SIAM J. COMPUT.
Vol. 36, No. 3, pp. 740–762

© 2006 Society for Industrial and Applied Mathematics

RANDOM k-SAT: TWO MOMENTS SUFFICE TO CROSS A SHARP THRESHOLD*

DIMITRIS ACHLIOPTAS[†] AND CRISTOPHER MOORE[‡]

Abstract. Many NP-complete constraint satisfaction problems appear to undergo a "phase transition" from solubility to insolubility when the constraint density passes through a critical threshold. In all such cases it is easy to derive upper bounds on the location of the threshold by showing that above a certain density the first moment (expectation) of the number of solutions tends to zero. We show that in the case of certain symmetric constraints, considering the second moment of the number of solutions yields nearly matching lower bounds for the location of the threshold. Specifically, we prove that the threshold for both random hypergraph 2-colorability (Property B) and random Not-All-Equal k-SAT is $2^{k-1}\ln 2 - O(1)$. As a corollary, we establish that the threshold for random k-SAT is of order $\Theta(2^k)$, resolving a long-standing open problem.

Key words. satisfiability, random formulas, phase transitions

AMS subject classifications. Primary, 68R99, 82B26; Secondary, 05C80

DOI. 10.1137/S0097539703434231

1. Introduction.

In the early 1900s, Bernstein [15] asked the following question: Given a collection of subsets of a set V, is there a partition of V into V_1, V_2 such that no subset is contained in either V_1 or V_2? If we think of the elements of V as vertices and of each subset as a hyperedge, the question can be rephrased as whether a given hypergraph can be 2-colored so that no hyperedge is monochromatic. Of particular interest is the setting where all hyperedges contain k vertices, i.e., k-uniform hypergraphs. This question was popularized by Erdős—who dubbed it "Property B" in honor of Bernstein—and has motivated some of the deepest advances in probabilistic combinatorics. Indeed, determining the smallest number of hyperedges in a non–2-colorable k-uniform hypergraph remains one of the most important problems in extremal graph theory, perhaps second only to the Ramsey problem [13].

A more modern problem, with a somewhat similar flavor, is Boolean Satisfiability: Given a Conjunctive Normal Form (CNF) formula F, is it possible to assign truth values to the variables of F so that it evaluates to true? Satisfiability has been the central problem of computational complexity since Cook [22] proved that it is complete for the class NP. The case where all clauses have the same size k is known as k-SAT and is NP-complete for all $k \geq 3$.

Random formulas and random hypergraphs have been studied extensively in probabilistic combinatorics in the last three decades. While there are a number of slightly different models for generating such structures "uniformly at random," we will see that results transfer readily between them. For the sake of concreteness, let $F_k(n,m)$ denote a formula chosen uniformly from among all $\binom{2^k\binom{n}{k}}{m}$ k-CNF formulas on n variables

[*] Received by the editors September 11, 2003; accepted for publication (in revised form) November 15, 2005; published electronically October 24, 2006.

http://www.siam.org/journals/sicomp/36-3/43423.html

[†] Department of Computer Science, University of California Santa Cruz, Santa Cruz, CA 95064 (optas@cs.ucsc.edu). This author's work was supported in part by the National Science Foundation CAREER award CCF-0546900. Part of this work was done while the author was with Microsoft Research.

[‡] Department of Computer Science, University of New Mexico, Albuquerque, NM 87131, and the Santa Fe Institute, Santa Fe, NM 87501 (moore@cs.unm.edu). This author's work was supported by the National Science Foundation under grants PHY-0200909, EIA-0218563, and CCR-0220070.

with m clauses. Similarly, let $H_k(n,m)$ denote a hypergraph chosen uniformly from among all $\binom{\binom{n}{k}}{m}$ k-uniform hypergraphs with n vertices and m hyperedges. We will say that a sequence of events $\mathcal{E}_n$ occurs *with high probability* (w.h.p.) if $\lim_{n\to\infty} \Pr[\mathcal{E}_n] = 1$ and *with uniformly positive probability* (w.u.p.p.) if $\liminf_{n\to\infty} \Pr[\mathcal{E}_n] > 0$. Throughout the paper, k will be arbitrarily large but fixed.

In recent years, random instances of both problems have been understood to undergo a "phase transition" as the ratio of constraints to variables passes through a critical threshold. That is, for a given number of vertices (variables), the probability that a random instance has a solution drops rapidly from 1 to 0 around a critical number of hyperedges (clauses). This sharp threshold phenomenon was discovered in the early 1990s, when several researchers [19, 49] performed computational experiments on $F_3(n, m = rn)$ and found that while for $r < 4.1$ almost all formulas are satisfiable, for $r > 4.3$ almost all are unsatisfiable. Moreover, as n increases, this transition narrows around $r \approx 4.2$. Along with similar results for other fixed $k \geq 3$ this has led to the following popular conjecture.

Satisfiability threshold conjecture. For each $k \geq 3$, there exists a constant r_k such that

$$\lim_{n\to\infty} \Pr[F_k(n,rn) \text{ is satisfiable}] = \begin{cases} 1 & \text{if } r < r_k, \\ 0 & \text{if } r > r_k. \end{cases}$$

In the last ten years, this conjecture has become an active area of interdisciplinary research, receiving attention in theoretical computer science, artificial intelligence, combinatorics, and, more recently, statistical physics. Much of the work on random k-SAT has focused on proving upper and lower bounds for r_k, both for the smallest computationally hard case $k = 3$ and for general k. At this point the existence of r_k has not been established for any $k \geq 3$. Nevertheless, we will take the liberty of writing $r_k \geq r^*$ to denote that for all $r < r^*$, $F_k(n,rn)$ is w.h.p. satisfiable; analogously, we will write $r_k \leq r^*$ to denote that for all $r > r^*$, $F_k(n,rn)$ is w.h.p. unsatisfiable.

As we will see, an elementary counting argument yields $r_k \leq 2^k \ln 2$ for all k. Lower bounds, on the other hand, have been exclusively algorithmic: To establish $r_k \geq r^*$ one shows that for $r < r^*$ some specific algorithm finds a satisfying assignment with probability that tends to 1. We will see that an extremely simple algorithm [20] already yields $r_k = \Omega(2^k/k)$. We will also see that while more sophisticated algorithms improve this bound slightly, to date no algorithm is known to find a satisfying truth assignment (even w.u.p.p.) when $r = \omega(k) \times 2^k/k$ for any $\omega(k) \to \infty$.

The threshold picture for hypergraph 2-colorability is completely analogous: For each $k \geq 3$, it is conjectured that there exists a constant c_k such that

$$\lim_{n\to\infty} \Pr[H_k(n,cn) \text{ is 2-colorable}] = \begin{cases} 1 & \text{if } c < c_k, \\ 0 & \text{if } c > c_k. \end{cases}$$

The same counting argument here implies $c_k < 2^{k-1} \ln 2$, while another simple algorithm yields $c_k = \Omega(2^k/k)$. Again, no algorithm is known to improve this bound asymptotically, leaving a multiplicative gap of order $\Theta(k)$ between the upper and lower bounds for this problem as well.

In this paper, we use the *second moment method* to show that random k-CNF formulas are satisfiable and random k-uniform hypergraphs are 2-colorable for density up to $2^{k-1} \ln 2 - O(1)$. Thus, we determine the threshold for random k-SAT within a factor of two and the threshold for Property B within a small additive constant.

Recall that $F_k(n, rn)$ is w.h.p. unsatisfiable if $r > 2^k \ln 2$. Our first main result is the following theorem.

THEOREM 1. *For all $k \geq 3$, $F_k(n, m = rn)$ is w.h.p. satisfiable if*

$$r \leq 2^{k-1} \ln 2 - 2.$$

Our second main result determines the Property B threshold within an additive $1/2 + o(1)$.

THEOREM 2. *For all $k \geq 3$, $H_k(n, m = cn)$ is w.h.p. non–2-colorable if*

$$c > 2^{k-1} \ln 2 - \frac{\ln 2}{2}. \tag{1}$$

There exists a sequence $t_k \to 0$ such that for all $k \geq 3$, $H_k(n, m = cn)$ is w.h.p. 2-colorable if

$$c < 2^{k-1} \ln 2 - \frac{\ln 2}{2} - \frac{1 + t_k}{2}. \tag{2}$$

The bound in (1) corresponds to the density for which the expected number of 2-colorings of $H_k(n, cn)$ is $o(1)$. Our main contribution is inequality (2), which we prove using the second moment method. In fact, our approach yields explicit lower bounds for the hypergraph 2-colorability threshold for each value of k (although these bounds lack an attractive closed form). We give the first few of these bounds in Table 1. We see that the gap between our upper and lower bounds converges to its limiting value of $1/2$ rather rapidly.

TABLE 1
Bounds for the 2-colorability threshold of random k-uniform hypergraphs.

k	3	4	5	6	7	8	9	10
Upper bound	2.410	5.191	10.741	21.833	44.014	88.376	177.099	354.545
Lower bound	1.5	4.083	9.973	21.190	43.432	87.827	176.570	354.027

Unlike the bounds for random k-SAT and hypergraph 2-colorability provided by analyzing algorithms, our arguments are nonconstructive: We establish that w.h.p. solutions exist for certain densities but do not offer any hint on how to find them. We believe that abandoning the algorithmic approach for proving such lower bounds is natural and, perhaps, necessary. At a minimum, the algorithmic approach is limited to the small set of rather naive algorithms whose analysis is tractable using current techniques. Perhaps more gravely, it could be that *no* polynomial-time algorithm can overcome the $\Theta(2^k/k)$ barrier. Determining whether this is true even for certain limited classes of algorithms, e.g., random walk algorithms, is a very interesting open problem.

In addition, by not seeking out some specific truth assignment, as algorithms do, the second moment method gives some first glimpses of the "geometry" of the set of solutions. Deciphering these first glimpses, getting clearer ones, and exploring potential interactions between the geometry of the set of solutions and computational hardness are great challenges that lie ahead.

We note that recently, and independently, Frieze and Wormald [34] applied the second moment method to random k-SAT in the case where k is a moderately growing function of n. Specifically, they proved that when $k - \log_2 n \to \infty$, $F_k(n,m)$ is w.h.p. satisfiable if $m < (1-\epsilon)m^*$ but is w.h.p. unsatisfiable if $m > (1+\epsilon)m^*$, where $m^* = (2^k \ln 2 - O(1))\, n$ and $\epsilon = \epsilon(n) > 0$ is such that $\epsilon n \to \infty$. Their result follows by a direct application of the second moment method to the number of satisfying assignments of $F_k(n,m)$. As we will see shortly, while this approach gives a very sharp bound when $k - \log_2 n \to \infty$, it fails for any fixed k and indeed for any $k = o(\log n)$.

