The Threshold for Random k-SAT is $2^k \log 2 - O(k)$

Dimitris Achlioptas
Microsoft Research, Redmond, WA
optas@microsoft.com

Yuval Peres*
Department of Statistics, University of California, Berkeley, CA
peres@stat.berkeley.edu

September 7, 2003

Abstract

Let $F_k(n,m)$ be a random k-CNF formula formed by selecting uniformly and independently m out of all possible k-clauses on n variables. It is well-known that if $r \geq 2^k \log 2$, then $F_k(n,rn)$ is unsatisfiable with probability that tends to 1 as $n \to \infty$. We prove that if $r \leq 2^k \log 2 - t_k$, where $t_k = O(k)$, then $F_k(n,rn)$ is satisfiable with probability that tends to 1 as $n \to \infty$.

Our technique, in fact, yields an explicit lower bound for the random k-SAT threshold for every k. For $k \geq 4$ our bounds improve all previously known such bounds.

1 Introduction

Call a disjunction of k Boolean variables a k-clause. For a set V of n Boolean variables, let $C_k(V)$ denote the set of all $2^k n^k$ possible k-clauses on V. A random k-CNF formula $F_k(n,m)$ is formed by selecting uniformly, independently and with replacement m clauses from C_k and taking their conjunction†. The study of such random k-CNF formulas has attracted substantial interest in logic, optimization, combinatorics, theory of algorithms and, more recently, statistical physics.

Say that a sequence of events $\mathcal{E}_n$ occurs with high probability (w.h.p.) if $\lim_{n\to\infty} \mathbf{P}[\mathcal{E}_n] = 1$ and with uniformly positive probability if $\liminf_{n\to\infty} \mathbf{P}[\mathcal{E}_n] > 0$. We emphasize that throughout the paper k is arbitrarily large but fixed, while $n \to \infty$. For each $k \geq 2$, let

$$\begin{aligned} r_k &\equiv \sup\{r : F_k(n,rn) \text{ is satisfiable w.h.p.}\} \ , \\ r_k^* &\equiv \inf\{r : F_k(n,rn) \text{ is unsatisfiable w.h.p.}\} \ . \end{aligned}$$

Clearly, $r_k \leq r_k^*$. The *Satisfiability Threshold Conjecture* asserts that $r_k = r_k^*$ for all $k \geq 3$. Our main result establishes an asymptotic form of this conjecture.

Theorem 1 *As $k \to \infty$,*

$$r_k = r_k^*(1 - o(1)) \ .$$

As we will see in Section 1.1, a classical and very simple argument gives $r_k^* \leq 2^k \log 2$. The following theorem implies that this bound is asymptotically tight. The theorem also sharpens the $o(1)$ term in Theorem 1.

*Research supported by NSF Grant DMS-0104073, NSF Grant DMS-0244479 and a Miller Professorship at UC Berkeley. Part of this work was done while visiting Microsoft Research.

†Our results hold in all common models for random k-SAT, e.g., when clause replacement is not allowed. See Section 3.

Theorem 2 *There exists a sequence $\delta_k \to 0$ such that for all $k \geq 3$,*

$$r_k \geq 2^k \log 2 - (k+1)\frac{\log 2}{2} - 1 - \delta_k \ .$$

Theorem 2 establishes that $r_k \sim 2^k \log 2$, in agreement with the predictions of Monasson and Zecchina [23] based on the "replica method" of statistical mechanics. Like most arguments based on the replica method, the approach in [23] is mathematically sophisticated but far from rigorous. To the best of our knowledge, our result is the first rigorous proof of a replica method prediction for any NP-complete problem at zero temperature.

Obtaining tight bounds for the thresholds r_k, r_k^* is a benchmark problem for a number of analytic and combinatorial techniques of wider applicability [11, 14, 17, 5]. The best bounds prior to our work for general k, from [1] and [9] respectively, differed roughly by a factor of 2:

$$2^{k-1} \log 2 - \Theta(1) \leq r_k \leq r_k^* \leq 2^k \log 2 - \Theta(1) \ .$$

Traditionally, lower bounds for r_k have been established by analyzing algorithms for finding satisfying assignments, i.e., by proving in each case that some specific algorithm succeeds w.h.p. on $F_k(n, rn)$ for r smaller than a certain value. Indeed, until very recently, all lower bounds for r_k were algorithmic and of the form $\Omega(2^k/k)$. The bound $r_k \geq 2^{k-1} \log 2 - \Theta(1)$ from [1], derived via a non-algorithmic argument, was the first to break the $2^k/k$ barrier.

Our proof of Theorem 2 is also non-algorithmic, based instead on a delicate application of the second moment method. By not going after some particular satisfying truth assignment, as algorithms do, our arguments offer some glimpses of the "geometry" of the set of satisfying truth assignments. Also, the proof yields an explicit lower bound for r_k for each $k \geq 3$. Already for $k \geq 4$ this improves all previously known lower bounds for r_k. Below, we compare our lower bound with the best known algorithmic lower bound [15, 18] and the best known upper bound [10, 9, 19] for some small values of k.

k	3	4	5	7	10	20	21
Upper bound	4.51	10.23	21.33	87.88	708.94	726,817	1,453,635
Our lower bound	2.68	7.91	18.79	84.82	704.94	726,809	1,453,626
Algorithmic lower bound	3.42	5.54	9.63	33.23	172.65	95,263	181,453

1.1 Background

Franco and Paull [13], in the early 80's, observed that $r_k^* \leq 2^k \log 2$. To see this, fix any truth assignment and observe that a random k-clause is satisfied by it with probability $1 - 2^{-k}$. Therefore, the expected number of satisfying truth assignments of $F_k(n, rn)$ is $[2(1 - 2^{-k})^r]^n = o(1)$ for $r \geq 2^k \log 2$. In 1990, Chao and Franco [3] complemented this by proving that for $r < 2^k/k$ a simple algorithm, called UNIT CLAUSE (UC), finds a satisfying truth assignment with uniformly positive probability.

At around the same time, experimental results by Cheeseman, Kanefsky and Taylor [4] and Mitchell, Selman and Levesque [22] suggested that random k-SAT, while a logical model, also behaves like a physical system in the sense that it appears to undergo a phase transition. Perhaps the first statement of the satisfiability threshold conjecture appeared about ten years ago in the work of Chvátal and Reed [5] who proved $r_2 = r_2^* = 1$ and, by analyzing an extension of UC, established that $r_k \geq (3/8)2^k/k$. A few years later, Frieze and Suen [15] improved this lower bound to $r_k \geq c_k 2^k/k$, where $\lim_{k\to\infty} c_k = 1.817\ldots$, and this remained the best bound for r_k until recently.

In a breakthrough paper, Friedgut [14] proved the existence of a *non-uniform* threshold.

Theorem 3 (Friedgut [14]) *For each $k \geq 2$, there exists a sequence $r_k(n)$ such that for every $\epsilon > 0$,*

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

As mentioned earlier, in [1], Moore and the first author established $r_k \geq 2^{k-1}\log 2 - 1$. Independently, Frieze and Wormald [16] proved that if k is allowed to grow with n, in particular if $k - \log_2 n \to +\infty$, then random k-SAT has a sharp threshold around $m = n(2^k + O(1))\log 2$. See [1] for further background.

The rest of the paper is organized as follows. In the next section we recall the argument in [1], highlight its main weakness and discuss how we overcome it. Our main idea can be implemented either by a simple weighting scheme or by a more refined large deviations argument. Both approaches yield $2^k \log 2$ as the leading term in the lower bound for r_k. The weighting scheme argument is more compact and technically simpler. However, it gives away a factor of four in the $\Theta(k)$ second order term. The large deviations analysis, on the other hand, is tight for our method, up to an additive $O(1)$. We present the weighting scheme argument in Sections 3—6. The additional material for the large deviations argument appears in Sections 7—9. In Section 10 we describe our derivation of explicit lower bounds for small values of k. We conclude with some discussion and open problems in Section 11.

2 Outline and heuristics

For any non-negative random variable X one can get a lower bound on $\mathbf{P}[X > 0]$ by the following inequality.

Lemma 1 *For any non-negative random variable X,*

$$\mathbf{P}[X > 0] \;\geq\; \frac{\mathbf{E}[X]^2}{\mathbf{E}[X^2]} \;\; . \tag{1}$$

In particular, if X denotes the number of satisfying assignments of a random formula $F_k(n, rn)$, one can get a lower bound on the probability of satisfiability by applying (1) to X. We will refer to this approach as the "vanilla" application of the second moment method. Indeed, the following immediate corollary of Theorem 3 implies that if $\mathbf{P}[X > 0] > 1/C$ for any constant $C > 0$, then $r_k \geq r$.

Corollary 1 *Fix $k \geq 2$. If $F_k(n, rn)$ is satisfiable with uniformly positive probability then $r_k \geq r$.*

Thus, if for a given r we have $\mathbf{E}[X^2] = O(\mathbf{E}[X]^2)$, then $r_k \geq r$. Unfortunately, as we will see, this is never the case: for every constant $r > 0$, there exists $\beta = \beta(r) > 0$ such that $\mathbf{E}[X^2] > (1+\beta)^n\, \mathbf{E}[X]^2$.

2.1 The vanilla second moment method fails

Given a CNF formula F on n variables let $\mathcal{S}(F) = \{\sigma : \sigma \text{ satisfies } F\} \subset \{0,1\}^n$ denote the set of satisfying truth assignments of F and let $X = X(F) = |\mathcal{S}(F)|$. Then, for a k-CNF formula with independent clauses $c_1, c_2, \ldots, c_m$

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

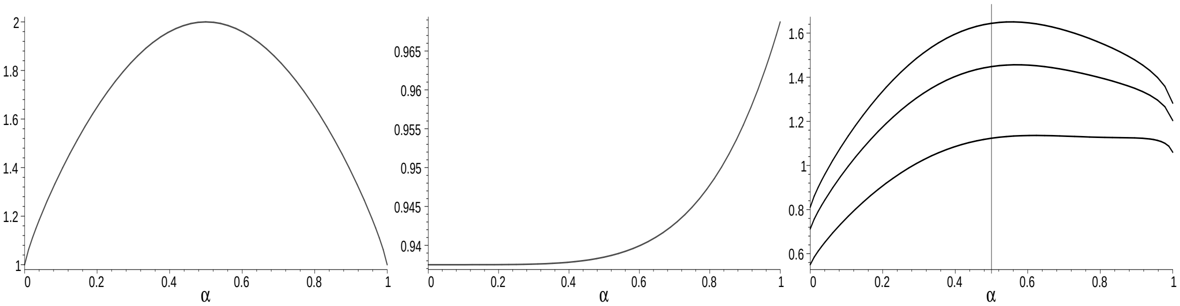
We claim that $\mathbf{E}[\mathbf{1}_{\sigma,\tau \in \mathcal{S}(c_i)}]$, i.e., the probability that a fixed pair of truth assignments σ, τ satisfy the ith random clause, depends only on the number of variables z to which σ and τ assign the same value. Specifically, if the overlap of σ and τ is $z = \alpha n$, we claim that this probability is

$$\mathbf{P}[\sigma, \tau \in \mathcal{S}(c_i)] = 1 - 2^{1-k} + 2^{-k}\alpha^k \equiv f_S(\alpha) \;\; . \tag{3}$$

This follows by 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 σ being satisfying and τ being satisfying as a function of their overlap. In particular, observe that truth assignments with overlap $n/2$ are uncorrelated since $f_S(1/2) = (1 - 2^{-k})^2 = \mathbf{P}[\sigma \text{ is satisfying}]^2$.

