ABSTRACT

Random $k$-SAT is the single most intensely studied example of a random constraint satisfaction problem. But despite substantial progress over the past decade, the threshold for the existence of satisfying assignments is not known precisely for any $k \geq 3$. The best current results, based on the second moment method, yield upper and lower bounds that differ by an additive $k \ln 2/2$, a term that is unbounded in $k$. (Achlioptas, Peres: STOC 2003). The basic reason for this gap is the inherent asymmetry of the Boolean values ‘true’ and ‘false’ in contrast to the perfect symmetry, e.g., among the various colors in a graph coloring problem. Here we develop a new asymmetric second moment method that allows us to tackle this issue head on for the first time in the theory of random CSPs. This technique enables us to compute the $k$-SAT threshold up to an additive $2 - \frac{1}{2} + O(1/k) \approx 0.19$. Independently of the rigorous work, physicists have developed a sophisticated but non-rigorous technique called the “cavity method” for the study of random CSPs (Mézard, Parisi, Zecchina: Science 2002). Our result matches the best bound that can be obtained from the so-called “replica symmetric” version of the cavity method, and indeed our proof directly harnesses parts of the physics calculations.

Categories and Subject Descriptors

G.2 [Discrete Mathematics]: General; F.2 [Analysis of Algorithms and Problem Complexity]: General

General Terms

Theory

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

STOC'13, June 1–4, 2013, Palo Alto, California, USA.
Copyright 2013 ACM 978-1-4503-2029-0/13/06 ...$15.00.
As has been noticed in prior work [4, 6], the second moment method is fundamentally ill-posed to deal with such asymmetries. Roughly speaking, the second moment method is based on the crucial assumption that in a random CSP instance, two randomly chosen solutions are perfectly uncorrelated. But in random k-SAT this is unfortunately not the case. Indeed, suppose that a variable \( x \) appears much more often positively than negatively throughout the formula. Then it seems reasonable to expect that a large fraction of the satisfying assignments set \( x \) to ‘true’, thereby satisfying all clauses where \( x \) appears positively. More generally, define the majority vote \( \sigma_{\text{maj}} \) to be the assignment that sets variables \( x \) to ‘true’ if it appears more often positively than negatively, and to ‘false’ otherwise. Then we expect that the set of satisfying assignments of a random formula “gravitates toward” \( \sigma_{\text{maj}} \). Unfortunately, the correlations among satisfying assignments induced by this drift toward \( \sigma_{\text{maj}} \) doom the second moment method. Previously this issue was sidestepped by symmetrizing artificially the problem [4, 6]. But this inevitably leaves a gap of size \( \Theta(k) \).

The main contribution of the present work is a new asymmetric second moment method that enables us to tackle this problem head on. A key feature of our method is that we harness directly the Belief Propagation calculation from physics, called the “replica symmetric case” of the cavity method in physics jargon. We are going to employ Belief Propagation directly as an “educated guess” in the design of algorithms such as Belief/Survey Propagation guided decimation.

We claim that then \( r_{k-\text{SAT}} \leq r_{\text{upper}} = 2^k \ln 2 - (1 + \ln 2)/2 + o_k(1) \), \hspace{1cm} (1)

where \( o_k(1) \) hides a term that tends to 0 for large \( k \). The best prior lower bound is due to Achiapotas and Peres [6], who used a “symmetric” second moment argument to show

\[ r_{k-\text{SAT}} \geq r_{\text{hal}} = 2^k \ln 2 - k \ln 2/2 - (1 + \ln 2/2) + o_k(1). \] \hspace{1cm} (2)

The bounds (1) and (2) leave an additive gap of \( k \cdot \ln 2 + 1/2 + o_k(1) \), i.e., the gap is unbounded in terms of \( k \).

**Theorem 1.** There is \( \varepsilon_k = o_k(1) \) such that

\[ r_{k-\text{SAT}} \geq r_{\text{BP}} = 2^k \ln 2 - 3 \ln 2/2 - \varepsilon_k. \] \hspace{1cm} (3)

Achiapotas and Peres asked whether \( r_{\text{upper}} - r_{k-\text{SAT}} \) is bounded by an absolute constant (independent of \( k \)). Theorem 1 answers this question, reducing the gap to \( \ln 2 - 1/2 \approx 0.19 \). No attempt at optimizing the error term \( \varepsilon_k \) has been made, but our proofs yield rather directly that \( \varepsilon_k = O(1/k) \).

Apart from the quantitative improvement, the main point of this paper is that we manage to solve the problem of asymmetry in random CSPs for the first time. To explain this point, we start by discussing what we mean by asymmetry and how it derails the second moment method. That this is so was already intuited in [4, 6]. In the next section, we are going to verify and elaborate on those discussions.

## 2. ASYMMETRY AND THE SECOND MOMENT METHOD

**The second moment method.** In general, the second moment method works as follows. Suppose that \( Z = Z(\Phi) \) is a non-negative random variable such that \( Z > 0 \) only if \( \Phi \) is satisfiable. Moreover, suppose that for some density \( r > 0 \) there is a number \( C = C(k) > 0 \) that may depend on \( k \) but not on \( n \) such that

\[ 0 < E[Z^2] \leq C \cdot E[Z]^2. \] \hspace{1cm} (4)

We claim that then \( r_{k-\text{SAT}} \geq r \). Indeed, the Paley-Zygmund inequality

\[ P[Z > 0] \geq \frac{E[Z^2]}{E[Z]} \] \hspace{1cm} (5)

implies that \( P[\Phi \text{ is satisfiable}] \geq P[Z > 0] \geq 1/C \). Because the right hand side remains bounded away from 0 as \( n \to \infty \), the following simple consequence of Friedgut’s sharp threshold result implies \( r_{k-\text{SAT}} \geq r \).

**Lemma 1** ([17]). Let \( k \geq 3 \). If for some \( r \) we have

\[ \liminf_{n \to \infty} P[\Phi \text{ is satisfiable}] > 0, \]

then \( r_{k-\text{SAT}} \geq r - o(1) \).

Hence, we “just” need to find a random variable that satisfies (5). Let \( S(\Phi) \) denote the set of satisfying assignments; then certainly \( Z = |S(\Phi)| \) is the most obvious choice. However, this “vanilla” second moment argument turns out to fail spectacularly. We need to understand why.

**Asymmetry and the majority vote.** The origin of the problem is that \( k \)-SAT is asymmetric in the following sense.
Suppose that we all know about the random formula $\Phi$ is for each variable $x$ the number $d_x$ of times that $x$ appears as a positive literal in the formula, and the number $d_{\neg x}$ of negative occurrences. Then our best stab at constructing a satisfying assignment seems to be the “majority vote” assignment $\sigma_{maj}$ where we set $x$ to true if $d_x > d_{\neg x}$ and to false otherwise. Indeed, by maximizing the total number of true literal occurrences, of which a satisfying assignment must put one in every clause, $\sigma_{maj}$ also maximizes the probability of being satisfiable.

Our proof of Theorem 1 allows us to formalize this observation, thereby verifying a conjecture from [6]. Let $\text{dist}(\cdot, \cdot)$ denote the Hamming distance.

**Corollary 1.** Let $r_{BP}$ be as in (3). There is a number $\delta = \delta(k) > 0$ such that for $2^k/k < r < r_{BP}$ w.h.p. we have

$$
\sum_{\sigma \in \mathcal{S}(\Phi)} \frac{\text{dist}(\sigma, \sigma_{maj})}{|\mathcal{S}(\Phi)|} \leq \left( \frac{1}{2} - \delta \right) \cdot n. 
$$

Hence, the average Hamming distance of $\sigma \in \mathcal{S}(\Phi)$ from $\sigma_{maj}$ is strictly smaller than $n/2$, i.e., the set $\mathcal{S}(\Phi)$ is “skewed toward” $\sigma_{maj}$ w.h.p.