We also note that since this work first appeared [4, 5], the line of attack we put forward has had several other successful applications. Specifically, in [7], the lower bound for the random k-SAT threshold was improved to $2^k \ln 2 - O(k)$ by building on the insights presented here. In [8], the method was successfully extended to random Max k-SAT, while in [9, 10] it was applied to random graph coloring. We discuss these subsequent developments in the conclusions.

1.1. The second moment method and the role of symmetry.

The version of the second moment method we will use is given by Lemma 1 and follows from a direct application of the Cauchy–Schwarz inequality (see Remark 3.1 in [38]).

LEMMA 1. *For any nonnegative random variable X,*

$$\Pr[X > 0] \ge \frac{\mathbf{E}[X]^2}{\mathbf{E}[X^2]}. \tag{3}$$

It is natural to try to apply Lemma 1 to random k-SAT by letting X be the number of satisfying truth assignments of $F_k(n,m)$. Unfortunately, as we will see, this "naive" application of the second moment method fails rather dramatically: For all $k \ge 1$ and every $r > 0$, $\mathbf{E}[X^2] > (1+\beta)^n\, \mathbf{E}[X]^2$ for some $\beta = \beta(k,r) > 0$. As a result, the second moment method gives only an exponentially small lower bound on the probability of satisfiability.

The key step in overcoming this failure lies in realizing that we are free to apply the second moment method to any random variable X such that $X > 0$ implies that the formula is satisfiable. In particular, we can let X be the size of any *subset* of the set of satisfying assignments. By choosing this subset carefully, we can hope to significantly reduce the variance of X relative to its expectation and use Lemma 1 to prove that the subset is frequently nonempty. Indeed, we will establish the satisfiability of random k-CNF by focusing on those satisfying truth assignments *whose complement is also satisfying.* In section 3 we will give some intuition for why the number of such assignments has much smaller variance than the number of all satisfying assignments. For now, we observe that considering only such satisfying assignments is equivalent to interpreting the random k-CNF formula $F_k(n,m)$ as an instance of Not-All-Equal (NAE) k-SAT, where a truth assignment σ is a solution if and only if under σ every clause contains at least one satisfied literal *and* at least one unsatisfied literal. In other words, our lower bound for the k-SAT threshold in Theorem 1 is, in fact, a lower bound for the NAE k-SAT threshold.

Indeed, for both random NAE k-SAT and random hypergraph 2-colorability we will apply Lemma 1 naively, i.e., by letting X be the number of solutions. This will give Theorem 2 and the values in Table 1 for hypergraph 2-colorability and, as we will see, exactly the same bounds for random NAE k-SAT. (The proof of Theorem 2 is a slight generalization of the proof for random NAE k-SAT.) We will see that this success of the naive second moment is due to the symmetry inherent in both problems, i.e., to the fact that the complement of a solution is also a solution. We feel that highlighting this role of symmetry—and showing how it can be exploited even in asymmetric problems like k-SAT—is our main conceptual contribution. Exploiting these ideas in other constraint satisfaction problems that have a permutation group acting on the variables' domain is an interesting area for further research.

1.2. Organization of the paper. In section 2 we give some background on random k-SAT and random hypergraph 2-colorability. In section 3 we explain why the second moment method fails when applied to k-SAT directly, and give some intuition for why counting only the NAE-satisfying assignments rectifies the problem. We also point out some connections to methods of statistical physics. In section 4 we lay the groundwork for bounding the second moment for both NAE k-SAT and hypergraph 2-colorability by dealing with some probabilistic preliminaries, introducing a "Laplace method" lemma for bounding certain sums, and outlining our strategy. The actual bounding occurs in sections 5 to 7. Specifically, in sections 5 and 6 we use the Laplace lemma to reduce the second moment calculations for both random NAE k-SAT and random hypergraph 2-colorability to the maximization of a certain function g on the unit interval, where g is independent of n. We maximize g in section 7 and prove the Laplace lemma in section 8. We conclude in section 9 by discussing some recent extensions of this work and proposing several open questions.

2. Related work.

2.1. Random k-SAT. The mathematical investigation of random k-SAT began with the work of Franco and Paull [31], who, among other results, observed that $F_k(n, m = rn)$ is w.h.p. unsatisfiable if $r \geq 2^k \ln 2$. To see this, let $C_k = 2^k\binom{n}{k}$ be the number of all possible k-clauses and let $S_k = (2^k - 1)\binom{n}{k}$ be the number of k-clauses consistent with a given truth assignment. Since any fixed truth assignment is satisfying with probability $\binom{S_k}{m}/\binom{C_k}{m} < (1-2^{-k})^m$, the expected number of satisfying truth assignments of $F_k(n, m = rn)$ is at most $[2(1 - 2^{-k})^r]^n = o(1)$ for $r \geq 2^k \ln 2$.

Shortly afterwards, Chao and Franco [18] complemented this result by proving that for all $k \geq 3$, if $r < 2^k/k$, then the following linear-time algorithm, called Unit Clause (uc), finds a satisfying truth assignment w.u.p.p.: If there exist unit clauses, pick one randomly and satisfy it; else pick a random unset variable and give it a random value. Note that since uc succeeds only w.u.p.p. (rather than w.h.p.) this does not imply a lower bound for r_k.

The satisfiability threshold conjecture gained a great deal of popularity in the early 1990s and has received an increasing amount of attention since then. The polynomial-time solvable case $k = 2$ was settled early on: Independently, Chvátal and Reed [20], Fernandez de la Vega [29], and Goerdt [35] proved that $r_2 = 1$. Chvátal and Reed [20], in addition to proving $r_2 = 1$, gave the first lower bound for r_k, strengthening the positive probability result of Chao and Franco [18] by analyzing the following refinement of uc, called Short Clause (sc): If there exist unit clauses, pick one randomly and satisfy it; else if there exist binary clauses, pick one randomly and satisfy a random literal in it; else pick a random unset variable and give it a random value. In [20], the authors showed that for all $k \geq 3$, sc finds a satisfying truth assignment w.h.p. for $r < (3/8)\,2^k/k$ and raised the question of whether this lower bound for r_k can be improved asymptotically.

A large portion of the work on the satisfiability threshold conjecture since then has been devoted to the first computationally hard case, $k = 3$, and a long series of results [16, 17, 33, 1, 11, 36, 41, 25, 42, 39, 24, 44, 40, 26, 31] has narrowed the potential range of r_3. Currently this is pinned between 3.52 by Kaporis, Kirousis, and Lalas [41] and Hajiaghayi and Sorkin [36] and 4.506 by Dubois, Boufkhad, and Mandler [25]. Upper bounds for r_3 come from probabilistic counting arguments, refining the above calculation of the expected number of satisfying assignments. Lower bounds, on the other hand, have come from analyzing progressively more sophisticated algorithms. Unfortunately, neither of these approaches helps narrow the asymptotic gap between the upper and lower bounds for r_k. The upper bounds improve $r_k \le 2^k \ln 2$ by only a small additive constant; the best algorithmic lower bound, due to Frieze and Suen [33], is $r_k \ge a_k 2^k/k$, where $\lim_{k\to\infty} a_k = 1.817\ldots$.

Two more results stand out in the study of random k-CNF formulas. In a breakthrough paper, Friedgut [32] proved the existence of a *nonuniform* satisfiability threshold, i.e., of a sequence $r_k(n)$ around which the probability of satisfiability goes from 1 to 0.

THEOREM 3 ([32]). *For each $k \ge 2$, there exists a sequence $r_k(n)$ such that for every $\epsilon > 0$,*

$$\lim_{n\to\infty} \Pr[F_k(n, rn) \text{ is satisfiable}] = \begin{cases} 1 & \text{if } r = (1-\epsilon)\, r_k(n), \\ 0 & \text{if } r = (1+\epsilon)\, r_k(n). \end{cases}$$

In [21], Chvátal and Szemerédi established a seminal result in proof complexity, by extending the work of Haken [37] and Urquhart [53] to random formulas. Specifically, they proved that for all $k \ge 3$, if $r \ge 2^k \ln 2$, then w.h.p. $f_k rn$ is unsatisfiable, but every resolution proof of its unsatisfiability contains at least $(1+\epsilon)^n$ clauses for some $\epsilon = \epsilon(k, r) > 0$. In [2], Achlioptas, Beame, and Molloy extended the main result of [21] to random CNF formulas that also contain 2-clauses, as this is relevant for the behavior of Davis–Putnam–Logemann–Loveland (DPLL) algorithms on random k-CNF. (DPLL algorithms proceed by setting variables sequentially, according to some heuristic, and backtracking whenever a contradiction is reached.) By combining the results in the present paper with the results in [2], it was recently shown [3] that a number of DPLL algorithms require exponential time *significantly below* the satisfiability threshold, i.e., for provably satisfiable random k-CNF formulas.

Finally, we note that if one chooses to live unencumbered by the burden of mathematical proof, powerful nonrigorous techniques of statistical physics, such as the "replica method," become available. Indeed, several claims based on the replica method have been subsequently established rigorously; thus it is frequently (but definitely not always) correct. Using this technique, Monasson and Zecchina [50] predicted $r_k \simeq 2^k \ln 2$. Like most arguments based on the replica method, their argument is mathematically sophisticated but far from rigorous. In particular, they argue that as k grows large, the so-called *annealed approximation* should apply. This creates an analogy with the second moment method which we discuss in section 3.4.

2.2. Random hypergraph 2-colorability. While Bernstein originally raised the 2-colorability question for certain classes of infinite set families [15], Erdős popularized the finite version of the problem [14, 27, 28, 43, 45, 51, 52] and the hypergraph representation. Recall that a 2-uniform hypergraph, i.e., a graph, is 2-colorable if and only if it has no odd cycle. In a random graph with cn edges this occurs with constant probability if and only if $c < 1/2$ (see [30] for more on the evolution of cycles in random graphs).

For all $k \ge 3$, on the other hand, hypergraph 2-colorability is NP-complete [46], and determining the 2-colorability threshold c_k for k-uniform hypergraphs $H_k(n, cn)$ remains open. Analogously to random k-SAT, we will take the liberty of writing $c_k \ge c^*$ if $H_k(n, cn)$ is w.h.p. 2-colorable for all $c < c^*$, and $c_k \le c^*$ if $H_k(n, cn)$ is w.h.p. non–2-colorable for all $c > c^*$.

