Sharp thresholds and the partition function

Amin Coja-Oghlan\textsuperscript{1} and Daniel Reichman\textsuperscript{2}

\textsuperscript{1} Goethe University, Mathematics Institute, 10 Robert Mayer St, Frankfurt 60325, Germany
\textsuperscript{2} The Weizmann Institute, Rehovot, Israel

E-mail: acoghlan@math.uni-frankfurt.de, daniel.reichman@gmail.com

Abstract. Let $\Phi$ be a random $k$-CNF formula over $n$ variables with $m = r \cdot n$ clauses and let $Z(\Phi)$ be the number of satisfying assignments. Assume that $k$ is sufficiently large and that $r \leq \left(1 - o_k(1)\right)2^k \ln(k)/k$, where $o_k(1)$ denotes a certain function that tends to 0 as $k$ gets large. We prove that in this case, $\Phi$ is satisfiable with probability 1 $O(1/n)$. Together with a recent result of Abbe and Montanari\textsuperscript{[arXiv:1006.3786]}, this implies that for such $k, r$ the limit $\lim_{n \to \infty} \frac{1}{n} \mathbb{E}[\ln(1 + Z(\Phi))]$ exists. The existence of this limit is related to the existence of a sharp threshold for satisfiability.

1. Introduction

Let $k \geq 3$, let $V = V_n = \{x_1, \ldots, x_n\}$ be a set of $n$ propositional variables and let $\Phi = \Phi_k(n, m)$ be a random $k$-CNF with $m$ clauses over the variables $V$, chosen uniformly from the set of all $(2n)^{km}$ such formulas. Unless specified otherwise, we assume that $m = \lceil r n \rceil$ for a number $r > 0$ that remains fixed as $n \to \infty$. We say that $\Phi$ has some property $\mathcal{A}$ with high probability ("w.h.p.") if $\lim_{n \to \infty} P[\Phi \in \mathcal{A}] = 1$.

One of the best-known open problems in the theory of random constraint satisfaction problems is the satisfiability threshold conjecture (e.g.,\textsuperscript{[6, 20]}). It states that for any $k \geq 3$ there exists a satisfiability threshold $r_k^*$ such that for any density $r < r_k^*$ (that remains fixed as $n \to \infty$), the random formula $\Phi$ is satisfiable w.h.p., while $\Phi$ is unsatisfiable w.h.p. for any $r > r_k^*$.

Although this conjecture remains open, Friedgut\textsuperscript{[13]} proved that for any $k \geq 3$ there exists a sharp threshold sequence $r_k(n)$ such that for any (fixed) $\varepsilon > 0$, the following is true:

- if $m/n < r_k(n) - \varepsilon$, then $\Phi$ is satisfiable w.h.p.
- if $m/n > r_k(n) + \varepsilon$, then $\Phi$ is unsatisfiable w.h.p.

The issue is that the sequence $r_k(n)$ is not known to converge. Thus, Friedgut’s result allows for the possibility that the density at which the satisfiability probability drops from $1 - o(1)$ to $o(1)$ varies with $n$.

Over the past decade, properties of random $k$-CNF formulas have been studied via sophisticated, albeit non-rigorous methods from statistical physics\textsuperscript{[21, 23, 25, 26]}. A key quantity of interest in these methods is the partition function, i.e., the number $Z(\Phi)$ of satisfying assignments. More precisely, because in the satisfiable regime $Z(\Phi)$ scales exponentially in $n$, it is natural to consider the “quenched average” $\frac{1}{n} \mathbb{E}[\ln(1 + Z(\Phi))]$, where we add 1 inside the logarithm because $Z(\Phi)$ might be equal to zero. The limit

$$\phi_k(r) = \lim_{n \to \infty} \frac{1}{n} \mathbb{E}[\ln(1 + Z(\Phi))]$$

(1)
is referred to as the free entropy density [24].

A priori the limit (1) may not exist for all \( r > 0 \). However, Abbe and Montanari [1] proved (among other things) the following sufficient condition for the existence of \( \phi_k(r) \).

**Theorem 1.1** ([1]) Suppose that \( k \geq 3 \) and \( r > 0 \) are such that for some number \( \varepsilon = \varepsilon(k, r) > 0 \) we have

\[
P[\Phi \text{ is satisfiable}] \geq 1 - O(\ln^{-1 - \varepsilon} n).
\]

Then the limit \( \phi_k(r) \) exists.

Abbe and Montanari also observed that the condition (2) is satisfied for \( r < 1 \) (for any \( k \geq 3 \)). Our second result gives a significantly better bound for sufficiently large values of \( k \).

The existence of the limit \( \phi_k(r) \) is related to the convergence of the sharp threshold sequence.

**Theorem 1.2** Let \( k \geq 3 \). If the limit \( \phi_k(r) \) exists for all \( r > 0 \), then the sequence \( r_k(n) \) converges.

Theorem 1.2 may actually be known to some experts in the area, but we are not aware of a proof of it appearing in the literature. We are going to give the (fairly easy) proof in Section 3.

There are two possible perspectives on Theorem 1.2 and its relationship to Theorem 1.1. On the one hand, one might argue that Theorem 1.2 just implies that proving the existence of \( \phi_k(r) \) is a difficult problem. On the other hand, more optimistically, given Theorems 1.1 and 1.2, in order to prove the existence of a sharp threshold for satisfiability, one “just” has to establish the bound (2). Indeed, a natural line of attack might be to extract bounds on \( P[\Phi \text{ is unsatisfiable}] \) for \( m/n < r_k(n) \) from Friedgut’s argument [13]. Unfortunately, meeting the condition (2) via this approach appears to be difficult. Yet there might be alternatives to Friedgut’s proof that do give such a bound. In fact, our second (and main) result establishes a much stronger bound than (2) for a range of densities.