Since the number of ordered pairs of assignments with overlap z is $2^n \binom{n}{z}$ we see that (2) and (3) imply

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



$\mathcal{E}(\alpha) = 1/(\alpha^\alpha(1-\alpha)^{1-\alpha})$ $\qquad f_S(\alpha) = 1 - 2^{1-k} + \alpha^k$ $\qquad \Lambda_S(\alpha) = 2\mathcal{E}(\alpha) f_S(\alpha)^r$

Figure 1: $k = 5$, $r = 14, 16, 20$ (top to bottom).

Writing $z = \alpha n$ and using the approximation $\binom{n}{z} = (\alpha^\alpha(1-\alpha)^{1-\alpha})^{-n} \times \mathrm{poly}(n)$ we get

$$\mathbf{E}[X^2] \geq 2^n \left(\max_{0 \leq \alpha \leq 1} \left[\frac{f_S(\alpha)^r}{\alpha^\alpha(1-\alpha)^{1-\alpha}} \right] \right)^n \times \mathrm{poly}(n) \equiv \left(\max_{0 \leq \alpha \leq 1} \Lambda_S(\alpha) \right)^n \times \mathrm{poly}(n) \ .$$

Note now that $\mathbf{E}[X]^2 = \left(2^n(1-2^{-k})^{rn}\right)^2 = \left(4 f_S(1/2)^r\right)^n = \Lambda_S(1/2)^n$. 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 only get an exponentially small lower bound for $\mathbf{P}[X > 0]$. 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. Indeed, for any constant $r > 0$ this is precisely what happens as the function Λ_S is maximized at some $\alpha > 1/2$. The reason for this is as follows: while the entropic factor $\mathcal{E}(\alpha) = 1/(\alpha^\alpha(1-\alpha)^{1-\alpha})$ is maximized when $\alpha = 1/2$, the function f_S has a positive derivative in $(0,1)$. Therefore, the derivative of Λ_S is never 0 at $1/2$, instead becoming 0 only when the correlation benefit balances with the penalty of decreasing entropy at some $\alpha > 1/2$.

2.2 Random NAE k-SAT and balance

In [1], the second moment method was applied successfully by considering only those satisfying truth assignments whose complement is also satisfying. Observe that this is equivalent to interpreting $F_k(n,m)$ as an instance of Not All Equal k-SAT, where σ is a solution iff under σ every clause has at least one satisfied literal *and* at least one unsatisfied literal. In particular, if σ, τ have overlap $z = \alpha n$ and c is a random clause

$$\mathbf{P}[\sigma, \tau \text{ NAE-satisfy } c] = 1 - 2^{2-k} + 2^{1-k}(\alpha^k + (1-\alpha)^k) \equiv f_N(\alpha) \ .$$

The key point is that f_N is symmetric around $\alpha = 1/2$ and, as a result, the product $\mathcal{E}(\alpha) f_N(\alpha)^r$ always has a local extremum at $1/2$. In [1] it was shown that for $r \leq 2^{k-1}\log 2 - 1$ this extremum is a global maximum, implying that for such r, $F_k(n,m)$ is w.h.p. [NAE-] satisfiable. It is worth noting that for $r \geq 2^{k-1}\log 2$, w.h.p. $F_k(n,m)$ is *not* NAE-satisfiable, i.e., the second moment method determines the NAE-satisfiability threshold within an additive constant. Intuitively, the symmetry of f_N stems from the fact that NAE-satisfying assignments come in complementary pairs and, thus, having overlap z with an NAE-satisfying assignment σ (and $n - z$ with $\overline{\sigma}$) is indistinguishable from having overlap $n - z$ with σ (and z with $\overline{\sigma}$).

The suspicion motivating this work is that the correlations behind the failure of the vanilla second moment method are mainly due to the following form of populism: *satisfying assignments tend to lean towards the majority vote truth assignment.* Observe that truth assignments that satisfy many literal occurrences in the random formula have significantly greater probability of being satisfying. At the same time, such assignments are highly correlated since, in order to satisfy many literal occurrences, they tend to agree with each other (and the majority truth assignment) on more than half the variables.

Note that our suspicion regarding populism is consistent with the success of the second moment method for random NAE k-SAT. In that problem, since we need to have at least one satisfied *and* at least one dissatisfied literal in each clause, leaning towards majority is a disadvantage. As intuition suggests, "middle of the road" assignments have the greatest probability of being NAE-satisfying. Alternatively, observe that conditioning on σ being NAE-satisfying does not increase the expected number of satisfied literal occurrences under σ, whereas conditioning on σ being only satisfying increases this expectation by a factor $2^k/(2^k-1)$ relative to the unconditional expectation $km/2$. To overcome these correlations, populism must be discouraged and the delicacy with which this is done determines the accuracy of the resulting bound.

An example from a different area, which was another inspiration for our work, is the recent proof of the Erdős-Taylor conjecture from 1960 for the simple random walk in the planar square lattice (see [12],[7] and for a popular account [24]). The conjecture was that the number of visits to the most frequently visited lattice site in the first n steps of the walk, is asymptotic to $(\log n)^2/\pi$. Erdős and Taylor [12] obtained a (sharp) upper bound via an easy calculation of the expectation of the number X_a of vertices visited at least $a(\log n)^2$ times. The lower bound they obtained was four times smaller than the conjectured value. In that setting the vanilla second moment method fails, since the events that two vertices u, v are visited frequently are highly correlated. The conjecture was proved in [7] by first recognizing the main source of the correlation in a certain "populism" (when the random walk spends a long time in the smallest disk containing both u and v). Replacing X_a by a weighted count that discourages such loitering, confirmed that this was indeed the source of excessive correlations as the weighted second moment was successful.

In a nutshell, our plan is to apply the second moment method to *balanced* satisfying truth assignments, i.e., truth assignments that satisfy, approximately, half of all km literal occurrences. As it turns out, choosing a concrete range to represent "approximately half" and only counting the satisfying assignments that fall within the range leads to analytic difficulties due to the polynomial corrections in certain large deviations estimates. Fortunately, these issues can be avoided by i) introducing a scheme that weights satisfying truth assignments according to their number of satisfied literal occurrences, and ii) tuning the scheme's control parameter so as to concentrate the weight on balanced assignments.

2.3 Weighted second moments: a transform

Recall that for a CNF formula F on n variables, $\mathcal{S} = \mathcal{S}(F) \subseteq \{0,1\}^n$ denotes the set of satisfying truth assignments of F. An attractive feature of the second moment method is that we are free to apply it to any random variable $X = X(F)$ such that $X > 0$ implies that $\mathcal{S} \neq \emptyset$. Sums of the form

$$X = \sum_{\sigma} w(\sigma, F)$$

clearly have this property if $w(\sigma, F) = 0$ for $\sigma \notin \mathcal{S}(F)$.

Weighting schemes as above can be viewed as *transforms* of the original problem and can be particularly effective in exploiting insights into the source of correlations. In particular, if $w(\sigma, F)$ has product structure over the clauses, then clause-independence allows one to replace expectations of products with products of expectations. With this in mind, let us consider random variables of the form

$$X = \sum_{\sigma} \prod_{c} w(\sigma, c) \ ,$$

where w is some arbitrary function. (Eventually, we will require that $w(\sigma, c) = 0$ if σ falsifies c.) For instance, if $w(\sigma, c)$ is the indicator that c is satisfied by σ, then X simply counts the number of satisfying truth assignments. By linearity of expectation and clause-independence we see that for any function w,

$$\mathbf{E}[X] = \sum_{\sigma} \prod_{c} \mathbf{E}[w(\sigma, c)] \ , \tag{4}$$

$$\mathbf{E}[X^2] = \sum_{\sigma,\tau} \prod_{c} \mathbf{E}[w(\sigma, c)\, w(\tau, c)] \ . \tag{5}$$

Since we are interested in random formulas where the literals are drawn uniformly, we will restrict attention to functions that are independent of the variable labels. That is, for every truth assignment σ and every clause $c = \ell_1 \vee \cdots \vee \ell_k$, we require that $w(\sigma, c) = w(\mathbf{v})$, where $v_i = +1$ if ℓ_i is satisfied under σ and -1 if ℓ_i is falsified under σ. With that assumption, (4) and (5) simplify to

$$\begin{aligned} \mathbf{E}[X] &= 2^n \left(\mathbf{E}[w(\sigma, c)]\right)^m \quad , & (6)\\ \mathbf{E}[X^2] &= \sum_{\sigma,\tau} \left(\mathbf{E}[w(\sigma, c)\, w(\sigma, \tau)]\right)^m \quad . & (7) \end{aligned}$$

Let $A = \{-1, +1\}^k$. Since literals are drawn uniformly and independently we see that for every σ,

$$\mathbf{E}[w(\sigma, c)] = \sum_{\mathbf{v} \in A} w(\mathbf{v})\, 2^{-k} \quad .$$

Similarly, for every pair of truth assignments σ, τ with overlap $z = \alpha n$,

$$\begin{aligned} \mathbf{E}[w(\sigma, c)\, w(\sigma, \tau)] &= \sum_{\mathbf{u},\mathbf{v} \in A} w(\mathbf{u}) w(\mathbf{v})\ 2^{-k} \prod_{i=1}^{k} \left(\alpha^{\mathbf{1}_{u_i = v_i}} (1-\alpha)^{\mathbf{1}_{u_i \neq v_i}}\right)\\ &\equiv \sum_{\mathbf{u},\mathbf{v} \in A} w(\mathbf{u}) w(\mathbf{v})\ \Phi_{\mathbf{u},\mathbf{v}}(\alpha)\\ &\equiv f_w(\alpha) \quad . & (8) \end{aligned}$$

In particular, observe that $\mathbf{E}[w(\sigma, c)]^2 = f_w(1/2)$, i.e., for every function w the weights assigned to truth assignments with overlap $n/2$ are independent.

Recalling the approximation $\binom{n}{z} = (\alpha^\alpha (1-\alpha)^{1-\alpha})^{-n} \times \mathrm{poly}(n)$ we see that (7),(8) imply

$$\begin{aligned} \mathbf{E}[X^2] &= 2^n \sum_{z=0}^{n} \binom{n}{z} f_w(z/n)^m & (9)\\ &\leq 2^n \left(\max_{0 \leq \alpha \leq 1} \left[\frac{f_w(\alpha)^r}{\alpha^\alpha (1-\alpha)^{1-\alpha}} \right] \right)^n \times \mathrm{poly}(n)\\ &\equiv \left(\max_{0 \leq \alpha \leq 1} \Lambda_w(\alpha) \right)^n \times \mathrm{poly}(n) \quad . & (10) \end{aligned}$$

Observe that $\Lambda_w(1/2)^n = (4 f_w(1/2)^r)^n = \mathbf{E}[X]^2$. Moreover, we will see later that a more careful analysis of the sum in (9) allows one to replace the polynomial factor in (10) by $O(1)$. Therefore, if $\Lambda_w(1/2)$ is the global maximum of Λ_w then $\mathbf{E}[X^2]/\mathbf{E}[X]^2 = O(1)$ and the second moment method succeeds.