Alon and Spencer [12] were the first to give bounds on the potential value of c_k. Specifically, they observed that, analogously to random k-SAT, the expected number of 2-colorings of $H_k(n, cn)$ is at most $[2(1-2^{1-k})^c]^n$ and concluded that $H_k(n, cn)$ is w.h.p. non–k-colorable if $c \geq 2^{k-1} \ln 2$. More importantly, by employing the Lovász local lemma, they proved that $H_k(n, cn)$ is w.h.p. 2-colorable if $c = O(2^k/k^2)$. Regarding the upper bound, it is easy to see that, in fact, $2(1-2^{1-k})^c < 1$ if $c = 2^{k-1} \ln 2 - (\ln 2)/2$, and this yields the upper bound of Theorem 2. Moreover, the techniques of [44, 24] can be used to improve this bound further to $2^{k-1} \ln 2 - (\ln 2)/2 - 1/4 + t_k$, where $t_k \to 0$.

The lower bound of [12] was improved by Achlioptas et al. [6] motivated by the analogies drawn in [12] between hypergraph 2-colorability and earlier work [18, 20] for random k-SAT. Specifically, it was shown in [6] that a simple, linear-time algorithm w.h.p. finds a 2-coloring of $H_k(n, cn)$ for $c = O(2^k/k)$, implying $c_k = \Omega(2^k/k)$. These were the best bounds for c_k prior to Theorem 2 of the present paper.

Finally, we note that Friedgut's result [32] applies to hypergraph 2-colorability as well, as presented in the following theorem.

THEOREM 4 ([32]). *For each $k \geq 3$, there exists a sequence $c_k(n)$ such that for every $\epsilon > 0$,*

$$\lim_{n\to\infty} \Pr[H_k(n, cn) \text{ is 2-colorable}] = \begin{cases} 1 & \text{if } c = (1-\epsilon)\, c_k(n), \\ 0 & \text{if } c = (1+\epsilon)\, c_k(n). \end{cases}$$

3. The second moment method: First look.

In the rest of the paper it will be convenient to work with a model of random formulas that differs slightly from $F_k(n, m)$. Specifically, to generate a random k-CNF formula on n variables with m clauses we simply generate a string of km independent random literals, each such literal being drawn uniformly from among all $2n$ possible ones. Note that this is equivalent to selecting, with replacement, m clauses from among all possible $2^k n^k$ ordered k-clauses. This choice of distribution for k-CNF formulas will simplify our calculations significantly. As we will see in section 4.1, the derived results can be easily transferred to all other standard models for random k-CNF formulas.

3.1. Random *k*-SAT.

For any formula F, given truth assignments $\sigma_1, \sigma_2, \ldots \in \{0,1\}^n$, we will write $\sigma_1, \sigma_2, \ldots \models F$ to denote that *all* of $\sigma_1, \sigma_2, \ldots$ satisfy F. Let $X = X(F)$ denote the number of satisfying assignments of a formula F. Then, for a k-CNF formula with random clauses $c_1, c_2, \ldots, c_m$ we have

$$\mathbf{E}[X] = \mathbf{E}\left[\sum_\sigma \mathbf{1}_{\sigma \models F}\right] = \sum_\sigma \mathbf{E}\left[\prod_{c_i} \mathbf{1}_{\sigma \models c_i}\right] = \sum_\sigma \prod_{c_i} \mathbf{E}[\mathbf{1}_{\sigma \models c_i}] = 2^n(1-2^{-k})^m, \tag{4}$$

since clauses are drawn independently and the probability that σ satisfies the ith random clause, i.e., $\mathbf{E}[\mathbf{1}_{\sigma \models c_i}]$, is $1 - 2^{-k}$ for every σ and i. Similarly, for $\mathbf{E}[X^2]$ we have

$$\mathbf{E}[X^2] = \mathbf{E}\left[\left(\sum_\sigma \mathbf{1}_{\sigma \models F}\right)^2\right] = \mathbf{E}\left[\sum_{\sigma,\tau} \mathbf{1}_{\sigma,\tau \models F}\right] = \sum_{\sigma,\tau} \prod_{c_i} \mathbf{E}[\mathbf{1}_{\sigma,\tau \models c_i}]. \tag{5}$$

We claim that $\mathbf{E}[\mathbf{1}_{\sigma,\tau \models c_i}]$, i.e., the probability that a fixed pair of truth assignments σ, τ satisfy the ith random clause, depends only on the number of variables z to which

σ and τ assign the same value. Specifically, if the overlap is $z = \alpha n$, we claim that this probability is

$$f_S(\alpha) = 1 - 2^{1-k} + 2^{-k}\alpha^k. \tag{6}$$

Our claim follows by inclusion-exclusion and observing that if c_i is not satisfied by σ, the only way for it to also not be satisfied by τ is for all k variables in c_i to lie in the overlap of σ and τ. Thus, f_S quantifies the correlation between the events that σ and τ are satisfying as a function of their overlap. In particular, observe that truth assignments with overlap $n/2$ are uncorrelated since $f_S(1/2) = (1 - 2^{-k})^2 = \Pr[\sigma \text{ is satisfying}]^2$.

Since the number of ordered pairs of assignments with overlap z is $2^n \binom{n}{z}$, we thus have

$$\mathbf{E}[X^2] = 2^n \sum_{z=0}^{n} \binom{n}{z} f_S(z/n)^m. \tag{7}$$

Writing $z = \alpha n$ and using the approximation $\binom{n}{z} = (\alpha^\alpha(1-\alpha)^{1-\alpha})^{-n} \times \text{poly}(n)$, we see that

$$\begin{aligned} \mathbf{E}[X^2] &= 2^n \left(\max_{0 \le \alpha \le 1} \left[\frac{f_S(\alpha)^r}{\alpha^\alpha (1-\alpha)^{1-\alpha}} \right] \right)^n \times \text{poly}(n) \\ &\equiv \left(\max_{0 \le \alpha \le 1} \Lambda_S(\alpha) \right)^n \times \text{poly}(n). \end{aligned}$$

At the same time observe that $\mathbf{E}[X]^2 = \left(2^n(1-2^{-k})^{rn}\right)^2 = (4 f_S(1/2)^r)^n = \Lambda_S(1/2)^n$. Therefore, if there exists some $\alpha \in [0,1]$ such that $\Lambda_S(\alpha) > \Lambda_S(1/2)$, then the second moment is exponentially greater than the square of the expectation and we get only an exponentially small lower bound for $\Pr[X > 0]$. Put differently, unless the dominant contribution to $\mathbf{E}[X^2]$ comes from "uncorrelated" pairs of satisfying assignments, i.e., pairs with overlap $n/2$, the second moment method fails.

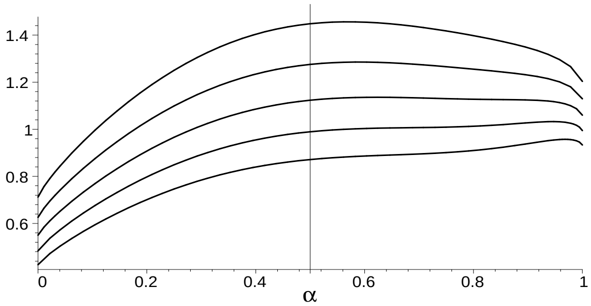
With these observations in mind, in Figure 1 we plot $\Lambda_S(\alpha)$ for $k = 5$ and different values of r. We see that, unfortunately, for all values of r shown, Λ_S is maximized at some $\alpha > 1/2$. If we look closely into the two factors comprising Λ_S, the reason for the failure of the second moment method becomes apparent: While the entropic factor $\left(\alpha^\alpha(1-\alpha)^{1-\alpha}\right)^{-1}$ is symmetric around $1/2$, the correlation function f_S is strictly increasing in $[0,1]$. Therefore, the derivative of Λ_S is never 0 at $1/2$, instead becoming 0 at some $\alpha > 1/2$ where the benefit of positive correlation balances with the cost of decreased entropy. (Indeed, this is true for all $k = o(\log n)$ and constant $r > 0$.)

3.2. Random NAE k-SAT. Let us now repeat the above analysis but with $X = X(F)$ being the number of NAE-satisfying truth assignments of a formula F. Recall that σ is an NAE-satisfying assignment if and only if under σ every clause has at least one satisfied literal *and* at least one unsatisfied literal. Thus, for a k-CNF formula with random clauses $c_1, c_2, \ldots, c_m$, proceeding as in (4), we get

$$\mathbf{E}[X] = 2^n(1 - 2^{1-k})^m, \tag{8}$$

since the probability that σ NAE-satisfies the ith random clause is $1 - 2^{1-k}$ for every σ and i.

Regarding the second moment, proceeding exactly as in (5), we write $\mathbf{E}[X^2]$ as a sum over the 4^n ordered pairs of assignments of the probability that both assignments



$k = 5$, $r = 16, 18, 20, 22, 24$ (top to bottom)

FIG. 1. *The nth root of the expected number of pairs of satisfying assignments at distance αn.*

are NAE-satisfying. As for k-SAT, for any fixed pair this probability depends only on the overlap. The only change is that if σ, τ agree on $z = \alpha n$ variables, then the probability that they both NAE-satisfy a random clause c_i is

$$\begin{aligned}\Pr[\sigma \text{ and } \tau \text{ NAE-satisfy } c_i] &= 1 - 2^{2-k} + 2^{1-k}\left(\alpha^k + (1-\alpha)^k\right) \\ &\equiv f_N(\alpha). \end{aligned} \tag{9}$$

Again, this claim follows from inclusion-exclusion and observing that for both σ, τ to NAE-violate c_i, the variables of c_i must either all be in the overlap of σ and τ or all be in their nonoverlap.

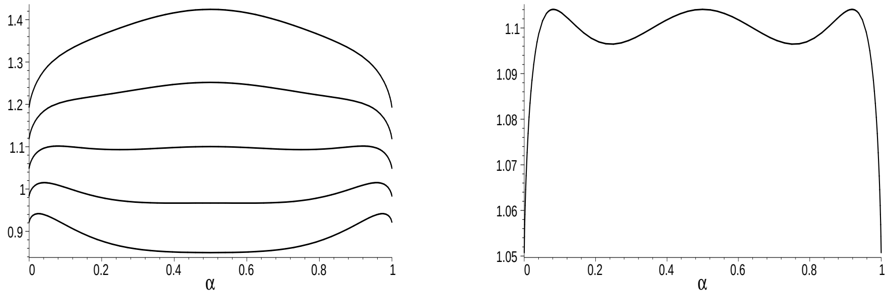
Applying Stirling's approximation for the factorial again and observing that the sum defining $\mathbf{E}[X^2]$ has only a polynomial number of terms, we now get (analogously to Λ_S in random k-SAT)

$$\begin{aligned}\mathbf{E}[X^2] &= 2^n \left(\max_{0 \le \alpha \le 1}\left[\frac{f_N(\alpha)^r}{\alpha^\alpha (1-\alpha)^{1-\alpha}}\right]\right)^n \times \operatorname{poly}(n) \\ &\equiv \left(\max_{0 \le \alpha \le 1} \Lambda_N(\alpha)\right)^n \times \operatorname{poly}(n). \end{aligned} \tag{10}$$

As before, it is easy to see that $\mathbf{E}[X]^2 = \Lambda_N(1/2)^n$. Therefore, if $\Lambda_N(1/2) > \Lambda_N(\alpha)$ for every $\alpha \neq 1/2$, then (10) implies that the ratio between $\mathbf{E}[X^2]$ and $\mathbf{E}[X]^2$ is at most polynomial in n. Indeed, with a more careful analysis of the interplay between the summation and Stirling's approximation, we will later show that whenever $\Lambda_N(1/2)$ is a global maximum, the ratio $\mathbf{E}[X^2]/\mathbf{E}[X]^2$ is bounded by a constant, implying that NAE-satisfiability holds w.u.p.p. So, all in all, again we hope that the dominant contribution to $\mathbf{E}[X^2]$ comes from pairs of assignments with overlap $n/2$.