**Theorem 1.3** There is a sequence \( \varepsilon_k \) that tends to 0 in the limit of large \( k \) such that

\[
P[\Phi \text{ is satisfiable}] \geq 1 - O(1/n) \quad \text{if } r < (1 - \varepsilon_k) \cdot 2^k \ln(k)/k.
\]

We emphasize that there is a number \( l = l(k) > 0 \) such that for any \( k \geq 3, r > 0 \) we have

\[
P[\Phi \text{ is satisfiable}] \leq 1 - \Omega(n^{-l})
\]

(where \( l = l(k) \to \infty \) in the limit of large \( k \)). This is because bounded-sized unsatisfiable subformulas appear with probability \( \Omega(n^{-l}) \). It would be interesting to figure out the best possible exponent \( l(k) \) for which (4) holds. For densities below the “pure literal threshold” (which is far below the density covered in (3)), the most likely unsatisfiable formulas can be quantified precisely [28].

The proof of Theorem 1.3 draws on ideas from algorithms for finding a satisfying assignment to a random \( k \)-SAT formula [8]. The possibility that such an approach is possible has been raised explicitly (but not carried out) in [1, following Remark 2]. However, rather than actually deriving the lower bound (3) directly by (going through the painstaking work of) tracing an algorithm, we pursue a more generic approach that may be applicable to other problems beyond random \( k \)-SAT. More precisely, we show that for any fixed \( \eta > 0 \), with probability \( 1 - \exp(-\Omega(n)) \) the random formula \( \Phi \) admits an assignment \( \sigma \) under which only \( \eta n \) clauses are unsatisfied. Furthermore, with probability \( 1 - O(1/n) \) such an “almost-satisfying” assignment \( \sigma \) can be turned into an actual satisfying assignment via a local-search type process. The latter is inspired by [8], but the fact that we only need to mend a fairly small number of violated clauses simplifies the analysis considerably (by comparison to [8]); see Section 4 for details.
Notation. For an integer $z$ we let $[z] = \{1, 2, \ldots, z\}$. Moreover, for $i \in [m]$ we denote by $\Phi_i$, the $i$th clause of the formula $\Phi$. Further, for $j \in [k]$ we let $\Phi_{ij}$ be the $j$th literal of $\Phi_i$. Hence, 

$$\Phi = \Phi_1 \land \cdots \land \Phi_m, \quad \Phi_i = \Phi_{i1} \lor \cdots \lor \Phi_{ik}.$$ 

For a literal $l \in \{x_1, \neg x_1, \ldots, x_n, \neg x_n\}$ we let $|l|$ denote the underlying variable.

We use asymptotic notation both with respect to $n$ and with respect to the clause length $k$. Asymptotics in $n$ are denoted by $O(\cdot)$ and asymptotics in $k$ by $O_k(\cdot)$. In particular, $o_k(1)$ signifies a term that tends to 0 for sufficiently large $k$.

2. Related work

Friedgut’s result [13] proves the existence of the threshold sequence $r_k(n)$, but does not reveal its location. For general values of $k$, the best current (rigorous) bounds on $r_k(n)$ derive from the first and the second moment method [3, 4, 9]: we have $r_k(n) = 2^k \ln 2 - O_k(1)$. For $k = 3$, the best current lower bound is obtained by tracing a certain linear-time satisfiability algorithm [17, 18]. Upper bounds have been obtained via (tricky) first moment arguments [11, 19, 22].

For large $k$, the best current (rigorously analyzed) polynomial-time algorithm finds satisfying w.h.p. for $r < (1 + \varepsilon_k)2^k \ln(k)/k$, with $\varepsilon_k \to 0$ in the limit of large $k$ [8]. It is no coincidence that this matches the bound in Theorem 1.3. More precisely, there are two reasons why the two bounds match. First, we are going to build upon ideas from [8]. Second, and more substantially, the point $r \sim 2^k \ln(k)/k$ marks the so-called dynamical replica symmetry breaking transition. This transition was predicted on the basis of physics arguments [21], and (to an extent) established rigorously [2]. Roughly speaking, the physics picture suggests that for $r > (1 + \varepsilon_k)2^k \ln(k)/k$ the geometry of the set of satisfying assignments renders local-search techniques ineffective. Since the proof of Theorem 1.3 builds upon local-search ideas, it is unsurprising that the argument stops working at $r \sim 2^k \ln(k)/k$.

The quantity $\phi_k(r)$ is closely related to the so-called free energy density at inverse temperature $\beta$, which is defined as follows. For a formula $\Phi$ and an assignment $\sigma$ let $E(\Phi, \sigma)$ denote the number of clauses of $\Phi$ that are violated under $\sigma$. Let

$$Z_\beta(\Phi) = \sum_{\sigma \in \{0,1\}^n} \exp(-\beta \cdot E(\Phi, \sigma))$$

be the partition function. Then the free energy density is

$$f_k(r, \beta) = -\lim_{n \to \infty} \frac{1}{\beta n} \mathbb{E} \left[ \ln Z_\beta(\Phi) \right].$$

Bayati, Gamarnik and Tetali [5] recently proved the existence of the limit (6) for any $k$ and $\beta, r \in (0, \infty)$. The proof is based on the interpolation method [12, 16].

As $\beta$ grows large, the partition function $Z_\beta(\Phi)$ is going to be concentrated on “good” assignments that only violate “relatively few” clauses. Indeed, in a sense $Z(\Phi)$ corresponds to the partition function $Z_\beta(\Phi)$ with $\beta = \infty$, and thus one might expect that for densities $r$ in the satisfiable regime, $\mathbb{E} \left[ \ln Z_\beta(\Phi) \right]$ provides a good approximation to $\mathbb{E} \left[ \ln (1 + Z(\Phi)) \right]$. To this extent, [5] instills hope that the limit $\phi_k(r)$ might indeed exist for all $k \geq 2, r \in (0, \infty)$.