A necessary condition for $\Lambda_w(1/2)$ to be a global maximum is that $\Lambda_w'(1/2) = 0$. Since $\Lambda_w(\alpha) = 2\mathcal{E}(\alpha) f_w(\alpha)^r$ and $\mathcal{E}'(1/2) = 0$, this dictates $f_w'(1/2) = 0$. Differentiating f_w we get

$$\begin{aligned} f_w'(\alpha) &= \sum_{\mathbf{u},\mathbf{v} \in A} w(\mathbf{u}) w(\mathbf{v})\ \Phi_{\mathbf{u},\mathbf{v}}(\alpha)\ \left[\log \Phi_{\mathbf{u},\mathbf{v}}(\alpha)\right]'\\ &= \sum_{\mathbf{u},\mathbf{v} \in A} w(\mathbf{u}) w(\mathbf{v})\ \Phi_{\mathbf{u},\mathbf{v}}(\alpha)\ \sum_{i=1}^{k} \left(\frac{\mathbf{1}_{u_i = v_i}}{\alpha} - \frac{\mathbf{1}_{u_i \neq v_i}}{1-\alpha} \right) \quad . \end{aligned}$$

In particular, letting $\mathbf{u} \cdot \mathbf{v}$ denote the inner product of $\mathbf{u}$ and $\mathbf{v}$, we see that

$$f_w'(1/2) = 2^{-2k+1} \sum_{\mathbf{u},\mathbf{v} \in A} w(\mathbf{u}) w(\mathbf{v})\ \mathbf{u} \cdot \mathbf{v} = 2^{-2k+1} \left(\sum_{\mathbf{u} \in A} w(\mathbf{u}) \mathbf{u} \right) \cdot \left(\sum_{\mathbf{v} \in A} w(\mathbf{v}) \mathbf{v} \right) \quad . \tag{11}$$

Therefore, for any function w

$$f_w'(1/2) = 0 \iff \sum_{\mathbf{v} \in A} w(\mathbf{v}) \mathbf{v} = 0 \quad . \tag{12}$$

We can interpret the vanilla application of the first moment method as using a function $w = w_S$ which assigns 0 to $(-1, \ldots, -1)$ and $1/(2^k - 1)$ to all other vectors. (It is convenient to always normalize w so that

$\sum_{\mathbf{v}} w(\mathbf{v}) = 1$.) The fact that w_S violates the r.h.s. of (12), implies that this attempt must fail. In [1], on the other hand, $w = w_N$ assigns 0 both to $(-1,\ldots,-1)$ and to $(+1,\ldots,+1)$ (and $1/(2^k-2)$ to all other vectors), thus satisfying (12) and enabling the second moment method. Nevertheless, this particular rebalancing of the vectors is rather heavy-handed since it makes it is twice as likely to assign zero to a random clause.

To achieve better results we would like to choose a function w that is "as close as possible" to w_S while satisfying (12). That is, we would like w to have minimal relative entropy with respect to w_S subject to (12) (see Definition 2.15 of [8]). Since w_S is constant over all $\mathbf{v} \neq (-1,\ldots,-1)$ and we must have $w(-1,\ldots,-1) = w_S(-1,\ldots,-1) = 0$, this means that w should have maximum entropy over $\mathbf{v} \neq (-1,\ldots,-1)$ while satisfying (12). So, all in all, we are seeking a maximum-entropy collection of weights for the vectors in A such that i) the all -1s vector has weight 0, ii) the weighted vectors cancel out.

For $\mathbf{x} \in A$, let $|\mathbf{x}|$ denote the number of +1s in $\mathbf{x}$. By summing the r.h.s. of (12) over the coordinates we see that a necessary condition for the optimality of w is

$$\sum_{\mathbf{v}\neq(-1,\ldots,-1)} w(\mathbf{v})(2|\mathbf{v}|-k) = 0 \ . \tag{13}$$

Maximizing entropy subject to (13) is a standard Lagrange multipliers problem. Its unique solution is

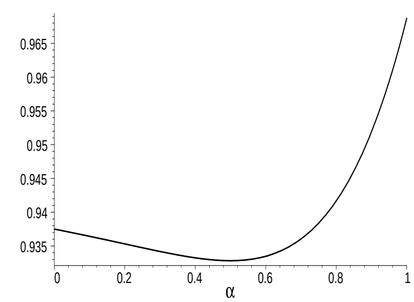
$$w(\mathbf{v}) = \frac{1}{Z}\lambda^{|\mathbf{v}|} \ , \tag{14}$$

where Z is a normalizing constant and λ satisfies $(1+\lambda)^{k-1} = 1/(1-\lambda)$ so that (13) is satisfied, i.e.,

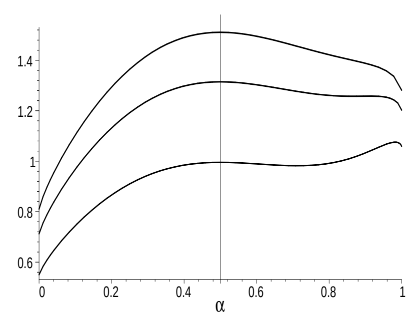
$$\sum_{j=1}^{k}\binom{k}{j}\lambda^j(2j-k) = k\left(1-(1+\lambda)^{k-1}(1-\lambda)\right) = 0 \ . \tag{15}$$

Note now that for w given by (14), symmetry ensures that all coordinates of $\sum_{\mathbf{v}} w(\mathbf{v})\mathbf{v}$ are equal. Since, by (15), the sum over these coordinates vanishes, we see that in fact (12) must hold as well. Therefore, w is indeed the optimal solution for our original problem.

We plot below the functions f_w and Λ_w corresponding to this weighting, for the values of k, r in Figure 1. (With a normalization for $\sum_u w(\mathbf{u})$ which makes the plot scale analogous to that in Figure 1 and which will be more convenient for computing f_w and Λ_w in the next section.)



$f_w(\alpha)$



$\Lambda_w(\alpha) = 2\mathcal{E}(\alpha)f_w(\alpha)^r$

Figure 2: $k = 5$, $r = 14, 16, 20$ (top to bottom).

In conclusion, if $L(\sigma, F)$ denotes the number of satisfied literal occurrences in F under σ, we will take

$$w(\sigma, F) \propto \prod_c \lambda^{L(\sigma,c)}\mathbf{1}_{\sigma\in\mathcal{S}(c)} \ , \tag{16}$$

where $(1+\lambda)^{k-1} = 1/(1-\lambda)$. The above weighting scheme yields Theorem 4, below, which we will prove in Sections 3—6. Theorem 4 has the same leading term as Theorem 2 but a linear correction term 4 times greater. This lost factor of 4 is due to our insistence that $w(\sigma, F)$ factorizes perfectly over the clauses. In Sections 7—9 we go beyond what can be achieved with perfect factorization by performing a truncation. This will allow us to prove Theorem 2 which gives a lower bound for r_k that is within an additive constant of the upper bound for the existence of balanced satisfying assignments.

Theorem 4 *There exists a sequence $\beta_k \to 0$ such that for all $k \geq 3$,*

$$r_k \geq 2^k \log 2 - 2(k+1)\log 2 - 1 - \beta_k \ .$$

3 Groundwork

Given a k-CNF formula F on n variables, recall that $\mathcal{S}(F)$ is the set of satisfying truth assignments of F. Given $\sigma \in \{0,1\}^n$ let $H = H(\sigma, F)$ be the number of satisfied literal occurrences in F under σ less the number of unsatisfied literal occurrences in F under σ. For any $0 < \gamma \leq 1$, let

$$X = \sum_{\sigma} \gamma^{H(\sigma,F)} \mathbf{1}_{\sigma \in \mathcal{S}(F)} \ .$$

(Note that $\gamma^{H(\sigma,F)} = \gamma^{2S(\sigma,F)-km}$, so this is consistent with (16) for $\gamma^2 = \lambda$.)

Recall that in $F_k(n,m)$ the m clauses $\{c_i\}_{i=1}^m$ are i.i.d. random variables, c_i being the conjunction of k i.i.d. random variables $\{\ell_{ij}\}_{j=1}^k$, each ℓ_{ij} being a uniformly random literal. Clearly, in this model a clause may be improper, i.e., it might contain repeated and/or contradictory literals. At the same time, though, observe that the probability that a random clause is improper is smaller than k^2/n and, moreover, the proper clauses are uniformly selected among all proper clauses. Therefore w.h.p. the number of improper clauses is $o(n)$ implying that if for a given r, $F_k(n, rn)$ is satisfiable w.h.p. then for $m = rn - o(n)$, the same is true in the model where we only select among proper clauses. The issue of selecting clauses without replacement is completely analogous as w.h.p. there are $o(n)$ clauses that contain the same k variables as some other clause.

3.1 The first moment

For any fixed truth assignment σ and a random k-clause $c = \ell_1 \vee \cdots \vee \ell_k$, since the literals $\ell_1, \ldots, \ell_k$ are i.i.d. we have

$$\begin{aligned}
\mathbf{E}[\gamma^{H(\sigma,c)} \mathbf{1}_{\sigma \in \mathcal{S}(c)}] &= \mathbf{E}[\gamma^{H(\sigma,c)}] - \mathbf{E}[\gamma^{-k} \mathbf{1}_{\sigma \notin \mathcal{S}(c)}] \\
&= \mathbf{E}\left[\prod_{\ell_i} \gamma^{H(\sigma,\ell_i)}\right] - (2\gamma)^{-k} \\
&= \left(\frac{\gamma + \gamma^{-1}}{2}\right)^k - (2\gamma)^{-k} \\
&\equiv \psi(\gamma) \ .
\end{aligned}$$

Thus, since the $m = rn$ clauses $c_1, c_2, \ldots, c_m$ are i.i.d.

$$\begin{aligned}
\mathbf{E}[X] &= \mathbf{E}\left[\sum_{\sigma} \gamma^{H(\sigma,F)} \mathbf{1}_{\sigma \in \mathcal{S}(F)}\right] \\
&= \sum_{\sigma} \mathbf{E}\left[\prod_{c_i} \gamma^{H(\sigma,c_i)} \mathbf{1}_{\sigma \in \mathcal{S}(c_i)}\right] \\
&= \sum_{\sigma} \prod_{c_i} \mathbf{E}\left[\gamma^{H(\sigma,c_i)} \mathbf{1}_{\sigma \in \mathcal{S}(c_i)}\right] \\
&= \left(2\psi(\gamma)^r\right)^n \ . \qquad (17)
\end{aligned}$$

3.2 The second moment

Let σ, τ be any pair of truth assignments that agree on $z = \alpha n$ variables. If $\ell_1, \ell_2, \dots \ell_k$ are i.i.d. uniformly random literals and $c = \ell_1 \vee \ell_2 \vee \cdots \vee \ell_k$ then

$$\begin{aligned}
\mathbf{E}\left[\gamma^{H(\sigma,\ell_i)+H(\tau,\ell_i)}\right] &= \alpha\left(\frac{\gamma^2+\gamma^{-2}}{2}\right)+1-\alpha \ , \\
\mathbf{E}\left[\gamma^{H(\sigma,\ell_i)+H(\tau,\ell_i)}\mathbf{1}_{\sigma\notin\mathcal{S}(c)}\right] &= 2^{-k}\left(\alpha\gamma^{-2}+(1-\alpha)\right) \ , \\
\mathbf{E}\left[\gamma^{H(\sigma,\ell_i)+H(\tau,\ell_i)}\mathbf{1}_{\sigma,\tau\notin\mathcal{S}(c)}\right] &= 2^{-k}\left(\alpha\gamma^{-2}\right) \ .
\end{aligned}$$

Since $\ell_1, \ell_2, \dots \ell_k$ are i.i.d., writing $\gamma^2 = 1-\varepsilon$, we have

$$\begin{aligned}
\mathbf{E}\left[\gamma^{H(\sigma,c)+H(\tau,c)}\mathbf{1}_{\sigma,\tau\in\mathcal{S}(c)}\right] &= \mathbf{E}\left[\gamma^{H(\sigma,c)+H(\tau,c)}\left(\mathbf{1}-\mathbf{1}_{\sigma\notin\mathcal{S}(c)}-\mathbf{1}_{\tau\notin\mathcal{S}(c)}+\mathbf{1}_{\sigma,\tau\notin\mathcal{S}(c)}\right)\right] \\
&= \mathbf{E}\left[\prod_i \gamma^{H(\sigma,\ell_i)+H(\tau,\ell_i)}\left(\mathbf{1}-\mathbf{1}_{\sigma\notin\mathcal{S}(c)}-\mathbf{1}_{\tau\notin\mathcal{S}(c)}+\mathbf{1}_{\sigma,\tau\notin\mathcal{S}(c)}\right)\right] \\
&= \left(\alpha\left(\frac{\gamma^2+\gamma^{-2}}{2}\right)+1-\alpha\right)^k - 2^{1-k}\left(\alpha\gamma^{-2}+(1-\alpha)\right)^k + 2^{-k}\left(\alpha\gamma^{-2}\right)^k \\
&= \frac{(2-2\varepsilon+\alpha\varepsilon^2)^k - 2(1-\varepsilon+\alpha\varepsilon)^k+\alpha^k}{2^k(1-\varepsilon)^k} && (18) \\
&\equiv \frac{f(\alpha)}{2^k(1-\varepsilon)^k} \ , && (19)
\end{aligned}$$

where the dependence of f on $\varepsilon = 1-\gamma^2$ is implicit. (Taking $\varepsilon = 1-\lambda$ in (18) yields the f_w of Figure 2.)