The crucial difference is that now the correlation function f_N is *symmetric* around 1/2 and, hence, so is Λ_N. As a result, the entropy-correlation product Λ_N always has a local extremum at 1/2. Moreover, since the entropic term is always maximized at $\alpha = 1/2$ and is independent of r, for sufficiently small r this extremum is a global maximum. With these considerations in mind, in Figure 2 we plot $\Lambda_N(\alpha)$ for $k = 5$ and various values of r.

Let us start with the picture on the left, where r increases from 8 to 12 as we go from top to bottom. For $r = 8, 9$ we see that indeed Λ_N has a global maximum at 1/2 and the second moment method succeeds. For the cases $r = 11, 12$, on the other hand, we see that $\Lambda_N(1/2)$ is actually a global minimum. In fact, we see that $\Lambda_N(1/2) < 1$,



$k = 5$, $r = 8, 9, 10, 11, 12$ (top to bottom)

$k = 5$, $r = 9.973$

FIG. 2. *The nth root of the expected number of pairs of NAE-assignments at distance αn.*

implying that $\mathbf{E}[X]^2 = \Lambda_N(1/2)^n = o(1)$ and so w.h.p. there are no NAE-satisfying assignments for such r. It is worth noting that for $r = 11$, even though $X = 0$ w.h.p., the second moment is exponentially large (since $\Lambda_N > 1$ near 0 and 1).

The most interesting case is $r = 10$. Here $\Lambda(1/2) = 1.0023\ldots$ is a local maximum and greater than 1, but the two global maxima occur at $\alpha = 0.08\ldots$ and $\alpha = 0.92\ldots$, where the function equals $1.0145\ldots$. As a result, again, the second moment method gives only an exponentially small lower bound on $\Pr[X > 0]$. Note that this is in spite of the fact that $\mathbf{E}[X]$ is now exponentially large. Indeed, the largest value for which the second moment succeeds for $k = 5$ is $r = 9.973\ldots$ when the two side peaks reach the same height as the peak at $1/2$ (see the plot on the right in Figure 2).

So, the situation can be summarized as follows. By requiring that we count only NAE-satisfying truth assignments, we make it roughly twice as hard to satisfy each clause. This manifests itself in the additional factor of 2 in the middle term of f_N compared to f_S. On the other hand, now, the third term of f, capturing "joint" behavior, is symmetric around 1/2, making Λ itself symmetric around 1/2. This enables the second moment method which, indeed, breaks down only when the density gets within an additive constant of the upper bound for the NAE k-SAT threshold.

3.3. How symmetry reduces variance. Given a truth assignment σ and an arbitrary CNF formula F, let $Q = Q(\sigma, F)$ denote the total number of literal *occurrences* in F satisfied by σ. With this definition at hand, a potential explanation of how symmetry reduces the variance is suggested by considering the following trivial refinement of our generative model: First (i) draw km literals uniformly and independently just as before and then (ii) partition the drawn literals randomly into k-clauses (rather than assuming that the first k literals form the first clause, the next k the second, etc.).

In particular, imagine that we have just finished performing the first generative step above and we are about to perform the second. Observe that at this point the value of Q has already been determined for every $\sigma \in \{0,1\}^n$. Moreover, for each fixed σ the conditional probability of yielding a satisfying assignment corresponds to a balls-in-bins experiment: Distribute $Q(\sigma)$ balls in m bins, each with capacity k, so that every bin receives at least one ball. It is clear that those truth assignments for which Q is large at the end of the first step have a big advantage in the second.

To get an idea of what Q typically looks like on $\{0,1\}^n$ we begin by observing that the number of occurrences of a fixed literal ℓ, B_ℓ, is distributed as $\mathrm{Bin}(km, 1/(2n))$.

Thus, $\mathbf{E}[B_\ell] = O(1)$ and, moreover, the random variables B_ℓ are very weakly correlated. In particular, Q takes its maximum value on the subcube of truth assignments where every variable is assigned its majority value and, typically, decreases gradually away from there. Thus, at the end of the first step the "more promising" truth assignments are highly correlated: In satisfying many literal occurrences (thus increasing their odds for the second step), they tend to overlap with each other (and the majority assignment) at more than half the variables.

In contrast, if we focus on NAE-satisfying assignments, at the end of the first step the most promising assignments σ are those for which $Q(\sigma)$ is very close to its average value $km/2$. So, when the problem is symmetric, the typical case becomes the most favorable case and the clustering around truth assignments that satisfy many literal occurrences disappears.

If indeed "populism," i.e., the tendency of each variable to assume its majority value in the formula, is the main source of correlations in random k-SAT, then the second moment method is a good candidate for k-CNF models which do not encourage this tendency.[1] For example, one such model is *regular* random k-SAT, in which every literal occurs exactly the same number of times. Such formulas can be analyzed using a model analogous to the configuration model of random graphs, i.e., by taking precisely d copies of each literal and partitioning the resulting $2dn$ copies into clauses randomly (exactly as in the second step of our two-step model for random k-SAT).

3.4. Geometry and connections to statistical physics. A key quantity in statistical physics is the *overlap distribution* between configurations of minimum energy, known as ground states. When a constraint satisfaction problem is satisfiable, ground states correspond to solutions, such as satisfying assignments, valid colorings, and so on. In the case of random k-SAT, the overlap distribution is the probability $P(\alpha)$ that a random pair of satisfying assignments have overlap αn. Our calculation of the expected number of pairs of solutions at each possible distance is thus a weighted average of $P(\alpha)$ over all formulas, whereby formulas with more solutions contribute more heavily. Physicists call this weighted average the "annealed approximation" of $P(\alpha)$ and denote it $P_{\mathrm{ann}}(\alpha)$. It is worth pointing out that, while the annealed approximation clearly overemphasizes formulas with more satisfying assignments, Monasson and Zecchina conjectured in [50], based on the replica method, that it becomes asymptotically tight as $k \to \infty$.

On a more rigorous footing, it is easy to see that as long as Λ has a global maximum at $1/2$, $P_{\mathrm{ann}}(\alpha)$ is tightly concentrated around $1/2$, since $\Lambda(\alpha)^n$ is exponentially smaller than $\Lambda(1/2)^n$ for all other α. Our results establish that Λ is maximized at $1/2$ for densities up to $2^{k-1}\ln 2 - O(1)$. In other words, for densities almost all the way to the threshold, in the annealed approximation, almost all pairs of solutions have distance $n/2 + \Theta(\sqrt{n})$, just as if solutions were scattered uniformly at random throughout the hypercube.

Note that even if $P(\alpha)$ is concentrated around $1/2$ (rather than just $P_{\mathrm{ann}}(\alpha)$) this still allows for a typical geometry where there are exponentially many exponentially large clusters, each centered at a random assignment. Indeed, this is precisely the picture suggested by some very recent groundbreaking work of Mézard, Parisi, and Zecchina [47] and Meźard and Zecchina [48], based on nonrigorous techniques of statistical physics. If this is indeed the true picture, establishing it rigorously would require considerations much more refined than the second moment of the number of

[1] We describe recent developments on this point in the conclusions.

solutions. More generally, getting a better understanding of the typical geometry and its potential implications for algorithms appears to us a very challenging and very important open problem.

4. Groundwork.

4.1. Generative models. Given a set V of n Boolean variables, let $C_k = C_k(V)$ denote the set of all proper *k-clauses* on V, i.e., the set of all $2^k\binom{n}{k}$ disjunctions of k literals involving distinct variables. Similarly, given a set V of n vertices, let $E_k = E_k(V)$ be the set of all $\binom{n}{k}$ k-subsets of V. As we saw, a random k-CNF formula $F_k(n, m)$ is formed by selecting uniformly a random m-subset of C_k, while a random k-uniform hypergraph $H_k(n, m)$ is formed by selecting uniformly a random m-subset of E_k.

While $F_k(n, m)$ and $H_k(n, m)$ are perhaps the most natural models for generating random k-CNF formulas and random k-uniform hypergraphs, respectively, there are a number of slight variations of each model. Those are largely motivated by amenability to certain calculations. To simplify the discussion we focus on models for random formulas in the rest of this subsection. All our comments transfer readily to models for random hypergraphs.

For example, it is fairly common to consider the clauses as ordered k-tuples (rather than as k-sets) and/or to allow replacement in sampling the set C_k. Clearly, for properties such as satisfiability the issue of ordering is irrelevant. Moreover, as long as $m = O(n)$, essentially the same is true for the issue of replacement. To see that, observe that w.h.p. the number of repeated clauses is $q = o(n)$ and the subset of $m-q$ distinct clauses is uniformly random. Thus, if a monotone decreasing property (such as satisfiability) holds with probability p for a given $m = r^*n$ when replacement is allowed, it holds with probability $p - o(1)$ for all $r < r^*$ when replacement is not allowed.

The issue of selecting the literals of each clause with replacement (which might result in some "improper" clauses) is completely analogous. That is, the probability that a variable appears more than once in a given clause is at most $k^2/n = O(1/n)$ and hence w.h.p. there are $o(n)$ improper clauses. Finally, we note that by standard techniques our results also transfer to the $F_k(n, p)$ model where every clause appears independently of all others with probability p, for any p such that the expected number of k-clauses is $r^*n - n^\beta$ for some $\beta > 1/2$ (see [33]).

4.2. Strategy and tools. Our plan is to consider random k-CNF formulas formed by generating km independently and identically distributed random literals, where $m = rn$, and proving that if $X = X(F)$ is the number of NAE-satisfying assignments, then the following lemma holds.