3. Proof of Theorem 1.2

Assuming that $\phi_k(r)$ exists for all $r > 0$, we are going to show that the sharp threshold sequence converges to $r^* = \inf \{r > 0 : \phi_k(r) = 0\}$. Observe that the function $\phi_k(r)$ is monotonically decreasing (because increasing $r$ corresponds to adding more random clauses, which cannot increase $Z$). Hence,

$$\phi_k(r) > 0 \quad \text{if} \quad 0 < r < r^*, \quad \text{while} \quad \phi_k(r) = 0 \quad \text{if} \quad r > r^*.$$
The proof of Theorem 1.2 consists of two steps: showing that $\Phi$ is satisfiable w.h.p. if $r < r^*$, and that it is unsatisfiable w.h.p. if $r > r^*$.

**Lemma 3.1** If $r < r^*$, then $\Phi$ is satisfiable w.h.p.

*Proof.* Equation (7) shows that $\phi_k(r) > 0$. As a first step, we claim that

$$\liminf_{n \to \infty} P[\Phi \text{ is satisfiable}] \geq \phi_k(r) > 0. \quad (8)$$

For assume that $P[\Phi \text{ is satisfiable}] < \phi_k(r)$ for infinitely many $n$. Then for infinitely many $n$,

$$E[\ln(1 + Z(\Phi))] \leq \phi_k(r) \ln 2 + o(1) < 0.9\phi_k(r), \quad (9)$$

because the total number of satisfying assignments cannot exceed $2^n$. However, (9) contradicts the fact that $\phi_k(r) = \lim_{n \to \infty} E[\ln(1 + Z(\Phi))]$. Thus, we have established (8).

Now, (8) implies that the sharp threshold sequence satisfies $r_k(n) \geq r - o(1)$. Because this holds for any $r < r^*$, we see that $\liminf_{n \to \infty} r_k(n) \geq r^*$. Therefore, for any density $r < r^*$ we have $P[\Phi \text{ is satisfiable}] = 1 - o(1)$, as desired. \hfill \Box

**Lemma 3.2** If $r > r^*$, then $\Phi$ is unsatisfiable w.h.p.

*Proof.* Assume towards a contradiction that $r > r^*$ but $P[\Phi \text{ is satisfiable}] \geq \delta = \Omega(1)$ for infinitely many $n$. It is well-known that the random formula $\Phi$ has $\alpha n$ isolated variables (i.e., variables that do not appear in any clause) w.h.p., where $\alpha = \alpha(k, r) > 0$ is independent of $n$. Furthermore, if $\sigma$ is a satisfying assignment of $\Phi$, then another satisfying assignment $\sigma'$ can be obtained by altering the truth values of any set of isolated variables. Consequently,

$$P[Z(\Phi) \geq 2^{\alpha n}] \geq P[\Phi \text{ is satisfiable}] - P[\text{there are at most } \alpha n \text{ isolated variables}] = \delta - o(1).$$

Therefore, we have $E[\ln(1 + Z(\Phi))] \geq \alpha(\delta - o(1))n$ for infinitely many $n$, while (7) yields $\phi_k(r) = \lim_{n \to \infty} E[\ln(1 + Z(\Phi))] = 0$. \hfill \Box

Finally, Theorem 1.2 is immediate from Lemmas 3.1 and 3.2.

**4. Proof of Theorem 1.3**

Unless otherwise specified, we assume that $k \geq k_0$ for a certain (large) constant $k_0$, and that $r \leq (1 - \varepsilon_k)2^k \ln(k)/k$ for a sequence $\varepsilon_k = o_k(1)$ that tends to 0 sufficiently slowly in the limit of large $k$. We also assume that $n$ is sufficiently big for our various estimates to hold.

4.1. *Proof strategy*

To prove Theorem 1.3, we take a detour through the $k$-NAESAT ("not-all-equal satisfiability") problem. Recall that an assignment $\sigma : V \to \{0, 1\}$ is NAE-satisfying for a formula $\Phi$ if both $\sigma$ and its complement $\bar{\sigma}$ (defined by changing the $i$th bit of $\sigma$ for every $i$, $\sigma_i$ to 1 $- \sigma_i$) satisfy $\Phi$. For a formula $\Phi$ and an assignment $\sigma$ we let $E_{\text{NAE}}(\Phi, \sigma)$ denote the number of clauses that are violated under either $\sigma$ or $\bar{\sigma}$. Thus, $\sigma$ is NAE-satisfying iff $E_{\text{NAE}}(\Phi, \sigma) = 0$. For a number $\eta > 0$ we let $Y_\eta(\Phi)$ be the number of assignments $\sigma$ such that $|E_{\text{NAE}}(\Phi, \sigma)| \leq \eta n$. Using arguments developed in [2, 10], we are going to establish the following in Section 4.2.

**Proposition 4.1** For any $\delta > 0$ there is $\eta_0 > 0$ such that for any $0 < \eta < \eta_0$ we have

$$P[Y_\eta(\Phi) < E[Y_\eta(\Phi)] \cdot \exp(-\delta n)] = O(n^{-2}). \quad (10)$$

Moreover, $E[Y_\eta(\Phi)] = 2^{(1-o_k(1))n}$.
The reason why we consider NAE-satisfiability as opposed to the “usual” satisfiability problem is that the statement corresponding to Proposition 4.1 would have been false. This is due to the inherent asymmetry of the $k$-SAT problem, which also causes the difficulty of computing $\frac{1}{n}\ln(1 + Z(\Phi))$; we refer to [9] for a detailed discussion.

