhanth Mohanty
University of California at Berkeley, CA, USA

Jeff Xu
Carnegie Mellon University, Pittsburgh, PA, USA

Abstract

An active topic in the study of random constraint satisfaction problems (CSPs) is the geometry of the space of satisfying or almost satisfying assignments as the function of the density, for which a precise landscape of predictions has been made via statistical physics-based heuristics. In parallel, there has been a recent flurry of work on *refuting* random constraint satisfaction problems, via nailing refutation thresholds for spectral and semidefinite programming-based algorithms, and also on *counting* solutions to CSPs. Inspired by this, the starting point for our work is the following question: *What does the solution space for a random CSP look like to an efficient algorithm?*

In pursuit of this inquiry, we focus on the following problems about random Boolean CSPs at the densities where they are unsatisfiable but no refutation algorithm is known.

1. **Counts.** For every Boolean CSP we give algorithms that with high probability certify a subexponential upper bound on the number of solutions. We also give algorithms to certify a bound on the number of large cuts in a Gaussian-weighted graph, and the number of large independent sets in a random d-regular graph.
2. **Clusters.** For Boolean 3CSPs we give algorithms that with high probability certify an upper bound on the number of *clusters* of solutions.
3. **Balance.** We also give algorithms that with high probability certify that there are no "unbalanced" solutions, i.e., solutions where the fraction of +1s deviates significantly from 50%.

Finally, we also provide hardness evidence suggesting that our algorithms for counting are optimal.

2012 ACM Subject Classification Theory of computation → Graph algorithms analysis

Keywords and phrases constraint satisfaction problems, certified counting, random graphs

Digital Object Identifier 10.4230/LIPIcs.CCC.2022.11

Related Version *Full Version*: https://arxiv.org/abs/2106.12710

Funding *Jun-Ting Hsieh*: Supported by NSF CAREER Award #2047933.
Sidhanth Mohanty: Supported by Google PhD Fellowship.
Jeff Xu: Supported by NSF CAREER Award #2047933.

Acknowledgements We would like to thank Pravesh Kothari, Prasad Raghavendra, and Tselil Schramm for their encouragement and thorough feedback on an earlier draft. We would also like to thank Tselil Schramm for enlightening discussions on refuting random CSPs.

1 Introduction

Constraint satisfaction problems (CSPs) are fundamental in the study of algorithm design and complexity theory. They are simultaneously simple and also richly expressive in capturing a wide range of computational tasks, which has led to fruitful connections to other areas of theoretical computer science (see, for example, [33, 8] for connections to cryptography, [21] for

applications to hardness of learning, and [25] for applications to average-case hardness). Hence, understanding them has received intense attention in the past few decades, leading to several comprehensive theories of their complexity. Some of the highlights include: the Dichotomy Theorem, which characterizes the worst-case complexity of satisfiability of CSPs via their algebraic properties [69, 14, 78], inapproximability results via the PCP Theorem [35], and the theory of optimal inapproximability based on connections between semidefinite programming and the Unique Games conjecture [41, 42, 65].

In this work, we are interested in the algorithmic aspects of random instances of CSPs. There has been a diverse array of phenomena about random CSPs illustrated in recent work, of dramatically varying nature depending on the ratio of the number of constraints to the number of variables, known as the *density*. Of central importance is the *satisfiability threshold*, which marks a phase transition where a random CSP instance shifts from being likely satisfiable to being likely unsatisfiable. When the density is well below the satisfiability threshold, there are several algorithms for tasks such as counting and sampling assignments to a random CSP instance [55, 39, 30, 11], whereas well above this threshold there are efficient algorithms for *certifying* that random CSPs are unsatisfiable [5]. The densities in the interim hold mysteries that we don't yet fully understand, and this work is an effort to understand the algorithmic terrain there. To make matters concrete, for now we will specialize the discussion of the problem setup and our work to the canonical 3SAT predicate.

Consider a random 3SAT formula $\boldsymbol{\mathcal{I}}$ on n variables and Δn clauses where each clause is sampled uniformly, independently, and adorned with uniformly random negations. Once the density Δ is a large enough constant, this random instance is unsatisfiable with high probability.[1] On the other hand, the widely believed Feige's random 3SAT hypothesis [25] conjectures that when Δ is any constant, there is no algorithm to *certify* that a random instance is unsatisfiable. Further, the best known algorithms for efficiently certifying that it is unsatisfiable require $\Delta \gtrsim \sqrt{n}$ [32, 16, 27, 5]. Moreover, when $\Delta \lesssim \sqrt{n}$ there is a lower bound against the Sum-of-Squares hierarchy [34, 70] (known to capture many algorithmic techniques), which suggests an *information-computation gap* and earns $\sqrt{n}$ the name *refutation threshold*.

In this picture, at both densities $n^{.25}$ and $n^{.35}$, $\boldsymbol{\mathcal{I}}$ is likely unsatisfiable but "looks" satisfiable to an efficient algorithm. But is there a concrete sense in which a random formula at density $n^{.25}$ is "more satisfiable" than one at density $n^{.35}$ from the lens of a polynomial-time algorithm? A natural measure of a 3SAT formula's satisfiability is its number of satisfying assignments, which motivates the following question.

> *What is the best efficiently certifiable upper bound on the number of assignments satisfying $\boldsymbol{\mathcal{I}}$?*

Our work provides an extensive study in this open direction.

In the context of 3SAT, our work proves:

▶ **Theorem 1** (Informal). *There is an efficient algorithm to certify with high probability that a random* 3SAT *formula with density $\Delta = n^{1/2-\delta}$ has at most $\exp(\widetilde{O}(n^{3/4+\delta/2}))$ satisfying assignments.*

In addition to certifying the number of satisfying assignments, we can certify that the solutions form clusters and upper bound the number of clusters under the refutation threshold.

[1] In fact, it is conjectured that there is a sharp threshold for unsatisfiability once Δ crosses some constant $\alpha_{\text{SAT}} \approx 4.267$.

Clusters. Besides the satisfiability threshold, random kSAT is conjectured to go through other phase transitions too, as predicted in the work of [45]. In particular, the *clustering threshold* is the density where the solution space is predicted to change from having one giant component to roughly resembling a union of several small Hamming balls, known as *clusters*, that are pairwise far apart in Hamming distance.

Much like the refutation threshold that marks where efficient algorithms can witness unsatisfiability, it is natural to ask if there is some regime under the refutation threshold where an efficient algorithm can witness a bound on the number of clusters of solutions. The following more nuanced version of Theorem 1 gives an answer to this question.

▶ **Theorem 2** (Informal). *There is an efficient algorithm to certify with high probability that the satisfying assignments of a random* 3SAT *formula with density* $\Delta = n^{1/2-\delta}$ *are covered by at most* $\exp(\widetilde{O}(n^{1/2+\delta}))$ *diameter-*$\widetilde{O}(n^{3/4+\delta/2})$ *clusters.*

Balance in the solution space. Suppose at density Δ, a typical 3SAT formula has $\sim \exp(c_\Delta n)$ satisfying assignments, then due to the uniformly random negations in clauses, each string is satisfying with probability $\sim \exp((c_\Delta - 1)n)$. Then one can show via the first moment method that with high probability there are no satisfying assignments with Hamming weight outside $\left[\frac{1}{2} - f(c_\Delta), \frac{1}{2} + f(c_\Delta)\right]$.[2] In particular, the intersection of the solution space with the set of unbalanced strings empties out under the satisfiability threshold. This raises the question:

> *Is there an efficient algorithm to certify that a random CSP instance has no unbalanced assignments at density significantly under the refutation threshold?*

We affirmatively answer this question and in the special case of 3SAT prove:

▶ **Theorem 3** (Informal). *There is an efficient algorithm to certify with high probability that a random* 3SAT *formula with density* $\Delta = n^{1/2-\delta}$ *has no satisfying assignments with Hamming weight outside*

$$\left[\frac{1}{2} - \widetilde{\Theta}\left(\frac{1}{n^{1/4-\delta/2}}\right), \frac{1}{2} + \widetilde{\Theta}\left(\frac{1}{n^{1/4-\delta/2}}\right)\right].$$

We illustrate our upper bounds for counting satisfying assignments and clusters in Figure 1. We delve into the precise technical statements of our results and the techniques involved in proving them in Section 1.1. Then to put our work in context, we survey and discuss existing work on information-computation gaps, and algorithmic work on counting, sampling and estimating partition functions in Section 1.2.