This asymmetry does not the second moment method. To see why, let

$$
w_{maj} = w_{maj}(\Phi) = \frac{\max \{d_x, d_{\neg x}\}}{km}
$$

denote the **majority weight** of $\Phi$. Then the larger $w_{maj}$, the more likely $\sigma_{maj}$ and assignments close to it are to be satisfying. In effect, the bigger $w_{maj}$, the more satisfying assignments we expect to have. The consequence of this is that the number $|\mathcal{S}(\Phi)|$ of satisfying assignments behaves like a “lottery”: its expectation is driven up by a tiny fraction of “lucky” formulas with $w_{maj}$ much bigger than expected.

Let us highlight this tradeoff, as it is characteristic of the kind of trouble that asymmetry causes. For $\xi > 0$ independent of $n$ but sufficiently small it turns out that for a certain constant $c > 0$,

$$
P[w_{maj} \sim E[w_{maj}]] + \xi = \exp\left[-(c\xi^2 + O(\xi^3))n\right].
$$

That is, the probability is exponentially small but, like in the Chernoff bound, the exponent is a quadratic function of $\xi$. By comparison, increasing the majority weight by $\xi$ boosts the expected number of satisfying assignments by a linear exponential factor: there is $c > 0$ such that

$$
E[|\mathcal{S}(\Phi)| | w_{maj} \sim E[w_{maj}]] + \xi = \exp\left[c\xi + O(\xi^2)\right]n \cdot E[|\mathcal{S}(\Phi)| | w_{maj} \sim E[w_{maj}]].
$$

The exponent in (8) is linear because for a typical assignment $\tau$ at distance $(\frac{1}{2} - \delta)n$ from $\sigma_{maj}$ increasing $w_{maj}$ by $\xi$ boosts the number of literals that are true under $\tau$ by $2\delta \cdot km$, a term that is linear in $\xi$.

Since the exponent is linear in (8) but quadratic in (7), there is a (small but) strictly positive $\xi > 0$ such that the “gain” $\exp\left[c\xi + O(\xi^2)\right]n$ in the expected number of satisfying assignments exceeds $\exp\left[-(c\xi^2 + O(\xi^3))n\right]$, which is the “penalty” for deviating from $E[w_{maj}]$. With little extra work, this observation leads to

**Lemma 2.** For any $k \geq 3$ and $r > 2^k/k$ we have

$$
|\mathcal{S}(\Phi)| \leq \exp\left(-\Omega(4^{-k}) \cdot n\right) \cdot E[|\mathcal{S}(\Phi)|] 
$$

w.h.p. Lemma 2 entails rather easily that the “vanilla” second moment argument fails dramatically. Indeed, as already noticed in [4, 6], we have $E[|\mathcal{S}(\Phi)|^2] \geq \exp(\Omega(n)) \cdot E[|\mathcal{S}(\Phi)|]^2$. Hence, we miss our mark (4) by an exponential factor. But Lemma 2 is witness to an even worse failure: not only does (4) fail to hold, but even the normally much more dependable first moment overshoots the “actual” number of satisfying assignments by an exponential factor! (Lemma 2 is an improvement of an observation from [1], showing that $|\mathcal{S}(\Phi)| \leq \exp(-\xi n)\cdot E[|\mathcal{S}(\Phi)|]$ w.h.p. for some very small $\xi = \xi(k) > 0$; we conjecture that the $4^{-k}$ term in Lemma 2 is tight.)

In summary, the drift toward $\sigma_{maj}$ and the resulting fluctuations of the majority weight induce a tremendous source of variance, derailing the “vanilla” second moment argument.

**Balanced assignments.** A natural way to sidestep this issue is to work with a ‘symmetric’ subset of $\mathcal{S}(\Phi)$. Perhaps the most obvious choice is the set $\mathcal{S}_{NAE}(\Phi)$ of NAE-solutions. In a landmark paper, Achlioptas and Moore [4] proved that indeed there is $C = C(k) > 0$ such that for $\mathcal{S}_{NAE} = \mathcal{S}_{NAE}(\Phi)$ we have

$$
E[|\mathcal{S}_{NAE}|^2] \leq \mathcal{C} \cdot E[|\mathcal{S}_{NAE}|^2]^2,
$$

for $r \geq 2^{-k} \cdot \ln 2 - O(k)$. (9)

As we saw above (cf. Lemma 1), this implies that

$$
r_{SAE - SAT} \geq 2^{-k} \cdot \ln 2 - O(k).
$$

However, a simple (first moment) calculation shows that for $r > 2^{-k} \cdot \ln 2$, the set $\mathcal{S}_{NAE}(\Phi)$ is empty w.h.p. Thus, the idea of working with NAE-solutions stops working at $r = 2^{-k} \cdot \ln 2$, about a factor of two below the satisfiability threshold.

Achlioptas and Peres [6] obtained a better bound by precipitating symmetry in a more subtle manner. Let us call $\sigma \in \{0, 1\}^n$ **balanced** if under $\sigma$ out of the $km$ literal occurrences in $\Phi$ exactly half are true (i.e., $\frac{km}{2} \pm 1$). Thus, balanced assignments are expressly forbidden from pandering to $\sigma_{maj}$. Now, let $\mathcal{S}_{bal}(\Phi)$ be the set of all balanced satisfying assignments, and set $\mathcal{S}_{bal} = |\mathcal{S}_{bal}(\Phi)|$. Achlioptas and Peres used a clever weighting scheme to prove that

$$
E[|\mathcal{S}_{bal}|^2] \leq \mathcal{C} \cdot E[|\mathcal{S}_{bal}|^2]^2
$$

for $r \leq r_{bal}$ (cf. (2)). (10)

As before, this implies that $r_{SAE - SAT} \geq r_{bal}$ (Lemma 1).

Yet as in the case of NAE-solutions, balanced satisfying assignments cease to exist way before the satisfiability threshold. Indeed, Achlioptas and Peres observed that $\mathcal{S}_{bal}(\Phi) = \emptyset$ for $r > 2^{-k} \cdot \ln 2 - k \ln 2$ w.h.p. In effect, to close in further on $r_{SAE - SAT}$ we will have to accommodate assignments that lean toward $\sigma_{maj}$. How can this be accomplished?

A **quick fix?** We saw that to make an asymmetric second moment argument work, we need to rule out fluctuations of the majority weight. A sensible way of implementing this is by actually fixing the entire vector $d = (d_x, d_{\neg x})_{x \in V}$ that counts the positively/negatively occurrences of each variable. More precisely, given a non-negative integer vector $d = (d_x, d_{\neg x})_{x \in V}$ with $\sum_{x \in V} d_x + d_{\neg x} = km$ let $\Phi_d$ denote a uniformly random $k$-CNF in which each variable $x$ appears $d_x$ times positively and $d_{\neg x}$ times negatively. Then we can split the generation of a random formula $\Phi$ into two steps:

First, choose the occurrence vector $d$ randomly from the “correct” distribution $D$.

Then, choose a random formula $\Phi_d$. 
The “correct” $D$ is as follows. Let $e = (e_x, e_y)_{x \in V}$ be a family of independent Poisson variables with mean $kr/2$ each. Moreover, let $\mathcal{E}$ be the event that $\sum_{x \in V} e_x + e_y = km$. Let $D$ be the conditional distribution of $e$ given $\mathcal{E}$. Then standard arguments show that the outcome of first choosing $d$ and then $\Phi_d$ is exactly the uniformly random $\Phi$.

The point of generating $\Phi$ in two steps as above is that given the outcome $d$ of the first step, the majority weight is fixed. Hence, if we could show that given a “typical” $d$, the second moment succeeds for $|S(\Phi_d)|$ we would obtain a lower bound on $r_{k-SAT}$. Unfortunately, matters are not so simple.

**Lemma 3.** W.h.p. for a vector $d$ chosen from $D$ we have $E[|S(\Phi_d)|^2] \geq \exp(\Omega(n)) \cdot E[|S(\Phi_d)|^2]$.

Let us stress the two levels of randomness in Lemma 3. First, there is the choice of $d$. Then, for a given $d$, we compare $E[|S(\Phi_d)|^2]$ and $E[|S(\Phi_d)|^2]$. Of course, both of these quantities depend on $d$, and we find that w.h.p. $d$ is such that the first exceeds the second by an exponential factor.

