Combinatorics, Probability and Computing (2018) 27, 496–530.
doi:10.1017/S0963548318000263

The Number of Satisfying Assignments of Random Regular k-SAT Formulas

AMIN COJA-OGHLAN[1†] and NICK WORMALD[2‡]

[1]Mathematics Institute, Goethe University, 10 Robert-Mayer-Straße, Frankfurt 60325, Germany
(e-mail: acoghlan@math.uni-frankfurt.de)

[2]Department of Mathematical Sciences, Monash University, VIC 3800, Australia
(e-mail: nick.wormald@monash.edu)

Received 9 July 2016; revised 11 April 2018

Let Φ be a random k-SAT formula in which every variable occurs precisely d times positively and d times negatively. Assuming that k is sufficiently large and that d is slightly below the critical degree where the formula becomes unsatisfiable with high probability, we determine the limiting distribution of the number of satisfying assignments.

2010 *Mathematics subject classification*: Primary 60C05
Secondary 05C80

1. Introduction

In order to study random instances of constraint satisfaction problems, it is key to get a handle on the number of solutions. In fact, in many examples such as k-colourability in random graphs the best current estimates of the threshold for the existence of solutions derive from calculating the second moment of the number of solutions [3, 11]. Furthermore, if the number of solutions is sufficiently concentrated, then typical properties of random solutions as well as the geometry of the set of solutions can be studied by way of the 'planted model', an easily accessible distribution [1]. However, prior to this work the limiting distribution of the number of solutions has not been determined precisely in any of the standard examples of random constraint satisfaction problems.

In this paper we show how the limiting distribution of the number of solutions can be obtained by combining the second moment method with a subtle application of the 'small subgraph conditioning' technique. The concrete problem that we deal with is the *random regular k-SAT problem*. In this model there are n Boolean variables $x_1, \ldots, x_n$ and $m = 2dn/k$ Boolean clauses

† The research leading to these results received funding from the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013) / ERC Grant Agreement no. 278857–PTCC.
‡ Research supported by the ARC Australian Laureate Fellowships grant FL120100125.

of length k. We always assume that k divides $2dn$. The random formula $\Phi_n(d,k)$ is obtained by choosing without replacement for each variable x_i precisely d out of the km available literal slots where x_i appears positively and another d slots where x_i appears negatively. Let Z be the number of satisfying assignments of $\Phi = \Phi_n(d,k)$.

For k exceeding a certain constant k_0 an explicit literal degree $d_{k\text{-SAT}}$ is known such that [9]

$$\begin{aligned} \liminf_{n\to\infty} \mathbb{P}[\Phi \text{ is satisfiable}] &> 0 \quad \text{if } d < d_{k\text{-SAT}}, \\ \lim_{n\to\infty} \mathbb{P}[\Phi \text{ is satisfiable}] &= 0 \quad \text{if } d > d_{k\text{-SAT}}. \end{aligned} \tag{1.1}$$

While the precise formula is cumbersome, in the limit of large k we have

$$2d_{k\text{-SAT}}/k = 2^k \ln 2 - k\ln 2/2 - (1+\ln 2)/2 + \varepsilon_k, \quad \text{where } \lim_{k\to\infty} \varepsilon_k = 0. \tag{1.2}$$

Our main result determines the limiting distribution of Z for degrees d almost (but not quite) matching $d_{k\text{-SAT}}$.

Theorem 1.1. *There exists a constant k_0 such that for all $k \geqslant k_0$ and $d > 0$ such that*

$$2d/k \leqslant 2^k \ln 2 - k\ln 2/2 - 4, \tag{1.3}$$

the following is true. Let $q = q(k) \in (0,1)$ be the unique solution to the equation

$$2q = 1 - (1-q)^k \tag{1.4}$$

Moreover, for $l \geqslant 1$ and $0 \leqslant t \leqslant l$ let

$$\lambda_{l,t} = \frac{1}{2l}\binom{l}{t}\left(\frac{(k-1)(d-1)}{2}\right)^l \left(\frac{d}{d-1}\right)^t \quad \delta_{l,t} = (-1)^t(2q-1)^l \tag{1.5}$$

and let $(\Lambda_{l,t})_{l,t}$ be a family of independent Poisson variables with $\mathbb{E}[\Lambda_{l,t}] = \lambda_{l,t}$. Then the random variable

$$W = \prod_{l\geqslant 1}\prod_{t\leqslant l}(1+\delta_{l,t})^{\Lambda_{l,t}} \exp(-\lambda_{l,t}\delta_{l,t}) \tag{1.6}$$

satisfies $\mathbb{E}[W^2] < \infty$, and with Z the number of satisfying assignments of the random formula $\Phi_n(d,k)$ we have

$$Z \cdot \frac{(4q(1-q))^{dn}\sqrt{2+2(k-1)q-k}}{2^n(2q)^m} \xrightarrow{n\to\infty} W \quad \textit{in distribution}. \tag{1.7}$$

It is not difficult to verify that

$$n\ln 2 + m\ln(2q) - (dn)\ln(4q(1-q)) = \Omega(n) \tag{1.8}$$

for d satisfying (1.3), and additionally that $\mathbb{E}|\ln W| < \infty$. Hence, (1.7) and (1.8) imply that $\ln Z = \Omega(n)$ w.h.p. for such d. The particular event $Z \geqslant 1$ is of particular interest.