Thus, for a random k-CNF formula whose $m = rn$ clauses $c_1, c_2, \dots, c_m$ are constructed independently

$$\begin{aligned}
\mathbf{E}[X^2] &= \mathbf{E}\left[\sum_\sigma \gamma^{H(\sigma,F)}\mathbf{1}_{\sigma\in\mathcal{S}(F)}\right]^2 \\
&= \sum_{\sigma,\tau}\mathbf{E}\left[\gamma^{H(\sigma,F)+H(\tau,F)}\mathbf{1}_{\sigma,\tau\in\mathcal{S}(F)}\right] \\
&= \sum_{\sigma,\tau}\mathbf{E}\left[\prod_{c_i}\gamma^{H(\sigma,c_i)+H(\tau,c_i)}\mathbf{1}_{\sigma,\tau\in\mathcal{S}(c_i)}\right] \\
&= \sum_{\sigma,\tau}\prod_{c_i}\mathbf{E}\left[\gamma^{H(\sigma,c_i)+H(\tau,c_i)}\mathbf{1}_{\sigma,\tau\in\mathcal{S}(c_i)}\right] \ . && (20)
\end{aligned}$$

Since the number of ordered pairs of assignments with overlap z is $2^n\binom{n}{z}$ and since the $m = rn$ clauses are identically distributed, (20) and (19) imply

$$\mathbf{E}[X^2] = 2^n\sum_{z=0}^n\binom{n}{z}\left(\frac{f(z/n)}{2^k(1-\varepsilon)^k}\right)^{rn} \ . \tag{21}$$

Observe now that for, any fixed value of ε, f^r is a real, positive and twice-differentiable. Thus, to bound the sum in (21) we can use the following lemma of [1]. The idea is that sums of these type are dominated by the contribution of $\Theta(n^{1/2})$ terms around the maximum term and the proof follows by applying the Laplace method of asymptotic analysis [6].

Lemma 2 *Let ϕ be any real, positive, twice-differentiable function on $[0,1]$ and let*

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

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 exist constants $B, C > 0$ such that for all sufficiently large n

$$B \times g_{\max}^n \ \leq\ S_n \ \leq\ C \times g_{\max}^n \ .$$

With Lemma 2 in mind, let us define

$$g_r(\alpha) = \frac{f(\alpha)^r}{\alpha^\alpha(1-\alpha)^{1-\alpha}} \ . \tag{22}$$

Let

$$s_k = 2^k \log 2 - 2\log 2(k+1) - 1 - 3/k \ .$$

We will prove that

Lemma 3 *Let ε be such that*

$$\varepsilon(2-\varepsilon)^{k-1} = 1 \ . \tag{23}$$

For all $k \geq 22$, if $r \leq s_k$ then $g_r(1/2) > g_r(\alpha)$ for all $\alpha \neq 1/2$, and $g_r''(1/2) < 0$.

As a result, for r, k, ε as in Lemma 3 we have

$$\mathbf{E}[X^2] < C \times \left(\frac{2g_r(1/2)}{(2(1-\varepsilon))^{kr}}\right)^n \ , \tag{24}$$

where $C = C(k)$ is independent of n. Observe now that (17) and the fact $\gamma^2 = 1-\varepsilon$ imply

$$\begin{aligned}
\mathbf{E}[X]^2 &= [(2\psi(\gamma)^r)^n]^2 \\
&= 4^n\left(\frac{f(1/2)}{2^k(1-\varepsilon)^k}\right)^{rn} \\
&= \left(\frac{2g_r(1/2)^n}{(2(1-\varepsilon))^{kr}}\right)^n \ .
\end{aligned} \tag{25}$$

Therefore, by (24) and (25) we see that for r, k, ε as in Lemma 3 we have

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

By Lemma 1, this implies $\mathbf{P}[X > 0] > 1/C$ and, hence, Lemma 3 along with Corollary 1 imply Theorem 4.

To prove Lemma 3 we will prove the following three lemmata. The first lemma holds for any $\varepsilon \in [0,1)$ and reduces the proof to the case $\alpha \geq 1/2$. The second lemma controls the behavior of f (and thus g_r) around $\alpha = 1/2$ and demands the judicious choice of ε specified by (23). We note that this is the only value of ε for which g_r has a local maximum at $1/2$, for any $r > 0$. The third lemma deals with α near 1. That case needs to be handled separately because g_r has another local maximum in that region. The condition $r \leq s_k$ aims precisely at keeping the value of g_r at this other local maximum smaller than $g_r(1/2)$.

Lemma 4 *For all $\varepsilon, x > 0$, $g_r(1/2+x) > g_r(1/2-x)$.*

Lemma 5 *Let ε satisfy (23). For all $k \geq 22$, if $r \leq 2^k \log 2$ then $g_r(1/2) > g_r(\alpha)$ for all $\alpha \in (1/2, 4/5]$ and $g_r''(1/2) < 0$.*

Lemma 6 *Let ε satisfy (23). For all $k \geq 22$, if $r \leq s_k$ then $g_r(1/2) > g_r(\alpha)$ for all $\alpha \in (4/5, 1]$.*

The following bound will be useful. If ε satisfies (23), then

$$2^{1-k} + k4^{-k} < \varepsilon < 2^{1-k} + 3k4^{-k} \ . \tag{26}$$

To prove (26) let $q(x) = x - 1/(2-x)^{k-1}$ and observe that for all $k \geq 3$, the quantity $q(2^{1-k} + ck4^{-k})$ is negative for $c = 1$ but positive for $c = 3$.

4 Proof of Lemma 4

Observe that $\alpha^\alpha(1-\alpha)^{1-\alpha}$ is symmetric around 1/2 and that $r > 0$. Therefore, it suffices to prove that $f(1/2+x) > f(1/2-x)$, for all $x > 0$. To do this we first note that for all $x \neq 0$,

$$\begin{aligned}
2^k f(1/2+x) &= \left((2-\varepsilon)^2 + 2x\varepsilon^2\right)^k - 2\left(2-\varepsilon+2x\varepsilon\right)^k + (1+2x)^k \\
&= \sum_{j=0}^{k} \binom{k}{j} \left[(2-\varepsilon)^{2(k-j)}(2x\varepsilon^2)^j - 2(2-\varepsilon)^{k-j}(2x\varepsilon)^j + (2x)^j\right] \\
&= \sum_{j=0}^{k} \binom{k}{j} (2x)^j \left[(2-\varepsilon)^{2(k-j)}\varepsilon^{2j} - 2(2-\varepsilon)^{k-j}\varepsilon^j + 1\right] \\
&= \sum_{j=0}^{k} \binom{k}{j} (2x)^j [(2-\varepsilon)^{k-j}\varepsilon^j - 1]^2 \ . \qquad (27)
\end{aligned}$$

Thus, for all $x > 0$,

$$f(1/2+x) - f(1/2-x) \ = \ 2^{-k}\sum_{j=0}^{k}\binom{k}{j} 2^j [(2-\varepsilon)^{k-j}\varepsilon^j - 1]^2 (x^j - (-x)^j) \ > \ 0 \ .$$

5 Proof of Lemma 5

We will prove that for all $k \geq 22$ and $r \leq 2^k \log 2$, g_r is strictly decreasing in $(1/2, 4/5]$. We have

$$f'(\alpha) = k\left[(2-2\varepsilon+\alpha\varepsilon^2)^{k-1}\varepsilon^2 - 2(1-\varepsilon+\alpha\varepsilon)^{k-1}\varepsilon + \alpha^{k-1}\right],$$

$$g_r'(\alpha) = \frac{f(\alpha)^{r-1}\left(rf'(\alpha) + f(\alpha)(\log(1-\alpha) - \log\alpha)\right)}{\alpha^\alpha(1-\alpha)^{1-\alpha}} \ . \qquad (28)$$

So, $f'(1/2) = k2^{-k+1}\left((2-\varepsilon)^{k-1}\varepsilon - 1\right)^2$ and since, by (23), we have $(2-\varepsilon)^{k-1}\varepsilon = 1$ we get

$$g_r'(1/2) \ = \ f'(1/2) \ = \ 0 \ . \qquad (29)$$

Since $g_r'(1/2) = 0$ and, by (27), $f(\alpha) > 0$ for all α we see that (28) implies that to prove that g_r is decreasing in $(1/2, 4/5]$ it suffices to prove that the derivative of

$$rf'(\alpha) + f(\alpha)(\log(1-\alpha) - \log\alpha) \qquad (30)$$

is negative in $(1/2, 4/5]$. We will actually prove this claim for $\alpha \in [1/2, 4/5]$. Since $f'(1/2) = 0$ this also establishes our claim that $g_r''(1/2) < 0$. The derivative of (30) is

$$rf''(\alpha) + f'(\alpha)(\log(1-\alpha) - \log\alpha) - f(\alpha)\left(\frac{1}{\alpha} + \frac{1}{1-\alpha}\right) \ . \qquad (31)$$

By considering (27), we see that f is non-decreasing in $[1/2, 1]$. Since $\log(1-\alpha) \leq \log\alpha$ for $\alpha \in [1/2, 1)$, it follows that in order to prove that the expression in (31) is negative it suffices to show that

$$rf''(\alpha) \leq f(\alpha)\left(\frac{1}{\alpha} + \frac{1}{1-\alpha}\right) \ .$$

Since, by definition, $\varepsilon < 1$ it follows that $\alpha\varepsilon^2 \leq 2\varepsilon$ implying that we can bound f'' as

$$\begin{aligned}
f''(\alpha) &= k(k-1)\left((2-2\varepsilon+\alpha\varepsilon^2)^{k-2}\varepsilon^4 - 2(1-\varepsilon+\alpha\varepsilon)^{k-2}\varepsilon^2 + \alpha^{k-2}\right) \\
&\leq k^2\left(2^{k-2}\varepsilon^4 + (4/5)^{k-2}\right) \ . \qquad (32)
\end{aligned}$$

At the same time, $1/\alpha + 1/(1-\alpha) \geq 4$ and $f(\alpha) \geq f(1/2) = 2^{-k}((2-\varepsilon)^k - 1)^2$. Therefore, if ε_u is any upper bound on ε it suffices to establish

$$r \times k^2 \left(2^{k-2}\varepsilon_u^4 + (4/5)^{k-2}\right) \leq 4 \times 2^{-k}((2-\varepsilon_u)^k - 1)^2 \ . \tag{33}$$

Invoking (26) to take $\varepsilon_u = 2^{1-k} + 3k4^{-k}$, it is easy to verify that (33) holds for $k \geq 22$ and $r = 2^k \log 2$. $\square$

Corollary 2 *For all $k \geq 65$, if $r \leq 2^k \log 2$ then $g_r(1/2) > g_r(\alpha)$ for all $\alpha \in (1/2, 9/10]$ and $g_r''(1/2) < 0$.*

Proof. If in (33) we replace 4/5 with 9/10 and take $r = 2^k \log 2$, then the inequality is valid for all $k \geq 65$.