The explanation for this is that even if we fix $d$, various other types of fluctuations remain, turning $|S(\Phi_d)|$ into a “lottery”. For instance, even given $d$ we compare $E[|S(\Phi_d)|^2]$ and $E[|S(\Phi_d)|^2]$. Unfortunately, for $\tau > r_{BP}$ the replica symmetric version (and in particular the Belief Propagation predictions that we depend upon) are conjectured to break down. According to the more sophisticated “1-step replica symmetry breaking” (1RSB) version of the cavity method, the reason for this is that at $\tau \sim r_{BP}$ a new type of correlation amongst satisfying assignments arises. To deal with these correlations, the physics methods replace Belief Propagation by the much more intricate Survey Propagation technique.

In [11] we managed to prove rigorously that the 1RSB prediction for the random $k$-NAE-SAT threshold is correct (up to an additive $2^{-\Omega(k)}$). However, [11] depends heavily on the fact that $k$-NAE-SAT is symmetric. While it would be very interesting to combine the merits of the present paper with those of [11], this appears to be quite challenging. Thus, putting the 1RSB calculation for random $k$-SAT on a rigorous foundation remains an important open problem.

That said, we believe that any such attempt would need to build upon the techniques developed in this paper.

3. RELATED WORK

The interest in random $k$-SAT originated largely from the experimental observation that there seems to be a sharp threshold for satisfiability and, moreover, that for certain densities $r < r_{k-SAT}$ to polynomial time algorithm is known to find a satisfying assignment w.h.p. [21, 23]. Currently, the precise $k$-SAT threshold is known (rigorously) only in two cases. Chvatal and Reed [8] and Goerdt [20] proved independently that $r_{2-SAT} = 1$. Of course, 2-SAT is special because there is a simple criterion for (un)satisfiability, which enables the proofs of [8, 20]. Unsurprisingly, these methods do not extend to $k > 2$. Additionally, the threshold is known precisely when $k > \log_2 n$, i.e., the clause length diverges as a function of $n$ [19]. In this case, the problem of asymmetry evaporates because the majority weight is sufficiently concentrated for the “vanilla” second moment method to succeed. (Note that Proposition 2 holds for any fixed $k$, but not for $k = k(n) \to \infty$.) The issue of asymmetry also disappears in the case of strongly regular formulas [29] where for some fixed $d$ we have $d_\sigma = d_\epsilon = d$ for all $x \in V$. In random $k$-XORSAT (random linear equations mod 2) the threshold for the existence of solutions is known precisely [14]. The proof relies on computing the second moment of the number of solutions (after the instance has been stripped down to a suitable core). In contrast to random $k$-SAT, the random $k$-XORSAT problem is symmetric (cf. Remark 3 below), albeit in a more subtle way than $k$-XORSAT.

Other problems where the second moment method succeeds are symmetric as well. Pioneering the use of the second moment method in random CSPs, Achlioptas and Moore [4] computed the random $k$-NAESAT threshold within an additive $1/2$. By enhancing this argument with insights from physics this gap can be narrowed to a mere $2^{-\Theta(k)}$ [11, 12]. Moreover, the best current bounds on the random (hyper)graph $k$-colorability thresholds are based on “vanilla” second moment arguments as well [5, 15]. In summary, in all the previous second moment arguments, the issue of asymmetry either did not appear at all by the nature of the problem [4, 5, 11, 12, 14, 15, 19], or it was sidestepped [6].

The best current algorithms for random $k$-SAT find satisfying assignments w.h.p. for densities up to $1.817 \cdot 2^{k/4}/k$ (better for small $k$) resp. $2^{k \ln(k)/k}$ (better for large $k$) [9, 18], a factor of $\Theta(k/k)$ below the satisfiability threshold. By comparison, the Lovasz Local Lemma and its algorithmic version succeed up to $r = \Theta(2^{1/k^2})$ [28].

Apart from experimental work [23], very little is known about the physics-inspired message passing algorithms (“Belief/Survey Propagation guided decimation”) [25]. The most basic variant of Belief Propagation guided decimation is known to fail w.h.p. on random formulas if $r > c \cdot 2^{k/4}/k$ for some constant $c > 0$ [10]. However, it is conceivable that Survey Propagation and/or other variants of Belief Propagation perform better.

4. THE RANDOM VARIABLE

Our goal is to make the second moment method work for a random variable that counts “asymmetric” satisfying assignments. In this section, we develop this random variable. The starting point, and the key ingredient, is simply a map $p : [0,1] \to [0,1]$. For the sake of clarity, we start by setting up the framework for generic maps $p$; below we will use the Belief Propagation formalism to pick the “optimal” $p$.

The idea is that $p$ prescribes how strongly the assignments that we work with lean toward the majority vote. Informally speaking, we are going to work with assignments such that a variable $x$ that occurs $d_x$ times positively and $d_\epsilon$ times negatively has a $p(d_\epsilon - d_\epsilon)$ chance of being set to ‘true’. 


Before we give a formal definition, we need to fix the number of times that each variable appears positively or negatively.

**Fixing the majority weight.** As we saw in Section 2, in order to make the second moment argument work, we need to rule out fluctuations of the majority weight. To achieve this, we follow the strategy outlined in Section 2. That is, we are going to work with formulas \( \Phi_d \) with a given vector \( d = (d_l, d_{-l}) \) of occurrence counts, where each variable \( x \) appears precisely \( d_x \) times positively and \( d_{-x} \) times negatively. As in Section 2, we let \( D \) denote the (conditional Poisson) distribution over sequences \( d \) such that first choosing \( d \) from \( D \) and then generating \( \Phi_d \) is equivalent to choosing a k-CNF \( \Phi \) uniformly at random.

**Fixing the marginals.** Now, fix one such vector \( d \). Then the map \( p : Z \to [0, 1] \) induces a map \( p_d \) from the set \( L = \{ x, \neg x : x \in V \} \) of literals to \([0, 1]\) in the natural way: we let

\[
p_d(x) = p(d_x) \quad \text{and} \quad p_d(\neg x) = 1 - p(x).
\]  

(11)

The idea is that, given \( d \), we should set variable \( x \) to ‘true’ with probability \( p_d(x) \).

To formalize this, we call \( p_d \) the \( p_d \)-type of the literal \( t \). Let \( \mathcal{L}_d = \{ p_d(l) : l \in L \} \) be the set of all possible \( p_d \)-types. We say that \( \sigma : V \to \{0, 1\} \) has \( p_d \)-marginals if for any type \( t \in \mathcal{L}_d \) we have

\[
\sum_{t \in L : p_d(t) = t} \sigma(t) \cdot d_t = t \cdot \sum_{t \in L : p_d(t) = t} d_t,
\]

(12)
i.e., among all occurrences of literals of type \( t \), a \( t \) fraction is true under \( \sigma \). This definition captures the above idea that variable \( x \) has a \( p_d(x) \) chance of being ‘true’.

**Fixing the clause types.** We define the \( p_d \)-type of a clause \( l_1 \lor \cdots \lor l_k \) as the \( k \)-tuple \((p_d(l_1), \ldots, p_d(l_k)) \) \( \in [0, 1]^k \) comprising of the individual literal types. Let \( \mathcal{L}_d = \mathcal{L}_d^{\Phi_d} \) be the set of all possible clause types. For each \( \ell \in \mathcal{L}_d \) let \( M_{\Phi_d}(\ell) \) be the set of indices \( i \in [m] \) such that \( \ell \) is a clause of \( \Phi_d \) and \( m_{\Phi_d}(\ell) = |M_{\Phi_d}(\ell)| \).

In addition to fluctuations of the majority weight, we also need to suppress fluctuations of the numbers \( m_{\Phi_d}(\ell) \). We are going to use the same trick as in the case of the majority weight. Namely, we split the generation of a random formula \( \Phi_d \) into two steps:

First, choose a vector \( m = (m(\ell))_{\ell \in \mathcal{L}} \) from the “correct” distribution \( M_d \).

Then, generate a formula \( \Phi_d(m) \) uniformly at random in which each variable \( x \) appears exactly \( d_x \) times positively and exactly \( d_{-x} \) times negatively and that has exactly \( m(\ell) \) clauses of type \( \ell \) for all \( \ell \in \mathcal{L} \).