Corollary 1.2. *For $k \geqslant k_0$ and d satisfying* (1.3) *we have*

$$\lim_{n\to\infty} \mathbb{P}[\Phi \textit{ is satisfiable}] = 1.$$

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

The constant 4 in (1.3) is not optimal. In fact, a truncated second moment argument as in [12] in combination with an argument similar to [5] might extend the above results up to the exact 'condensation threshold' of the regular k-SAT problem, although both steps would require substantial technical work. For an in-depth explanation of the condensation phenomenon we refer to [5].

Related work

Random regular k-SAT instances were first studied by Rathi, Aurell, Rasmussen and Skoglund [22] via the second moment method. They proved that

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

for degrees d close to $d_{k\text{-SAT}}$. The latter was determined by Coja-Oghlan and Panagiotou [9] by a second moment argument that incorporates 'Survey Propagation', a technique from statistical physics [19]. A closely related paper by Ding, Sly and Sun [14] studies the regular k-NAESAT problem, which asks for a satisfying assignment whose inverse is satisfying as well. In fact, Ding, Sly and Sun have an argument based on Fourier analysis that shows that the NAE-satisfiability probability is not just bounded away from 0 but actually converges to 1 (in contrast to (1.1)). Recently Sly, Sun and Zhang [24] extended this argument to calculate the expectation of the nth root of the number of NAE-solutions. This is quite a difficult problem due to a phenomenon known as 'replica symmetry breaking' in physics [19]. However, [24] does not determine the limiting distribution.

Conceptually the regular k-SAT model is simpler than the better known uniform model where a specific number of clauses are drawn uniformly and independently. This is because the local structure of regular formulas fluctuates less as each variable has precisely d positive and d negative occurrences and the total number of cycles of a fixed length is bounded w.h.p. In the case of uniformly random k-SAT formulas Frieze and Wormald [16] used the second moment method to determine the k-SAT threshold in the case that $k = k(n) \to \infty$ as $n \to \infty$. Moreover, for clause lengths k that remain fixed as $n \to \infty$, Achlioptas and Moore [2] significantly improved the previous lower bound on the satisfiability threshold by applying the second moment method to the number of NAE-solutions. Working with 'balanced' assignments instead, Achlioptas and Peres [4] improved the NAE-lower bound by a factor of two. This left an additive gap of $\Theta(k)$ between the lower bound and an upper bound of Kirousis, Kranakis, Krizanc and Stamatiou [18]. Coja-Oghlan and Panagiotou [9, 10] narrowed the gap to a function that tends to 0 in the limit of large k by a second moment argument inspired by Survey Propagation. Finally, Ding, Sly and Sun [15] determined the precise satisfiability threshold in uniformly random formulas for sufficiently large k via a second moment argument that fully rigorizes the Survey Propagation calculations.

We prove Theorem 1.1 by combining the second moment argument from [10] with small subgraph conditioning. This method was originally developed to prove that random regular graphs of degree at least three are Hamiltonian w.h.p. [23]. Using Skorokhod's representation theorem, Janson [17] showed that small subgraph conditioning can be used to obtain limiting distributions. However, Janson's result does not seem to apply directly in our context. Instead, we perform a variance analysis along the lines of [23] for a family of random variables that count satisfying assignments with certain peculiar properties.

Based on an early version of the present paper, the technique explained in Section 2 was used by Rassmann [21] to analyse the number of 2-colourings of random k-uniform hypergraphs.

Notation and preliminaries

Throughout the paper we tacitly assume that n is sufficiently large, that k exceeds a sufficiently large constant k_0 and that d satisfies (1.3). We encode the Boolean values 'true' and 'false' by 1 and -1, respectively. Moreover, we extend truth assignments $\sigma : \{x_1, \ldots, x_n\} \to \{\pm 1\}$ to the set of literals by letting $\sigma(\neg x_i) = -\sigma(x_i)$. We use O-notation with respect to both n and k, with the convention that $O(1)$, $o(1)$ *etc.* always refer to the limit as $n \to \infty$. For a number l and an integer $h \geqslant 0$ we write

$$l^{\underline{h}} = \prod_{0 \leqslant i < h} (l - i)$$

for the falling factorial; in particular, $l^{\underline{0}} = 1$. Further, with the convention $\ln 0 = -\infty$, $0 \ln 0 = 0 \ln \frac{0}{0} = 0$, we recall that the Kullback–Leibler divergence of two probability distributions $p = (p_x)_{x \in \mathcal{X}}, q = (q_x)_{x \in \mathcal{X}}$ on a finite set $\mathcal{X}$ is

$$D_{\mathrm{KL}}(q \| p) = \sum_{x \in \mathcal{X}} q_x \ln \frac{q_x}{p_x} \in [0, \infty]. \tag{1.9}$$

Further, viewing $p = (p_x)_{x \in \mathcal{X}}, q = (q_x)_{x \in \mathcal{X}}$ as vectors in $\mathbb{R}^{\mathcal{X}}$, we let

$$\|p - q\|_2 = \sqrt{\sum_{x \in \mathcal{X}} (p_x - q_x)^2}.$$

Finally, we denote the scalar product of vectors ξ, η by $\langle \xi, \eta \rangle$ and we write 1 for the vector with all entries equal to one (in any dimension).