1.1 Our Contributions

In this section, we give a more detailed technical description of our contributions. To set the stage for doing so, we first formally clarify the notion of *certification* and some preliminaries on constraint satisfaction problems.

Fix a sample space Ω, a probability distribution $\mathcal{D}$ over Ω, and a function $f : \Omega \to \mathbb{R}$. For example, Ω is the space of 3SAT instances, $\mathcal{D}$ is the distribution of instances given by the random 3SAT model, and f is the number of satisfying assignments.

[2] where f is chosen so that the number of strings outside that Hamming range is $\ll \exp((c_\Delta - 1)n)$.

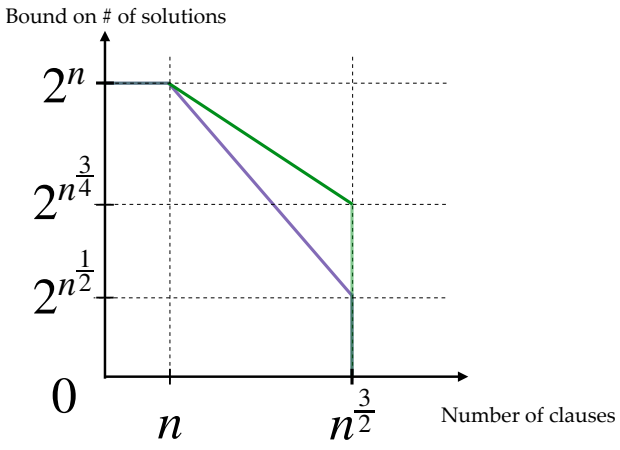

Figure 1 Our results for 3SAT. **Green**: certifiable upper bound on the number of satisfying assignments. **Purple**: upper bound on the number of clusters of satisfying assignments. In the case of kSAT, the green plot looks identical but with n replaced by $n^{(k-1)/2}$ and $n^{3/2}$ replaced by $n^{k/2}$.

▶ **Definition 4.** *We say that a deterministic algorithm $\mathcal{A}$ certifies that $f \leqslant C$ with probability over $1-p$ over $\mathcal{D}$ if $\mathcal{A}$ satisfies*

1. *For all $\omega \in \Omega$, $f(\omega) \leqslant \mathcal{A}(\omega)$.*
2. *For a random sample $\boldsymbol{\omega} \sim \mathcal{D}$, $\mathcal{A}(\boldsymbol{\omega}) \leqslant C$ with probability over $1-p$.*

We emphasize that an algorithm that always outputs the typical value of f is *not* a certification algorithm: it will satisfy the second condition but not the first. Thus, in several average-case problems, there are gaps between the typical value and the best known certifiable upper bound.

▶ Remark 5. Due to the guarantees of $\mathcal{A}$, one can think of the "transcript" of the algorithm on input ω as being a proof that $f(\omega) \leqslant \mathcal{A}(\omega)$.

▶ **Definition 6.** *A predicate $P : \{\pm 1\}^k \to \{0,1\}$ is any Boolean function that is not a constant function. An instance $\mathcal{I}$ of a constraint satisfaction problem on predicate P and vertex set $[n]$ is a collection of clauses, where a clause is a pair (c,S) with $c \in \{\pm 1\}^k$ and $S \in [n]^k$. Given $x \in \{\pm 1\}^n$, the value of $\mathcal{I}$ on x is:*

$$\mathcal{I}(x) \coloneqq \frac{1}{|\mathcal{I}|} \sum_{(c,S)\in\mathcal{I}} P(c_1 x_{S_1}, \ldots, c_k x_{S_k}).$$

We say x satisfies a clause (c,S) if $P(c_1 x_{S_1}, \ldots, c_k x_{S_k}) = 1$, and say x is $(1-\eta)$-satisfying if $\mathcal{I}(x) \geqslant 1-\eta$. If $\eta = 0$, we say x is exactly satisfying.

▶ Remark 7. An important predicate instrumental in all our results is the kXOR predicate, defined as follows:

$$k\mathsf{XOR}(x_1, \ldots, x_k) = \prod_{i=1}^{k} x_i.$$

In this work we are concerned with random CSPs. We defer an exact description of the random model to Section 2.3 of the full version (note however that the common random models used in the literature are all qualitatively similar; cf. [5, Appendix D]). Our first result is an algorithm certifying a subexponential upper bound on the number of $(1-\eta)$-satisfying assignments for random CSPs.

▶ **Theorem 8.** *Let $\boldsymbol{\mathcal{I}}$ be a random kCSP instance on any predicate P on n variables and Δn clauses. For every $\varepsilon > 0$ and $\eta \in [0, \eta_0]$ for some constant $\eta_0 > 0$, there is an algorithm that certifies with high probability that the number of $(1-\eta)$-satisfying assignments to $\boldsymbol{\mathcal{I}}$ is upper bounded by:*[3]

$$\exp\left(O\left(\eta \log \frac{1}{\eta}\right) n\right) \cdot \exp\left(\widetilde{O}\left(\sqrt{\frac{n^{(k+1)/2}}{\Delta}}\right)\right) \cdot \exp\left(O\left(\frac{n^{1+\varepsilon}}{\Delta^{1/(k-2)}}\right)\right).$$

To more easily parse the statement, let's plug in concrete parameters.

▶ Remark 9. Let's fix the predicate to be kSAT for any $k \geqslant 3$, $\eta = 0$, and $\Delta = n^{k/2-1.1}$. The quantity of interest is the number of exactly satisfying solutions to a random kSAT formula at a density strictly smaller than the refutation threshold of $\widetilde{\Omega}(n^{k/2-1})$. Then, we get an algorithm that with high probability certifies that the number of exactly satisfying assignments is at most: $\exp(\widetilde{O}(n^{0.8}))$, which is a subexponential bound. More generally, our algorithms certify a subexponential bound on the number of satisfying assignments for kSAT for $\Delta = n^{k/2-1.5+c}$ for any $c > 0$ and this bound improves as we increase c.

The proof of Theorem 8 relies on 3 ingredients of increasing complexity. The first is the simple observation that given a kCSP instance $\mathcal{I}$ on any predicate P, there is a transformation to a kSAT instance $\mathcal{I}'$ such that:

(i) For any $\eta > 0$, if x is $(1-\eta)$-satisfying for $\mathcal{I}$, then it is also $(1-\eta)$-satisfying for $\mathcal{I}'$.

(ii) If $\boldsymbol{\mathcal{I}}$ is a random instance of a CSP on P with density Δ, then $\boldsymbol{\mathcal{I}}'$ is a random instance of kSAT with density Δ.

This reduction is described in the proof of Corollary 4.8 of the full version.

The second ingredient is a generalization of the "3XOR-principle" of [25, 27], which we call the "kXOR-principle". The kXOR principle, which we state below, reduces count certification/refutation for a random kSAT formula to the same task on a random kXOR formula.

▶ **Lemma 10.** *Let $\boldsymbol{\mathcal{I}}$ be a random kSAT formula on $m = \Delta n$ clauses. There is an efficient algorithm that with high probability certifies that any $(1-\eta)$-satisfying assignment of $\boldsymbol{\mathcal{I}}$ must kXOR-satisfy at least $\left(1 - O(\eta) - \widetilde{O}\left(\sqrt{\frac{n^{(k-3)/2}}{\Delta}}\right)\right) m$ clauses.*

We detail the proof in Section 3 of the full version, which is close to the reduction from generic CSP refutation to kXOR refutation in [5] based on the Fourier expansion.