LEMMA 2. *For all $\epsilon > 0$, $k \geq k_0(\epsilon)$, and $r < 2^{k-1}\ln 2 - (1 + \ln 2)/2 - \epsilon$, there exists some constant $C = C(k, r) > 0$ such that for all sufficiently large n,*

$$\mathbf{E}[X^2] < C \times \mathbf{E}[X]^2.$$

By Lemma 1 and our discussion in section 4.1, this implies that $F_k(n, rn - o(n))$ is NAE-satisfiable, and thus satisfiable, w.u.p.p. Therefore, for all r as in Lemma 2, $F_k(n, rn)$ is satisfiable w.u.p.p. To boost this to a high probability result, thus establishing Theorem 1, we employ the following immediate corollary of Theorem 3.

COROLLARY 1. *If $F_k(n, r^*n)$ is satisfiable w.u.p.p., then for all $r < r^*$, $F_k(n, rn)$ is satisfiable w.h.p.*

Friedgut's arguments [32] also apply to NAE k-SAT, implying that $F_k(n, rn)$ is w.h.p. NAE-satisfiable for r as in Lemma 2. Thus, Lemma 2 readily yields (12) below, while (11) comes from noting that the expected number of NAE-satisfying assignments is $[2(1-2^{1-k})^r]^n$. (Similarly to hypergraphs, the techniques of [44, 24] can be used to improve the bound in (11) to $2^{k-1}\ln 2 - (\ln 2)/2 - 1/4 + t_k$, where $t_k \to 0$.) Indeed, we will see that the proof of Theorem 5 will yield Theorem 2 for random hypergraphs with little additional effort.

THEOREM 5. *For all $k \geq 3$, $F_k(n, m = rn)$ is w.h.p. non–NAE-satisfiable if*

$$r > 2^{k-1}\ln 2 - \frac{\ln 2}{2}. \tag{11}$$

There exists a sequence $t_k \to 0$ such that for all $k \geq 3$, $F_k(n, m = rn)$ is w.h.p. NAE-satisfiable if

$$r < 2^{k-1}\ln 2 - \frac{\ln 2}{2} - \frac{1+t_k}{2}. \tag{12}$$

As we saw in section 3.2, the second moment of the number of NAE-satisfying assignments is

$$2^n \sum_{z=0}^{n} \binom{n}{z} f_N(z/n)^{rn}.$$

A slightly more complicated sum will occur when we bound the second moment of the number of 2-colorings. To bound both sums we will use the following lemma which we prove in section 8.

LEMMA 3 (Laplace lemma). *Let ϕ be a positive, twice-differentiable function on $[0, 1]$ and let $q \geq 1$ be a fixed integer. Let $t = n/q$ and let*

$$S_n = \sum_{z=0}^{t} \binom{t}{z}^q \phi(z/t)^n.$$

Letting $0^0 \equiv 1$, define g on $[0, 1]$ as

$$g(\alpha) = \frac{\phi(\alpha)}{\alpha^\alpha\,(1-\alpha)^{1-\alpha}}.$$

If there exists $\alpha_{\max} \in (0, 1)$ such that $g(\alpha_{\max}) \equiv g_{\max} > g(\alpha)$ for all $\alpha \neq \alpha_{\max}$ and $g''(\alpha_{\max}) < 0$, then there exists a constant $C = C(q, g_{\max}, g''(\alpha_{\max}), \alpha_{\max}) > 0$ such that for all sufficiently large n,

$$S_n < C\,n^{-(q-1)/2}\,g_{\max}^n.$$

5. Bounding the second moment for NAE *k*-SAT.

Recall that if X is the number of NAE-assignments, then

$$\mathbf{E}[X] = 2^n(1-2^{1-k})^{rn}$$

and

$$\mathbf{E}[X^2] = 2^n \sum_{z=0}^{n} \binom{n}{z} f_N(z/n)^{rn}, \tag{13}$$

where

$$f_N(\alpha) = 1 - 2^{2-k} + 2^{1-k}\left(\alpha^k + (1-\alpha)^k\right).$$

To bound the sum in (13) we apply Lemma 3 with $q = 1$ and $\phi(\alpha) = f_N(\alpha)^r$. Thus, $g = g_r$, where

$$g_r(\alpha) = \frac{f_N(\alpha)^r}{\alpha^\alpha(1-\alpha)^{1-\alpha}}. \tag{14}$$

To show that Lemma 3 applies, we will prove in section 7 that the following lemma holds.

Lemma 4. *For every $\epsilon > 0$, there exists $k_0 = k_0(\epsilon)$ such that for all $k \geq k_0$, if*

$$r < 2^{k-1}\ln 2 - \frac{\ln 2}{2} - \frac{1}{2} - \epsilon,$$

then $g_r(\alpha) < g_r(1/2)$ for all $\alpha \neq 1/2$, and $g_r''(1/2) < 0$.

Therefore, for all r, k, and ϵ as in Lemma 4, there exists a constant $C = C(k,r) > 0$ such that

$$\mathbf{E}[X^2] < C \times 2^n g_r(1/2)^n.$$

Since $\mathbf{E}[X]^2 = 2^n g_r(1/2)^n$, we get that for all r, k, ϵ as in Lemma 4

$$\mathbf{E}[X^2] < C \times \mathbf{E}[X]^2.$$

6. Bounding the second moment for hypergraph 2-colorability.

Just as for NAE k-SAT, it will be easier to work with the model in which generating a random hypergraph corresponds to choosing km vertices uniformly at random with replacement and letting the first k vertices form the first hyperedge, the second k vertices form the second hyperedge, etc.

In [5] we proved (2) of Theorem 2 by letting X be the set of all 2-colorings and using a convexity argument to show that $\mathbf{E}[X^2]$ is dominated by the contribution of *balanced* colorings, i.e., colorings with an equal number of black and white vertices. Here we follow a simpler approach suggested by Karger; namely, we *define* X to be the number of balanced 2-colorings. We emphasize that, while technically convenient, the restriction to balanced 2-colorings is not essential for the second moment method to succeed on hypergraph 2-colorability; i.e., one has $\mathbf{E}[X^2] = O(\mathbf{E}[X]^2)$ even if X is the number of all 2-colorings.

Of course, in order for balanced colorings to exist n must be even and we will assume that in our calculations below. To get Theorem 2 for all sufficiently large n, we observe that if for a given c^*, $H_k(2n, m = 2c^*n)$ is w.h.p. 2-colorable, then for all $c < c^*$, $H_k(n, cn)$ is w.h.p. 2-colorable since deleting a random vertex of $H_k(2n, 2c^*n)$ w.h.p. removes $o(n)$ edges. With this in mind, in the following we let X be the number of balanced 2-colorings and assume that n is even.

Since the vertices in each hyperedge are chosen uniformly with replacement, the probability that a random hyperedge is bichromatic in a fixed balanced partition is $1 - 2^{1-k}$. Since there are $\binom{n}{n/2}$ such partitions and the m hyperedges are drawn independently, we have

$$\mathbf{E}[X] = \binom{n}{n/2}\left(1 - 2^{1-k}\right)^m. \tag{15}$$

To calculate the second moment, as we did for [NAE] k-SAT, we write $\mathbf{E}[X^2]$ as a sum over all pairs of balanced partitions. In order to estimate this sum we first observe that if two balanced partitions σ and τ have exactly z black vertices in common, then they must also have exactly z white vertices in common. Thus σ and τ define four groups of vertices: z that are black in both, z that are white in both, $n/2-z$ that are black in σ and white in τ, and $n/2-z$ that are white in σ and black in τ. Clearly, a random hyperedge is monochromatic in both σ and τ if and only if all its vertices fall into the same group. Since the vertices of each hyperedge are chosen uniformly with replacement, this probability is

$$2\left(\frac{z}{n}\right)^k + 2\left(\frac{n/2-z}{n}\right)^k = 2^{1-k}\left[\left(\frac{2z}{n}\right)^k + \left(1-\frac{2z}{n}\right)^k\right].$$

Thus, by inclusion-exclusion, the probability that a random hyperedge is bichromatic in both σ and τ is

$$1 - 2^{2-k} + 2^{1-k}\left[\left(\frac{2z}{n}\right)^k + \left(1-\frac{2z}{n}\right)^k\right] = f_N(2z/n),$$

where $f_N(\alpha) = 1 - 2^{2-k} + 2^{1-k}(\alpha^k + (1-\alpha)^k)$ is the function we defined for NAE k-SAT in (9).

Moreover, observe that the number of pairs of partitions with such overlap is

$$\binom{n}{z,\ z,\ n/2-z,\ n/2-z} = \binom{n}{n/2}\binom{n/2}{z}^2.$$

Since hyperedges are drawn independently and with replacement, by summing over z we thus get

$$\mathbf{E}[X^2] = \binom{n}{n/2}\sum_{z=0}^{n/2}\binom{n/2}{z}^2 f_N(2z/n)^{cn}.$$

To bound this sum we apply Lemma 3 with $q=2$ and $\phi(\alpha) = f_N(\alpha)^c$. Felicitously, we find ourselves maximizing a function g_c which, if we replace c with r, is exactly the same function g_r we defined in (14) for NAE k-SAT. Thus, setting $c=r$ where k, r and ϵ are as in Lemma 4, g_c is maximized at $\alpha = 1/2$ with $g''(1/2) < 0$, and Lemma 3 implies that there exists a constant $C = C(r,k) > 0$ such that

$$\mathbf{E}[X^2] < C\,n^{-1/2}\binom{n}{n/2} g_c(1/2)^n.$$

We now bound $\mathbf{E}[X]$ from below using Stirling's approximation (29) and get

$$\frac{\mathbf{E}[X^2]}{\mathbf{E}[X]^2} < C \times \frac{n^{-1/2}\binom{n}{n/2} g_c(1/2)^n}{\binom{n}{n/2}^2 (1-2^{1-k})^{2cn}} = C \times \frac{n^{-1/2}\,2^n}{\binom{n}{n/2}} \to C \times \sqrt{\frac{\pi}{2}}.$$

To complete the proof, analogously to [NAE] k-SAT, we use the following "boosting" corollary of Theorem 4.

COROLLARY 2. *If $H_k(n, c^*n)$ is w.u.p.p. 2-colorable, then for all $c < c^*$, $H_k(n, cn)$ is w.h.p. 2-colorable.*

7. Proof of Lemma 4. We need to prove $g_r''(1/2) < 0$ and $g_r(\alpha) < g_r(1/2)$ for all $\alpha \neq 1/2$. As g_r is symmetric around $1/2$, we can restrict to $\alpha \in (1/2, 1]$. We divide $(1/2, 1]$ into two parts and handle them with two separate lemmata. The first lemma deals with $\alpha \in (1/2, 0.9]$ and also establishes that $g_r''(1/2) < 0$.