2. Overview

The basic insight behind small subgraph conditioning is that the fluctuations of $\ln Z$ can be attributed to the number of certain small sub-structures of the random formula Φ. To elaborate, we rephrase the definition of Φ by modifying what is essentially a bijection model due to Békéssy, Békéssy and Komlós [7] in the context of matrices with given line sums. With the incorporation of signs, it becomes the following: we view Φ as a uniformly random bijection

$$[m] \times [k] \to \{x_1, \ldots, x_n\} \times [d] \times \{\pm 1\}, \quad (i, j) \mapsto \Phi[i, j]. \tag{2.1}$$

Thus, (2.1) maps each clause index $i \in [m]$ and each position $j \in [k]$ in that clause to a Boolean variable $x \in \{x_1, \ldots, x_n\}$, an index $h \in [d]$ (denoting which of the d copies of the literal is used), and a sign $s \in \{\pm 1\}$ indicating whether the variable appears as a positive or as a negative literal. In terms of propositional formulas, the triple $\Phi[i, j]$ corresponds to the literal x if $s = 1$ and $\neg x$ if $s = -1$. Let us write $\partial(i, j) = \partial_\Phi(i, j)$ for the first and $\mathrm{sign}(i, j) = \mathrm{sign}_\Phi(i, j)$ for the last component of $\Phi[i, j]$. Then an assignment $\sigma : \{x_1, \ldots, x_n\} \to \{\pm 1\}$ satisfies Φ if and only if $\min_{i \in [m]} \max_{j \in [k]} \mathrm{sign}(i, j) \sigma(\partial(i, j)) = 1$. Thus, we can write

$$Z = \sum_{\sigma : \{x_1, \ldots, x_n\} \to \{\pm 1\}} \prod_{i=1}^{m} \left[1 - \prod_{j=1}^{k} \frac{1 - \mathrm{sign}(i, j) \sigma(\partial(i, j))}{2} \right].$$

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

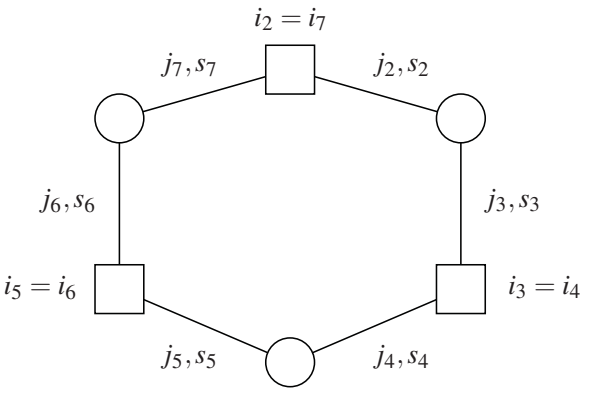

Figure 1. The indices along a cycle with $l = 3$ clauses in the factor graph. The squares represent clauses and the circles variables.

Because (2.1) is a bijection each variable appears precisely $2d$ times in total in the corresponding propositional formula, namely d times positively and d times negatively. Further, for a literal l and an index $h \in [d]$ we let $\partial(l,h) = \partial_\Phi(l,h)$ denote the pair $(i,j) \in [m] \times [k]$ such that $\Phi[i,j] = (x,h,1)$ if $l = x$ and $\Phi[i,j] = (x,h,-1)$ if $l = \neg x$.

It is natural to represent Φ by a bipartite multigraph, the *factor graph* $G(\Phi)$. It has vertices $[m]$ corresponding to the clauses and vertices $\{x_1,\ldots,x_n\}$ representing the Boolean variables. For each pair $(i,j) \in [m] \times [k]$ we insert an edge between i and the variable x such that $\Phi[i,j] \in \{x\} \times [d] \times \{\pm 1\}$. Additionally, we annotate the edge by $\mathrm{sign}(i,j) \in \{\pm 1\}$. Of course, $G(\Phi)$ may well have multiple edges.

Because the factor graph is sparse and random, standard arguments show that it is unlikely to contain many short cycles. Hence, if we explore the factor graph from a randomly chosen root clause for some bounded number $2l$ of steps, then we will typically see a 'deterministic' tree in which each clause has degree k and every variable has d positive and d negative occurrences. However, a bounded number of clauses will take part in any cycles of length at most $2l$. As it will be important to keep track of the literal signs traversed along the cycle, for a given $s = (s_2,\ldots,s_{2l+1}) \in \{\pm 1\}^{2l}$ we let $C_s = C_s(\Phi)$ be the number of cycles of length $2l$ in which the initial literal has sign s_2, the second one has sign s_3, *etc.* (The starting index is chosen for convenient index arithmetic.) We call s the *sign pattern* of the cycle. Moreover, to avoid overcounting we always deem the clause with the smallest index the starting point of the cycle, and the cycle is oriented towards the slot of that clause with the smaller index. Formally, given $l \geqslant 1$ and a sign pattern $s = (s_2,\ldots,s_{2l+1}) \in \{\pm 1\}^{2l}$, let C_s be the number of sequences $(i_2,j_2),\ldots,(i_{2l+1},j_{2l+1}) \in [m] \times [k]$ such that

CY1 $i_2 = i_{2l+1} = \min\{i_2,\ldots,i_{2l}\}$ and $i_2,\ldots,i_{2l}$ are pairwise distinct,
CY2 $i_{t+1} = i_t$ if t is odd,
CY3 $\partial(i_t,j_t) = \partial(i_{t+1},j_{t+1})$ if t is even but $\partial(i_2,j_2),\ldots,\partial(i_{2l},j_{2l})$ are pairwise distinct,
CY4 we have $j_2 < j_{2l+1}$,
CY5 $\mathrm{sign}(i_t,j_t) = s_t$ for all t.

See Figure 1 for an illustration. Moreover, for $\ell \geqslant 1$ let $\mathcal{F}_\ell = \mathcal{F}_{\ell,n}(d,k)$ be the σ-algebra generated by the random variables C_s with $s \in \bigcup_{l \leqslant \ell}\{\pm 1\}^{2l}$.