For the sake of a notationally simple sketch, let's restrict ourselves to the case $\eta = 0$. We can write $k\mathsf{SAT}(x_1, \ldots, x_k) = (1 - 2^{-k}) + 2^{-k} x_1 x_2 \cdots x_k + q(x_1, \ldots, x_k)$ where q is a degree-$(k-1)$ polynomial without a constant term. Thus, given a random kSAT instance $\boldsymbol{\mathcal{I}}$ and any satisfying assignment x:

$$1 = \boldsymbol{\mathcal{I}}(x) = 1 - 2^{-k} + 2^{-k} \frac{1}{|\boldsymbol{\mathcal{I}}|} \sum_{(c,S) \in \boldsymbol{\mathcal{I}}} \prod_{i=1}^{k} c_i x_{S_i} + \frac{1}{|\boldsymbol{\mathcal{I}}|} \sum_{c,S \in \boldsymbol{\mathcal{I}}} q(c_1 x_{S_1}, \ldots, c_k x_{S_k}).$$

Once $\Delta \gtrsim n^{(k-3)/2}$ the refutation algorithm of [5] can be employed to certify that the last term is insignificantly small by virtue of the last term being a degree-$(k-1)$ polynomial with no constant term. This would force $2^{-k} \frac{1}{|\boldsymbol{\mathcal{I}}|} \sum_{(c,S) \in \boldsymbol{\mathcal{I}}} \prod_{i=1}^{k} c_i x_{S_i}$ to be near 1, which is the same as saying x must kXOR-satisfy most clauses.

[3] We use the convention that $\eta \log \frac{1}{\eta} = 0$ when $\eta = 0$.

Our third ingredient for Theorem 8 is a count certification algorithm for kXOR, which we prove in Section 4 of the full version.

▶ **Theorem 11.** *For constant $k \geqslant 3$, consider a random kXOR instance with n variables and Δn clauses. For any constant $\varepsilon > 0$, there is a polynomial-time algorithm that certifies with high probability that the number of $(1-\eta)$-satisfying assignments is at most*

$$\exp\left(O\left(\eta \log \frac{1}{\eta}\right) n\right) \cdot \exp\left(O\left(\frac{n^{1+\varepsilon}}{\Delta^{1/(k-2)}}\right)\right).$$

In fact, the certification algorithm only depends on the hypergraph structure of the kXOR instance and not the signings of each clause. This is crucial since our algorithm recursively looks at $(k-1)$XOR subinstances with unknown signings. The stronger statement we prove is:

▶ **Theorem 12.** *For constant $k \geqslant 2$, consider a random k-uniform hypergraph $\boldsymbol{H}$ on n vertices and Δn hyperedges where $\Delta \gg \log n$. For $\varepsilon > 0$, there is a polynomial-time algorithm that certifies with high probability that the number of $(1-\eta)$-satisfying assignments to any kXOR instance on $\boldsymbol{H}$ is at most*

$$\exp\left(O\left(\eta \log \frac{1}{\eta}\right) n\right) \cdot \begin{cases} 1 & \text{if } k = 2 \\ \exp\left(\widetilde{O}\left(\frac{n^{1+\varepsilon}}{\Delta^{1/(k-2)}}\right)\right) & \text{if } k \geqslant 3. \end{cases}$$

Theorem 12 is of interest beyond algorithmic considerations as it gives a high-probability bound on the number of approximate solutions for *any* kXOR formula on a random hypergraph.

▶ Remark 13. Gaussian elimination is able to count exact solutions to an explicit kXOR instance but fails for counting $(1-\eta)$-satisfying assignments or when the signings are unknown.

We now give a brief sketch of our proof of Theorem 12. Given a random k-uniform hypergraph, we would like to certify that *any* kXOR instance on this hypergraph has no more than $\exp\left(O(\eta \log \frac{1}{\eta})n\right) \cdot \exp\left(\widetilde{O}\left(\frac{n^{1+\varepsilon}}{\Delta^{1/(k-2)}}\right)\right)$ approximate solutions. We will first present an overview in the context of 2XOR as the "base case", and then explain the algorithm for 3XOR to illustrate the "recursive step".

2XOR sketch. Let's consider a random graph $\boldsymbol{G}$ on n vertices and Δn edges where $\Delta \gg \log n$. Then, its degrees concentrate and its normalized Laplacian has a large spectral gap (more precisely, a spectral gap of $1 - O\left(\frac{1}{\sqrt{\Delta}}\right)$). As a consequence of Cheeger's inequality, any set S containing fewer than half the vertices has roughly half its edges leaving – which quantitatively would be around $\Delta|S|$. We prove that a large spectral gap and concentration of degrees is all that is necessary for any 2XOR instance to have an appropriately bounded number of satisfying assignments.

Now let $\mathcal{I}$ be any 2XOR instance on $\boldsymbol{G}$. The key observation is that if x and x' are two $(1-\eta)$-satisfying assignments for $\mathcal{I}$, then the pointwise product $y \coloneqq x \circ x'$ is $(1-2\eta)$-satisfying for $\mathcal{I}_+$, the 2XOR instance on $\boldsymbol{G}$ obtained by setting the sign on all constraints to $+1$. The constraints violated by y are the ones on the cut between S_+ and S_-, the positive and negative vertices in y respectively. There are roughly $\Delta \cdot \min\{|S_+|, |S_-|\}$, and consequently $\min\{|S_+|, |S_-|\} \leqslant 2\eta n$ since y is $(1-2\eta)$-satisfying. In particular, y either has at most $2\eta n$ positive entries or $2\eta n$ negative entries. The upshot is the number of $(1-\eta)$-satisfying assignments of $\mathcal{I}$ is at most $\exp(O(\eta \log \frac{1}{\eta})n))$. This sketched argument is carefully carried out in Section 4.1 of the full version.

3XOR sketch. Now, let $\boldsymbol{H}$ be a random hypergraph on n vertices and Δn hyperedges. The observation here is that for any 3XOR instance $\mathcal{I}$ on $\boldsymbol{H}$, any assignment x that $(1-\eta)$-satisfies $\mathcal{I}$ also approximately satisfies a particular *induced* 2XOR *instance* of a fixed subset of variables S. The induced 2XOR instance's underlying graph G is fixed and distributed like a random graph, and only the signings on the edges vary as we vary x. That lets us run the algorithm for 2XOR on G to obtain an upper bound F on all induced instances on G, which then yields a bound of $2^{|S|} \cdot F$. This is where we use that our algorithm depends only on the underlying graph, hence avoiding an enumeration of all assignments to variables in S.

We immediately see that for a fixed subset S, the above procedure throws away most of the clauses (keeping only clauses that have 1 variable in S). Thus, it is clearly suboptimal to look at just one subset S. To resolve this, we partition the variables into subsets $S_1, \ldots, S_\ell$, run the algorithm on each of them, and aggregate the results. This is explained in detail in the proofs of Lemma 4.6 and Theorem 4.4 of the full version.

Clustering. Our next result is an algorithm to upper bound the number of clusters formed by the solutions. Given $x \in \{\pm 1\}^n$, we call the Hamming ball $B(x, r)$ a *radius-r cluster* or *diameter-$2r$ cluster*. For 3CSPs we prove in Corollary 5.2 of the full version:

▶ **Theorem 14.** *Let P be any 3-ary predicate, and let $\boldsymbol{\mathcal{I}}$ be a random instance of P on n variables and Δn clauses. Let $\eta \in [0, \eta_0]$ where η_0 is a universal constant, and let $\theta \coloneqq 8\eta + O\left(\sqrt{\frac{\log^5 n}{\Delta}}\right)$. There is an algorithm that certifies with high probability that the $(1-\eta)$-satisfying assignments to $\boldsymbol{\mathcal{I}}$ as a P-CSP instance are covered by at most*

$$\exp(O(\theta^2 \log(1/\theta))n)$$

diameter-(θn) clusters.