LEMMA 5. *Let $\alpha \in (1/2, 0.9]$. For all $k \geq 74$, if $r \leq 2^{k-1} \ln 2$, then $g_r(\alpha) < g_r(1/2)$ and $g_r''(1/2) < 0$.*

The second lemma deals with $\alpha \in (0.9, 1]$.

LEMMA 6. *Let $\alpha \in (0.9, 1]$. For every $\epsilon > 0$ and all $k \geq k_0(\epsilon)$, if $r \leq 2^{k-1} \ln 2 - \frac{\ln 2}{2} - \frac{1}{2} - \epsilon$, then $g_r(\alpha) < g_r(1/2)$.*

Combining Lemmata 5 and 6 we see that for every $\epsilon > 0$ and $k \geq k_0 = k_0(\epsilon)$, if

$$r \leq 2^{k-1} \ln 2 - \frac{\ln 2}{2} - \frac{1}{2} - \epsilon,$$

then $g_r(\alpha) < g_r(1/2)$ for all $\alpha \neq 1/2$ and $g_r''(1/2) < 0$, establishing Lemma 4.

We prove Lemmata 5 and 6 below. The reader should keep in mind that we have made no attempt to optimize the value of k_0 in Lemma 6, aiming instead for proof simplicity. For the lower bounds presented in Table 1 we computed numerically, for each k, the largest value of r for which the conclusions of Lemma 4 hold. In each case, the condition $g''(1/2) < 0$ was satisfied with room to spare, while establishing $g(1/2) > g(\alpha)$ for all $\alpha \neq 1/2$ was greatly simplified by the fact that g never has more than three local extrema in $[0, 1]$.

Proof of Lemma 5. We will first prove that for $k \geq 74$, g_r is strictly decreasing in $\alpha = (1/2, 0.9]$, thus establishing $g_r(\alpha) < g_r(1/2)$. Since g_r is positive, to do this it suffices to prove that $(\ln g_r)' = g_r'/g_r < 0$ in this interval. In fact, since $g_r'(\alpha) = (\ln g_r)' = 0$ at $\alpha = 1/2$, it will suffice to prove that for $\alpha \in [1/2, 0.9]$ we have $(\ln g_r)'' < 0$. Now,

$$\begin{aligned}(\ln g_r(\alpha))'' &= r\left(\frac{f''(\alpha)}{f(\alpha)} - \frac{f'(\alpha)^2}{f(\alpha)^2}\right) - \frac{1}{\alpha(1-\alpha)} \\ &\leq r\,\frac{f''(\alpha)}{f(\alpha)} - \frac{1}{\alpha(1-\alpha)}. \qquad (16)\end{aligned}$$

To show that the right-hand side (R.H.S.) of (16) is negative we first note that for $\alpha \geq 1/2$ and $k > 3$,

$$f''(\alpha) = 2^{1-k} k(k-1)(\alpha^{k-2} + (1-\alpha)^{k-2}) < 2^{2-k} \alpha^{k-2} k^2$$

is monotonically increasing. Therefore, $f''(\alpha) \leq f''(0.9) < 2^{2-k}\, 0.9^{k-2}\, k^2$.

Moreover, for all α, $f(\alpha) \geq f(1/2) = (1-2^{-k})^2$. Therefore, since $1/(\alpha(1-\alpha)) \geq 4$ and $r \leq 2^{k-1} \ln 2$, it suffices to observe that for all $k \geq 74$,

$$(2^{k-1} \ln 2) \times \frac{2^{2-k}\, 0.9^{k-2}\, k^2}{(1-2^{-74})^2} - 4 < 0.$$

Finally, recalling that $g'(1/2) = 0$ and using

$$(\ln g_r)'' = \frac{g_r''(\alpha)}{g_r(\alpha)} - \frac{g_r'(\alpha)^2}{g_r(\alpha)^2},$$

we see that $g_r''(1/2) < 0$ since $(\ln g_r)''(1/2) < 0$. □

Proof of Lemma 6. We let $h(\alpha) = -\alpha \ln \alpha - (1-\alpha)\ln(1-\alpha)$ denote the entropy function and for all $\alpha > 1/2$ we define

$$w(\alpha) \equiv \frac{f(\alpha) - f(1/2)}{f(1/2)} = \frac{2^{1-k}(\alpha^k + (1-\alpha)^k - 2^{1-k})}{(1-2^{1-k})^2} > 0.$$

By the definition of g_r, we thus see that $g_r(\alpha) < g_r(1/2)$ if and only if

$$\frac{r}{\ln 2 - h(\alpha)} < \frac{1}{\ln(1 + w(\alpha))}. \tag{17}$$

Moreover, we observe that for any $x > 0$,

$$\frac{1}{\ln(1+x)} \geq \frac{1}{x} + \frac{1}{2} - \frac{x}{12}.$$

Since $f(\alpha) - f(1/2) < 2^{1-k}$ and $f(1/2) > 1 - 2^{2-k}$, we thus see that (17) holds as long as

$$\frac{r}{\ln 2 - h(\alpha)} < \frac{2^{k-1} - 2}{\alpha^k + (1-\alpha)^k - 2^{1-k}} + \frac{1}{2} - \frac{2^{1-k}}{12(1-2^{2-k})}. \tag{18}$$

Now observe that for any $0 < \alpha < 1$ and $0 \leq q < \alpha^k$,

$$\frac{1}{\alpha^k - q} \geq 1 + k(1-\alpha) + q.$$

Since $\alpha > 1/2$ we can set $q = 2^{1-k} - (1-\alpha)^k$, yielding

$$\frac{1}{\alpha^k + (1-\alpha)^k - 2^{1-k}} \;\geq\; 1 + k(1-\alpha) + 2^{1-k} - (1-\alpha)^k.$$

Since $2^k(1-\alpha)^k < 5^{-k}$, we find that (18) holds as long as $r \leq \phi(y) - 2^{3-k}$, where

$$\phi(\alpha) \equiv \big(\ln 2 - h(\alpha)\big)\left(2^{k-1} + (2^{k-1} - 2)k(1-\alpha) - \frac{1}{2}\right).$$

We are thus left to minimize ϕ in $(0.9, 1]$. Since ϕ is differentiable, its minima can only occur at 0.9 or 1, or where $\phi' = 0$. The derivative of ϕ is

$$\phi'(\alpha) = (2^{k-1} - 2) \times \left[-k\,(\ln 2 - h(\alpha)) + (\ln \alpha - \ln(1-\alpha))\left(1 + k(1-\alpha) + \frac{3}{2^k - 4}\right)\right]. \tag{19}$$

Note now that for all $k > 1$

$$\lim_{\alpha \to 1} \frac{\phi'(\alpha)}{\ln(1-\alpha)} = -\frac{2^k - 1}{2};$$

i.e., the derivative of ϕ as $\alpha \to 1$ becomes positively infinite. At the same time,

$$\phi'(0.9) < -0.07 \times 2^k k + 1.1\,(2^k - 1) + 0.3\,k$$

is negative for $k \geq 16$. Therefore, ϕ is minimized in the interior of $(0.9, 1]$ for all $k \geq 16$. Setting ϕ' to zero gives

$$-\ln(1-\alpha) = \frac{k\,(\ln 2 - h(\alpha))}{1 + k(1-\alpha) + 3/(2^k - 4)} - \ln \alpha. \tag{20}$$

By "bootstrapping" we derive a tightening series of lower bounds on the solution for the left-hand side (L.H.S.) of (20) for $\alpha \in (0.9, 1)$. Note first that we have an easy upper bound,

$$-\ln(1-\alpha) < k\ln 2 - \ln\alpha. \tag{21}$$

At the same time, if $k > 2$, then $3/(2^k-4) < 1$, implying

$$-\ln(1-\alpha) > \frac{k\,(\ln 2 - h(\alpha))}{2+k(1-\alpha)} - \ln\alpha. \tag{22}$$

If we write $k(1-\alpha) = B$, then (22) becomes

$$-\ln(1-\alpha) > \frac{\ln 2 - h(\alpha)}{1-\alpha}\left(\frac{B}{B+2}\right) - \ln\alpha. \tag{23}$$

By inspection, if $B \geq 3$, the R.H.S. of (23) is greater than the L.H.S. for all $\alpha > 0.9$, yielding a contradiction. Therefore, $k(1-\alpha) < 3$ for all $k > 2$. Since $\ln 2 - h(\alpha) > 0.36$ for $\alpha > 0.9$, we see that for $k > 2$, (22) implies

$$-\ln(1-\alpha) > 0.07\,k. \tag{24}$$

Finally, observe that (24) implies that as k increases, the denominator of (20) approaches 1.

To bootstrap, we note that since $\alpha > 1/2$ we have

$$\begin{aligned}
h(\alpha) &\leq -2(1-\alpha)\ln(1-\alpha) && (25)\\
&< 2\,\mathrm{e}^{-0.07\,k}(k\ln 2 - \ln 0.9) && (26)\\
&< 2\,k\,\mathrm{e}^{-0.07\,k},
\end{aligned}$$

where (26) relies on (21) and (24). Moreover, $\alpha > 1/2$ implies $-\ln\alpha \leq 2(1-\alpha) < 2\,\mathrm{e}^{-0.07\,k}$. Thus, by using (24) and the fact $1/(1+x) > 1-x$ for all $x > 0$, (20) gives for $k \geq 3$

$$\begin{aligned}
-\ln(1-\alpha) &> \frac{k\,(\ln 2 - h(\alpha))}{1+k(1-\alpha)+3/(2^k-4)}\\
&> \frac{k\,(\ln 2 - 2\,k\,\mathrm{e}^{-0.07\,k})}{1+2\,k\,\mathrm{e}^{-0.07\,k}}\\
&> k\,(\ln 2 - 2\,k\,\mathrm{e}^{-0.07\,k})(1-2\,k\,\mathrm{e}^{-0.07\,k})\\
&> k\ln 2 - 4\,k^2\,\mathrm{e}^{-0.07\,k}. && (27)
\end{aligned}$$

For $k \geq 166$, $4\,k^2\,\mathrm{e}^{-0.07\,k} < 1$. Thus, by (27), we have $1-\alpha < 3 \times 2^{-k}$. This, in turn, implies $-\ln\alpha \leq 2(1-\alpha) < 6 \times 2^{-k}$ and thus, by (25) and (21), we have for $\alpha > 0.9$

$$h(\alpha) < 6 \times 2^{-k}(k\ln 2 - \ln\alpha) < 5\,k\,2^{-k}. \tag{28}$$

Plugging (28) into (20) to bootstrap again, we get that for $k \geq 166$

$$\begin{aligned}
-\ln(1-\alpha) &> \frac{k\,(\ln 2 - 5\,k\,2^{-k})}{1+3\,k\,2^{-k}+3/(2^k-4)}\\
&> \frac{k\,(\ln 2 - 5\,k\,2^{-k})}{1+6\,k\,2^{-k}}\\
&> k\,(\ln 2 - 5\,k\,2^{-k})(1-6\,k\,2^{-k})\\
&> k\ln 2 - 11\,k^2\,2^{-k}.
\end{aligned}$$

Since $e^x < 1 + 2x$ for $x < 1$ and $11\,k^2\,2^{-k} < 1$ for $k > 10$, we see that for $k \geq 166$,

$$1 - \alpha < 2^{-k} + 22\,k^2\,2^{-2k}.$$

Plugging into (21) the fact $-\ln\alpha < 6 \times 2^{-k}$, we get $-\ln(1-\alpha) < k\ln 2 + 6 \times 2^{-k}$. Using that $\mathrm{e}^{-x} \geq 1 - x$ for $x \geq 0$, we get the closely matching upper bound,

$$1 - \alpha > 2^{-k} - 6 \times 2^{-2k}.$$

Thus, we see that for $k \geq 166$, ϕ is minimized at an $\alpha_{\min}$ which is within δ of $1 - 2^{-k}$, where $\delta = 22\,k^2\,2^{-2k}$. Let T be the interval $[1-2^{-k}-\delta, 1-2^{-k}+\delta]$. Clearly the minimum of ϕ is at least $\phi(1-2^{-k}) - \delta \times \max_{\alpha \in T} |\phi'(\alpha)|$. It is easy to see from (19) that if $\alpha \in T$, then $|\phi'(\alpha)| \leq 2\,k\,2^k$.