Proposition 4.1 shows not only that w.h.p. the random formula $\Phi$ has plenty of assignments $\sigma$ such that $|E_{\text{NAE}}(\Phi, \sigma)| \leq \eta n$, but also allows us to study the typical properties of such assignments. Formally, let us define the Gibbs distribution denoted by $G_\eta$ (we omit the obvious dependency of $n$ and $m$ in notation) as the distribution on pairs $(\Phi, \sigma)$ induced by the following experiment:

- Sample a random formula $\Phi$.
- Then, sample an assignment $\sigma \in \{0, 1\}^n$ such that $E_{\text{NAE}}(\Phi, \sigma) \leq \eta n$ uniformly.

The Gibbs distribution is cumbersome to work with directly. But Proposition 4.1 allows us to approximate this distribution by another one that is easier to cope with. Namely, the so-called planted distribution, denoted $P_\eta$, is induced by the following experiment (cf. [2]):

- Sample a random assignment $\sigma \in \{0, 1\}^n$.
- Choose a $k$-CNF $\Phi(\sigma)$ uniformly out of all formulas with $n$ variables and $m$ clauses such that $E_{\text{NAE}}(\Phi(\sigma), \sigma) \leq \eta n$.

Combining Proposition 4.1 with a double-counting argument akin to the one used in [2], we obtain

**Proposition 4.2** Assume that $\delta, \eta$ are such that (10) is satisfied. Then for any event $B$ we have

\[ P_{G_\eta}[B] \leq \exp(2\delta n) \cdot P_{P_\eta}[B] + O(n^{-2}). \]

Equipped with Proposition 4.2, we perform the key step of the proof in Section 4.3, where we prove the following. Let us say that a map $\tau : V \to \{0, 1, *\}$ satisfies a clause $\Phi_i$ if the clause contains a literal $l$ such that $\tau(x) = 1$ if $l = x \in V$ is a positive literal, and $\tau(x) = 0$ if $l = \neg x$ is negative.

**Proposition 4.3** There exist numbers $\eta_0 > 0, \gamma > 0$ such that for all $0 < \eta < \eta_0$ in the distribution $P_\eta$ with probability at least $1 - \exp(-\gamma n)$ the following is true.

There is a map $\tau : V \to \{0, 1, *\}$ such that $|\tau^{-1}(*)| \leq 4^{-k}n$ and such that each clause has one of the following two properties.

**T1.** either the clause is satisfied under $\tau$,

**T2.** or there occur three variables in the clause that are set to * under $\tau$.

Combining Propositions 4.2 and 4.3, we obtain

**Corollary 4.4** With probability $1 - O(n^{-2})$ the random formula $\Phi$ admits an assignment $\tau$ as in Proposition 4.3.

Furthermore, a standard first moment argument yields the following.

**Lemma 4.5** With probability $1 - O(1/n)$ the random formula $\Phi$ has the following property.

Let $S \subset V$ be a set of size $|S| \leq 4^{-k}n$. Let $I \subset [m]$ be the set of indices such that for all $i \in I$ there are three indices $1 \leq j_1 < j_2 < j_3 \leq k$ such that $|\Phi_{i,j_1}|, |\Phi_{i,j_2}|, |\Phi_{i,j_3}| \in S$. Then $|I| \leq |S|$. (11)
Proof. For a set $S \subset V$ and a set $I \subset [m]$ let $E(S, I)$ be the event that each clause $\Phi_i$, $i \in I$, features three occurrences of variables in $S$. Let $s \leq n/4^k$ be an integer and let $E(s)$ be the event that there exist sets $S \subset V$ and $I \subset [m]$ of size $|S| = |I| = s$ such that $E(S, I)$ occurs. By the union bound and because the clauses of $\Phi$ are chosen uniformly and independently, we have

$$P[\mathcal{E}(s)] \leq \sum_{S, I:|S| = |I| = s} P[\mathcal{E}(S, I)] \leq \binom{n}{s} \binom{m}{s} \left( \frac{k}{s} \right)^s \leq (k^3 2^k s/n)^s.$$  

Hence, again by the union bound $P \left[ \bigcup_{1 \leq s \leq n/4^k} \mathcal{E}(s) \right] \leq \sum_{1 \leq s \leq n/4^k} (k^3 2^k s/n)^s = O(1/n)$. \hfill $\square$

Proof of Theorem 1.3. Suppose that $\Phi$ admits an assignment $\tau$ as in Proposition 4.3. Let $M$ be the set of indices $i \in [m]$ such that $\tau$ fails to satisfy $\Phi_i$. Moreover, let $S = \tau^{-1}(\star)$. Set up a bipartite graph $B$ on $M \cup S$ in which $i \in M$ is adjacent to all variables $x \in S$ that occur in $\Phi_i$. If (11) holds, then by Hall’s theorem, $B$ contains a matching $M$ that covers all of $M$. Thus, we can construct a satisfying assignment $\sigma$ by setting $\sigma(x) = \tau(x)$ if $\tau(x) \neq \star$, and by setting $\sigma(x)$ so that the clause that $x$ is matched to under $M$ is satisfied if $x$ is covered by $M$. (If $\tau(x) = \star$ but $x$ is not covered by $M$, we can set $\sigma(x)$ to either value.) Finally, Theorem 1.3 follows because Corollary 4.4 shows that there is an assignment $\tau$ as above with probability $1 - O(n^{-2})$, and because (11) holds with probability $1 - O(1/n)$ by Lemma 4.5. \hfill $\square$

4.2. Proof of Proposition 4.1

The proof is based on studying the number $Z_{\text{NAE}}(\Phi)$ of NAE-satisfying assignments of $\Phi$ along with the partition function

$$Z_{\beta,\text{NAE}}(\Phi) = \sum_{\sigma \in [0,1]^v} \exp(-\beta \cdot E_{\text{NAE}}(\Phi, \sigma)) \quad \text{for } \beta \in (0, \infty).$$  

Notice that, in contrast to (5), in (12) we work with the number $E_{\text{NAE}}(\Phi, \sigma)$ of clauses that are NAE-violated. Clearly, for any $\beta > 0$ we have $Z_{\beta,\text{NAE}} \geq Z_{\text{NAE}}$. Hence, to obtain a lower bound on $Z_{\beta,\text{NAE}}$, we are going to establish one for $Z_{\text{NAE}}$. The starting point is the following bound on the second moment of $Z_{\text{NAE}}$.