Inspecting the proof of counting 2XOR (specifically the argument about $\mathcal{I}_+$), we see that it additionally certifies that the approximate solutions form clusters. In a similar fashion, we certify that any pair of $(1-\eta)$-satisfying assignments to a random 3SAT instance must have Hamming distance close to 0 or roughly $\frac{n}{2}$, i.e. the solutions form clusters where the clusters are roughly $\frac{n}{2}$ apart. The main ingredient is an efficient algorithm to certify an important structural result of random 3-uniform hypergraphs, allowing us to reason about the constraints violated in $\mathcal{I}_+$. In fact, this ingredient will also be a crucial step in refuting CSPs under global cardinality constraints in Section 6 of the full version. The upshot is that we will be able to certify that any pair of solutions is either ρ-close or $\frac{1-\rho}{2}$-far.

The second ingredient is a result in coding theory. Since the clusters are roughly $\frac{1\pm\rho}{2}n$ apart in Hamming distance, the number of clusters must be upper bounded by the cardinality of the largest ρ-balanced binary error-correcting code. The best known upper bound is $2^{O(\rho^2 \log(1/\rho))n}$ by [49] (see also [7]), which yields our final result. Complete details are in Section 5 of the full version.

Balance. We observe that the idea of hypergraph expansion can be applied to the problem of strongly refuting random CSPs with *global cardinality constraints*. This problem was first investigated by Kothari, O'Donnell, and Schramm [43], where they proved that under the refutation threshold $n^{k/2}$, the polynomial-time regime of the Sum-of-Squares hierarchy cannot refute the instance even with the global cardinality constraint $\sum_{i=1}^n x_i = B$ for any integer $B \in [-O(\sqrt{n}), O(\sqrt{n})]$ (here we assume $x \in \{\pm 1\}^n$). On the other hand, they proved once that $|B| > n^{3/4}$, Sum-of-Squares could indeed refute a random kXOR instance up to a factor of $\sqrt{n}$ under the refutation threshold.

We say an assignment x is ρ-biased if $\frac{1}{n}\left|\sum_{i\in[n]} x_i\right| \geqslant \rho$. We give a strong refutation algorithm for random instances of all Boolean CSPs under the constraint that the solution is "unbalanced".

▶ **Theorem 15.** *Let P be any k-variable predicate and let $\boldsymbol{\mathcal{I}}$ be a random CSP instance on $m \coloneqq n^{\frac{k-1}{2}+\beta}$ clauses where $\beta > 0$. For every constant $\rho > 0$, there is an efficient algorithm that certifies that $\boldsymbol{\mathcal{I}}$ has no 2ρ-biased assignment which $(1 - O(\rho^k))$-satisfies $\boldsymbol{\mathcal{I}}$ as a P-CSP instance.*

▶ Remark 16. Compared to [43], our result is a strong refutation algorithm for all CSPs, whereas their algorithm is specific for kXOR and only a weak refutation (refuting only exactly satisfying assignments). For $k = 3$, we match their cardinality constraint requirement. However, for $k \geqslant 4$, we require a slightly stronger cardinality assumption.

The formal statements and proofs are detailed in Section 6 of the full version. Akin to the case for counting solutions, we employ the reduction of every kCSP to kSAT and the kXOR principle to reduce the problem to strongly refuting kXOR under global cardinality constraints.

The first main insight is that given a graph G which is a sufficiently good spectral expander, we can efficiently certify that any 2XOR instance on G, where the number of positive constraints is roughly equal to the number of negative constraints, has no unbalanced approximately satisfying assignments. The proof of this is based on using the expander mixing lemma to show that any imbalanced assignment x must satisfy $x_u x_v = +1$ for $\gg \frac{1}{2}$ of the edges, which then lets us lower bound the number of negative constraints that are violated.

Then given a random kXOR instance $\boldsymbol{\mathcal{I}}$, we pick some set of ρn vertices S and consider all clauses with exactly $k-2$ vertices in S and 2 variables outside S. If we place an edge between the two variables outside S for every clause, we get some random graph $\boldsymbol{G}$. Now consider any assignment y to the variables in S. For this chosen set of clauses to be (nearly) satisfied, the assignment to variables outside S must nearly satisfy the induced 2XOR instance on the graph $\boldsymbol{G}$ whose signings are determined by y. The second insight is that we can efficiently certify that for any assignment y the induced 2XOR instance has a roughly equal number of positive and negative constraints. This is possible since the quantity $\#\text{positive constraints}(y) - \#\text{negative constraints}(y)$ is the objective value of a particular random $(k-2)$XOR instance on assignment y, which we can certify tight bounds on using the algorithm of [5].

Certified counting for subspace problems. So far, we have developed certification algorithms for CSPs mainly based on analyses of random hypergraphs. For other inherently different problems such as counting solutions to the SK model, we turn to a different technique. Our main insight is that for several problems, the approximate solutions must lie close to a small-dimensional linear subspace. Thus, we can reduce the problem to counting the number of (Boolean) vectors close to a subspace. We name this technique *dimension-based count certification* since the algorithms and their guarantees only depend on the dimension of the subspace.

▶ **Theorem 17.** *Let V be a linear subspace of dimension αn in $\mathbb{R}^n$. For any $\varepsilon \in (0, 1/4)$, the number of Boolean vectors in $\left\{\pm\frac{1}{\sqrt{n}}\right\}^n$ that are ε away from V is upper bounded by $2^{(H_2(4\varepsilon^2)+\alpha\log\frac{3}{\varepsilon})n}$.*

We note that the upper bound is almost tight.

We now give a brief overview of the proof of Theorem 17. First, we upper bound the maximum number of (normalized) Boolean vectors that can lie within any ε'-ball. Secondly, we take an ε-net of the unit ball in the subspace V (i.e. $B_1(0) \cap V$). We simply multiply the two quantities to get the upper bound, which only depends on the dimension of V.

Next, we apply this technique to two problems: the Sherrington-Kirkpatrick model and the independent sets in random d-regular graphs.

Sherrington-Kirkpatrick (SK). Given $\boldsymbol{M}$ sampled from $\mathsf{GOE}(n)$, the SK problem is to compute

$$\mathsf{OPT}(\boldsymbol{M}) = \max_{x \in \{\pm 1\}^n} x^\top \boldsymbol{M} x.$$

This problem can also be interpreted as finding the largest cut in a Gaussian-weighted graph. The SK model arises from the spin-glass model studied in statistical physics [71]. Talagrand [73] famously proved that $\mathsf{OPT}(\boldsymbol{M})$ concentrates around $2\mathsf{P}^* n^{3/2} \approx 1.526 n^{3/2}$, where P^* is the *Parisi constant*, first predicted by Parisi [61, 62].

Recently, the problem of certifying an upper bound for $\mathsf{OPT}(\boldsymbol{M})$ has received wide attention. A natural algorithm is the *spectral refutation*: $\mathsf{OPT}(\boldsymbol{M}) \leqslant n \cdot \lambda_{\max}(\boldsymbol{M})$. Since $\lambda_{\max}(\boldsymbol{M})$ concentrates around $2\sqrt{n}$, the algorithm certifies that $\mathsf{OPT}(\boldsymbol{M}) \leqslant (2 + o(1))n^{3/2}$, which we call the *spectral bound*. Clearly, there is a gap between the spectral bound and the true value, and it is natural to ask whether there is an algorithm that beats the spectral bound. Surprisingly, building on works by [58, 54, 46], Ghosh et. al. [31] showed that even the powerful Sum-of-Squares hierarchy cannot certify a bound better than $(2 - o(1))n^{3/2}$ in subexponential time. We also mention an intriguing work by Montanari [56] where he gave an efficient algorithm for the *search problem* – to find a solution with objective value close to $\mathsf{OPT}(\boldsymbol{M})$ with high probability (assuming a widely-believed conjecture from statistical physics). However, we emphasize that his algorithm is not a certification algorithm (recall Definition 4).