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

By the standard decomposition of the variance, we can write for any $\ell \geqslant 1$

$$\mathbb{E}[Z^2] - \mathbb{E}[Z]^2 = \mathbb{E}[\mathbb{E}[Z|\mathcal{F}_\ell]^2 - \mathbb{E}[Z]^2] + \mathbb{E}[\mathbb{E}[Z^2|\mathcal{F}_\ell] - \mathbb{E}[Z|\mathcal{F}_\ell]^2]. \tag{2.2}$$

The term $\mathbb{E}[\mathbb{E}[Z|\mathcal{F}_\ell]^2 - \mathbb{E}[Z]^2]$ accounts for the amount of variance induced by the fluctuations of the number of cycles of length at most 2ℓ. Given the number of cycles of length at most 2ℓ, the conditional variance $\mathrm{Var}[Z|\mathcal{F}_\ell] = \mathbb{E}[\mathbb{E}[Z^2|\mathcal{F}_\ell] - \mathbb{E}[Z|\mathcal{F}_\ell]^2]$ remains. Generally, small subgraph conditioning is based on showing that

$$\lim_{\ell\to\infty} \limsup_{n\to\infty} \mathbb{E}\left[\frac{\mathbb{E}[Z^2|\mathcal{F}_\ell] - \mathbb{E}[Z^2]}{\mathbb{E}[Z]^2}\right] = 0. \tag{2.3}$$

In other words, in the limit of large ℓ and n, with n growing much faster than ℓ, the second summand in (2.2) is negligible. Thus, once we condition on the number of short cycles the variance is tiny. If so, then the limiting distribution of $\ln Z$ is just the limit of $\ln \mathbb{E}[Z|\mathcal{F}_\ell]$ as $n, \ell \to \infty$, which is determined by the joint distribution of the number of short cycles.

Due to the combinatorial nature of the regular k-SAT problem a direct attempt at proving (2.3) leads to fairly unpleasant calculations. Indeed, the inherent asymmetry of the Boolean values 'true' and 'false' causes the formula for the second moment of Z to involve implicit parameters that we find tedious to track directly (although it might be possible). Similar issues arise in other random constraint satisfaction problems as well. Further, they also appear in the formula for the k-SAT threshold in the regular k-SAT problem [9].

In this case, we are able to develop a version of the small subgraph conditioning argument that does not require such extensive calculations. To this end, we decompose Z into a sum of contributions that are tractable by fairly simple combinatorial considerations. Specifically, let $\Sigma = \{\pm 1\}^k \setminus \{(-1,\ldots,-1)\}$ be the set of all $2^k - 1$ truth value combinations that satisfy a Boolean clause (*i.e.* everything but 'all-false'). Also, let $\mathcal{M}(d,k,n)$ be the set of all probability distributions $\mu = (\mu(\sigma))_{\sigma\in\Sigma}$ on Σ such that $m\mu(\sigma)$ is an integer for all $\sigma \in \Sigma$ and

$$\sum_{\sigma\in\Sigma} \mu(\sigma)\langle\sigma, 1\rangle = 0. \tag{2.4}$$

(The relevance of this constraint will be made clear.) In addition, define $Z_\mu = Z_\mu(\Phi)$ as the number of truth assignments $\tau : \{x_1,\ldots,x_n\} \to \{\pm 1\}$ such that

$$\mu(\sigma) = \frac{1}{m}\sum_{i=1}^{m}\prod_{j=1}^{k} 1\{\mathrm{sign}(i,j)\tau(\partial(i,j)) = \sigma_j\} \quad \text{for all } \sigma \in \Sigma.$$

In words, Z_μ is the number of satisfying assignments of Φ such that for each $\sigma \in \Sigma$ precisely $m\mu(\sigma)$ clauses are satisfied according to the 'truth value pattern' σ. Since the total number of true literals and false literals are equal, all possible distributions on Σ satisfy (2.4) and are included in $\mathcal{M}(d,k,n)$, and thus

$$Z = \sum_{\mu\in\mathcal{M}(d,k,n)} Z_\mu. \tag{2.5}$$

Crucially, (2.5) decomposes the random variable Z, whose value is typically exponential in n for the regime of d,k that we deal with, into a *polynomial* number $|\mathcal{M}(d,k,n)| \leqslant O(n^{|\Sigma|})$ of summands.

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

We are going to apply small subgraph conditioning to the individual random variables Z_μ rather than Z. The key advantage is that we will be able to evaluate the second moment of Z_μ almost mechanically by way of the central limit theorem for random permutations [8].

This approach is facilitated by the observation that only a fairly small subset of $\mathcal{M}(d,k,n)$ contributes to (2.5) significantly. In fact, recalling q from (1.4), define a probability distribution $\bar{\mu}$ on Σ by letting

$$\bar{\mu}(\sigma) = \frac{(q(1-q))^{k/2}}{1-(1-q)^k}\left(\frac{q}{1-q}\right)^{\frac{1}{2}\sum_{j=1}^k \sigma_j}. \tag{2.6}$$

Further, let $\mathcal{M}_\omega = \mathcal{M}_\omega(d,k,n)$ be the set of all $\mu \in \mathcal{M}(d,k,n)$ such that $\|\mu - \bar{\mu}\|_2 \leqslant \omega m^{-1/2}$. Then our strategy is to show that for any fixed number $\omega > 0$ the double limit (2.3) with Z replaced by Z_μ vanishes uniformly for $\mu \in \mathcal{M}_\omega$. In Section 3 we calculate the first moments of the random variables Z_μ.