Lemma 4.6 ([3]) For any $k \geq 3$ there is a number $C(k) > 0$ such that for $r < 2^{k-1} \ln 2 - 2$ we have $E \left[ Z_{\text{NAE}}(\Phi)^2 \right] \leq C(k) \cdot E \left[ Z_{\text{NAE}}(\Phi) \right]^2$. Moreover, $E \left[ Z_{\text{NAE}}(\Phi) \right] = \exp(\Omega(n))$.

To turn Lemma 4.6 into a lower bound on $Z_{\text{NAE}}(\Phi)$, we remember the Paley-Zygmund inequality: if $Y \geq 0$ is a random variable with $0 < E \left[ Y^2 \right] < \infty$, then

$$P \left[ Y \geq t \cdot E \left[ Y \right] \right] \geq (1 - t)^2 E \left[ Y^2 \right] / E \left[ Y^2 \right] \quad \text{for any } t \in (0, 1).$$

Hence, Lemma 4.6 yields the following result (similar bounds have been used in [2, 10]).

Corollary 4.7 Suppose that $k \geq 3$ and $r < 2^{k-1} \ln 2 - 2$. There exists a number $\alpha = \alpha(k) > 0$ such that $P \left[ Z_{\text{NAE}} \geq \alpha \cdot E \left[ Z_{\text{NAE}} \right] \right] \geq \alpha$.

We proceed by showing (by a standard argument, cf. [5]) that $Z_{\text{NAE}}$ is tightly concentrated.

Lemma 4.8 Let $k \geq 3$ and let $\beta, r > 1$ be arbitrary but independent of $n$. Then

$$P \left[ \left| \ln Z_{\beta,\text{NAE}}(\Phi) - E \left[ \ln Z_{\beta,\text{NAE}}(\Phi) \right] \right| > 100 \beta \sqrt{m \ln n} \right] \leq n^{-100}.$$
Proof. Let $\Phi[t] = \Phi_1 \land \cdots \land \Phi_t$ be the formula comprising the first $t$ clauses of $\Phi$ ($0 \leq t \leq m$). Fix an assignment $\sigma$. Then

$$\exp(-\beta E_{\text{NAE}}(\Phi[t+1], \sigma)) = \begin{cases} \exp(-\beta E_{\text{NAE}}(\Phi[t], \sigma)) & \text{if } \sigma \text{ NAE-satisfies } \Phi_{t+1}, \\ \exp(-\beta E_{\text{NAE}}(\Phi[t], \sigma) - \beta) & \text{otherwise.} \end{cases}$$

Hence, for any $0 \leq t < m$ we have $|\ln Z_{\beta,\text{NAE}}(\Phi[t+1]) - \ln Z_{\beta,\text{NAE}}(\Phi[t])| \leq \beta$, i.e., the random variables $(\ln Z_{\beta,\text{NAE}}(\Phi[t]))_{0 \leq t \leq m}$ satisfy a Lipschitz condition. Because the clauses are independent, it follows from Azuma’s inequality that

$$P \left[ \left| \ln Z_{\beta,\text{NAE}}(\Phi) - E[\ln Z_{\beta,\text{NAE}}(\Phi)] \right| > \lambda \right] \leq 2 \exp \left[ - \frac{\lambda^2}{2 \beta^2 m} \right] \quad (\lambda > 0).$$

Setting $\lambda = 100\beta \sqrt{m} \ln n$ completes the proof. □

Corollary 4.9 Let $k \geq 3$ and let $\beta, r > 1$ be arbitrary but independent of $n$. Then

$$E[\ln Z_{\beta,\text{NAE}}(\Phi)] \geq \ln E[Z_{\text{NAE}}(\Phi)] - n^{0.51}.$$

Proof. Once more we use a standard concentration argument (reminiscent of Frieze’s argument for proving the concentration of the chromatic number of random graphs). Assume towards a contradiction that $E[\ln Z_{\beta,\text{NAE}}(\Phi)] < \ln E[Z_{\text{NAE}}(\Phi)] - n^{0.51}$. Let $\alpha > 0$ be as in Corollary 4.7. Since $Z_{\beta,\text{NAE}} \geq Z_{\text{NAE}}$, Lemma 4.8 implies

$$P \left[ Z_{\text{NAE}}(\Phi) \geq \alpha E[Z_{\text{NAE}}(\Phi)] \right] \leq P \left[ \ln Z_{\beta,\text{NAE}}(\Phi) \geq \ln E[Z_{\text{NAE}}(\Phi)] - O(1) \right]$$

$$\leq P \left[ \ln Z_{\beta,\text{NAE}}(\Phi) \geq \ln \ln E[Z_{\beta,\text{NAE}}(\Phi)] + n^{0.51} - O(1) \right] \leq n^{-100},$$

in contradiction to Corollary 4.7. □

Proof of Proposition 4.1. Let $\eta > 0$ be sufficiently small and choose $\beta = \beta(\eta) > 0$ big enough so that $2^{\eta} \exp(-\beta m) < 1$. Lemma 4.8 and Corollary 4.9 imply that with probability $1 - O(n^{-100})$ we have $Z_{\beta,\text{NAE}} \geq E[Z_{\text{NAE}}] \exp(-n^{2/3}) = \exp(\Omega(n))$ (by Lemma 4.6). In this case, we have

$$E[Z_{\text{NAE}}(\Phi)] \exp(-n^{2/3}) \leq Z_{\beta,\text{NAE}} \leq Y_\eta(\Phi) + \sum_{\sigma : E_{\text{NAE}}(\sigma, \Phi) > \eta m} \exp(-\beta E_{\text{NAE}}(\sigma, \Phi)) \leq Y_\eta(\Phi) + 1 \quad [\text{because } 2^\eta \exp(-\beta \eta m) < 1]. \quad (13)$$