In the spirit of this work, a natural question is to certify an upper bound on the number of assignments $x \in \{\pm 1\}^n$ such that $x^\top \boldsymbol{M} x \geqslant 2(1-\eta)n^{3/2}$ for some $\eta > 0$.

▶ **Theorem 18.** *Let $\boldsymbol{M} \sim \mathsf{GOE}(n)$. Given $\eta \in (0, \eta_0)$ for some universal constant η_0, there is an algorithm certifying that at most $2^{O(\eta^{3/5} \log \frac{1}{\eta})n}$ assignments $x \in \{\pm 1\}^n$ satisfy $x^\top \boldsymbol{M} x \geqslant 2(1-\eta)n^{3/2}$.*

Our proof first looks at the eigenvalue distribution of $\boldsymbol{M}$, which follows the *semicircle law*. This shows that any x that achieves close to the spectral bound must be close to the top eigenspace of $\boldsymbol{M}$ (of dimension determined by the semicircle law). Then, we directly apply Theorem 17. See Section 7.1 of the full version for complete details.

Independent sets in d-regular graphs. The largest independent set size (the *independence number*) in a random d-regular graph has been studied extensively. It is well-known that with high probability, the independence number is $\leqslant \frac{2n \log d}{d}$ for a sufficiently large constant d (cf. [12, 76]). The current best known *certifiable* upper bound is via the smallest eigenvalue of the adjacency matrix (often referred to as Hoffman's bound, cf. [26, 13]): Let $\boldsymbol{A}$ be the adjacency matrix, and let $\lambda \coloneqq -\lambda_{\min}(\boldsymbol{A})$. Then, $|S| \leqslant \frac{\lambda}{d+\lambda} n$ for all independent sets S.

It is also well-established that $\lambda \leqslant 2\sqrt{d-1} + o(1)$ with high probability. Thus, we can certify that the independence number is at most $C_d n$ where $C_d \coloneqq \frac{2\sqrt{d-1}}{d+2\sqrt{d-1}}$.

The natural question for us is to certify an upper bound on the number of independent sets larger than $C_d(1-\eta)n$ for some $\eta > 0$.

▶ **Theorem 19.** *For a random d-regular graph on n vertices, given $\eta \in (0, \eta_0)$ for some universal constant η_0, there is an algorithm certifying that there are at most $2^{O(\eta^{3/5} \log \frac{1}{\eta})n}$ independent sets of size $C_d(1-\eta)n$.*

The proof is very similar to the SK model. We first map each independent set S to a vector $y_S \in \mathbb{R}^n$ such that if S is large, then y_S is close to the bottom eigenspace of $\boldsymbol{A}$. Then, using a variant of Theorem 17, we upper bound the number of such vectors that are close to the eigenspace. We carry out the proof in full detail in Section 7.2 of the full version.

Optimality for counting kCSP solutions. Finally, we give evidence suggesting that our algorithmic upper bounds are close to optimal. Our hardness results are built on the hypothesis that there is no efficient *strong* refutation algorithm for random kXOR under the refutation threshold (in the regime $n^{\varepsilon} \ll \Delta \ll n^{k/2-1}$). Although no NP-hardness results are known, this hypothesis is widely believed to be true. In particular, the problem was shown to be hard for the Sum-of-Squares semidefinite programming hierarchy [34, 70, 44], which is known to capture most algorithmic techniques for average-case problems. Thus, improving our results would imply a significant breakthrough.

We show that assuming this hypothesis is true, then we cannot certify an upper bound on the number of $(1-\eta)$-satisfying assignments better than $\exp(O(\eta n))$.

▶ **Theorem 20.** *If there is an efficient algorithm that with high probability can certify a bound of $\exp(\frac{\eta n}{10k})$ on the number of $(1-\eta)$-satisfying assignments to $\boldsymbol{\mathcal{I}}$, then there is an efficient algorithm that with high probability can certify that $\boldsymbol{\mathcal{I}}$ has no $(1-\eta/2)$-satisfying assignments.*

This shows that the term $\exp(O(\eta \log \frac{1}{\eta})n)$ in Theorem 8 and Theorem 11 is tight up to log factors. Our proof is simple: given a $(1-\eta/2)$-satisfying assignment and a small set S, we can flip the assignments to S arbitrarily and still be $(1-\eta)$-satisfying. Hence the number of $(1-\eta)$-satisfying assignments is at least $2^{|S|}$. Thus, an upper bound better than this would imply that there is no $(1-\eta/2)$-satisfying assignments. See Section 8.1 of the full version for complete details.

Surprisingly, the optimality of Theorem 8 suggests that there is a phase transition for certifiable counting at the refutation threshold. For concreteness, take random kSAT for example,

▶ Remark 21. At $m = \widetilde{\Omega}(n^{k/2})$, there is a strong refutation algorithm [5] which certifies that no $(1-\eta)$-satisfying assignment exists (even for constant $\eta < 1/2$). However, at $m = n^{k/2-\varepsilon}$ and take $\eta = n^{-\frac{1}{4}+\frac{\varepsilon}{2}}$, we can at best certify that the number of $(1-\eta)$-satisfying assignments is at most $\exp(O(n^{\frac{3}{4}+\frac{\varepsilon}{2}}))$. See also Figure 1 for illustration.

Optimality for counting independent sets. We also show barriers to improving Theorem 19, which can be viewed as a weak hardness evidence. Specifically, we show that improving the upper bound of Theorem 19 to $\exp(O(\eta \log(1/\eta)n))$ would imply beating Hoffman's bound by a factor of $1-\eta/2$ (for any small constant η), which would be an interesting algorithmic breakthrough.

▶ **Theorem 22.** *Let $\boldsymbol{G}$ be a random d-regular graph. Given constant $\eta \in (0, 1/2)$, if there is an efficient algorithm that with high probability certifies a bound of* $\exp\left(\frac{C_d}{4}\eta \log(1/\eta)n\right)$ *on the number of independent sets of size $C_d(1-\eta)n$, then there is an algorithm that with high probability certifies that $\boldsymbol{G}$ has no independent set of size $(1-\eta/2)C_d n$.*

The proof is a simple observation that for any independent set S, all subsets of S are also independent sets. Thus, if S is of size $(1-\eta/2)C_d n$, then we can lower bound the number of subsets of size $(1-\eta)C_d n$. We give a short proof in Section 8.2 of the full version. We note the interesting gap between $\eta^{3/5}$ and η in the exponent of the upper and lower bounds respectively, and we conjecture that there may be an algorithm matching the lower bound.

1.2 Context and related work

Information-computation gaps in CSPs. This work is very closely related to the line of work on information-computation gaps. In the context of certification in random CSPs, the most well-understood information-gaps are in that of refutation of random CSPs. Feige's random 3SAT hypothesis was one of the earliest conjectured gaps. As discussed earlier, while unsatisfiability for random 3SAT set in at constant density, it was conjectured by Feige that certifying this was hard at all constant densities. Further, integrality gaps for the Sum-of-Squares hierarchy of [34, 70] seem to point to hardness up to density $\sqrt{n}$. The wide information-computation gap is a main motivation for us to understand what an efficient algorithm can certify about the landscape of solutions in the regime between the satisfiability threshold and the refutation threshold. We refer the reader to the introduction of [5] for a comprehensive treatment of the literature on information-computation gaps for refuting random CSPs prior to their work, CSPs more broadly, as well as connections to other areas of theoretical computer science.