Formally, the “correct” \( M_d \) is just the distribution of the random vector \( m_{\Phi_d} = (m_{\Phi_d}(\ell))_{\ell \in \mathcal{L}} \) that counts the clauses by types in the “unrestricted” formula \( \Phi_d \). It is easily verified that the overall outcome of the above experiment is identical to \( \Phi_d \). From now on, we fix both \( d \) and \( m \).

Given \( d, m \) there is a simple way of generating the random formula \( \Phi_d(m) \). Namely, create \( d_l \) clones of each literal \( \ell \), and put all the clones of a given \( p_d \)-type on a pile. Then the formula \( \Phi_d(m) \) is simply the result of matching the clones on the type \( t \) pile randomly to all the clauses where a literal of type \( t \) is required.

An assignment \( \sigma \) with \( p_d \)-marginals splits each pile into two subsets, namely the clones that are true under \( \sigma \) and those that are false. For each type \( t \), among the clones in the type \( t \) pile, a \( t \)-fraction are true, since \( \sigma \) has \( p_d \)-marginals. Therefore, we expect that under the random matching, for each clause type \( \ell = (\ell_1, \ldots, \ell_k) \) and each index \( j \), in an \( \ell_j \)-fraction of that clauses the \( j \)th literal is matched to a ‘true’ clone.

**Judicious assignment.** This observation motivates the following definition. Let \( \Phi_{d,m} \) denote \( \Phi_d(m) \) if for all clause types \( \ell = (\ell_1, \ldots, \ell_k) \in \mathcal{L} \) and all \( j \in [k] \) we have

\[
\sum_{i \in M_{\Phi_{d,m}}(\ell)} \sigma(\Phi_{d,m,i,j}) = m(\ell) \cdot \ell_j,
\]

(12)

where \( \Phi_{d,m,i,j} \) denotes the \( j \)th literal of the \( i \)th clause of \( \Phi_{d,m} \), and the sum is over all \( i \) such that the \( i \)th clause has type \( \ell \). Let \( \mathcal{S}_p(\Phi_{d,m}) \) be the set of \( p \)-judicious satisfying assignments, and set \( Z_p(\Phi_{d,m}) = |\mathcal{S}_p(\Phi_{d,m})| \).

Given that \( \sigma \) is \( p \)-judicious, in order for \( \sigma \) to be satisfying we just need that for each type \( \ell \) the ‘true’ clones are distributed so that each clause receives at least one. Thus, the event of being satisfying is merely a matter of how exactly the ‘true’ clones are “shuffled” amongst the clauses of type \( \ell \), while for each \( j \) the total number of ‘true’ clones of type \( \ell_j \) is fixed. In particular, this shuffling occurs independently for each clause type. Such random shuffling problems tend to be amenable to the second moment method. Therefore, it seems reasonable to expect that a second moment argument succeeds for \( Z_p(\Phi_{d,m}) \). This is indeed the case for \( r < r_{BP} = 1 + \ln 2 \approx 0.3 \). However, to actually reach \( r_{BP} \) we need to control one further parameter.

**Fixing the cluster size.** According to the physics predictions [24, 25], for \( r_{marg} < r < r_{BP} \) the set of satisfying assignments decomposes into an exponential number of well-separated ‘clusters’. More precisely, we expect that w.h.p. for any two satisfying \( \sigma, \tau \) either \( \text{dist}(\sigma, \tau) < 0.01n \) (if \( \sigma, \tau \) belong to the same cluster), or \( \text{dist}(\sigma, \tau) > 0.49n \) (different clusters). Formally, we simply define the cluster of \( \sigma \) as

\[
\mathcal{C}_\sigma = \{ \tau \in \mathcal{S}(\Phi) : \text{dist}(\sigma, \tau) \leq 0.01n \}.
\]

The intuitive reason why the second moment argument for \( Z_p(\Phi_{d,m}) \) breaks down for \( r \) close to \( r_{BP} \) is that the cluster sizes \( |\mathcal{C}_\sigma(\Phi_{d,m})| \) fluctuate. A similar problem occurred in prior work on random \( k \)-NAESAT [11, 12].

As in those papers, the problem admits a remarkably simple solution: let us call an assignment \( \sigma \) good in \( \Phi_{d,m} \) if

\[
|\mathcal{C}_\sigma(\Phi_{d,m})| \leq E[Z_p(\Phi_{d,m})].
\]

(13)

Let \( \mathcal{S}_{p,good}(\Phi_{d,m}) \) be the set of all good \( \sigma \in \mathcal{S}_p(\Phi_{d,m}) \). To avoid fluctuations of the cluster size, we are just going to work with \( Z_{p,good} = |\mathcal{S}_{p,good}(\Phi_{d,m})| \).

**The second moment bound.** We now face the task of estimating the first and the second moment of \( Z_{p,good}(\Phi_{d,m}) \). The result can be summarized as follows.

**Theorem 2.** Suppose \( r_{marg} < r < r_{BP} \), where \( r_{BP} \) is as in (3). There exists \( C = C(k) \) and a map \( p = p_B : Z \to [0, 1] \) such that for \( d \) chosen from \( D \) and for \( m \) chosen from \( M_d \) w.h.p.

\[
0 < E[Z_{p,good}(\Phi_{d,m})^2] \leq C \cdot E[Z_{p,good}(\Phi_{d,m})]^2.
\]
Together with Paley-Zygmund (5), Theorem 2 shows that with \(d\) chosen from \(D\) and \(m\) chosen from \(M_d\) w.h.p.

\[
P[\Phi_{d,m} \text{ is satisfiable}] \geq P[Z_{p,good}((d,m)) > 0] \geq \frac{E[Z_{p,good}((d,m))]^2}{E[Z_{p,good}((d,m))]^2} \geq \frac{1}{C}.
\]

The construction of \(D, M_d\) ensures that choosing \(\Phi\) at random is the same as first picking \(d\) from \(D\) and \(m\) from \(M_d\) and then generating \(\Phi_{d,m}\). Therefore, (14) implies \(\lim_{n \to \infty} P[\Phi \text{ is satisfiable}] > 0\), so that Lemma 1 yields \(r_k-SAT \geq r_{BP}\). Hence, we are left to prove Theorem 2. We begin by constructing the map \(p_{BP}\).

**Guessing the marginals.** For a set \(\emptyset \neq S \subset \{0,1\}^V\) and a variable \(x\) we define the \(S\)-marginal of \(x\) as

\[
\mu_S(x) = \sum_{\sigma \in \Sigma} \frac{\sigma(x)}{|S|}.
\]

The definition of ‘\(p_d\)-judicious’ is guided by the idea that \(p_d(x)\) should prescribe the marginal of \(x\) in the set of all \(p_d\)-judicious satisfying assignments. Hence, in order to make the set of \(p_d\)-judicious assignments as good an approximation of the entire set of satisfying assignments as possible, we better pick \(p\) so that \(p_d(x)\) is a good approximation to the actual marginal \(\mu_S(\Phi_d)(x)\) of \(x\) in the set of all satisfying assignments. The problem is that, because of the asymmetry of the \(k\)-SAT problem, these marginals are highly non-trivial quantities. Indeed, on general formulas \(\Phi\) the marginals \(\mu_S(\Phi)(x)\) are \#P-hard to compute.

However, according to the physicists’ cavity method, on random formulas with density \(r < r_{BP}\) the marginals can be computed by means of an efficient message passing algorithm called **Belief Propagation** [24]. While the mechanics of these are not important in our context, the result is:

**Conjecture 1.** Suppose that \(r_{val} < r < r_{BP}\). Let \(d\) be chosen from \(D\) and let \(x\) be a variable. Then w.h.p.

\[
\mu_S(\Phi_d)(x) = \frac{1}{2} + \frac{d_x - d_{\neg x}}{2^{k+1}} + O \left( \frac{d_x - d_{\neg x}}{2^k} \right)^2.
\]

We observe that (16) is in line with the notion that \(S(\Phi_d)\) is “skewed toward” \(\sigma_{maj}\). Indeed, the conjecture quantifies how much so. Motivated by Conjecture 1, we define

\[
p_{BP}(z) = \begin{cases} 
\frac{1}{2} + \frac{z}{2^{k+1}} & \text{if } |z| \leq 10\sqrt{k^2 \ln k}, \\
\frac{1}{2} & \text{otherwise}.
\end{cases}
\]

Under the distribution \(D\), the random variables \(d_x, d_{\neg x}\) are asymptotically independent Poisson with mean \(kr/2\) (cf. Section 2). Therefore,

\[
E_d \left[ (d_x - d_{\neg x})^2 \right] = kr \leq k^2 \ln 2,
\]

and standard concentration inequalities show that w.h.p. there are no more than \(n/k^{30}\) variables \(x\) with \((d_x - d_{\neg x})^2 > 100k^2 \ln k\). Hence, \(p_{d} = p_{BP,d}\) is (asymptotically) equal to the conjectured value on the bulk of variables w.h.p.