Furthermore, because a given assignment NAE-satisfies a random clause with probability $1 - 2^{-k}$, and because the $m$ clauses of $\Phi$ are chosen independently, we have

$$E[Y_\eta(\Phi)] \geq E[Z_{\text{NAE}}(\Phi)] = 2^n (1 - 2^{-k})^m = 2^{(1-\alpha_k(1))n} \quad [\text{as } r \leq 2^k \ln(k)/k]. \quad (14)$$

Conversely,

$$E[Y_\eta(\Phi)] = 2^n \cdot P \left[ \text{Bin}(m, 2^{-k}) \leq \eta m \right] \sim 2^n \left( \frac{m}{\eta m} \right) 2^{(1-\eta)m} (1 - 2^{-k})^{m - \eta m}$$

$$\leq 2^n (1 - 2^{-k})^m \cdot \exp \left[ \eta m \left( 1 - \ln \eta + \ln r + (1 - k) \ln 2 - \ln(1 - 2^{-k}) \right) \right] = E[Z_{\text{NAE}}] \cdot \exp \left[ \eta m \left( 1 - \ln \eta + \ln r + (1 - k) \ln 2 - \ln(1 - 2^{-k}) \right) \right]. \quad (15)$$

Since $\lim_{\eta \to 0} \eta \left( 1 - \ln \eta + \ln r + (1 - k) \ln 2 - \ln(1 - 2^{-k}) \right) = 0$, (15) shows that for any given $\alpha > 0$ we can choose $\eta$ small enough so that $E[Y_\eta] \leq \exp(\alpha n)E[Z_{\text{NAE}}]$. Thus, the assertion follows from (13) and (14). □
4.3. Proof of Proposition 4.3
Throughout this section we assume that $0 < \eta < \eta_0$ for a small enough number $\eta_0 = \eta_0(k) > 0$. We start from a pair $(\Phi, \sigma)$ chosen from $P_\eta$; without loss of generality, we may assume that $\sigma = 1$ is the all-true assignment. We are going to construct the desired map $\tau$ via the following process.

(i) Initially, let $\tau = \sigma$.
(ii) While there is a clause $\Phi_l$ that is unsatisfied under $\tau$ and that does not contain at least three variables that take the value $*$ under $\tau$, pick the least such index $i$.
(iii) Let us say that a variable $x$ supports a clause $\Phi_l$ under $\tau$ if
- $\tau(x) \in \{0, 1\}$,
- $\Phi_l$ has at most two positive literals, and
- assigning $x$ the value $1 - \tau(x)$ while keeping the values of all other variables deprives $\Phi_l$ of satisfied literals (where literals whose underlying variables are set to $*$ do not count as satisfied).

If there are at least three indices $j \in [k - 3]$ such that the variable $|\Phi_{ij}|$ does not support a clause under $\tau$, then pick any three such indices $j$ and set them to $*$ under $\tau$.
(iv) If such three indices do not exist, set $\tau(|\Phi_{ij}|) = *$ for $j = k - 2, k - 1, k$.

The map $\tau$ that results from this process clearly satisfies conditions $T1$ and $T2$. However, it is non-trivial to upper bound the number of variables assigned $*$ in the course of the above process. To accomplish this, we need a few basic properties of the random pair $(\Phi, \sigma)$. Let us call a clause $\Phi_l$ critical if there is a variable $x$ that supports $\Phi_l$; hence, $\Phi_l$ has no more than two positive literals, and flipping a single variable may render $\Phi_l$ unsatisfied.

**Lemma 4.10** With probability $1 - \exp(-\Omega(n))$ the following two statements hold.

(i) The total number of clauses that are critical under $\sigma$ is at most $n(1 - \varepsilon_k + 1/k)\ln k$.
(ii) There are at least $\frac{1}{2}k^{2k-1}n$ variables that do not support a clause under $\tau_0$.

Lemma 4.10 follows from our assumption that $r \leq (1 - \varepsilon_k)^2k \ln(k)/k$ and standard concentration bounds.

**Lemma 4.11** Let $\Omega(1) < \alpha < k^{-4}$. With probability $1 - \exp(-\Omega(n))$ the following is true.

Let $S \subset V$ be a set of size $|S| = \alpha n$. The total number of clauses that have at most 2 positive literals, one of which belongs to $S$, is bounded by

$$k^3 \alpha \ln(\alpha) \cdot n.$$  \hspace{1cm} (16)

**Proof.** Fix a set $S$ of size $\alpha n$. Then the number $X_S$ of clauses that have at most 2 positive literals, one of which belongs to $S$, has a binomial distribution with mean $\leq \alpha k^3n$. Hence, by the Chernoff bound $P[X_S < -k^3 \alpha \ln(\alpha)n] \leq \exp(k^3 \alpha \ln(\alpha)n)$. Thus, by the union bound

$$P[\exists S : X_S > -k^3 \alpha \ln(\alpha)] \leq \binom{n}{\alpha n} \exp(k^3 \alpha \ln(\alpha)n) \leq \exp[\alpha n(1 - \ln \alpha + k^3 \ln \alpha)] \leq \exp(-\Omega(n)),$$

as claimed. \hfill \Box

**Corollary 4.12** With probability $1 - \exp(-\Omega(n))$ the following is true.

Let $S$ be a set of size $|S| \leq n/k^6$. The number of clauses that are not critical under $\sigma$ but that become so once we set the variables in $S$ to $*$ is bounded by $n/k^3$.  \hspace{1cm} (17)
After these preliminaries we come to the actual analysis of the above process that yields $\tau$. We characterize its state at time $t$ by maps $\tau_t : V \to \{0, 1, *\}$ and

$$\pi_t : [m] \times [k] \to \{\pm 1, x_1, \bar{x}_1, \ldots, x_n, \bar{x}_n\}.$$  

Let $\tau_0 = \sigma$. Moreover, we define

$$\pi_0(i, j) = \begin{cases} \Phi_{ij} & \text{if } |\Phi_{ij}| \text{ supports clause } \Phi_i, \\ \mathrm{sign}(\Phi_{ij}) & \text{otherwise.} \end{cases}$$

Each time step of the process corresponds to mending one clause $\Phi_i$ (i.e., making sure that $\Phi_i$ receives three $*$-variables). As time progresses, $\pi_t$ will summarise the information about $\Phi$ that has been revealed thus far.