The situation for general constraint satisfaction problems beyond XOR and SAT was considered in the work of [5], which gave algorithms to refute all CSPs at density $n^{t/2-1}$ where t is the smallest integer such that there is no t-wise uniform distribution supported on the predicate's satisfying assignments. Then somewhat surprisingly, the work of [66] gave algorithms for refuting random CSPs between constant density and the $n^{t/2-1}$ threshold from [5], whose running time smoothly interpolated between exponential time at constant density to polynomial time at the [5] threshold, with a (steadily improving) subexponential running time in the intermediate regime. The algorithms of [5, 66] are spectral, and can be captured within the Sum-of-Squares hierarchy. Finally the work of [44] (presaged by [9]) established that the algorithm of [66] was tight for Sum-of-Squares in all regimes, thereby nailing a characterization for the exact gaps (up to logarithmic factors) for all random CSPs.

Solution geometry in random CSPs. One of the earlier predictions using nonrigorous physics techniques was the location of the 3SAT satisfiability threshold in the works of [53, 52]. In particular, they conjectured that there is a sharp threshold at a constant $\alpha_{\mathrm{SAT}} \approx 4.267$. These works put forth the "1-step replica symmetry breaking hypothesis" (a conjectured property of the solution space in random kSAT; we refer the reader to the introduction of [22] for a description), which was the starting point for several subsequent works. These techniques were used to precisely predict the kSAT satisfiability threshold for all values of k [50], proved for large k in a line of work culminating in [22] and building on [2, 3, 18, 19].

Eventually, the works of [45, 57] predicted that besides the satisfiability threshold, random kSAT goes through other phase transitions too, and gave conjectures for their locations. A notable one connected to this work is the *clustering threshold*, for which there has been

rigorous evidence given in the works of [51, 4, 1]. Above the clustering threshold, the solution space is predicted to break into exponentially many exponential-sized clusters far away from each other in Hamming distance. More precisely, there is some function Σ for which there are $\exp(\Sigma(s,\Delta)n)$ clusters of size approximately $\exp(sn)$ each. In particular, this leads to the prediction that the number of solutions at density Δ is roughly $\max_s\{\exp((s+\Sigma(s,\Delta))n)\}$. Another phase transition of interest is the *condensation threshold*, where the number of clusters of solutions drops to a constant.

Approximate Counting for CSPs. Approximate counting of solutions in CSPs has attracted much attention in recent years. There have been numerous positive algorithmic results for approximately counting solutions in (i) sparse CSPs in the worst case, (ii) sparse random CSPs well under the satisfiability threshold. The takeaway here is that even though the problems we consider get harder as we approach the satisfiability threshold, if one goes well under the threshold the algorithmic problems once again become tractable.

One exciting line of research for worst-case CSPs is the problem of approximately counting satisfying assignments of a $k\mathsf{SAT}$ formula under conditions similar to those of the Lovász Local Lemma (LLL) [24]. A direct application of the LLL shows that if the maximum degree D of the *dependency graph* is $\leqslant 2^k/e$, then the formula is satisfiable. Building on works of [55, 28, 29, 38], Jain, Pham, and Vuong [39] recently showed that there is an algorithm for approximate counting well under the LLL thresholds, i.e. when $D \lesssim 2^{k/5.741}$ (hiding factors polynomial in k), using techniques similar to an algorithmic version of the LLL. Further, the algorithms of [55, 38] are deterministic, which may suggest their techniques are amenable to obtaining certifiable counts. However, it was shown that the problem of approximately counting solutions to a $k\mathsf{SAT}$ formula is NP-hard when $D \gtrsim 2^{k/2}$ by [11], well in the sparse regime, which suggests a hard phase between the highly sparse setting and the dense setting we are concerned with.

For random $k\mathsf{SAT}$, the exact satisfiability threshold that was established by Ding, Sly, and Sun [22] takes on value $\alpha_{\mathrm{SAT}} = 2^k \ln 2 - \frac{1}{2}(1+\ln 2) + o_k(1)$. And similarly, well below the satisfiability threshold, Galanis, Goldberg, Guo, and Yang [30] adapted Moitra's techniques [55] to the random setting and developed a polynomial-time algorithm when the density $\Delta \leqslant 2^{k/301}$ and k sufficiently large.

Closely related to the counting problem is approximating the partition function of random $k\mathsf{SAT}$, for which there have also been positive algorithmic results. Specifically, given a random $k\mathsf{SAT}$ instance $\boldsymbol{\mathcal{I}}$, the partition function is defined as $Z(\boldsymbol{\mathcal{I}},\beta) \coloneqq \sum_\sigma e^{-\beta H(\sigma)}$, where $H(\sigma)$ is the number of unsatisfied clauses under assignment σ. The partition function can be viewed as a weighted (or "permissive") version of the counting problem. Montanari and Shah [59] first showed that the Belief Propagation algorithm approximately computes the partition function at $\Delta \sim \frac{2\log k}{k}$; their analysis is based on correlation decay (or the *Gibbs uniqueness property*). Recently, [17] further showed that Belief Propagation succeeds as long as the random $k\mathsf{SAT}$ model satisfies a *replica symmetry* condition, conjectured to hold up to $\Delta \sim 2^k \ln k/k$. See also the works of [45, 60, 15] for further details of this matter.

Counting independent sets and related problems. Another counting problem that has been the subject of active study is that of counting independent sets, especially in the statistical physics community. For a graph G with maximum degree d, let $\mathsf{IS}(G)$ be the set of independent sets in G. The task is to estimate the *independence polynomial* $Z_G(\lambda) = \sum_{I\in\mathsf{IS}(G)} \lambda^{|I|}$, also known as the partition function of the *hard-core model* with *fugacity* λ in the physics literature. Earlier works by [23, 74] developed randomized algorithms based on *Glauber dynamics* to

estimate $Z_G(\lambda)$ when $\lambda \leqslant \frac{2}{d-2}$. In a major breakthrough, Weitz [75] showed a deterministic algorithm, based on correlation decay, that approximates $Z_G(\lambda)$ when $0 \leqslant \lambda < \lambda_c$, where $\lambda_c := \frac{(d-1)^{d-1}}{(d-2)^d}$. Sly and Sun [72] later proved that this is tight: no efficient approximate algorithm for $Z_G(\lambda)$ exists for $\lambda > \lambda_c$ unless $\mathsf{NP} = \mathsf{RP}$.

Recently, Barvinok initiated a line of research on estimating partition functions using the *interpolation method* (see Barvinok's recent book [10]). The main idea is to estimate the low-order Taylor approximation of $\log Z_G(\lambda)$ provided that the polynomial $Z_G(\lambda)$ does not vanish in some region in $\mathbb{C}$. This approach led to deterministic algorithms that match Weitz's result and work even for negative or complex λ's [63, 64]. These polynomial-based approaches were also used to obtain deterministic algorithms for counting colorings in bounded degree graphs [47], estimating the Ising model partition function [48], and algorithms for a counting version of the Unique Games problem [20].

There has also been works on worst-case upper bounds of $Z_G(\lambda)$ for d-regular graphs. Zhao proved that for any d-regular graph G and any $\lambda \geqslant 0$, $Z_G(\lambda) \leqslant (2(1+\lambda)^d - 1)^{n/2d}$ [77]. In particular, setting $\lambda = 1$, this shows that the total number of independent sets is bounded by $(2^{d+1} - 1)^{n/2d}$, settling a conjecture by Alon [6] and Kahn [40].

Certifying bounds on partition functions and free energy. A recent line of work [67, 68, 37] is focused on an approach based on a convex programming relaxation of entropy to certify upper bounds on the *free energy* of the Ising model (weighted 2XOR), both in the worst case and in the average case. While on the surface level, these approaches differ significantly from ours, an interesting direction is to investigate if these entropy-based convex programming relaxations can achieve our algorithmic results.