6 Proof of Lemma 6

First observe that the inequality $g_r(1/2) > g_r(\alpha)$ is equivalent to

$$\left(\frac{f(\alpha)}{f(1/2)}\right)^r < 2\alpha^\alpha(1-\alpha)^{1-\alpha} \ . \tag{34}$$

Recall now that, by (27), f is increasing in $(1/2, 1]$ implying $f(\alpha) - f(1/2) > 0$ and that for all $x \geq 0$, $\log(1+x) \leq x$. Thus, the logarithm of the left hand side above can be bounded as

$$\begin{aligned} r\log\left(\frac{f(\alpha)}{f(1/2)}\right) &= r\log\left(1 + \frac{f(\alpha)-f(1/2)}{f(1/2)}\right) \\ &\leq r\left(\frac{f(\alpha)-f(1/2)}{f(1/2)}\right) \ . \end{aligned}$$

So, if we let $h(\alpha) = -\alpha\log\alpha - (1-\alpha)\log(1-\alpha)$ we see that (34) holds if

$$r < (\log 2 - h(\alpha)) \times \frac{f(1/2)}{f(\alpha) - f(1/2)} \ .$$

To get a lower bound on $f(1/2)$ we use the upper bound for ε from (26), yielding

$$\begin{aligned} f(1/2) &= (2 - 2\varepsilon + \varepsilon^2/2)^k - 2(1-\varepsilon/2)^k + (1/2)^k \\ &> (2(1-\varepsilon))^k - 2 \\ &> 2^k(1-k\varepsilon) - 2 \\ &> 2^k(1 - k(2^{1-k} + 3k4^{-k})) - 2 \\ &= 2^k - 2k - 2 - 3k^2 2^{-k} \ . \end{aligned} \tag{35}$$

To get an upper bound on $f(\alpha) - f(1/2)$ we let $\alpha = 1/2 + x$ and consider the sum in (27). By our choice of ε in (23) we see that: i) the term corresponding to $j = 1$ vanishes yielding (36), and ii) for all $j > 1$, $0 < (2-\varepsilon)^{k-j}\varepsilon^j < 1$ yielding (37). That is,

$$f(1/2 + x) = f(1/2) + 2^{-k}\sum_{j=2}^{k}\binom{k}{j}(2x)^j[(2-\varepsilon)^{k-j}\varepsilon^j - 1]^2 \tag{36}$$

$$\leq f(1/2) + 2^{-k}\sum_{j=0}^{k}\binom{k}{j}(2x)^j \tag{37}$$

$$= f(1/2) + \alpha^k \ . \tag{38}$$

Therefore, we see that (34) holds as long as

$$r \leq \frac{\log 2 - h(\alpha)}{\alpha^k} \times f(1/2) \equiv \phi(\alpha) \times f(1/2) \ .$$

We start by getting a lower bound for ϕ for all $\alpha \in (1/2, 1]$. For that, we let $y = 1 - \alpha$ and observe that for all $0 < y \le 1/2$

$$-h(1-y) \;>\; \log(1-y) + y\log y \;>\; -y - y^2 + y\log y \tag{39}$$

and

$$\frac{1}{(1-y)^k} > (1+y)^k > 1 + ky \ .$$

Therefore,

$$\begin{aligned} \phi(1-y) &= \frac{\log 2 - h(1-y)}{(1-y)^k} \\ &> (1+ky)(\log 2 - y(1 + y - \log y)) \ . \end{aligned} \tag{40}$$

Writing $y = d/2^k$ and substituting into (40) we get that for all $1/2 \le \alpha < 1$,

$$\begin{aligned} \phi(\alpha) &= \phi(1 - d2^{-k}) \\ &> \left(1 + kd2^{-k}\right)\left(\log 2 - d2^{-k}\left(1 + d2^{-k} - \log(d2^{-k})\right)\right) \\ &= \log 2 + d(\log d - 1)2^{-k} - \frac{d^2}{4^k}\left(1 + k\left(1 + d2^{-k} - \log(d2^{-k})\right)\right) \\ &\ge \log 2 - 2^{-k} - \frac{d^2}{4^k}\left(1 + k\left(1 + d2^{-k} - \log(d2^{-k})\right)\right) \\ &= \log 2 - 2^{-k} - (1-\alpha)^2\left(1 + k\left(2 - \alpha - \log(1-\alpha)\right)\right) \\ &\equiv b(\alpha) \ . \end{aligned} \tag{41}$$

Since ϕ is differentiable, to bound it in $(4/5, 1]$ it suffices to consider its value at $4/5, 1$ and wherever

$$\phi'(\alpha) = \frac{\alpha\log\alpha - \alpha\log(1-\alpha) - k\log 2 + kh(\alpha)}{\alpha^{k+1}} = 0 \ . \tag{42}$$

We start by observing that for $k \ge 6$

$$\phi'(4/5) < 0 \ .$$

At the other end, we see that

$$\lim_{\alpha\to 1}\frac{\phi'(\alpha)}{\log(1-\alpha)} = -1 \ ,$$

implying that the derivative of ϕ becomes positively infinite as we approach 1. Therefore, we can limit our search to the interior of $(4/5, 1)$ for $k \ge 6$.

By setting ϕ' to zero, (42) gives

$$\log(1-\alpha) = \log\alpha - \frac{k\log 2 - kh(\alpha)}{\alpha}$$

which, since $1/2 < \alpha < 1$, implies

$$\log(1-\alpha) \le -k(\log 2 - h(\alpha)) \ . \tag{43}$$

Moreover, since $\log 2 - h(4/5) > 1/6$, we see that (43) implies $\alpha > 1 - e^{-k/6}$ for all k. Note now that if $\alpha > 1 - e^{-ck}$ for any $c > 0$ then (39) implies $h(\alpha) < e^{-ck}(1 + e^{-ck} + ck)$. Since $\alpha > 1 - e^{-k/6}$, we thus get

$$h(\alpha) \;<\; e^{-k/6}(1 + e^{-k/6} + k/6) \;<\; e^{-k/6}(2 + k/6) \;\equiv\; Q(k) \ . \tag{44}$$

Plugging (44) into (43), we conclude that

$$\alpha > 1 - e^{-k(\log 2 - Q(k))} \equiv \alpha_k^* \ . \tag{45}$$

Since for $k \ge 12$ we have $\alpha_k^* > 4/5$, this means that ϕ is decreasing in $(4/5, \alpha_k^*]$ for $k \ge 12$.

Note now that the function b bounding ϕ from below in (41) is increasing in $[0,1]$. Combined with the fact that ϕ is decreasing in $(4/5, \alpha_k^*]$ this implies that $b(\alpha_k^*)$ is a lower bound for ϕ in $(4/5, 1]$, i.e.,

$$\begin{aligned} \phi(\alpha) &> b(\alpha_k^*) \\ &> \log 2 - 2^{-k} - 2/(k2^k) \ , \end{aligned} \tag{46}$$

where (46) holds for all $k \geq 22$. Combining (46) with (35), we get that for all $k \geq 22$ if

$$r < 2^k \log 2 - 2\log 2(k+1) - 1 - 3/k$$

then $g(1/2) > g(\alpha)$ for all $\alpha \neq 1/2$.

7 Further refinement: truncation and weighting

Given a k-CNF formula F on n variables, recall that $\mathcal{S} = \mathcal{S}(F) \subseteq \{0,1\}^n$ is the set of satisfying truth assignments of F. Recall also that for $\sigma \in \{0,1\}^n$, by $H(\sigma, F)$ we denote the number of satisfied *literal occurrences* in F under σ less the number of unsatisfied literal occurrences. Let $\mathcal{S}^+ = \{\sigma \in \mathcal{S} : H(\sigma, F) \geq 0\}$.

For any $0 < \gamma \leq 1$ let

$$\begin{aligned} X &= \sum_{\sigma \in \mathcal{S}} \gamma^{H(\sigma,F)} \ , \\ X_+ &= \sum_{\sigma \in \mathcal{S}^+} \gamma^{H(\sigma,F)} \ . \end{aligned}$$

In computing the second moment of X in the previous sections, it becomes clear that one needs to control the contribution to $\mathbf{E}[X^2]$ from pairs of truth assignments with high overlap. Close examination of these pairs shows that the dominant contributions come from those pairs amongst them that have *fewer* than half of their literals satisfied. If we compute the second moment of X_+ instead, these highly correlated pairs are avoided. Our argument for this is motivated by Cramer's classical "change of measure" technique in large deviation theory.

Specifically, let $\varepsilon_0 < 1$ satisfy

$$\varepsilon_0 = \frac{1}{(2-\varepsilon_0)^{k-1}} \ . \tag{47}$$

Lemma 7 below asserts that if $\gamma^2 = 1 - \varepsilon_0$, where ε_0 is specified by (47), then the first moments of X and X_+ are comparable.

Lemma 7 *If $\gamma^2 = 1 - \varepsilon_0$ then as $n \to \infty$*

$$\frac{\mathbf{E}[X_+]}{\mathbf{E}[X]} \to 1/2 \ .$$

Let σ, τ be any pair of truth assignments that agree on $z = \alpha n$ variables. If we write $\theta^2 = 1 - \varepsilon$ then from (18) we have

$$\begin{aligned} \mathbf{E}\left[\theta^{H(\sigma,c)+H(\tau,c)} \mathbf{1}_{\sigma,\tau \in \mathcal{S}(c)}\right] &= \frac{(2 - 2\varepsilon + \alpha\varepsilon^2)^k - 2(1 - \varepsilon + \alpha\varepsilon)^k + \alpha^k}{2^k(1-\varepsilon)^k} \\ &\equiv f(\alpha, \varepsilon) \ . \end{aligned} \tag{48}$$

(Observe that the function $f(\alpha, \varepsilon)$ in (48) above is identical to $f(\alpha)(2(1-\varepsilon))^{-k}$, where $f(\alpha)$ is as in (19). In the earlier sections, since ε was fixed, this dependence on ε was suppressed to simplify notation.)