In summary, the problem with the “vanilla” second moment argument is that the drift toward the \(\sigma_{maj}\) induces correlations amongst satisfying assignments. Indeed, they are correlated with the majority assignment and thus with each other. We circumvent this problem by explicitly prescribing the marginal probability that each variable is set to ‘true’. One could think of this as working with the intersection of \(S(\Phi)\) with a particular “surface” within the Hamming cube \(\{0,1\}^n\), namely the assignments with \(p_d\)-marginals. Within this surface, all assignments are slanted equally toward \(\sigma_{maj}\). The Belief Propagation-informed definition of \(p_{BP}\) is meant to ensure that the surface that we consider with is (about) the most populous one, i.e., the one with the largest number of satisfying assignments in it. The core of our argument will be to show that with respect to the marginal distribution \(p_{DBP}\), i.e., within the surface that \(p_{DBP}\) defines, two random elements of \(S_p(\Phi_{d,m})\) are typically uncorrelated (Proposition 2 below). But before we come to that, we need to compute the “first moment”, i.e., the expected number of good \(p_{BP}\)-judicious satisfying assignments.

**Remark 1.** Belief Propagation actually leads to a stronger prediction than Conjecture 1. Namely, it yields a conjecture for \(\mu_S(\Phi_d)(x)\) up to an additive error then tends to 0 as \(n \to \infty\). However, (a) this stronger conjecture is not in explicit form, and (b) it does not only depend on \(d_x, d_{\neg x}\), but also on various other parameters. In any case, even a more accurate prediction would not yield a better constant than \(\frac{1}{2}\ln 2\) in Theorem 1.

**Remark 2.** In the present framework, the notion of balanced satisfying assignments from [6] simply corresponds to working with the constant map \(p_{val} : Z \to [0,1], z \mapsto \frac{1}{2}\). This highlights that the improvement that we obtain here stems from choosing the non-constant map \(p_{BP}\) inspired by Belief Propagation.

**Remark 3.** The definition (15) of the marginal of a variable with respect to some set does give rise to a formal notion of ‘symmetric problem’. Namely, we could call a binary random CSP symmetric if its set \(S_{CSP}(\Phi)\) of solutions is such that for each variable \(x\) w.h.p. \(\mu_{SCSP}(\Phi)(x) = \frac{1}{2} + o(1)\).

Clearly, \(k\)-NAESAT passes this test as \(\mu_{S_{k-NAE}}(\Phi)(x) = \frac{1}{2}\) for all \(x\) with certainty. Similarly, the problem of having a balanced satisfying assignment is symmetric [6], as is random \(k\)-XORSAT.

From here on out we keep the assumptions of Theorem 2. In particular, we assume \(r_{val} < r < r_{BP}\). Let \(d\) be chosen from \(D\), and let \(m\) be chosen from \(M_d\). Let \(p = p_{BP}\) be as in (17) and \(p_d\) as in (11).

## 5. THE FIRST MOMENT

Let \(r > \frac{1}{2}\ln 2\) be such that \(r = 2^k \ln 2 - \rho\).

**Proposition 1.** W.h.p. \(d, m\) are such that

\[
E[Z_{p,good}((d,m))] = \exp \left[ \frac{n}{2^k} \left( \rho - \ln \frac{2}{2} + o_k(1) \right) \right].
\]

We begin by computing \(E[Z_{p}((d,m))]\). By definition, any assignment that is \(p_d\)-judicious has \(p_d\)-marginals. Thus, let \(\mathcal{H}_{p}(d) \subset \{0,1\}^V\) denote the set of all assignments that have \(p_d\)-marginals. Then by the linearity of expectation,

\[
E[Z_{p}((d,m))] = \sum_{\sigma \in \mathcal{H}_p(d)} P[\sigma \in S_p(\Phi_{d,m})].
\]
Lemma 4. Let \( \chi(z) = -z \ln z - (1 - z) \ln(1 - z) \) denote the entropy function. Then w.h.p. \( \mathbf{d} \) is such that
\[
\ln |\mathcal{H}_p(\mathbf{d})| \sim n \sum_{x \in V} \chi(p(x)).
\]

Taylor expanding \( \chi(z) \) around \( z = 1/2 \) and exploiting the definition (17) of \( p \) we obtain (after a lengthy but straightforward calculation) that w.h.p. \( \mathbf{d} \) is such that
\[
\frac{1}{n} \ln |\mathcal{H}_p(\mathbf{d})| = \ln 2 - \frac{k \ln 2}{2^k} + o_k(2^{-k}).
\]

As a next step we compute the probability of the event "\( \sigma \in S_p(\Phi_{d,m}) \)" for \( \sigma \in \mathcal{H}_p(\mathbf{d}) \).

Lemma 5. W.h.p. \( \mathbf{d}, \mathbf{m} \) are such that for any \( \sigma \in \mathcal{H}_p(\mathbf{d}) \),
\[
\frac{1}{n} \ln P[\sigma \in S_p(\Phi_{d,m})] = -\ln 2 - \frac{k \ln 2}{2^k} + O(1)
\]

Let us defer the proof of Lemma 5, which is the core of the first moment computation, for a little while. Combining (18)–(20) we see that w.h.p. over the choice of \( \mathbf{d}, \mathbf{m} \) we have
\[
\frac{1}{n} \ln E[Z_p(\Phi_{d,m})] = \ln |\mathcal{H}_p(\mathbf{d})| + \ln P[\sigma \in S_p(\Phi_{d,m})]
\sim 2^{-k} \left( \rho - \frac{\ln 2}{2} + o_k(1) \right) \cdot n
\]

To obtain the expectation of \( Z_{p,\text{good}} \), we show the following.

Lemma 6. W.h.p. over the choice of \( \mathbf{d}, \mathbf{m} \) we have
\[
E[Z_{p,\text{good}}(\Phi_{d,m})] \sim E[Z_{p}(\Phi_{d,m})].
\]

The proof of Lemma 6 is based on arguments developed in [1] for analyzing the geometry of the set of satisfying assignments. Combining (21) and Lemma 6 yields Proposition 1. Proof of Lemma 5. In the random formula \( \Phi_{d,m} \) there are dependencies amongst the clauses, arising, e.g., from prescribing the precise number of occurrences for each literal. The key idea of the proof is to work with a different probability space in which the clauses and even the individual literals behave independently.

The elements of this new space \( \hat{\Omega} \) are all 0/1 vectors
\[
(\hat{\sigma}_{ij}(\ell))_{\ell \in \mathcal{L}, j \in [m(\ell)], i \in [k]}
\]

The idea is that \( \hat{\sigma}_{ij}(\ell) \) is going to represent the truth value of the \( j \)th literal of the \( i \)th clause of type \( \ell \). The probability distribution \( \hat{P} \) on \( \hat{\Omega} \) is defined via a parameter vector
\[
\mathbf{q} = (q_{i,j})_{\ell \in \mathcal{L}, j \in [k]}
\]

with entries in \([0, 1] \): each \( \hat{\sigma}_{ij}(\ell) \) is the result of a Bernoulli experiment with success probability \( q_{i,j} \), and these experiments are independent for all \( \ell, i, j \). We will choose \( \mathbf{q} \) below so that we can compute the first moment (relatively) easily.