1.3 Open directions

In this section we suggest a couple of avenues for further investigation on the themes related to this work.

Worst-case complexity of certified counting. In this work, we deal mostly with random CSPs. Here we present a worst-case version of the problem, specialized to 3SAT. A classic result due to [35] is that it is NP-hard to distinguish between a $(7/8+\varepsilon)$-satisfiable 3SAT formula from a fully satisfiable 3SAT formula. However, it is unclear what the complexity of a version of this question is when there is a stronger promise on the satisfiable 3SAT formula.

▶ **Question 23.** Consider the following algorithmic task:

> Given a 3SAT formula $\mathcal{I}$ under the promise that it is either $(7/8+\varepsilon)$-satisfiable, or has at least T fully satisfying assignments, decide which of the two categories $\mathcal{I}$ falls into.

What is the complexity of the above problem?

We remark that this problem is similar to counting-3SAT, but subtly different.

Certifying optimal bounds on number of exactly satisfying kSAT solutions. In the context of kSAT, while our algorithms can certify subexponential bounds for both exactly satisfying assignments and approximately satisfying assignments, the matching evidence of hardness is only for the approximate version of the problem. Thus, it is still possible that there is an algorithm to certify an even tighter bound than ours for the problem of counting exactly satisfying assignments to a random kSAT formula. This motivates the following question:

▶ **Question 24.** What is the tightest bound an efficient algorithm can certify on the number of solutions to a random kSAT instance?

We conjecture that the algorithms presented in this paper are indeed optimal. An approach to providing hardness evidence for this is to construct a hard planted distribution, and prove it is hard within the *low-degree likelihood ratio* framework of [36]. We outline a possible approach in Section 8.3 of the full version to construct a planted distribution for readers interested in this problem.

Properties of arbitrary CSP instances on random hypergraphs. In the context of approximate kXOR, our certification algorithms for solution counts and cluster counts depend only on the hypergraph structure and not the random negations. Hence, they also prove nontrivial statements about the solution space of any XOR instance on a random hypergraph, which are potentially useful in the context of quiet planting or semi-random models of CSPs. However, our certification algorithms for other CSPs, such as kSAT, heavily make use of the random signings in the reduction to kXOR.

▶ **Question 25.** Can all the results related to certifying bounds on number of solutions/ clusters in this work for random kSAT instances be generalized to arbitrary kSAT instances on random hypergraphs?

References

1 Dimitris Achlioptas and Amin Coja-Oghlan. Algorithmic barriers from phase transitions. In *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 793–802. IEEE, 2008.

2 Dimitris Achlioptas and Cristopher Moore. The asymptotic order of the random k-SAT threshold. In *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.*, pages 779–788. IEEE, 2002.

3 Dimitris Achlioptas and Yuval Peres. The threshold for random k-sat is $2^k(\ln 2 - o(k))$. In *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, pages 223–231, 2003.

4 Dimitris Achlioptas and Federico Ricci-Tersenghi. On the solution-space geometry of random constraint satisfaction problems. In *Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, pages 130–139, 2006.

5 Sarah R Allen, Ryan O'Donnell, and David Witmer. How to refute a random CSP. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, pages 689–708. IEEE, 2015.

6 Noga Alon. Independent sets in regular graphs and sum-free subsets of finite groups. *Israel journal of mathematics*, 73(2):247–256, 1991.

7 Noga Alon. Perturbed identity matrices have high rank: Proof and applications. *Combinatorics, Probability & Computing*, 18(1-2):3, 2009.

8 Benny Applebaum, Boaz Barak, and Avi Wigderson. Public-key cryptography from different assumptions. In *Proceedings of the forty-second ACM symposium on Theory of computing*, pages 171–180, 2010.

9 Boaz Barak, Siu On Chan, and Pravesh K Kothari. Sum of squares lower bounds from pairwise independence. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 97–106, 2015.

10 Alexander Barvinok. *Combinatorics and complexity of partition functions*, volume 9. Springer, 2016.

11 Ivona Bezáková, Andreas Galanis, Leslie Ann Goldberg, Heng Guo, and Daniel Stefankovic. Approximation via correlation decay when strong spatial mixing fails. *SIAM Journal on Computing*, 48(2):279–349, 2019.

12 Béla Bollobás. The independence ratio of regular graphs. *Proceedings of the American Mathematical Society*, pages 433–436, 1981.

13 Andries E Brouwer and Willem H Haemers. *Spectra of graphs*. Springer Science & Business Media, 2011.

14 Andrei Bulatov, Peter Jeavons, and Andrei Krokhin. Classifying the complexity of constraints using finite algebras. *SIAM journal on computing*, 34(3):720–742, 2005.

15 Amin Coja-Oghlan. Belief propagation guided decimation fails on random formulas. *Journal of the ACM (JACM)*, 63(6):1–55, 2017.

16 Amin Coja-Oghlan, Andreas Goerdt, and André Lanka. Strong refutation heuristics for random k-SAT. *Combinatorics, Probability & Computing*, 16(1):5, 2007.

17 Amin Coja-Oghlan, Noëla Müller, and Jean B Ravelomanana. Belief Propagation on the random k-SAT model. *arXiv preprint*, 2020. `arXiv:2011.02303`.

18 Amin Coja-Oghlan and Konstantinos Panagiotou. Going after the k-SAT threshold. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 705–714, 2013.

19 Amin Coja-Oghlan and Konstantinos Panagiotou. The asymptotic k-SAT threshold. *Advances in Mathematics*, 288:985–1068, 2016.

20 Matthew Coulson, Ewan Davies, Alexandra Kolla, Viresh Patel, and Guus Regts. Statistical physics approaches to Unique Games. *arXiv preprint arXiv:1911.01504*, 2019.

21 Amit Daniely, Nati Linial, and Shai Shalev-Shwartz. From average case complexity to improper learning complexity. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 441–448, 2014.

22 Jian Ding, Allan Sly, and Nike Sun. Proof of the satisfiability conjecture for large k. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 59–68, 2015.

23 Martin Dyer and Catherine Greenhill. On Markov chains for independent sets. *Journal of Algorithms*, 35(1):17–49, 2000.

24 Paul Erdős and László Lovász. Problems and results on 3-chromatic hypergraphs and some related questions. In *Colloquia Mathematica Societatis Janos Bolyai 10. Infinite and Finite Sets, Keszthely (Hungary)*. Citeseer, 1973.

25 Uriel Feige. Relations between average case complexity and approximation complexity. In *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*, pages 534–543, 2002.

26 Uriel Feige and Eran Ofek. Spectral techniques applied to sparse random graphs. *Random Structures & Algorithms*, 27(2):251–275, 2005.

27 Uriel Feige and Eran Ofek. Easily refutable subformulas of large random 3CNF formulas. *Theory of Computing*, 3(1):25–43, 2007.

28 Weiming Feng, Heng Guo, Yitong Yin, and Chihao Zhang. Fast sampling and counting k-SAT solutions in the local lemma regime. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 854–867, 2020.

29 Weiming Feng, Kun He, and Yitong Yin. Sampling Constraint Satisfaction Solutions in the Local Lemma Regime. *arXiv preprint*, 2020. `arXiv:2011.03915`.

30 Andreas Galanis, Leslie Ann Goldberg, Heng Guo, and Kuan Yang. Counting solutions to random CNF formulas. *arXiv preprint*, 2019. `arXiv:1911.07020`.

31 Mrinalkanti Ghosh, Fernando Granha Jeronimo, Chris Jones, Aaron Potechin, and Goutham Rajendran. Sum-of-squares lower bounds for Sherrington-Kirkpatrick via planted affine planes. *arXiv preprint*, 2020. `arXiv:2009.01874`.

32 Andreas Goerdt and André Lanka. Recognizing more random unsatisfiable 3-SAT instances efficiently. *Electronic Notes in Discrete Mathematics*, 16:21–46, 2003.