Thus, if F is a random formula consisting of $m = rn$ independent clauses then for any $\theta^2 = 1 - \varepsilon \geq \gamma^2$,

$$\begin{aligned} \mathbf{E}\left[\gamma^{H(\sigma,F)+H(\tau,F)} \mathbf{1}_{\sigma,\tau \in \mathcal{S}^+(F)}\right] &\leq \mathbf{E}\left[\theta^{H(\sigma,F)+H(\tau,F)} \mathbf{1}_{\sigma,\tau \in \mathcal{S}^+(F)}\right] \\ &\leq \mathbf{E}\left[\theta^{H(\sigma,F)+H(\tau,F)} \mathbf{1}_{\sigma,\tau \in \mathcal{S}(F)}\right] \\ &= f(\alpha, \varepsilon)^m \ . \end{aligned} \tag{49}$$

The crucial point is that (49) holds for any $\varepsilon \le 1-\gamma^2$, allowing us to optimize ε with respect to α. In particular if $\gamma^2 = 1-\varepsilon_0$ then (49) implies

$$\mathbf{E}\left[\gamma^{H(\sigma,F)+H(\tau,F)}\mathbf{1}_{\sigma,\tau\in\mathcal{S}^+(F)}\right] \quad\le\quad \left[\inf_{\varepsilon\le\varepsilon_0} f(z/n,\varepsilon)\right]^m \quad .$$

Thus, following the derivation of (21), we deduce that

$$\mathbf{E}[X_+^2] \le 2^n \sum_{z=0}^{n} \binom{n}{z} \left[\inf_{\varepsilon\le\varepsilon_0} f(z/n,\varepsilon)\right]^{rn} \quad . \tag{50}$$

Let us define

$$g_r(\alpha,\varepsilon) = \frac{f^r(\alpha,\varepsilon)}{\alpha^\alpha(1-\alpha)^{1-\alpha}} \quad .$$

Observe that by Lemma 7 and (25),

$$3\mathbf{E}[X_+]^2 > \mathbf{E}[X]^2 = g_r(1/2,\varepsilon_0)^n \quad . \tag{51}$$

Assume now that there exists a piecewise-constant function ξ such that for some value of r we have $g_r(1/2,\varepsilon_0) > g_r(\alpha,\xi(\alpha))$ for all $\alpha \ne 1/2$. Then, by decomposing the sum in (50) along the pieces of ξ and applying Lemma 2 to each piece, we can conclude that $\mathbf{E}[X_+^2] < C \times \mathbf{E}[X_+]^2$, for some $C = C(k)$. Lemma 1 and Corollary 1 then imply $r_k \ge r$.

Let

$$\rho_k = 2^k \log 2 - \frac{\log 2}{2}(k+1) - 1 - 50k^3\,2^{-k} \quad .$$

We will prove

Lemma 8 *Let*

$$\xi(\alpha) = \begin{cases} \varepsilon_0 & \textit{if } \alpha \in [1/10, 9/10] \\ \\ \varepsilon_0/2 & \textit{otherwise.} \end{cases}$$

For all $k \ge 166$, if $r \le \rho_k$ then $g_r(1/2,\varepsilon_0) > g_r(\alpha,\xi(\alpha))$ for all $\alpha \ne 1/2$, and the second derivative of g_r with respect to α is negative at $\alpha = 1/2$.

To prove Lemma 8 we first observe that since ξ is symmetric around 1/2, Lemma 4 implies that we only need to consider the case $\alpha \ge 1/2$. Also, since $\xi(\alpha) = \varepsilon_0$ for $\alpha \in [1/2, 9/10]$, Corollary 2 establishes both our claim regarding the second derivative of g_r at $\alpha = 1/2$ and $g_r(1/2,\varepsilon_0) > g_r(\alpha,\xi(\alpha))$ for $\alpha \in (1/2, 9/10]$. Thus, besides Lemma 7, it suffices to prove that

Lemma 9 *For all $k \ge 166$, if $r \le \rho_k$ then for all $\alpha \in (9/10, 1]$ $g_r(1/2,\varepsilon_0) > g_r(\alpha,\varepsilon_0/2)$.*

8 Proof of Lemma 7

By linearity of expectation, it suffices to prove that for $\gamma^2 = 1-\varepsilon_0$ and every σ

$$\frac{\mathbf{E}[\gamma^{H(\sigma,F)}\mathbf{1}_{\sigma\in\mathcal{S}^+(\mathcal{F})}]}{\mathbf{E}[\gamma^{H(\sigma,F)}\mathbf{1}_{\sigma\in\mathcal{S}(\mathcal{F})}]} \to \frac{1}{2} \quad . \tag{52}$$

Recalling that formulas in our model are sequences of i.i.d. random literals $\ell_1,\ldots,\ell_{km}$, let $\mathbf{P}(\cdot)$ denote the probability assigned by our distribution to any such sequence, i.e., $(2n)^{-km}$. Now, fix any truth assignment σ and consider an auxiliary distribution $\mathbf{P}_\gamma$ on k-CNF formulas where the km literals are again i.i.d., but where now for each fixed literal ℓ

$$\mathbf{P}_\gamma[H(\sigma,\ell)=1] = \frac{\gamma}{\gamma+\gamma^{-1}} \quad .$$

Observe that since $\gamma \le 1$ this probability is at most $1/2$. Thus,

$$\mathbf{E}_\gamma[H(\sigma,\ell)] \;=\; \frac{\gamma-\gamma^{-1}}{\gamma+\gamma^{-1}} \;=\; \frac{\gamma^2-1}{\gamma^2+1} \;=\; \frac{-\varepsilon_0}{2-\varepsilon_0} \;.$$

So, for a random k-clause c

$$\begin{aligned}
\mathbf{E}_\gamma[H(\sigma,c)\mathbf{1}_{\sigma\in\mathcal{S}(c)}] &= \mathbf{E}_\gamma[H(\sigma,c)] - \mathbf{E}_\gamma[-k\mathbf{1}_{\sigma\notin\mathcal{S}(c)}] \\
&= \frac{-k\varepsilon_0}{2-\varepsilon_0} + k\left(\frac{\gamma^{-1}}{\gamma+\gamma^{-1}}\right)^k \\
&= k\left(-\frac{\varepsilon_0}{2-\varepsilon_0} + \left(\frac{1}{2-\varepsilon_0}\right)^k\right) \;.
\end{aligned}$$

Since $\varepsilon_0 = 1/(2-\varepsilon_0)^{k-1}$ we see that $\mathbf{E}_\gamma[H(\sigma,c)\mathbf{1}_{\sigma\in\mathcal{S}(c)}] = 0$.

By literal independence, for any specific clause c_0

$$\mathbf{P}_\gamma(c_0) = \frac{\gamma^{H(\sigma,c_0)}\mathbf{P}(c_0)}{(\gamma+\gamma^{-1})^k} \,. \tag{53}$$

Let $Z(\gamma) = \mathbf{E}_\gamma[\mathbf{1}_{\sigma\in\mathcal{S}(c)}]$ and $Z_1(\gamma) = Z(\gamma)(\gamma+\gamma^{-1})^k$. For any clause c_0, define

$$\widetilde{\mathbf{P}}_\gamma(c_0) = \frac{\mathbf{P}_\gamma(c_0)\mathbf{1}_{\sigma\in\mathcal{S}(c_0)}}{Z(\gamma)} = \frac{\gamma^{H(\sigma,c_0)}\mathbf{P}(c_0)\mathbf{1}_{\sigma\in\mathcal{S}(c_0)}}{Z_1(\gamma)} \;, \tag{54}$$

where the second equality follows from (53). Now pick m i.i.d. clauses with the distribution in (54). Any fixed formula F_0 will be obtained with probability

$$\widetilde{\mathbf{P}}_\gamma(F_0) = \frac{\gamma^{H(\sigma,F_0)}\mathbf{P}(F_0)\mathbf{1}_{\sigma\in\mathcal{S}(F_0)}}{Z_1(\gamma)^m} \;. \tag{55}$$

Since $\widetilde{\mathbf{E}}_\gamma[H(\sigma,c)] = 0$, the central limit theorem yields,

$$\widetilde{\mathbf{P}}_\gamma[H(\sigma,F) \ge 0] \to \frac{1}{2}$$

as $n \to \infty$. By (55), this is equivalent to (52).

9 Proof of Lemma 9

Write $\varepsilon_1 = \varepsilon_0/2$ (to simplify notation). Observe that the inequality $g_r(1/2,\varepsilon_0) > g_r(\alpha,\varepsilon_1)$ is equivalent to

$$\left(\frac{f(\alpha,\varepsilon_1)}{f(1/2,\varepsilon_0)}\right)^r < 2\alpha^\alpha(1-\alpha)^{1-\alpha} \;. \tag{56}$$

If $h(\alpha) = -\alpha\log\alpha - (1-\alpha)\log(1-\alpha)$ denotes the entropy function, then (56) is equivalent to

$$r < \frac{\log 2 - h(\alpha)}{\log(1+w)} \;,$$

where

$$w = \frac{f(\alpha,\varepsilon_1) - f(1/2,\varepsilon_0)}{f(1/2,\varepsilon_0)} \;.$$

We will prove $f(\alpha,\varepsilon_1) - f(1/2,\varepsilon_0) < 2^{1-k}$. Therefore, recalling that for all $x > -1$,

$$\frac{1}{\log(1+x)} \ge \frac{1}{x} + \frac{1}{2} - \frac{x}{12} \;,$$

we see that (56) holds if

$$\frac{r}{\log 2 - h(\alpha)} < \frac{f(1/2,\varepsilon_0)}{f(\alpha,\varepsilon_1) - f(1/2,\varepsilon_0)} + \frac{1}{2} - \frac{1}{2^k f(1/2,\varepsilon_0)} \ . \tag{57}$$

To get a lower bound on $f(1/2,\varepsilon_0)$ we use the upper bound for ε_0 from (26). Thus, for all $k \geq 5$

$$\begin{aligned} 2^k f(1/2,\varepsilon_0) &= \frac{(2-2\varepsilon_0+\varepsilon_0^2/2)^k - 2(1-\varepsilon_0/2)^k + (1/2)^k}{(1-\varepsilon_0)^k} \\ &> \frac{(2-2\varepsilon_0)^k - 2}{(1-\varepsilon_0)^k} \\ &= 2^k - \frac{2}{(1-\varepsilon_0)^k} \\ &> 2^k - 2 - 2(1+k\varepsilon_0) \\ &> 2^k - 2 - k2^{-k+1} \ . \end{aligned} \tag{58}$$

To get an upper bound on the numerator of w we let $\alpha = 1/2 + x$ and consider the sum in (27) (recall that (27) holds for all ε and that $f(\alpha)$ in (27) is merely $2^k(1-\varepsilon)^k f(\alpha,\varepsilon)$). First, we observe that for all $\varepsilon \in [0,1)$,

$$\begin{aligned} 2^k(1-\varepsilon)^k f(\alpha,\varepsilon) &= 2^{-k}\sum_{j=0}^{k}\binom{k}{j}(2\alpha-1)^j[(2-\varepsilon)^{k-j}\varepsilon^j - 1]^2 \\ &\equiv T_2(\alpha,\varepsilon) + 2^{-k}\sum_{j=2}^{k}\binom{k}{j}(2\alpha-1)^j[(2-\varepsilon)^{k-j}\varepsilon^j - 1]^2 \\ &\leq T_2(\alpha,\varepsilon) + 2^{-k}\sum_{j=2}^{k}\binom{k}{j}(2\alpha-1)^j \\ &= T_2(\alpha,\varepsilon) + \alpha^k - k2^{-k}(2\alpha-1) - 2^{-k} \ . \end{aligned} \tag{59}$$

Next, we will prove that

$$\begin{aligned} \frac{T_2(\alpha,\varepsilon_1)}{2^k(1-\varepsilon_1)^k} - f(1/2,\varepsilon_0) &= \frac{\left((2-\varepsilon_1)^k - 1\right)^2}{4^k(1-\varepsilon_1)^k} + \frac{k(2\alpha-1)\left((2-\varepsilon_1)^{k-1}\varepsilon_1 - 1\right)^2}{4^k(1-\varepsilon_1)^k} - \frac{\left((2-\varepsilon_0)^k - 1\right)^2}{4^k(1-\varepsilon_0)^k} \\ &< \alpha k 2^{-2k-1}(1-\varepsilon_0)^{-k-1} \ . \end{aligned} \tag{60}$$

For this, define $\Upsilon_1(\varepsilon) = 1 - (2-\varepsilon)^{k-1}\varepsilon$ so that $\Upsilon_1(\varepsilon_0) = 0$. For $\varepsilon < \varepsilon_0$ we infer that

$$0 < \Upsilon_1(\varepsilon) \leq 1 - (2-\varepsilon_0)^{k-1}\varepsilon = 1 - \varepsilon/\varepsilon_0 \ . \tag{61}$$