For each \( \ell = (\ell_1, \ldots, \ell_k) \in \mathcal{L} \) and each \( j \in [m(\ell)] \) let \( S_i(\ell) \) be the event that \( \max_{j \in [m(\ell)]} \hat{\sigma}_{ij}(\ell) = 1 \). This is going to mirror the event that the \( i \)th clause of type \( \ell \) is satisfied. Let
\[
S = \bigcap_{\ell \in \mathcal{L}} \bigcap_{i \in [m(\ell)]} S_i(\ell)
\]

which is going to reflect the event that all clauses are satisfied. Further, for any \( j \in [k] \) let \( B_j(\ell) \) be the event that
\[
\sum_{i \in [m(\ell)]} \hat{\sigma}_{ij}(\ell) = m(\ell) \cdot \ell_j.
\]

Let \( B = \bigcap_{\ell \in \mathcal{L}, j \in [k]} B_j(\ell) \) to capture the event of being judicious.

We observed in Section 4 that given \( \mathbf{d}, \mathbf{m} \), choosing \( \Phi_{d,m} \) amounts to generating a random matching between literal occurrences of each type \( t \) and clauses where literals of type \( t \) are required. This observation leads to

Lemma 7. Assume that \( \mathbf{q} \) satisfies \( \hat{P}[B] = 0 \). Then for any \( \sigma \in \mathcal{H}_p(\mathbf{d}) \) we have
\[
P[\sigma \in S_p(\Phi_{d,m}) | \sigma \text{ is } p_{d,t} \text{-judicious}] = \hat{P}[S | B].
\]

Suppose that \( \sigma \) has \( p \)-marginals. Viewing \( \Phi_{d,m} \) as a random matching, we see that for each \( \ell \in \mathcal{L} \) and for each \( j \in [k] \) the expected fraction of clauses of type \( \ell \) whose \( j \)th literal is true under \( \sigma \) equals \( \ell_j \). Hence, a local limit theorem yields
\[
P[\sigma \text{ is } p_{d,t} \text{-judicious}] = n^{-O(1)}
\]
for all \( \sigma \in \mathcal{H}_p(\mathbf{d}) \). (22)

We are left to compute \( \hat{P}[S | B] \). By the definition of \( \hat{P} \), it is quite easy to compute \( \hat{P}[S], \hat{P}[B] \) individually. Indeed, because the \( \hat{\sigma}_{ij}(\ell) \) are mutually independent, for any \( \ell \in \mathcal{L} \) and any \( i \in [m(\ell)] \) we have
\[
\hat{P}[S_i(\ell)] = 1 - \prod_{j=1}^{k}(1 - q_{i,j}), \text{ whence (23)}
\]
\[
\hat{P}[S] = \prod_{\ell \in \mathcal{L}} \left[ 1 - \prod_{j=1}^{k}(1 - q_{i,j}) \right]^{m(\ell)}. \quad (24)
\]

Once more by independence, for any \( \ell \in \mathcal{L}, j \in [k] \) the sum \( \sum_{i \in [m(\ell)]} \hat{\sigma}_{ij}(\ell) \) has a binomial distribution \( \text{Bin}(m(\ell), q_{i,j}) \).

As a consequence,
\[
\hat{P}[B] = \prod_{\ell,j} P[\text{Bin}(m(\ell), q_{i,j}) = m(\ell) \cdot \ell_j + O(1)]
\]
\[
= \exp\left[ o(n) + \sum_{\ell,j} m(\ell) \psi(q_{i,j}, \ell_j) \right], \quad (25)
\]

where
\[
\psi(x, y) = -y \ln \left( \frac{y}{x} \right) - (1 - y) \ln \left( \frac{1 - y}{1 - x} \right)
\]

denotes the Kullback-Leibler divergence. We stress that (24) and (25) hold for any \( \mathbf{q} \). Hence, if we could choose \( \mathbf{q} \) so that
\[
\hat{P}[B | S] = \exp(-o(n)), \quad (27)
\]
then
\[
\hat{P}[S | B] = \hat{P}[B | S] \cdot \hat{P}[S] / \hat{P}[B] \]
\[
= \exp(-o(n)) \cdot \hat{P}[S] / \hat{P}[B]. \quad (28)
\]

Lemma 8. There is \( \mathbf{q} \) such that (27) holds and
\[
q_{i,j} = \ell_j - 2^{-k-1} + \hat{O}(2^{-3k/2}) \quad \text{for all } \ell, j. \quad (29)
\]

Proof. By (23), for any \( \ell, j \) we have
\[
E[\sum_{i \in [m(\ell)]} \hat{\sigma}_{ij}(\ell)] = \frac{m(\ell)q_{i,j}}{1 - \prod_{j=1}^{k}(1 - q_{i,j})}.
\]

Hence, if we could choose \( \mathbf{q} \) so that
\[
\frac{q_{i,j}}{1 - \prod_{j=1}^{k}(1 - q_{i,j})} = \ell_j \quad \text{for all } \ell, j, \quad (30)
\]
then the local limit theorem for sums of independent random variables would imply $\mathbb{P}[B|S] = \exp(-o(n))$. Using the inverse function theorem from analysis, one can show that there is indeed a $q$ that satisfies both (29) and (30). $\square$

Plugging the definition (17) of $p = p_{BP}$ into (24)–(29), we can now compute $\ln \mathbb{P}[S|B] = \ln \mathbb{P}[S] - \ln \mathbb{P}[B]$ asymptotically. The result of this is the expression given in (20). Thus, Lemma 5 follows from Lemma 7 and (22).

6. THE SECOND MOMENT

We aim to prove the second part of Theorem 2. Thus, we need to estimate the expected number $Z = |S_{p,\text{good}}(\Phi_{d,m})|^2$ of pairs of good $p$-judicious satisfying assignments. The very definition of ‘good’ entails an easy bound if $\text{dist}(\sigma,\tau)$ is small. Indeed, let $Z_{\text{near}}$ be the number of pairs $(\sigma,\tau) \in S_{p,\text{good}}(\Phi_{d,m})$ with $\text{dist}(\sigma,\tau) \leq 0.01n$.

**Lemma 9.** We have $E[Z_{\text{near}}(\Phi_{d,m})] \leq E[Z_p(\Phi_{d,m})]^2$.

**Proof.** The bound (13) ensures that with certainty for any $\sigma \in S_{p,\text{good}}(\Phi_{d,m})$ we have

$$|\{\tau \in S_{p,\text{good}}(\Phi_{d,m}) : \text{dist}(\sigma,\tau) \leq 0.01n\}| \leq |C_0(\Phi_{d,m})| \leq E[Z_p(\Phi_{d,m})].$$

Hence, by the linearity of expectation,

$$E[Z_{\text{near}}(\Phi_{d,m})] = E \sum_{\sigma \in S_{p,\text{good}}(\Phi_{d,m})} |\{\tau \in S_{p,\text{good}}(\Phi_{d,m}) : \text{dist}(\sigma,\tau) \leq 0.01n\}| \leq E[Z_p(\Phi_{d,m})] \cdot E[Z_{p,\text{good}}(\Phi_{d,m})] \leq E[Z_p(\Phi_{d,m})]^2,$$

as claimed. $\square$

There is another range of distances for which we can get a quick bound. Let $\xi = \frac{n}{2^k}$ and let $Z_{\text{med}}$ be the number of pairs $(\sigma,\tau) \in S(\Phi_{d,m})$ such that $\text{dist}(\sigma,\tau) > 0.01n$ and $|\text{dist}(\sigma,\tau) - \frac{n}{2^k}| > \xi n$. A rather crude calculation yields the following.