Proposition 2.1. *The first moments satisfy*

$$\mathbb{E}[Z] \sim \frac{2^n(2q)^m(4q(1-q))^{-dn}}{\sqrt{2+2(k-1)q-k}} = \exp(\Omega(n)) \quad \textit{and} \tag{2.7}$$

$$\lim_{\omega\to\infty}\liminf_{n\to\infty}\sum_{\mu\in\mathcal{M}_\omega}\frac{\mathbb{E}[Z_\mu]}{\mathbb{E}[Z]} = 1. \tag{2.8}$$

Furthermore, for any $\omega > 0$ we have

$$\limsup_{n\to\infty}\max_{\mu\in\mathcal{M}_\omega}|\ln\mathbb{E}[Z_\mu] + \ln|\mathcal{M}_\omega| - \ln\mathbb{E}[Z]| < \infty. \tag{2.9}$$

In addition, we need to work out the covariance of Z_μ and the cycle counts C_s. As a first step, we study the unconditional distribution of the random variables C_s. For $l \geqslant 1$ and $s = (s_2,\ldots,s_{2l+1}) \in \{\pm1\}^{2l}$ define

$$\lambda_s = \frac{1}{2l}\left(\frac{k-1}{2}\right)^l (d(d-1))^{l/2}\left(\frac{d-1}{d}\right)^{\frac{1}{2}\sum_{i=1}^l s_{2i}s_{2i+1}}. \tag{2.10}$$

Proposition 2.2. *Let $S \subset \bigcup_{l\geqslant1}\{\pm1\}^l$ be a fixed finite set of sign patterns. Moreover, let $(c_s)_{s\in S}$ be a fixed family of non-negative integers. Then*

$$\lim_{n\to\infty}\mathbb{P}[\forall s\in S: C_s = c_s] = \prod_{s\in S}\mathbb{P}[\mathrm{Po}(\lambda_s) = c_s]. \tag{2.11}$$

Further, for $l \geqslant 1$ and $s = (s_2,\ldots,s_{2l+1}) \in \{\pm1\}^{2l}$ let

$$M_1 = \begin{pmatrix} q & 1-q \\ 1-q & q\end{pmatrix}, \qquad M_{-1} = \begin{pmatrix} 1-q & q \\ q & 1-q\end{pmatrix}, \qquad \delta_s = -1 + \mathrm{tr}\prod_{i=1}^l M_{s_{2i}s_{2i+1}}. \tag{2.12}$$

Since

$$M_1\begin{pmatrix}1\\1\end{pmatrix} = M_{-1}\begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix}, \quad M_1\begin{pmatrix}-1\\1\end{pmatrix} = -M_{-1}\begin{pmatrix}-1\\1\end{pmatrix} = (2q-1)\begin{pmatrix}-1\\1\end{pmatrix}, \tag{2.13}$$

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

we obtain

$$\delta_s = (-1)^{\sum_{i=1}^{l}(1-s_{2i}s_{2i+1})/2}(2q-1)^l. \tag{2.14}$$

Proposition 2.3. *Let $S \subset \bigcup_{l\geqslant 1}\{\pm 1\}^l$ be a finite set, let $(c_s)_{s\in S}$ be a family of non-negative integers and let $\omega > 0$. Then*

$$\lim_{n\to\infty}\max_{\mu\in\mathcal{M}_\omega}\left|\frac{\mathbb{E}[Z_\mu 1\{\forall s\in S: C_s = c_s\}]}{\mathbb{E}[Z_\mu]} - \prod_{s\in S}\mathbb{P}[\mathrm{Po}((1+\delta_s)\lambda_s) = c_s]\right| = 0. \tag{2.15}$$

Moreover, $\delta_s > -1$ for all s, $(2d-1)(k-1)(1-4q(1-q)) < 1$ and

$$\sum_{l\geqslant 1}\sum_{s\in\{\pm 1\}^l}\lambda_s\delta_s^2 = -\frac{1}{2}\ln(1-(2d-1)(k-1)(1-4q(1-q))). \tag{2.16}$$

The proofs of Propositions 2.2 and 2.3 can be found in Section 4. Finally, in Section 5 we establish the following bound on the second moments of the Z_μ.

Proposition 2.4. *For any $\omega > 0$ we have*

$$\limsup_{n\to\infty}\max_{\mu\in\mathcal{M}_\omega}\mathbb{E}[Z_\mu^2]/\mathbb{E}[Z_\mu]^2 \leqslant (1-(2d-1)(k-1)(1-4q(1-q)))^{-1/2}.$$

We now derive Theorem 1.1 from Propositions 2.1–2.4. Basically, we are going to argue that the variance of the random variables Z_μ comes almost entirely from the variation in their expected values conditional upon C_s, as described at (2.2). Although we do not use any technical statements from those papers directly, the argument is an adaptation of conditioning from [17, 20, 23] to the present context, which has one critical twist: instead of working with a single random variable Z, we need to control all the random variables Z_μ with $\mu\in\mathcal{M}_\omega$ for a fixed $\omega > 0$ simultaneously. In fact, ultimately we are going to have to take the limit $\omega\to\infty$ as well. Recalling that $\mathcal{F}_\ell$ is the σ-algebra generated by the random variables C_s with $s\in\bigcup_{l\leqslant\ell}\{\pm 1\}^{2l}$, we begin with the following bound.