More precisely, suppose we have already defined $\tau_0, \ldots, \tau_{t-1}$. Then $\tau_t$ is obtained as follows. Suppose at time $t$ we mend clause $\Phi_{i_t}$. Let $\tau_t$ be the assignment obtained after steps (iii) and (iv) above, i.e., $\tau_t$ is obtained from $\tau_{t-1}$ by setting up to three of the variables in $\Phi_{i_t}$ to *. We define

$$\pi_t(i, j) = \begin{cases} \Phi_{ij} & \text{if either } i = i_t, |\Phi_{ij}| \text{ supports clause } \Phi_i, \text{ or } \tau_t(\Phi_{ij}) = *, \\ \pi_{t-1}(i, j) & \text{otherwise.} \end{cases}$$

Let $\mathcal{A}_t = \tau_t^{-1}(*)$. Moreover, let $T$ be the stopping time of the process, i.e., the first time when all clauses are either satisfied under $\tau_t$ or contain at least three variables $x$ with $\tau_t(x) = *$. In addition, let $(\mathcal{F}_t)_{t \geq 0}$ be the filtration generated by $\tau_t$, $\pi_t$. The following observation (“principle of deferred decisions”) is immediate from the construction.

**Fact 4.13** For any $t \geq 0$, given $\mathcal{F}_t$ the variables $|\Phi_{ij}|$ with $\pi_t(i, j) = \pm 1$ are independently uniformly distributed over $V \setminus \mathcal{A}_t$.

Let $\theta = 2\eta n$. We aim to show that $T \leq \theta$ with probability $1 - \exp(-\Omega(n))$. To prove this, we need to bound the number of times that step (iv) is executed (observe that new unsatisfied clauses not containing three $*$ can only be generated in step (iv), hence it suffices to consider the number of iterations of step (iv)). Thus, let us call a variable $x$ t-free if $\tau_{t-1}(x) \neq *$ and if $x$ does not support a clause under $\tau_{t-1}$. Moreover, let us call step $t$ a failure if there are fewer than three t-free variables in $\{|\Phi_{ij}| : j \in [k-3]\}$.

**Lemma 4.14** Suppose we run the process for $t \leq \theta$ steps. Then with probability $1 - \exp(-\Omega(n))$ there are at most $\theta/k^9$ failures.

**Proof.** By Corollary 4.12 we may assume that (17) holds. In addition, we may assume that 1. and 2. in Lemma 4.10 are satisfied. We claim that at any time $t \leq \theta$,

$$P \{\text{step } t \text{ is a failure} | \mathcal{F}_{t-1} \} \leq k^{-10}. \quad (18)$$

Indeed, by the definition of the process, the clause $\Phi_{i_t}$ has at least $k - 6$ literals $j \in [k - 3]$ such that $\pi_{t-1}(i_t, j) \in \{\pm 1\}$. Fact 4.13 shows that for all such $j$, the variable $|\Phi_{ij}|$ is uniformly distributed over $V \setminus \mathcal{A}_{i_t-1}$, independently of the others. Furthermore, we claim that the total number of variables that are t-free is at least $\frac{1}{4}k^{\varepsilon k - 1}n$. Indeed, there are at least $\frac{1}{4}k^{\varepsilon k - 1}n$ variables that do not support a clause under $\tau_0 = \sigma$ (by item 2. in Lemma 4.10). Moreover, by (17) (assuming $\eta$ is small enough) the number of such variables that fail to be t-free is bounded by $n/k^3$. Hence, for each variable $|\Phi_{ij}|$ with $\pi_{t-1}(i_t, j) \in \{\pm 1\}$ and $j \in [k - 3]$ the probability of being t-free is at least $\frac{1}{4}k^{\varepsilon k - 1}$. Thus, the probability that at most two of them are t-free is bounded by

$$\xi = k^2(1 - k^{\varepsilon k - 1}/4)^{k-5} \leq k^2 \exp(-(k - 5)k^{\varepsilon k - 1}/4) \leq k^{-10}.$$


Finally, because (18) provides a uniform bound for all \( t \leq \theta \), the total number of failures is stochastically dominated by a binomial variable \( \text{Bin}(\theta, k^{-10}) \). Thus, the assertion follows from the Chernoff bound.

\[ \Box \]

**Corollary 4.15** With probability \( 1 - \exp(-\Omega(n)) \) the stopping time of the process is \( T \leq \theta \).

**Proof.** By Lemma 4.11 we may assume that (16) holds. In addition, we may assume that 1. and 2. in Lemma 4.10 are satisfied, and that the total number of failures \( t \leq \theta \) is bounded by \( \theta/k^3 \) (by Lemma 4.14). Let \( F \) be the set of all \( t \leq \theta \) that are failures and let \( \mathcal{B} = \bigcup_{t \in F} \mathcal{A}_t \setminus \mathcal{A}_{t-1} \) contain all the variables that were added to \( \mathcal{A}_t \) at steps \( t \in F \). Let us say that clause \( \Phi_i \) is \( t \)-unhappy if there is a time \( s \leq t \) such that \( \pi_s(i, j) \neq 1 \) for all \( j \in [k] \) and \( |\{j \in [k] : \pi_s(i, j) = -1\}| \geq k - 2 \).