33 Oded Goldreich. Candidate one-way functions based on expander graphs. In *Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation*, pages 76–87. Springer, 2011.

34 Dima Grigoriev. Complexity of Positivstellensatz proofs for the knapsack. *computational complexity*, 10(2):139–154, 2001.

35 Johan Håstad. Some optimal inapproximability results. *Journal of the ACM (JACM)*, 48(4):798–859, 2001.

36 Samuel B Hopkins and David Steurer. Efficient Bayesian estimation from few samples: community detection and related problems. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 379–390. IEEE, 2017.

37 Vishesh Jain, Frederic Koehler, and Andrej Risteski. Mean-field approximation, convex hierarchies, and the optimality of correlation rounding: a unified perspective. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 1226–1236, 2019.

38 Vishesh Jain, Huy Tuan Pham, and Thuy Duong Vuong. Towards the sampling Lovász Local Lemma. *arXiv preprint*, 2020. `arXiv:2011.12196`.

39 Vishesh Jain, Huy Tuan Pham, and Thuy-Duong Vuong. On the sampling Lovász Local Lemma for atomic constraint satisfaction problems. *arXiv preprint*, 2021. `arXiv:2102.08342`.

40 Jeff Kahn. An entropy approach to the hard-core model on bipartite graphs. *Combinatorics, Probability & Computing*, 10(3):219, 2001.

41 Subhash Khot. On the power of unique 2-prover 1-round games. In *Proceedings of the thiry-fourth annual ACM symposium on Theory of computing*, pages 767–775, 2002.

42 Subhash Khot, Guy Kindler, Elchanan Mossel, and Ryan O'Donnell. Optimal inapproximability results for MAX-CUT and other 2-variable CSPs? *SIAM Journal on Computing*, 37(1):319–357, 2007.

43 Pravesh Kothari, Ryan O'Donnell, and Tselil Schramm. SOS lower bounds with hard constraints: think global, act local. *arXiv preprint*, 2018. `arXiv:1809.01207`.

44 Pravesh K Kothari, Ryuhei Mori, Ryan O'Donnell, and David Witmer. Sum of squares lower bounds for refuting any CSP. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 132–145, 2017.

45 Florent Krzakała, Andrea Montanari, Federico Ricci-Tersenghi, Guilhem Semerjian, and Lenka Zdeborová. Gibbs states and the set of solutions of random constraint satisfaction problems. *Proceedings of the National Academy of Sciences*, 104(25):10318–10323, 2007.

46 Dmitriy Kunisky and Afonso S Bandeira. A tight degree 4 sum-of-squares lower bound for the Sherrington–Kirkpatrick Hamiltonian. *Mathematical Programming*, pages 1–39, 2020.

47 Jingcheng Liu, Alistair Sinclair, and Piyush Srivastava. A deterministic algorithm for counting colorings with 2Δ colors. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1380–1404. IEEE, 2019.

48 Jingcheng Liu, Alistair Sinclair, and Piyush Srivastava. The Ising partition function: Zeros and deterministic approximation. *Journal of Statistical Physics*, 174(2):287–315, 2019.

49 Robert McEliece, Eugene Rodemich, Howard Rumsey, and Lloyd 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.

50 Stephan Mertens, Marc Mézard, and Riccardo Zecchina. Threshold values of random k-sat from the cavity method. *Random Structures & Algorithms*, 28(3):340–373, 2006.

51 Marc Mézard, Thierry Mora, and Riccardo Zecchina. Clustering of solutions in the random satisfiability problem. *Physical Review Letters*, 94(19):197205, 2005.

52 Marc Mézard, Giorgio Parisi, and Riccardo Zecchina. Analytic and algorithmic solution of random satisfiability problems. *Science*, 297(5582):812–815, 2002.

53 Marc Mézard and Riccardo Zecchina. Random k-satisfiability problem: From an analytic solution to an efficient algorithm. *Physical Review E*, 66(5):056126, 2002.

54 Sidhanth Mohanty, Prasad Raghavendra, and Jeff Xu. Lifting sum-of-squares lower bounds: degree-2 to degree-4. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 840–853, 2020.

55 Ankur Moitra. Approximate counting, the Lovász local lemma, and inference in graphical models. *Journal of the ACM (JACM)*, 66(2):1–25, 2019.

56 Andrea Montanari. Optimization of the sherrington-kirkpatrick hamiltonian. In *Proceedings of the 60th IEEE Symposium on Foundations of Computer Science*, pages 1417–1433, 2019.

57 Andrea Montanari, Federico Ricci-Tersenghi, and Guilhem Semerjian. Clusters of solutions and replica symmetry breaking in random k-satisfiability. *Journal of Statistical Mechanics: Theory and Experiment*, 2008(04):P04004, 2008.

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

59 Andrea Montanari and Devavrat Shah. Counting good truth assignments of random k-SAT formulae. *arXiv preprint*, 2006. `arXiv:cs/0607073`.

60 Dmitry Panchenko. Spin glass models from the point of view of spin distributions. *Annals of Probability*, 41(3A):1315–1361, 2013.

61 Giorgio Parisi. Infinite number of order parameters for spin-glasses. *Physical Review Letters*, 43(23):1754, 1979.

62 Giorgio Parisi. A sequence of approximated solutions to the SK model for spin glasses. *Journal of Physics A: Mathematical and General*, 13(4):L115, 1980.

63 Viresh Patel and Guus Regts. Deterministic polynomial-time approximation algorithms for partition functions and graph polynomials. *SIAM Journal on Computing*, 46(6):1893–1919, 2017.

64 Han Peters and Guus Regts. On a conjecture of Sokal concerning roots of the independence polynomial. *The Michigan Mathematical Journal*, 68(1):33–55, 2019.

65 Prasad Raghavendra. Optimal algorithms and inapproximability results for every CSP? In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 245–254, 2008.

66 Prasad Raghavendra, Satish Rao, and Tselil Schramm. Strongly refuting random CSPs below the spectral threshold. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 121–131, 2017.

67 Andrej Risteski. How to calculate partition functions using convex programming hierarchies: provable bounds for variational methods. In *Conference on Learning Theory*, pages 1402–1416. PMLR, 2016.

68 Andrej Risteski and Yuanzhi Li. Approximate maximum entropy principles via goemans-williamson with applications to provable variational methods. *Advances in Neural Information Processing Systems*, 29:4628–4636, 2016.

69 Thomas J Schaefer. The complexity of satisfiability problems. In *Proceedings of the tenth annual ACM symposium on Theory of computing*, pages 216–226, 1978.

70 Grant Schoenebeck. Linear level Lasserre lower bounds for certain k-CSPs. In *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 593–602. IEEE, 2008.

71 David Sherrington and Scott Kirkpatrick. Solvable model of a spin-glass. *Physical review letters*, 35(26):1792, 1975.

72 Allan Sly and Nike Sun. The computational hardness of counting in two-spin models on d-regular graphs. In *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 361–369. IEEE, 2012.

73 Michel Talagrand. The Parisi formula. *Annals of mathematics*, pages 221–263, 2006.

74 Eric Vigoda. A note on the Glauber dynamics for sampling independent sets. *the electronic journal of combinatorics*, 8(1):R8, 2001.

75 Dror Weitz. Counting independent sets up to the tree threshold. In *Proceedings of the thirty-eighth annual ACM symposium on Theory of computing*, pages 140–149, 2006.

76 Nicholas C Wormald. Models of random regular graphs. *London Mathematical Society Lecture Note Series*, pages 239–298, 1999.

77 Yufei Zhao. The number of independent sets in a regular graph. *Combinatorics, Probability and Computing*, 19(2):315–320, 2010.

78 Dmitriy Zhuk. A Proof of the CSP Dichotomy Conjecture. *Journal of the ACM (JACM)*, 67(5):1–78, 2020.