Lemma 2.5. *For any $\omega > 0$ we have*

$$\lim_{\ell\to\infty}\limsup_{n\to\infty}\max_{\mu\in\mathcal{M}_\omega}\mathbb{E}\left[\frac{\mathbb{E}[Z_\mu^2|\mathcal{F}_\ell] - \mathbb{E}[Z_\mu|\mathcal{F}_\ell]^2}{\mathbb{E}[Z_\mu]^2}\right] = 0.$$

Proof. Spelled out in detail, we aim to prove that

$$\forall\varepsilon > 0\,\exists\ell_0 = \ell_0(\varepsilon) > 0\,\forall\ell > \ell_0\,\exists n_0 = n_0(\varepsilon,\ell) > 0\,\forall n > n_0, \mu\in\mathcal{M}_\omega:$$
$$\mathbb{E}[\mathbb{E}[Z_\mu^2|\mathcal{F}_\ell] - \mathbb{E}[Z_\mu|\mathcal{F}_\ell]^2] < \varepsilon\,\mathbb{E}[Z_\mu]^2.$$

For $\ell\geqslant 1$ and $B > 0$ let $\Gamma(\ell, B)$ be the set of all families $c = (c_s)_{s\in\bigcup_{l\leqslant\ell}\{\pm 1\}^{2l}}$ of integers $0\leqslant c_s\leqslant B$. By Propositions 2.2 and 2.3 for any $\varepsilon > 0$ we can choose $B = B(\varepsilon) > 0$, $\ell_0(\varepsilon) > 0$ sufficiently large that, for any $\ell\geqslant\ell_0(\varepsilon)$ for sufficiently large $n\geqslant n_0(\varepsilon,\ell,B)$, all $\mu\in\mathcal{M}_\omega$ satisfy the following

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

(the first is by definition):

$$\begin{aligned}\mathbb{E}[\mathbb{E}[Z_\mu|\mathcal{F}_\ell]^2] &\geqslant \sum_{c\in\Gamma(\ell,B)}\prod_{l=1}^{\ell}\prod_{s\in\{\pm1\}^{2l}}\frac{\mathbb{E}[Z_\mu 1\{\forall l\leqslant\ell, s\in\{\pm1\}^{2l}: C_s=c_s\}]^2}{\mathbb{P}[\forall l\leqslant\ell, s\in\{\pm1\}^{2l}: C_s=c_s]}\\ &\geqslant \exp(-\varepsilon^2)\,\mathbb{E}[Z_\mu]^2\sum_{c\in\Gamma(\ell,B)}\prod_{l=1}^{\ell}\prod_{s\in\{\pm1\}^{2l}}\frac{\mathbb{P}[\mathrm{Po}((1+\delta_s)\lambda_s)=c_s]^2}{\mathbb{P}[\mathrm{Po}(\lambda_s)=c_s]}\\ &= \exp(-\varepsilon^2)\,\mathbb{E}[Z_\mu]^2\sum_{c\in\Gamma(\ell,B)}\prod_{l=1}^{\ell}\prod_{s\in\{\pm1\}^{2l}}\frac{((1+\delta_s)\lambda_s)^{2c_s}}{c_s!\lambda_s^{c_s}\exp(2(1+\delta_s)\lambda_s-\lambda_s)}\\ &= \exp(-\varepsilon^2)\,\mathbb{E}[Z_\mu]^2\prod_{l=1}^{\ell}\prod_{s\in\{\pm1\}^{2l}}\exp(-2(1+\delta_s)\lambda_s+\lambda_s)\sum_{j=0}^{B}\frac{(1+\delta_s)^{2j}\lambda_s^j}{j!}\\ &\geqslant \mathbb{E}[Z_\mu]^2\exp\Bigl[-2\varepsilon^2+\sum_{l\geqslant1}\sum_{s\in\{\pm1\}^{2l}}\delta_s^2\lambda_s\Bigr]. \end{aligned}\tag{2.17}$$

The last step here uses the fact that the number of possible λ_s, as defined in (2.10), is bounded for fixed k, d and l. Since

$$\mathbb{E}[Z_\mu^2]=\mathbb{E}[\mathbb{E}[Z_\mu^2|\mathcal{F}_\ell]]=\mathbb{E}[\mathbb{E}[Z_\mu^2|\mathcal{F}_\ell]-\mathbb{E}[Z_\mu|\mathcal{F}_\ell]^2]+\mathbb{E}[\mathbb{E}[Z_\mu|\mathcal{F}_\ell]^2],$$

Proposition 2.4 and (2.17) imply that for sufficiently large ℓ, n and all $\mu\in\mathcal{M}_\omega$ we have

$$\mathbb{E}[\mathbb{E}[Z_\mu^2|\mathcal{F}_{\ell,n}]-\mathbb{E}[Z_\mu|\mathcal{F}_{\ell,n}]^2]\leqslant\varepsilon\,\mathbb{E}[Z_\mu]^2,$$

as desired. □

Corollary 2.6. *For any $\alpha>0$ we have*

$$\lim_{\ell\to\infty}\limsup_{n\to\infty}\mathbb{P}[|Z-\mathbb{E}[Z|\mathcal{F}_\ell]|>\alpha\,\mathbb{E}[Z]]=0.$$

Proof. Proposition 2.1 shows that for any $\alpha>0$ there is $\omega>0$ such that

$$\liminf_{n\to\infty}\sum_{\mu\in\mathcal{M}_\omega}\frac{\mathbb{E}[Z_\mu]}{\mathbb{E}[Z]}>1-\alpha^2.\tag{2.18}$$