Therefore, the function

$$\Upsilon_2(\varepsilon) = \frac{k(2\alpha-1)\Upsilon_1(\varepsilon)^2}{(1-\varepsilon)^k}$$

satisfies

$$\Upsilon_2(\varepsilon_1) \leq \frac{k(2\alpha-1)}{4(1-\varepsilon_1)^k} < \frac{k(\alpha-1/2)}{2(1-\varepsilon_0)^{k+1}} \ . \tag{62}$$

Next, define

$$\Upsilon_3(\varepsilon) = \frac{\left((2-\varepsilon)^k - 1\right)^2}{(1-\varepsilon)^k} \ .$$

Differentiation gives

$$-\Upsilon_3'(\varepsilon) \ = \ k\frac{(2-\varepsilon)^k - 1}{(1-\varepsilon)^{k+1}}\,\Upsilon_1(\varepsilon) \ \leq \ k\left(\frac{2-\varepsilon}{1-\varepsilon}\right)^k \frac{\Upsilon_1(\varepsilon)}{1-\varepsilon_0} \ .$$

Since $\frac{2-\varepsilon}{1-\varepsilon}$ is increasing in ε, we deduce using (61) that for $\varepsilon < \varepsilon_0$,

$$-\Upsilon_3'(\varepsilon) \le k\frac{(2-\varepsilon_0)^k}{(1-\varepsilon_0)^{k+1}}\left(1-\frac{\varepsilon}{\varepsilon_0}\right) .$$

As $\int_{\varepsilon_1}^{\varepsilon_0}(1-\varepsilon/\varepsilon_0)\, d\varepsilon = \varepsilon_0/8$, we conclude that

$$\Upsilon_3(\varepsilon_1) - \Upsilon_3(\varepsilon_0) \le k\frac{(2-\varepsilon_0)^k\varepsilon_0}{8(1-\varepsilon_0)^{k+1}} \le \frac{k}{4(1-\varepsilon_0)^{k+1}} . \tag{63}$$

Adding the inequalities (62) and (63), then dividing by 4^k, yields (60).

Combining (59) and (60) and requiring $k \ge 6$ for (64) we get

$$\begin{aligned}
f(\alpha,\varepsilon_1) - f(1/2,\varepsilon_0) &< \frac{T_2(\alpha,\varepsilon_1) + \alpha^k - k2^{-k}(2\alpha-1) - 2^{-k}}{2^k(1-\varepsilon_1)^k} - f(1/2,\varepsilon_0) \\
&< \frac{\alpha k 2^{-2k-1}}{(1-\varepsilon_0)^{k+1}} + \frac{\alpha^k - k2^{-k}(2\alpha-1) - 2^{-k}}{2^k(1-\varepsilon_1)^k} \\
&= \frac{\alpha^k - \alpha k 2^{-k-1}\left(4 - \frac{(1-\varepsilon_1)^k}{(1-\varepsilon_0)^{k+1}}\right) + 2^{-k}(k-1)}{2^k(1-\varepsilon_1)^k} \\
&< \frac{\alpha^k - \alpha k 2^{-k-1}\left(3 - k2^{-k+1}\right) + 2^{-k}(k-1)}{2^k(1-\varepsilon_1)^k} &(64) \\
&< \frac{\alpha^k - 3\alpha k 2^{-k-1} + 2^{-k}(k-1) + 4^{-k}k^2}{2^k(1-\varepsilon_1)^k} \quad . &(65)
\end{aligned}$$

Observe now that for $k \ge 3$ (65) establishes our promised claim $f(\alpha,\varepsilon_1) - f(1/2,\varepsilon_0) < 2^{-k+1}$. Moreover, combining (58) and (65) we get (66), while the fact $\alpha > 9/10$ implies (67)

$$\begin{aligned}
\frac{f(1/2,\varepsilon_0)}{f(\alpha,\varepsilon_1) - f(1/2,\varepsilon_0)} &> (1-\varepsilon_1)^k \times \frac{2^k - 2 - k2^{-k+1}}{\alpha^k - 3\alpha k 2^{-k-1} + 2^{-k}(k-1) + k^2 4^{-k}} &(66) \\
&> (1-\varepsilon_1)^k \times \frac{2^k - 2}{\alpha^k - 3\alpha k 2^{-k-1} + 2^{-k}(k-1)} - (2/3)^k \quad . &(67)
\end{aligned}$$

Recall now that for any $0 < \alpha < 1$ and $0 \le q < \alpha^k$,

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

Observe that $3\alpha k 2^{-k-1} - 2^{-k}(k-1) < \alpha^k$ for $\alpha \ge 2/3$. Since $\alpha > 9/10$, we thus have

$$\frac{1}{\alpha^k - 3\alpha k 2^{-k-1} + 2^{-k}(k-1)} \ge 1 + k(1-\alpha) + 3\alpha k 2^{-k-1} - 2^{-k}(k-1) \quad .$$

Thus, by (57),(58) and (67) we see that (56) holds as long as $r < (1-\varepsilon_1)^k\phi(\alpha) - 2 \times (2/3)^k$ where

$$\phi(\alpha) \equiv \big(\log 2 - h(\alpha)\big)\left(2^k(k+1) - 3k - \frac{1}{2} - \alpha k\left(2^k - \frac{7}{2}\right)\right) .$$

We are thus left to minimize ϕ in $(9/10, 1]$. It will be convenient to define

$$\begin{aligned}
B &= 2^k(k+1) - 3k - \frac{1}{2} &(68) \\
C &= k\left(2^k - \frac{7}{2}\right) &(69)
\end{aligned}$$

and rewrite

$$\phi(\alpha) = \big(\log 2 - h(\alpha)\big)\,(B - \alpha C) \ .$$

Since ϕ is differentiable its minima can only occur at $9/10, 1$ or where

$$\phi'(\alpha) = \log\left(\frac{\alpha}{1-\alpha}\right)(B - \alpha C) - (\log 2 - h(\alpha))\,C = 0 \ . \tag{70}$$

Note now that

$$\lim_{\alpha\to 1} \frac{\phi'(\alpha)}{\log(1-\alpha)} = -(B - C) < 0$$

and, thus, the derivative of ϕ becomes positively infinite as we approach 1. At the same time,

$$\phi'(9/10) < 2.2B - 2.3C$$

which is negative for $k \geq 23$. Therefore, ϕ is minimized in the interior of $(9/10, 1]$ for all $k \geq 23$. Setting the derivative of ϕ to zero gives

$$\begin{aligned} -\log(1-\alpha) &= (\log 2 - h(\alpha)) \times \frac{C}{B - \alpha C} - \log\alpha \\ &= (\log 2 - h(\alpha)) \times \frac{k}{1 + k(1-\alpha) + \frac{k+6}{2^{k+1}-7}} - \log\alpha \ . \end{aligned} \tag{71}$$

By "bootstrapping" we will derive a tightening series of bounds on the solution of (71) in $\alpha \in (9/10, 1)$. Note first that we have an easy upper bound,

$$-\log(1-\alpha) < k\log 2 - \log\alpha \ . \tag{72}$$

At the same time, if $k \geq 3$ then $(k+6)/(2^{k+1}-7) \leq 1$, implying

$$-\log(1-\alpha) \geq \frac{k\,(\log 2 - h(\alpha))}{2 + k(1-\alpha)} - \log\alpha \ . \tag{73}$$

If we write $k(1-\alpha) = D$ then (73) becomes

$$-\log(1-\alpha) \geq \frac{\log 2 - h(\alpha)}{1-\alpha}\left(\frac{D}{D+2}\right) - \log\alpha \ . \tag{74}$$

By inspection, if $D \geq 3$ the r.h.s. of (74) is greater than the l.h.s. for all $\alpha > 9/10$, yielding a contradiction. Therefore, $k(1-\alpha) < 3$ for all $k \geq 3$. Since $\log 2 - h(\alpha) > 0.36$ for $\alpha > 9/10$, we see that for $k \geq 3$, (73) implies

$$-\log(1-\alpha) \quad > \quad 0.07\,k \qquad \text{or, equivalently,} \tag{75}$$

$$1-\alpha \quad < \quad \mathrm{e}^{-0.07\,k} \ . \tag{76}$$

Observe now that (76) implies

$$k(1-\alpha) < k\,\mathrm{e}^{-0.07k} \ , \tag{77}$$

and, hence, as k increases the denominator of (71) actually approaches 1.

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

$$\begin{aligned} h(\alpha) &\leq -2(1-\alpha)\log(1-\alpha) & (78)\\ &< 2\,\mathrm{e}^{-0.07\,k}(k\log 2 - \log 0.9) & (79)\\ &< 2\,k\,\mathrm{e}^{-0.07\,k} & (80) \end{aligned}$$

where (79) relies on (76) and (72). Moreover, $\alpha > 1/2$ implies $-\log\alpha \le 2(1-\alpha)$ which, by (76) implies $-\log\alpha < 2\,\mathrm{e}^{-0.07\,k}$. Thus, starting with (71), using (77), taking $k \ge 3$ and using (80), and finally using $1/(1+x) > 1-x$ for all $x > 0$ we get

$$\begin{aligned} -\log(1-\alpha) &> \frac{k\,(\log 2 - h(\alpha))}{1 + k\,\mathrm{e}^{-0.07\,k} + \frac{k+6}{2^{k+1}-7}} \\ &> \frac{k\,(\log 2 - 2\,k\,\mathrm{e}^{-0.07\,k})}{1 + 2\,k\,\mathrm{e}^{-0.07\,k}} \\ &> k\,(\log 2 - 2\,k\,\mathrm{e}^{-0.07\,k})(1 - 2\,k\,\mathrm{e}^{-0.07\,k}) \\ &> k \log 2 - 4\,k^2\,\mathrm{e}^{-0.07\,k} \quad . \end{aligned} \tag{81}$$

For $k \ge 166$, $4\,k^2\,\mathrm{e}^{-0.07\,k} < 1$. Thus, for such k, (81) implies $1-\alpha < 3 \times 2^{-k}$. This, in turn, implies $-\log\alpha \le 2(1-\alpha) < 6 \times 2^{-k}$ and so, by (78) and (72), we have that for all $k \ge 166$ and $\alpha > 9/10$

$$h(\alpha) < 6 \times 2^{-k}(k\log 2 - \log\alpha) < 5\,k\,2^{-k} \quad . \tag{82}$$

Plugging (82) into (71) to bootstrap again, we get (analogously to the derivation of(81)) that

$$\begin{aligned} -\log(1-\alpha) &> \frac{k\,(\log 2 - 5\,k\,2^{-k})}{1 + 3\,k\,2^{-k} + \frac{k+6}{2^{k+1}-7}} \\ &> \frac{k\,(\log 2 - 5\,k\,2^{-k})}{1 + 6\,k\,2^{-k}} \\ &> k\,(\log 2 - 5\,k\,2^{-k})(1 - 6\,k\,2^{-k}) \\ &> k\log 2 - 11\,k^2\,2^{-k} \quad . \end{aligned}$$

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

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

Plugging into (72) the fact $-\log\alpha < 6 \times 2^{-k}$ we get $-\log(1-\alpha) < k\log 2 + 6 \times 2^{-k}$. Using that $\mathrm{e}^{-x} \ge 1 - x$ for $x \ge 0$, we get the closely matching upper bound,

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

Thus, we see that for $k \ge 166$, 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

$$\phi(1-2^{-k}) - \delta \times \max_{\alpha\in T} |\phi'(\alpha)| \quad .$$

Using very crude bounds, it is easy to see from (70) that if $\alpha \in T$ then $|\phi'(\alpha)| \le 2\,k\,2^k$.