**Lemma 10.** W.h.p. over the choice of $d,m$ we have $E[Z_{\text{med}}(\Phi_{d,m})] = o(1)$.

Thus, we are left to analyze the number $Z_{\text{centre}}$ of pairs $(\sigma,\tau) \in S(\Phi_{d,m})$ such that $|\text{dist}(\sigma,\tau) - \frac{n}{2^k}| \leq \xi n$. We zoom in on this range by quantifying the similarity between two assignments more accurately. Define the **overlap** of $(\sigma,\tau) \in \{0,1\}^V$ in $\Phi_{d,m}$ to be the vector

$$\omega(\sigma,\tau) = \omega_{\Phi_{d,m}}(\sigma,\tau) = (\omega_{\ell,j}(\sigma,\tau))_{\ell \in L, j \in [k]},$$

where

$$\omega_{\ell,j}(\sigma,\tau) = \frac{1}{m(\Phi_{d,m})} \sum_{i \in M_{\Phi_{d,m}}(\ell)} \sigma(M_{\Phi_{d,m}}(i,j)) \tau(M_{\Phi_{d,m}}(i,j)).$$

Thus, $\omega_{\ell,j}(\sigma,\tau)$ is the fraction of clauses of type $\ell$ in $\Phi_{d,m}$ whose $j$th literal is true under both $\sigma,\tau$. Let $\omega^* = (\omega^*_{\ell,j})$ with $\omega^*_{\ell,j} = \ell^2$ for all $\ell, j$.

**Lemma 11.** W.h.p. over the choice of $d,m$ the following is true. Choose two assignments $\sigma,\tau$ with $p$-marginals uniformly and independently. Then $E[\omega_{\Phi_{d,m}}(\sigma,\tau)] = \omega^*$.

For a vector $\omega = (\omega_{\ell,j})$ we let $Z_{\omega}$ denote the number of all $(\sigma,\tau) \in S_{p}(\Phi_{d,m})$ such that $\|\omega(\sigma,\tau) - \omega^*\|_{\infty} \leq O(1/n)$. The key step of the second moment analysis can be summarized as follows.

**Proposition 2.** There is $\zeta = \zeta(k) > 0$ such that w.h.p. over the choice of $d,m$ for all $\omega$ such that $\|\omega - \omega^*\|_{\infty} \leq 2\zeta$ we have

$$E[Z_{\omega}(\Phi_{d,m})] \leq \exp\left(-\zeta n \cdot \|\omega - \omega^*\|_{2}^{2}\right) \cdot E[Z_{\omega^*}(\Phi_{d,m})].$$

Before we come to the proof of Proposition 2, let us indicate how it implies the second moment bound. For $\delta > 0$ let $Z_{\omega,\delta}$ be the number of $(\sigma,\tau) \in S_{p}(\Phi_{d,m})$ such that $\|\omega(\sigma,\tau) - \omega^*\|_{\infty} \leq \delta$. Proposition 2 shows that the contribution of $Z_{\omega}$ decays exponentially in $\|\omega - \omega^*\|_{2}^{2}$. Therefore, with a bit of calculus we obtain

$$E[Z_{\omega,\ast,2\zeta}(\Phi_{d,m})] \leq C \cdot E[Z_{\omega,\ast,1/\sqrt{\pi}}(\Phi_{d,m})].$$

Furthermore, for $\sigma,\tau$ with $\text{dist}(\sigma,\tau) \leq \xi$ we have

$$\|\omega^* - E[\omega_{\Phi_{d,m}}(\sigma,\tau)]\| \leq \xi.$$

Indeed, $\omega_{\Phi_{d,m}}(\sigma,\tau)$ is sufficiently concentrated about its expectation to obtain

$$E[Z_{\text{centre}}(\Phi_{d,m})] \sim E[Z_{\omega,\ast,2\zeta}(\Phi_{d,m})].$$

As $\omega^*$ is the expected overlap of two perfectly uncorrelated assignments $\sigma,\tau$ with $p_{4}$-marginals (cf. Lemma 11), it relatively straightforward to verify that

$$E[Z_{\omega,\ast,1/\sqrt{\pi}}(\Phi_{d,m})] \leq C' \cdot E[Z_{p}(\Phi_{d,m})]^2$$

for some $C' = C'(k) > 0$. Combining (32)–(34), we find

$$E[Z(\Phi_{d,m})] \leq C'' \cdot E[Z_{p}(\Phi_{d,m})]^2$$

for some $C'' = C''(k) > 0$. Finally, Theorem 2 follows by combining (35) with Lemmas 6, 9 and 10.

**Establishing Proposition 2.** Let us first assume that $\|\omega - \omega^*\|_{\infty} \leq \xi$. To compute $E[Z_{\omega}(\Phi_{d,m})]$ we need to estimate for each pair $\sigma,\tau$ with $\omega_{\Phi_{d,m}}(\sigma,\tau) = \omega$ the probability that $\sigma,\tau \in S_{p}(\Phi_{d,m})$. Similarly as in the computation of the first moment, we are going to work with a different probability space $(\Omega, \hat{\mathbb{P}})$. This time, $\hat{\Omega}$ consists of all vectors of 0/1 pairs

$$(\hat{\sigma}_{\ell,j}(\ell), \hat{\tau}_{\ell,j}(\ell))_{\ell \in L, j \in [m(\ell)], j \in [k]}$$

The distribution $\hat{\mathbb{P}}$ is defined by means of a vector

$$q = (q_{a,b,\ell,j})_{\ell \in L, j \in [k], a,b \in \{0,1\}}$$

that satisfies $\sum_{a,b \in \{0,1\}} q_{a,b,\ell,j} = 1$ and $q_{a,0,\ell,j} = q_{0,1,\ell,j} = 1$ for all $\ell,j$. Given $q$, we let

$$\hat{\mathbb{P}}[\hat{\sigma}_{\ell,j}(\ell) = a, \hat{\tau}_{\ell,j}(\ell) = b] = q_{a,b,\ell,j} \quad (a,b \in \{0,1\}),$$

independently for all $\ell, i, j$. The intended semantics is that $\hat{\sigma}_{\ell,j}(\ell), \hat{\tau}_{\ell,j}(\ell)$ represent the truth values of the $j$th literal of the $i$th clause of type $\ell$ under a pair of assignments. Let

$$q_{0,1,\ell,j} = q_{1,0,\ell,j} + q_{0,0,\ell,j}$$

denote the marginal probability that $\hat{\sigma}_{\ell,j}(\ell) = 1$.

Let $S_{\ell}(\ell)$ denote the event that

$$\max_{\ell \in L} \hat{\sigma}_{\ell,j}(\ell) = \max_{\ell \in L} \hat{\tau}_{\ell,j}(\ell) = 1,$$
and let \( S = \bigcap_{i,j} S_i(\ell) \). Further, let \( B_j(\ell) \) denote the event \[
\sum_{i \in m(\ell)} \tilde{\sigma}_{ij}(\ell) = \sum_{i \in m(\ell)} \tilde{\tau}_{ij}(\ell) = m(\ell) \cdot \ell_j,
\]
and let \( B = \bigcap_{j \in [k]} B_j(\ell) \). Finally, let \( \dot{\omega} = (\dot{\omega}_{\ell,j}) \) denote the vector with entries \[
\dot{\omega}_{\ell,j} = \frac{\sum_{i \in m(\ell)} \tilde{\sigma}_{ij}(\ell) \tilde{\tau}_{ij}(\ell) / m(\ell)}{\ell_j}.
\]
In analogy to Lemma 7, we obtain

**Lemma 12.** Let \( \sigma, \tau \in \{0,1\}^V \) have \( p_d \)-marginals. Then \[
P[\sigma, \tau \in S_p(\Phi_{d,m}) | \omega_{\Phi_{d,m}}(\sigma, \tau) = \omega] = \tilde{P}[S | B, \dot{\omega} = \omega].
\]

As in the proof of Lemma 7, to compute \( \tilde{P}[S | B, \dot{\omega} = \omega] \) we are going to choose \( q \) so as to maximize \( \tilde{P}[B, \dot{\omega} = \omega] \). This allows us to express the \( \tilde{P}[S | B, \dot{\omega} = \omega] \) as a quotient of a term that factorises over clauses and a bunch of binomial large deviations.