In words, at some time \( s \leq t \) clause \( \Phi_i \) did neither contain three \( * \)-variables nor at least one positive literal.

Because the pair \((\Phi, \sigma)\) was chosen from the distribution \( P_\eta \), no more than \( \eta n \) clauses are \( 0 \)-unhappy. Hence, if \( T > \theta \), then there must be at least \( \theta/2 \) clauses that are \( \theta \)-unhappy but not \( 0 \)-unhappy. Furthermore, all of these clauses have at most two positive literals, at least one of which belongs to \( B \). This contradicts (16), because \( |\mathcal{B}| \leq 3|F| \leq 3\theta/k^3 \).

\[ \Box \]

**Proof of Proposition 4.3.** Corollary 4.15 yields \( P[T \leq \theta] \geq 1 - \exp(-\Omega(n)) \). Since in each step of the process at most three variables are set to \(*\), we conclude that \( P[|\mathcal{A}_T| \leq 3\theta] \geq 1 - \exp(-\Omega(n)) \).

Finally, for sufficiently small \( \eta \) we have \( 3\theta/n \leq 4^{-k} \).

\[ \Box \]

**Acknowledgments**

The first author thanks David Gamarnik, Will Perkins and Prasad Tetali for helpful discussions. The second author has been supported in part by The Israel Science Foundation (grant No. 621/12) and by the Citi Foundation. The research leading to these results has received funding from the European Research Council under the European Union’s Seventh Framework Programme (FP/2007-2013) / ERC Grant Agreement n. 278857–PTCC.

**References**

[1] Abbe E and Montanari A 2010 On the concentration of the number of solutions of random satisfiability formulas Preprint CoRR/1006.3786

[2] Achlioptas D and Coja-Oghlan A 2008 Algorithmic barriers from phase transitions Proc. 49th FOCS pp 793–802

[3] Achlioptas D and Moore C 2006 Random \( k \)-SAT: two moments suffice to cross a sharp threshold SIAM J. Comput. 36 740–62

[4] Achlioptas D and Peres Y 2004 The threshold for random \( k \)-SAT is \( 2^k \ln 2 - O(k) \) J. Amer. Math. Soc. 17 947–73

[5] Bayati M, Gamarnik D and Tetali P 2010 Combinatorial approach to the interpolation method and scaling limits in sparse random graphs Proc. 42nd STOC pp 105–14

[6] Cheeseman P, Kanefsky B and Taylor W 1991 Where the really hard problems are Proc. IJCAI pp 331–7

[7] Chvátal V and Reed B 1992 Mick gets some (the odds are on his side) Proc. 33th FOCS pp 620–7

[8] Coja-Oghlan A 2010 A better algorithm for random \( k \)-SAT SIAM J. Comput. 39 2823–64

[9] Coja-Oghlan A and Panagiotou K 2013 Going after the \( k \)-SAT threshold Proc. 35th STOC pp 705-14

[10] Coja-Oghlan A and Zdeborová L 2012 The condensation transition in random hypergraph 2-coloring Proc. 23rd SODA pp 241–50

[11] Dubois O, Bouchard Y and Mandler J 2000 Typical random 3-SAT formulae and the satisfiability threshold Proc. 11th SODA pp 126–7

[12] Franz S and Leone M 2003 Replica bounds for optimization problems and diluted spin systems J. Statist. Phys. 111 535–64

[13] Friedgut E 1999 Sharp thresholds of graph properties, and the \( k \)-SAT problem J. Amer. Math. Soc. 12 1017–54

[14] Frieze A and Suen S 1996 Analysis of two simple heuristics on a random instance of \( k \)-SAT J. Algorithms 20 312–55
[15] Frieze A and Wormald N 2005 Random k-Sat: a tight threshold for moderately growing k Combinatorica 25 297–305
[16] Guerra F 2003 Broken replica symmetry bounds in the mean field spin glass model Comm. Math. Phys. 233 1–12
[17] Hajiaghayi M and Sorkin G 2003 The satisfiability threshold of random 3-SAT is at least 3.52 IBM Research Report RC22942
[18] Kaporis A, Kirovssis L and Lalas E 2006 The probabilistic analysis of a greedy satisfiability algorithm Random Structures Algorithms 28 444–80
[19] Kirovssis L, Kranakis E, Krizanc D and Stamatiiou Y 1998 Approximating the unsatisfiability threshold of random formulas Random Structures Algorithms 12 253–69
[20] Kirkpatrick S and Selman B 1994 Critical behavior in the satisfiability of random boolean expressions Science 264 1297–301
[21] Krzakala F, Montanari A, Ricci-Tersenghi F, Semerjian G and Zdeborová L 2007 Gibbs states and the set of solutions of random constraint satisfaction problems Proc. National Academy of Sciences 104 pp 10318–23
[22] Maneva E and Sinclair A 2008 On the satisfiability threshold and clustering of solutions of random 3-SAT formulas Theoret. Comput. Sci. 407 359–69
[23] Mertens S, Mézard M and Zecchina R 2006 Threshold values of random K-SAT from the cavity method Random Structures Algorithms 28 340–73
[24] Mézard M and Montanari A 2009 Information, Physics and Computation (Oxford: Oxford University Press)
[25] Mézard M, Parisi G and Zecchina R 2002 Analytic and algorithmic solution of random satisfiability problems Science 297 812–5
[26] Monasson R and Zecchina R 1996 Entropy of the K-satisfiability problem Phys. Rev. Lett. 76 3881–3885
[27] Panchenko D and Talagrand M 2004 Bounds for diluted mean-fields spin glass models Probab. Theory Related Fields 130 319–36
[28] Scott A and Sorkin G 2010 Structure of random r-SAT below the pure literal threshold Preprint CoRR/1008.1260