Now, since for $k \ge 1$ we have $\log(1-2^{-k}) > -2^{-k} - 2^{-2k}$, a simple calculation gives

$$\phi(1-2^{-k}) > 2^k \log 2 + \frac{\log 2}{2}(k-1) - 1 - 2k^2\,2^{-k} \quad . \tag{83}$$

Therefore,

$$\phi_{\min} > 2^k \log 2 + \frac{\log 2}{2}(k-1) - 1 - 46\,k^3\,2^{-k} \quad .$$

Finally, recall that (56) holds as long as $r < (1-\varepsilon_1)^k\phi_{\min} - 2 \times (2/3)^k$. Using the upper bound for ε_0 from (26) we get

$$\begin{aligned} (1-\varepsilon_1)^k \times \phi_{\min} &> \left(1 - 2^{-k} - \frac{2k}{4^k}\right)^k \times \left(2^k\log 2 + \frac{\log 2}{2}(k-1) - 1 - \frac{46k^3}{2^k}\right) \\ &> \left(1 - k2^{-k} - \frac{2k^2}{4^k}\right) \times \left(2^k\log 2 + \frac{\log 2}{2}(k-1) - 1 - \frac{46k^3}{2^k}\right) \\ &> 2^k\log 2 - \frac{\log 2}{2}(k+1) - 1 - \frac{50k^3}{2^k} \\ &= \rho_k \quad . \end{aligned}$$

10 Bounds for specific values of k

Recall from our discussion in Section 3 that in order to establish $r \geq r_k$ it suffices to prove that there exists some $\varepsilon \in [0, 1)$ for which the function g_r defined in (22), i.e.,

$$g_r(\alpha) = \frac{f(\alpha)^r}{\alpha^\alpha(1-\alpha)^{1-\alpha}} = \frac{\left((2 - 2\varepsilon + \alpha\varepsilon^2)^k - 2(1 - \varepsilon + \alpha\varepsilon)^k + \alpha^k\right)^r}{\alpha^\alpha(1-\alpha)^{1-\alpha}} \ , \tag{84}$$

has a unique global maximum at 1/2. Recall also that for any r the only choice of ε for which $g_r''(1/2) < 0$ is the one mandated by (23). Thus, for any fixed k one can get a lower bound for r_k by: i) solving (23), ii) substituting the solution to (84), and iii) plotting the resulting function to check whether $g_r(1/2) > g_r(\alpha)$ for all $\alpha \neq 1/2$. As g_r never has more than three local maxima this is very straightforward and yields the lower bounds referred to as "simple" lower bounds in Table 10 below.

As mentioned in the Introduction, the simple weighting scheme yielding Theorem 4 does not yield the best possible lower bound afforded by applying the second moment method to balanced satisfying assignments. For that, one has to use the significantly more refined argument which we presented in Sections 7—9. That argument also eventually reduces to proving $g_r(1/2) > g_r(\alpha)$ for all $\alpha \neq 1/2$. Now, though, ε is allowed to depend on α, subject only to $\varepsilon \leq \varepsilon_0$, where ε_0 is the solution of (23). Naturally, at $\alpha = 1/2$ one still has to take $\varepsilon = \varepsilon_0$ so that the derivative of g_r vanishes, but for larger α (where the danger is) it turns out that decreasing ε somewhat helps. The bounds reported in Table 1 in the Introduction (and replicated below as the "refined" bounds) are, indeed, the result of such optimization of ε as a function of α.

Specifically, for $k \leq 5$ we considered 10,000 equally spaced values of $\alpha \in [0, 1]$ and for each such value found $\varepsilon \leq \varepsilon_0$ such that the condition $g_r(\alpha, \varepsilon) < g_r(1/2, \varepsilon_0)$ holds with a bit of room. (For $k > 4$ we solved (23), defining ε_0, numerically to 10 digits of accuracy. For the optimization we exploited convexity to speed up the search.) Having determined such values of ε, we (implicitly) assigned to every not-chosen point in $[0, 1]$ the value of ε at the nearest chosen point. Finally, we computed a (crude) upper bound on the derivative of g_r with respect to α in $[0, 1]$. This bound on the derivative, along with our room factor, then implied that for every point that we did not check, the value of g_r was sufficiently close to its value at the corresponding chosen point to also be dominated by $g_r(1/2, \varepsilon_0)$. For $k > 5$, we only partitioned $[0, 1]$ into two intervals, namely $[1/10, 9/10]$ and its complement. Assigning the values ε_0 and $\varepsilon_0/2$, respectively, to all the points in each interval yielded the bounds for such k.

k	3	4	5	7	10	20	21
Upper bound	4.51	10.23	21.33	87.88	708.94	726,817	1,453,635
Refined lower bound	2.68	7.91	18.79	84.82	704.94	726,809	1,453,626
Simple lower bound	2.54	7.31	17.61	82.63	701.53	726,802	1,453,619

11 Conclusions

We proved that the random k-SAT threshold satisfies $r_k \sim 2^k \log 2$. In particular, we proved that random k-CNF formulas with density $2^k \log 2 - k(\log 2)/2 - O(1)$ have exponentially many balanced satisfying truth assignments. That is, truth assignments that have at least one satisfied literal in every clause yet, in total, satisfy only as many literal occurrences as a random truth assignment.

Our argument leaves a gap of order $\Theta(k)$ with the first moment upper bound $2^k \log 2$. With respect to this gap it is worth pointing out that the best known techniques [9, 19] for improving this upper bound only give $r_k \leq 2^k \log 2 - b_k$ where $b_k \to (1 + \log 2)/2$. At the same time, it is not hard to prove that for $r = 2^k \log 2 - k(\log 2)/2$, i.e., within an additive constant from our lower bound, w.h.p. there are no satisfying truth assignments that satisfy only $km/2 + o(km)$ literal occurrences. Thus, any asymptotic improvement over our lower bound would mean that tendencies toward the majority assignment become essential as we approach the threshold.

The gap between the upper bound and the best algorithmic lower bound $r_k = \Omega(2^k/k)$, seems to us much more significant (and is certainly much bigger!). The lack of progress in the last ten years suggests the possibility that no polynomial time algorithm can improve the lower bound asymptotically. At the same time, in a completely different direction, Mézard and Zecchina [21] recently used the non-rigorous cavity method of statistical physics to obtain detailed predictions for the satisfiability threshold suggesting that $r_k = 2^k \log 2 - O(1)$. (See also [20] for an overview.) Insights from this analysis led them to an intriguing algorithm called "survey propagation" (described in [21, 2]) that seems to perform well on random instances of k-SAT close to the threshold, at least for small k. (Its performance is especially impressive for $k = 3$.) A rigorous analysis of this algorithm is still lacking, though, and it remains unclear whether its success for values of r close to the threshold extends to large k.

The success of the second moment method for balanced satisfying truth assignments suggests that such assignments form a "mist" in $\{0,1\}^n$ and, as a result, they might be hard to find by algorithms based on local updates. Moreover, as k increases the influence exerted by the majority vote assignment becomes less and less significant as most literals occur very close to their expected $kr/2$ times. As a result, the structure of the space of solutions may well be different for small k (e.g. $k = 3, 4$) and for larger k.

To summarize, the following key questions remain:

1. Is $2^k \log 2 - r_k$ bounded?
2. Is there an **algorithmic threshold** $\lambda_k = o(2^k)$ so that for $r > \lambda_k$, no polynomial-time algorithm can find a satisfying truth assignment for the random formula $F_k(n, rn)$ with uniformly positive probability?

Acknowledgments

We are grateful to Cris Moore for illuminating conversations and to Mike Molloy for helpful comments. We are indebted to Chris Calabro for a careful reading and for a correction to a previous version of this paper. Part of this work was done while the authors participated in the focused research group on discrete probability at BIRS, July 12-26, 2003.

References

[1] D. Achlioptas and C. Moore. The asymptotic order of the random k-SAT threshold. In *Proc. 43th Annual Symposium on Foundations of Computer Science*, pages 126–127, 2002.

[2] A. Braunstein, M. Mézard, and R. Zecchina. Survey propagation: an algorithm for satisfiability. Preprint, 2002.

[3] 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(3):289–314, 1990.

[4] P. Cheeseman, B. Kanefsky, and W. Taylor. Where the really hard problems are. In *Proc. 12th International Joint Conference on Artificial Intelligence (IJCAI-91) Vol. 1*, pages 331–337, 1991.

[5] V. Chvátal and B. Reed. Mick gets some (the odds are on his side). In *Proc. 33th Annual Symposium on Foundations of Computer Science*, pages 620–627, 1992.

[6] N. G. de Bruijn. *Asymptotic methods in analysis.* Dover Publications Inc., New York, 3rd edition, 1981.

[7] A. Dembo, Y. Peres, J. Rosen and O. Zeitouni. Thick points for planar Brownian motion and the Erdős-Taylor conjecture on random walk. *Acta Math.*, 186:239–270, 2001.

[8] A. Dembo and O. Zeitouni. *Large deviations techniques and applications.* Springer Verlag, New York, 2nd edition, 1998.

[9] O. Dubois and Y. Boufkhad. A general upper bound for the satisfiability threshold of random r-SAT formulae. *J. Algorithms*, 24(2):395–420, 1997.

[10] O. Dubois, Y. Boufkhad, and J. Mandler. Typical random 3-SAT formulae and the satisfiability threshold. In *Proc. 11th Annual Symposium on Discrete Algorithms*, pages 126–127, 2000.

[11] P. Erdős and L. Lovász. Problems and results on 3-chromatic hypergraphs and some related questions. Colloq. Math. Soc. János Bolyai, Vol. 10, 609–627.

[12] P. Erdős and S. J. Taylor. Some problems concerning the structure of random walk paths. *Acta Sci. Hung.* 11:137–162, 1960.

[13] J. Franco and M. Paull. Probabilistic analysis of the Davis–Putnam procedure for solving the satisfiability problem. *Discrete Appl. Math.*, 5(1):77–87, 1983.

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

[15] A. M. Frieze and S. Suen. Analysis of two simple heuristics on a random instance of k-SAT. *J. Algorithms*, 20(2):312–355, 1996.

[16] A. Frieze and N. C. Wormald. Random k-SAT: a tight threshold for moderately growing k. In *Proc. 5th International Symposium on Theory and Applications of Satisfiability Testing*, pages 1–6, 2002.

[17] S. Janson, Y. C. Stamatiou, and M. Vamvakari. Bounding the unsatisfiability threshold of random 3-SAT. *Random Structures Algorithms*, 17(2):103–116, 2000.

[18] A. Kaporis, L. M. Kirousis, and E. G. Lalas. The probabilistic analysis of a greedy satisfiability algorithm. In *Proc. 10th Annual European Symposium on Algorithms*, volume 2461 of *Lecture Notes in Computer Science*, pages 574–585. Springer, 2002.

[19] L. M. Kirousis, E. Kranakis, D. Krizanc, and Y. Stamatiou. Approximating the unsatisfiability threshold of random formulas. *Random Structures Algorithms*, 12(3):253–269, 1998.

[20] M. Mézard, G. Parisi, and R. Zecchina. Analytic and Algorithmic Solution of Random Satisfiability Problems. *Science*, 297: 812-815, 2002.

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

[22] D. G. Mitchell, B. Selman, and H. J. Levesque. Hard and easy distributions of SAT problems. In *Proc. 10th National Conference on Artificial Intelligence*, pages 459–462, 1992.

[23] R. Monasson and R. Zecchina. Statistical mechanics of the random K-satisfiability model. *Phys. Rev. E (3)*, 56(2):1357–1370, 1997.

[24] I. Stewart. Where drunkards hang out. *Nature*, News and Views, October 18, 2001.