**Lemma 13.** There exists \( q = q(\omega) \) such that \[
\ell_j = \frac{q_{\ell,j} - (q_{\ell,j} - q_{\ell,j}^{11}) \prod_{h \neq j} (1 - q_{\ell,h})}{1 - 2 \prod_{h=1}^k (1 - q_{\ell,h}) + \prod_{h=1}^k (1 - 2q_{\ell,h} + q_{\ell,h}^{11})},
\]
\[
\omega_{\ell,j} = \frac{1 - 2 \prod_{h=1}^k (1 - q_{\ell,h}) + \prod_{h=1}^k (1 - 2q_{\ell,h} + q_{\ell,h}^{11})}{1 - 2 \prod_{h=1}^k (1 - q_{\ell,h}) + \prod_{h=1}^k (1 - 2q_{\ell,h} + q_{\ell,h}^{11})}
\]
for all \( \ell \in L, j \in [k] \). For this \( q \), and with \( \psi \) as in (26) let \[
P(\omega) = \ln \left[ 1 - 2 \sum_{j=1}^k (1 - q_{\ell,j}) + \prod_{j=1}^k (1 - 2q_{\ell,j} + q_{\ell,j}^{11}) \right] - \sum_{j \in [k]} \left[ \psi(q_{\ell,j}^{11}, \omega_{\ell,j}) + (1 - \omega_{\ell,j}) \psi \left( \frac{1 - 2q_{\ell,j} + q_{\ell,j}^{11}}{1 - q_{\ell,j}^{11}}, \frac{1 - 2\ell_j + \omega_{\ell,j}}{1 - \ell_j} \right) \right]
\]
for any \( \ell \in L \), and set \( P(\omega) = \sum_{\ell \in L} \frac{m(\ell)}{n} P(\omega) \). Then \( \tilde{P}[S | B, \dot{\omega} = \omega] = \Theta(1) \cdot \exp \left[ n \cdot P(\omega) \right] \).

To complete the proof, we need to analyze the function \( P(\omega) \).

**Lemma 14.** The function \( P \) has two continuous derivatives. These satisfy \[
\frac{\partial}{\partial \omega_{\ell,j}} P(\omega^*) = 0,
\]
\[
\frac{\partial^2}{\partial \omega_{\ell,k} \partial \omega_{\ell,j}} P(\omega) \leq 4^{-k+o(k)}
\]
for all \( \ell \in L, j, k \in [k] \) and all \( \omega \) such that \( \|\omega - \omega^*\|_\infty \leq 2\xi \).

The fact that the first derivative of \( P \) vanishes at \( \omega^* \) is crucial. Indeed, because of this we can use Taylor’s theorem to bound \( P \) around \( \omega^* \) by a quadratic function, obtaining \[
P(\omega) \leq P(\omega^*) + 4^{-k+o(k)} \sum_{\ell \in L} \frac{m(\ell)}{n} \|\omega_{\ell} - \omega_{\ell}^*\|^2.
\]
where \( \omega_{\ell} = (\omega_{\ell,j})_{j \in [k]} \). To obtain the desired bound on \( E[Z_\omega] \), we need to estimate the number of pairs \((\sigma, \tau)\) with overlap \( \omega \). A somewhat delicate analysis shows that this number can be bounded by a function \( H(\omega) \) such that \[
H(\omega) \leq \exp \left[ -2^{-k+o(k)} \sum_{\ell \in L} \frac{m(\ell)}{n} \|\omega_{\ell} - \omega_{\ell}^*\|^2 \right].
\]

Combining (36) and (37) yields \[
\frac{E[Z_{\omega}(\Phi_{d,m})]}{E[Z_{\omega}^*(\Phi_{d,m})]} \leq C' \cdot \frac{H(\omega)}{H(\omega^*)} \cdot \frac{P(\omega)}{P(\omega^*)}
\]
for certain \( C' = C'(k), \zeta = \zeta(k) > 0 \), as desired.

**Acknowledgment.** The first author thanks Dimitris Achlioptas for helpful discussions on the second moment method. The authors thank Charilaos Efthymiou for many helpful comments that led to an improved presentation of this work.

7. REFERENCES

[1] D. Achlioptas, A. Coja-Oghlan: Algorithmic barriers from phase transitions. Proc. 49th FOCS (2008) 793–802.
[2] D. Achlioptas, R. M. Mendaca-Mendez: Unsatisfiability Bounds for Random CSPs from an Energetic Interpolation Method. Proc. 39th ICALP (2012) 1–12.
[3] D. Achlioptas, R. M. Mendaca-Mendez: Exponential lower bounds for DPLL algorithms on satisfiable random 3-CNF formulas. Proc. 15th SAT (2012) 327–340.
[4] D. Achlioptas, C. Moore: Random k-SAT: two moments suffice to cross a sharp threshold. SIAM Journal on Computing 36 (2006) 740–762.
[5] D. Achlioptas, A. Naor: The two possible values of the chromatic number of a random graph. Annals of Mathematics 162 (2005) 1333–1349.
[6] D. Achlioptas, Y. Peres: The threshold for random k-SAT is \( 2^k \ln 2 - O(k) \). Journal of the AMS 17 (2004) 947–973.
[7] M. Bayati, D. Gamarnik, P. Tetali: Combinatorial approach to the interpolation method and scaling limits in sparse random graphs. Proc. 42nd STOC (2010) 105–114.
[8] V. Chvátal, B. Reed: Mick gets some (the odds are on his side). Proc. 33th FOCS (1992) 620–627.
[9] A. Coja-Oghlan: A better algorithm for random k-SAT. SIAM J. Computing 39 (2010) 2823–2864.
[10] A. Coja-Oghlan: On belief propagation guided decimation for random k-SAT. Proc. 22nd SODA (2011) 957–966.
[11] A. Coja-Oghlan, K. Panagiotou: Catching the k-NAESAT threshold. Proc. 43rd STOC (2012) 899–908.
[12] A. Coja-Oghlan, L. Zdeborová: The condensation transition in random hypergraph 2-coloring. Proc. 23rd SODA (2012) 241–250.
[13] O. Dubois, Y. Boukhad: A general upper bound for the satisfiability threshold of random r-SAT formulae. J. Algorithms 24 (1997) 395–420.
[14] O. Dubois, J. Mandel: The 3-XORSAT threshold. Proc. 43rd FOCS (2002) 769–778.
[15] M. Dyer, A. Frieze, C. Greenhill: On the chromatic number of a random hypergraph. Preprint (2012).
[16] S. Franz, M. Leone: Replica bounds for optimization problems and diluted spin systems. J. Statist. Phys. 111 (2003) 535–564.
[17] E. Friedgut: Sharp Thresholds of Graph Properties, and the $k$-SAT Problem. J. AMS 12 (1999) 1017–1054.
[18] A. Frieze, S. Suen: Analysis of two simple heuristics on a random instance of $k$-SAT. Journal of Algorithms 20 (1996) 312–355.
[19] A. Frieze, N. Wormald: Random $k$-Sat: a tight threshold for moderately growing $k$. Combinatorica 25 (2005) 297–305.
[20] A. Goerdt: A threshold for unsatisfiability. Proc. 17th MFCS (1992) 264–274.
[21] S. Kirkpatrick, B. Selman: Critical behavior in the satisfiability of random boolean expressions. Science 264 (1994) 1297–1301.
[22] L. Kirousis, E. Kranakis, D. Krizanc, Y. Stamatiou: Approximating the unsatisfiability threshold of random formulas. Random Structures Algorithms 12 (1998) 253–269.
[23] L. Kroc, A. Sabharwal, B. Selman: Message-passing and local heuristics as decimation strategies for satisfiability. Proc 24th SAC (2009) 1408–1414.
[24] F. Krzakala, A. Montanari, F. Ricci-Tersenghi, G. Semerjian, L. Zdeborová: Gibbs states and the set of solutions of random constraint satisfaction problems. Proc. National Academy of Sciences 104 (2007) 10318–10323.
[25] M. Mézard, G. Parisi, R. Zecchina: Analytic and algorithmic solution of random satisfiability problems. Science 297 (2002) 812–815.
[26] M. Molloy: The freezing threshold for $k$-colourings of a random graph. Proc. 43rd STOC (2012) 921–930.
[27] A. Montanari, R. Restrepo, P. Tetali: Reconstruction and clustering in random constraint satisfaction problems. SIAM J. Discrete Math. 25 (2011) 771–808.
[28] R. Moser, G. Tardos: A constructive proof of the general Lovász local lemma. J. ACM 57 (2010).
[29] V. Rathi, E. Aurell, L. K. Rasmussen, M. Skoglund: Bounds on threshold of regular random $k$-SAT. Proc. 12th SAT (2010) 264–277.