Now, a simple calculation using that $\ln(1-2^{-k}) > -2^{-k} - 2^{-2k}$ for $k \geq 1$ gives

$$\begin{aligned}\phi(1-2^{-k}) &= \frac{1}{2}\big((2^k - k)\ln 2 + (2^k - 1)\ln(1-2^{-k})\big) \times \big(1 + (k-1)\,2^{-k} - k\,2^{2-2k}\big)\\ &> 2^{k-1}\ln 2 - \frac{\ln 2}{2} - \frac{1}{2} - k^2\,2^{-k}.\end{aligned}$$

Therefore,

$$\phi_{\min} \geq 2^{k-1}\ln 2 - \frac{\ln 2}{2} - \frac{1}{2} - 45\,k^3\,2^{-k}.$$

Finally, recall that (17) holds as long as $r < \phi_{\min} - 2^{3-k}$, for example, if

$$r < 2^{k-1}\ln 2 - \frac{\ln 2}{2} - \frac{1}{2} - 46\,k^3\,2^{-k}.$$

Clearly, we can take $k_0 = O(\ln \epsilon^{-1})$ so that for all $k \geq k_0$ the error term $46\,k^3\,2^{-k}$ is smaller than any $\epsilon > 0$. □

8. Proof of Lemma 3. The idea behind Lemma 3 is that sums of this type are dominated by the contribution of $\Theta(n^{1/2})$ terms around the maximum term. The proof amounts to replacing the sum by an integral and using the Laplace method for asymptotic integrals [23].

We start by establishing two upper bounds for the terms of S_n, a crude one and one which is sharper when $\alpha = z/t$ is bounded away from both 0 and 1. For the sharper bound we will use the following form of Stirling's approximation, valid for all $n > 0$:

$$\sqrt{2\pi n} < \frac{n!}{(n/\mathrm{e})^n} < \sqrt{2\pi n}\,(1 + 1/n)\,. \tag{29}$$

The zth term of S_n is $\binom{t}{z}^q \phi(z/t)^n$, where $n = qt$ and $\phi(\alpha) = g(\alpha)\,\alpha^\alpha(1-\alpha)^{1-\alpha}$. Fix any $\delta > 0$ and suppose that $z = \alpha t$, where $\alpha \in [\delta, 1-\delta]$. Then (29) yields

$$\binom{t}{z}^q \phi(z/t)^n \,<\, s(\alpha)\,g(\alpha)^n \left(1 + \frac{q}{n}\right)^q, \tag{30}$$

where $s(\alpha) = (2\pi\alpha(1-\alpha)t)^{-q/2}$. In addition to (30), valid for $z \in [t\delta, t(1-\delta)]$, we will also use a cruder bound, valid for all $0 \leq z \leq t$. Namely, by induction on $t - z$ it is easy to show that $\binom{t}{z} \leq t^t/[z^z(t-z)^{t-z}]$, implying

$$\binom{t}{z}^q \phi(z/t)^n \,<\, g(\alpha)^n. \tag{31}$$

Recall now that $g(\alpha_{\max}) > g(\alpha)$ for all $\alpha \neq \alpha_{\max}$. If I_ϵ denotes the interval $[\alpha_{\max} - \epsilon, \alpha_{\max} + \epsilon]$, then for every $\epsilon > 0$, there exists a constant $g_\epsilon < g(\alpha_{\max}) = g_{\max}$ such that $g(\alpha) < g_\epsilon$ for all $\alpha \notin I_\epsilon$. Let $z_\epsilon^- = \lfloor(\alpha_{\max} - \epsilon)t\rfloor$ and $z_\epsilon^+ = \lceil(\alpha_{\max} + \epsilon)t\rceil$, and let

$$S_n^{(\epsilon)} = \sum_{z=z_\epsilon^-}^{z_\epsilon^+} \binom{t}{z}^q \phi(z/t)^n. \tag{32}$$

We use (30) to bound the terms in $S_n^{(\epsilon)}$ and (31) to bound the remaining terms of S_n. Since $\lim_{n\to\infty} (1 + q/n)^q = 1$, and since $\lim_{n\to\infty} n^s\, g_\epsilon^n / g_{\max}^n = 0$ for any s, we see that for every $\epsilon > 0$

$$S_n < (C_\epsilon t)^{-q/2} \times \sum_{z=z_\epsilon^-}^{z_\epsilon^+} g(z/t)^n \tag{33}$$

for any constant $C_\epsilon > 2\pi \times \min\{(\alpha_{\max} - \epsilon)(1 - \alpha_{\max} + \epsilon), (\alpha_{\max} + \epsilon)(1 - \alpha_{\max} - \epsilon)\}$.

Say that a twice-differentiable function $\psi(x)$ is *unimodal* on an interval $[a, b]$ if ψ' has a unique zero $c \in [a, b]$ with $a < c < b$ and, furthermore, $\psi''(c) < 0$. Since $g_{\max} > g(\alpha)$ for all $\alpha \neq \alpha_{\max}$ and $g''(\alpha_{\max}) < 0$, we can take ϵ small enough so that g is unimodal on I_ϵ. This implies that $\ln g$ is also unimodal on I_ϵ and, for $n \geq 1$, that g^n is unimodal also. For any function $\gamma(x)$ which is nonnegative and unimodal on an interval $[a, b]$ with maximum $\gamma_{\max}$, no matter how tightly peaked, we have

$$\sum_{z=\lfloor at\rfloor}^{\lceil bt\rceil} \gamma(z/t) \leq t \int_a^b \gamma(x)\, \mathrm{d}x + \gamma_{\max},$$

and thus

$$\sum_{z=z_\epsilon^-}^{z_\epsilon^+} g(z/t)^n \leq \frac{n}{q} \int_{I_\epsilon} g(x)^n\, \mathrm{d}x + g_{\max}^n. \tag{34}$$

We evaluate this last integral using Lemma 7, i.e., the Laplace method for asymptotic integrals.

LEMMA 7 (see [23, section 4.2]). *Let $h(x)$ be unimodal on $[a, b]$, where c is the unique zero of h' in $[a, b]$. Then*

$$\lim_{n\to\infty} \int_a^b \mathrm{e}^{nh(x)}\, \mathrm{d}x \sim \sqrt{\frac{2\pi}{n\, |h''(c)|}}\, \mathrm{e}^{nh(c)}.$$

Applying Lemma 7 to (34) with $h = \ln g$ and $c = \alpha_{\max}$, we see that

$$S_n < C\, n^{-(q-1)/2}\, g_{\max}^n,$$

where $C = (2\pi)^{-(q-1)/2} \times q^{q/2} \times \sqrt{g_{\max}/|g''(\alpha_{\max})|}$. □

9. Conclusions. Before this work, lower bounds on the thresholds of random constraint satisfaction problems were largely derived by analyzing very simple heuristics. Here, instead, we derive such bounds by applying the second moment method to the number of solutions. In particular, for random NAE k-SAT and random hypergraph 2-colorability we determine the location of the threshold within a small additive constant for all k. As a corollary, we establish that the asymptotic order of the random k-SAT threshold is $\Theta(2^k)$, answering a long-standing open question.

Since this work first appeared [4, 5], our methods have been extended and applied to other problems. For random k-SAT, Achlioptas and Peres [7] confirmed our suspicion (see section 3.3) that the main source of correlations in random k-SAT is the "populist" tendency of satisfying assignments toward the majority vote assignment. By considering a carefully constructed random variable which focuses on balanced solutions, i.e., on satisfying assignments that satisfy roughly half of all literal occurrences, they showed $r_k \geq 2^k \ln 2 - k/2 - O(1)$, establishing $r_k \sim 2^k \ln 2$.

In [8], Achlioptas, Naor, and Peres extended the approach of balanced solutions to Max k-SAT. Let us say that a k-CNF formula is p-satisfiable if there exists a truth assignment which satisfies at least $(1 - 2^{-k} + p2^{-k})$ of all clauses; note that every k-CNF is 0-satisfiable. For $p \in (0, 1]$ let $r_k(p)$ denote the threshold for $F_k(n, m = rn)$ to be p-satisfiable (so that $r_k(1) = r_k$). In [8], the result $r_k = r_k(1) \sim 2^k \ln 2$ of [7] was extended to all $p \in (0, 1]$, showing that

$$r_k(p) \sim \frac{2^k \ln 2}{p + (1-p)\ln(1-p)}.$$

In both [7] and [8], controlling the variance crucially depends on focusing on an appropriate subset of solutions (akin to our NAE-assignments but less heavy-handed). In [9], Achlioptas and Naor applied the naive second moment method to the canonical symmetric constraint satisfaction problem, i.e., to the number of k-colorings of a random graph. Bearing out our belief that the naive approach should work for symmetric problems, they obtained asymptotically tight bounds for the k-colorability threshold, and in [10] Achlioptas and Moore extended this analysis to random d-regular graphs. The difficulty here is that the "overlap parameter" is a $k \times k$ matrix rather than a single real $\alpha \in [0, 1]$. Since $k \to \infty$, this makes the asymptotic analysis dramatically harder and much closer to the realm of statistical mechanics calculations.

We propose several questions for further work.