Pick a small $\varepsilon=\varepsilon(\alpha,\omega)$. By Lemma 2.5 we can choose $\ell=\ell(\alpha,\varepsilon,\omega)$ sufficiently large that for large n all $\mu\in\mathcal{M}_\omega$ satisfy

$$\mathbb{E}[\mathbb{E}[Z_\mu^2|\mathcal{F}_\ell]-\mathbb{E}[Z_\mu|\mathcal{F}_\ell]^2]<\varepsilon\mathbb{E}[Z_\mu]^2.\tag{2.19}$$

Now define

$$X_\mu=|Z_\mu-\mathbb{E}[Z_\mu|\mathcal{F}_\ell]|1\{|Z_\mu-\mathbb{E}[Z_\mu|\mathcal{F}_\ell]|>\alpha\,\mathbb{E}[Z_\mu]\},\quad X=\sum_{\mu\in\mathcal{M}_\omega}X_\mu.$$

Then

$$X<\alpha\sum_{\mu\in\mathcal{M}_\omega}\mathbb{E}[Z_\mu]\Rightarrow\Bigl|\sum_{\mu\in\mathcal{M}_\omega}Z_\mu-\mathbb{E}[Z_\mu|\mathcal{F}_\ell]\Bigr|\leqslant2\alpha\sum_{\mu\in\mathcal{M}_\omega}\mathbb{E}[Z_\mu].\tag{2.20}$$

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Furthermore, using Chebyshev's inequality at the step introducing the variance,

$$\begin{aligned}\mathbb{E}[X_\mu|\mathcal{F}_\ell] &\leqslant \sum_{j\geqslant 0} 2^{j+1}\alpha\,\mathbb{E}[Z_\mu]\,\mathbb{P}[X_\mu > 2^j\alpha\,\mathbb{E}[Z_\mu]]\\ &\leqslant \sum_{j\geqslant 0} 2^{j+1}\alpha\,\mathbb{E}[Z_\mu]\,\mathbb{P}[|Z_\mu - \mathbb{E}[Z_\mu|\mathcal{F}_\ell]| > 2^j\alpha\,\mathbb{E}[Z_\mu]]\\ &\leqslant \sum_{j\geqslant 0}\frac{\mathrm{Var}[Z_\mu|\mathcal{F}_\ell]}{2^{j-1}\alpha\,\mathbb{E}[Z_\mu]} \leqslant \frac{4\mathrm{Var}[Z_\mu|\mathcal{F}_\ell]}{\alpha\,\mathbb{E}[Z_\mu]}.\end{aligned}$$

Hence,

$$\mathbb{E}[X|\mathcal{F}_\ell] \leqslant \frac{4}{\alpha}\sum_{\mu\in\mathcal{M}_\omega}\frac{\mathrm{Var}[Z_\mu|\mathcal{F}_\ell]}{\mathbb{E}[Z_\mu]} = \frac{4}{\alpha}\mathbb{E}[Z]\sum_{\mu\in\mathcal{M}_\omega}\frac{\mathrm{Var}[Z_\mu|\mathcal{F}_\ell]}{\mathbb{E}[Z_\mu]^2}\frac{\mathbb{E}[Z_\mu]}{\mathbb{E}[Z]}. \tag{2.21}$$

Further, by Proposition 2.1 there is a number $\gamma = \gamma(\omega)$ such that $\mathbb{E}[Z_\mu]/\mathbb{E}[Z] \leqslant \gamma/|\mathcal{M}_\omega|$ for all $\mu \in \mathcal{M}_\omega$. Therefore, (2.21) yields

$$\mathbb{E}[X|\mathcal{F}_\ell] \leqslant \frac{4\gamma\mathbb{E}[Z]}{\alpha|\mathcal{M}_\omega|}\sum_{\mu\in\mathcal{M}_\omega}\frac{\mathrm{Var}[Z_\mu|\mathcal{F}_\ell]}{\mathbb{E}[Z_\mu]^2}.$$

Choosing ε sufficiently small, we obtain from (2.19) and the tower rule that

$$\mathbb{E}[X] = \mathbb{E}[\mathbb{E}[X|\mathcal{F}_\ell]] \leqslant \frac{4\gamma\mathbb{E}[Z]}{\alpha|\mathcal{M}_\omega|}\sum_{\mu\in\mathcal{M}_\omega}\frac{\mathbb{E}[\mathrm{Var}[Z_\mu|\mathcal{F}_\ell]]}{\mathbb{E}[Z_\mu]^2} \leqslant \frac{4\varepsilon\gamma\mathbb{E}[Z]}{\alpha} \leqslant \alpha^2\,\mathbb{E}[Z]. \tag{2.22}$$

Combining with (2.18) and (2.20), for n sufficiently large we obtain

$$\begin{aligned}\mathbb{P}\Big[\Big|\sum_{\mu\in\mathcal{M}_\omega} Z_\mu - \mathbb{E}[Z_\mu|\mathcal{F}_\ell]\Big| \leqslant 2\alpha\sum_{\mu\in\mathcal{M}_\omega}\mathbb{E}[Z_\mu]\Big] &\geqslant \mathbb{P}\Big[X < \alpha\sum_{\mu\in\mathcal{M}_\omega}\mathbb{E}[Z_\mu]\Big]\\ &\geqslant \mathbb{P}[X < \alpha(1-2\alpha^2)\,\mathbb{E}[Z]]\\ &\geqslant 1-2\alpha\end{aligned}$$

for α sufficiently small (using Markov's inequality and noting that X is non-negative), as desired. □