1. Does the second moment method give tight lower bounds on the threshold of all constraint satisfaction problem with a permutation symmetry?
2. Does it perform well for problems that are symmetric "on average"? For example, does it perform well for *regular* random k-SAT where every literal appears an equal number of times?
3. What rigorous connections can be made between the success of the second moment method and the notion of "replica symmetry" in statistical physics?
4. Is there a polynomial-time algorithm that succeeds with uniformly positive probability close to the threshold, or at least for $r = \omega(k) \times 2^k/k$ where $\omega(k) \to \infty$?

Acknowledgments. We are grateful to Paul Beame, Ehud Friedgut, Michael Molloy, Assaf Naor, Yuval Peres, Alistair Sinclair, and Chris Umans for reading earlier versions and making many helpful suggestions, and to Remi Monasson for discussions on the replica method. We would like to thank Henry Cohn for bringing [23] to our attention. Finally, we would like to thank the anonymous referees for a number of excellent suggestions.

REFERENCES

[1] D. Achlioptas, *Setting two variables at a time yields a new lower bound for random* 3*-SAT*, in Proceedings of the 32nd Annual ACM Symposium on Theory of Computing, 2000, pp. 28–37.

[2] D. Achlioptas, P. Beame, and M. Molloy, *A sharp threshold in proof complexity*, J. Comput. System Sci., 68 (2004), pp. 238–268.

[3] D. Achlioptas, P. Beame, and M. Molloy, *Exponential bounds for DPLL below the satisfiability threshold*, in Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms, New Orleans, 2004, pp. 132–133.

[4] D. Achlioptas and C. Moore, *The asymptotic order of the random k-SAT threshold*, in Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002, pp. 779–788.

[5] D. Achlioptas and C. Moore, *On the* 2*-colorability of random hypergraphs*, in Randomization and Approximation Techniques in Computer Science, Lecture Notes in Comput. Sci. 2483, Springer-Verlag, Berlin, 2002, pp. 78–90.

[6] D. Achlioptas, J. H. Kim, M. Krivelevich, and P. Tetali, *Two-coloring random hypergraphs*, Random Structures Algorithms, 20 (2002), pp. 249–259.

[7] D. Achlioptas and Y. Peres, *The random k-SAT threshold is* $2^k \ln 2 - O(k)$, J. Amer. Math. Soc., 17 (2004), pp. 947–973.

[8] D. Achlioptas, A. Naor, and Y. Peres, *On the maximum satisfiability of random formulas*, in Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science, 2003, pp. 362–370.

[9] D. Achlioptas and A. Naor, *On the k-colorability threshold*, Ann. of Math. (2), 162 (2005), pp. 1333–1349.

[10] D. Achlioptas and C. Moore, *The chromatic number of random regular graphs*, in Proceedings of the 8th International Workshop on Randomization and Computation, Lecture Notes in Comput. Sci. 3122, Springer-Verlag, Berlin, 2004, pp. 219–228.

[11] D. Achlioptas and G. B. Sorkin, *Optimal myopic algorithms for random* 3*-SAT*, in Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science, 2000, pp. 590–600.

[12] N. Alon and J. Spencer, *A Note on Coloring Random k-Sets*, manuscript.

[13] N. Alon and J. Spencer, *The Probabilistic Method*, Wiley & Sons, New York, 1992.

[14] J. Beck, *On* 3*-chromatic hypergraphs*, Discrete Math., 24 (1978), pp. 127–137.

[15] F. Bernstein, *Zur theorie der trigonometrische reihe*, Leipz. Ber., 60 (1908), pp. 325–338.

[16] A. Z. Broder, A. M. Frieze, and E. Upfal, *On the satisfiability and maximum satisfiability of random* 3*-CNF formulas*, in Proceedings of the Fourth Annual ACM-SIAM Symposium on Discrete Algorithms, Austin, TX, 1993, pp. 322–330.

[17] M.-T. Chao and J. Franco, *Probabilistic analysis of two heuristics for the* 3*-satisfiability problem*, SIAM J. Comput., 15 (1986), pp. 1106–1118.

[18] M.-T. Chao and J. Franco, *Probabilistic analysis of a generalization of the unit-clause literal selection heuristics for the k-satisfiability problem*, Inform. Sci., 51 (1990), pp. 289–314.

[19] P. Cheeseman, R. Kanefsky, and W. Taylor, *Where the really hard problems are*, in Proceedings of the 12th International Joint Conference on Artificial Intelligence, 1991, pp. 331–337.

[20] V. Chvátal and B. Reed, *Mick gets some (the odds are on his side)*, in Proceedings of the 33rd Annual IEEE Symposium on Foundations of Computer Science, 1992, pp. 620–627.

[21] V. Chvátal and E. Szemerédi, *Many hard examples for resolution*, J. ACM, 35 (1988), pp. 759–768.

[22] S. A. Cook, *The complexity of theorem-proving procedures*, in Proceedings of the 3rd Annual ACM Symposium on Theory of Computing, 1971, pp. 151–158.

[23] N. G. de Bruijn, *Asymptotic Methods in Analysis*, Dover, New York, 1981.

[24] O. Dubois and Y. Boufkhad, *A general upper bound for the satisfiability threshold of random r-SAT formulae*, J. Algorithms, 24 (1997), pp. 395–420.

[25] O. Dubois, Y. Boufkhad, and J. Mandler, *Typical random* 3*-SAT formulae and the satisfiability threshold*, in Electronic Colloquium on Computational Complexity 10, 2003; available online from http://www.informatik.uni-trier.de/~ley/db/journals/eccc/eccc10.html; also available in Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms, San Francisco, 2000, pp. 126–127.

[26] A. El Maftouhi and W. Fernandez de la Vega, *On random* 3*-SAT*, Combin. Probab. Comput., 4 (1995), pp. 189–195.

[27] P. Erdős, *On a combinatorial problem*, Nordisk Mat. Tidskr., 11 (1963), pp. 5–10.

[28] P. Erdős and L. Lovász, *Problems and results on* 3*-chromatic hypergraphs and some related questions*, in Infinite and Finite Sets, Vol. II, Colloq. Math. Soc. Janos Bolyai 10, North–Holland, Amsterdam, 1975, pp. 609–627.

[29] W. Fernandez de la Vega, *On Random* 2*-SAT*, manuscript, 1992.

[30] P. Flajolet, D. E. Knuth, and B. Pittel, *The first cycles in an evolving graph*, Discrete Math., 75 (1989), pp. 167–215.

[31] J. Franco and M. Paull, *Probabilistic analysis of the Davis–Putnam procedure for solving the satisfiability problem*, Discrete Appl. Math., 5 (1983), pp. 77–87.

[32] E. Friedgut, *Necessary and sufficient conditions for sharp thresholds of graph properties, and the k-SAT problem*, J. Amer. Math. Soc., 12 (1999), pp. 1017–1054.

[33] A. M. Frieze and S. Suen, *Analysis of two simple heuristics on a random instance of k-SAT*, J. Algorithms, 20 (1996), pp. 312–355.

[34] A. Frieze and N. C. Wormald, *Random k-SAT: A tight threshold for moderately growing k*, Combinatorica, 25 (2005), pp. 297–305.

[35] A. Goerdt, *A threshold for unsatisfiability*, J. Comput. System Sci., 53 (1996), pp. 469–486.

[36] M. Hajiaghayi and G. B. Sorkin, *The satisfiability threshold of random* 3*-SAT is at least* 3.52, submitted; available online from http://www.arxiv.org/abs/math.CO/0310193.

[37] A. Haken, *The intractability of resolution*, Theoret. Comput. Sci., 39 (1985), pp. 297–308.

[38] S. Janson, T. Łuczak, and A. Ruciński, *Random Graphs*, John Wiley & Sons, New York, 2000.

[39] S. Janson, Y. C. Stamatiou, and M. Vamvakari, *Bounding the unsatisfiability threshold of random* 3*-SAT*, Random Structures Algorithms, 17 (2000), pp. 103–116.

[40] A. Kamath, R. Motwani, K. Palem, and P. Spirakis, *Tail bounds for occupancy and the satisfiability threshold conjecture*, Random Structures Algorithms, 7 (1995), pp. 59–80.

[41] A. Kaporis, L. M. Kirousis, and E. Lalas, *Selecting complementary pairs of literals*, in Proceedings of LICS 2003 Workshop on Typical Case Complexity and Phase Transitions, 2003.

[42] A. Kaporis, L. M. Kirousis, Y. C. Stamatiou, M. Vamvakari, and M. Zito, *The unsatisfiability threshold revisited*, Discrete Math., to appear.

[43] M. Karoński and T. Łuczak, *Random hypergraphs*, in Combinatorics, Paul Erdős Is Eighty, Vol. 2 (Kesztheley, 1993), Bolyai Soc. Math. Stud. 2, Janos Bolyai Math. Soc., Budapest, 1996, pp. 283–293.

[44] L. M. Kirousis, E. Kranakis, D. Krizanc, and Y. Stamatiou, *Approximating the unsatisfiability threshold of random formulas*, Random Structures Algorithms, 12 (1998), pp. 253–269.

[45] M. Krivelevich and B. Sudakov, *The chromatic numbers of random hypergraphs*, Random Structures Algorithms, 12 (1998), pp. 381–403.

[46] L. Lovász, *Coverings and coloring of hypergraphs*, in Proceedings of the Fourth Southeastern Conference on Combinatorics, Graph Theory, and Computing, Boca Raton, FL, 1973, pp. 3–12.

[47] M. Mézard, G. Parisi, and R. Zecchina, *Analytic and algorithmic solution of random satisfiability problems*, Science, 297 (2002), pp. 812–815.

[48] M. Mézard and R. Zecchina, *Random K-satisfiability: From an analytic solution to a new efficient algorithm*, Phys. Rev. E (3), 66 (2002), 056126.

[49] D. G. Mitchell, B. Selman, and H. J. Levesque, *Hard and easy distributions of SAT problems*, in Proceedings of the 10th National Conference on Artificial Intelligence, 1992, pp. 459–462.

[50] R. Monasson and R. Zecchina, *Statistical mechanics of the random K-satisfiability model*, Phys. Rev. E (3), 56 (1997), pp. 1357–1370.

[51] J. Radhakrishnan and A. Srinivasan, *Improved bounds and algorithms for hypergraph* 2*-coloring*, Random Structures Algorithms, 16 (2000), pp. 4–32.

[52] J. Schmidt-Pruzan, E. Shamir, and E. Upfal, *Random hypergraph coloring algorithms and the weak chromatic number*, J. Graph Theory, 8 (1985), pp. 347–362.

[53] A. Urquhart, *Hard examples for resolution*, J. ACM, 34 (1987), pp. 209–219.