Lemma 2.7. *Let*

$$U_\ell = \sum_{l=1}^{\ell}\sum_{s\in\{\pm 1\}^{2l}} C_s\ln(1+\delta_s) - \lambda_s\delta_s. \tag{2.23}$$

Then

$$\limsup_{\ell\to\infty}\limsup_{n\to\infty}\mathbb{P}[|\ln\mathbb{E}[Z|\mathcal{F}_\ell] - \ln\mathbb{E}[Z] - U_\ell| > \varepsilon] = 0 \quad \textit{for any } \varepsilon > 0. \tag{2.24}$$

Proof. Let $B > 0$, let $\mathcal{C}_B$ be the event that $C_s \leqslant B$ for all $l \leqslant \ell$ and $s \in \{\pm 1\}^{2l}$ and define $U_{\ell,B} = U_\ell 1\{\Phi \in \mathcal{C}_B\}$. Proposition 2.2 ensures that for any $\ell, \varepsilon > 0$ there is $B > 0$ such that

$$\mathbb{P}[\mathcal{C}_B] > 1-\varepsilon. \tag{2.25}$$

Additionally, choose $\omega > 0$ sufficiently large that for a sufficiently small $\alpha = \alpha(\varepsilon,\ell,B)$ we have for n sufficiently large, using (2.18), that $\sum_{\mu\in\mathcal{M}_\omega}\mathbb{E}[Z_\mu] \geqslant (1-\alpha)\,\mathbb{E}[Z]$. Then, noting $\lambda_s \geqslant 0$ and

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

using (2.5), Propositions 2.2 and 2.3 imply that for any assignment of values to c_s, $s \in \{\pm 1\}^{2l}$, with $c_s \leqslant B$ for all s we have for large n

$$\begin{aligned}\mathbb{E}[Z|\forall l \leqslant \ell, s \in \{\pm 1\}^{2l} : C_s = c_s] &\geqslant \sum_{\mu \in \mathcal{M}_\omega} \mathbb{E}[Z_\mu | \forall l \leqslant \ell, s \in \{\pm 1\}^{2l} : C_s = c_s] \\ &\geqslant \exp(-\varepsilon)\,\mathbb{E}[Z_\mu] \prod_{l \leqslant \ell} \prod_{s \in \{\pm 1\}^{2l}} \frac{\mathbb{P}[\mathrm{Po}((1+\delta_s)\lambda_s) = c_s]}{\mathbb{P}[\mathrm{Po}(\lambda_s) = c_s]} \\ &= \exp(-\varepsilon)\,\mathbb{E}[Z_\mu] \prod_{l \leqslant \ell, s} (1+\delta_s)^{c_s} \exp(-\delta_s \lambda_s). \end{aligned} \tag{2.26}$$

Similarly, assuming that α is chosen sufficiently small, for sufficiently large n we have (bounding $\mathbb{E}[Z|W]$ by $\mathbb{E}[Z]/\mathbb{P}[W]$ in the first step)

$$\begin{aligned}\mathbb{E}[Z|\forall l \leqslant \ell, s \in \{\pm 1\}^{2l} : C_s = c_s] &\leqslant \frac{2\alpha\,\mathbb{E}[Z]}{\prod_{l \leqslant \ell, s} \mathbb{P}[\mathrm{Po}(\lambda_s) = c_s]} \\ &\quad + \sum_{\mu \in \mathcal{M}_\omega} \mathbb{E}[Z_\mu | \forall l \leqslant \ell, s \in \{\pm 1\}^{2l} : C_s = c_s] \\ &\leqslant \exp(\varepsilon)\,\mathbb{E}[Z_\mu] \prod_{l \leqslant \ell, s} (1+\delta_s)^{c_s} \exp(-\delta_s \lambda_s). \end{aligned} \tag{2.27}$$

Combining (2.25), (2.26) and (2.27) and taking logarithms completes the proof of (2.24). □

Proof of Theorem 1.1. Let $(\Lambda_s)_{l,s}$ be a family of independent Poisson variables with $\mathbb{E}\,\Lambda_s = \lambda_s$. For $\ell \geqslant 1$ we define

$$W_\ell = \prod_{l=1}^{\ell} \prod_{s \in \{\pm 1\}^{2l}} (1+\delta_s)^{\Lambda_s} \exp(-\lambda_s \delta_s).$$

Then Proposition 2.2 shows that for each ℓ the random variables U_ℓ from Lemma 2.7 converge in distribution to $\ln W_\ell$ as $n \to \infty$. Moreover, comparing (2.10) and (2.14) with (1.5), we see that the distribution of W_ℓ coincides with the distribution of

$$\prod_{l \leqslant \ell} \prod_{0 \leqslant t \leqslant l} (1+\delta_s)^{\Lambda_{l,t}} \exp(-\lambda_{l,t}\delta_{l,t}).$$

Furthermore, following [17, Section 5] we note that the sequence $(W_\ell)_\ell$ is a martingale because $\mathbb{E}[(1+\delta_s)^{\Lambda_s} \exp(-\lambda_s\delta_s)] = 1$ for all sign patterns s and is in fact L^2-bounded as

$$\mathbb{E}[((1+\delta_s)^{\Lambda_s} \exp(-\lambda_s\delta_s))^2] = \exp(\delta_s^2 \lambda_s)$$

and $\sum_s \delta_s^2 \lambda_s < \infty$. Hence, the L^2 version of the martingale convergence theorem implies that W is well-defined and that the W_ℓ converge to W almost surely and in L^2 as $\ell \to \infty$. Therefore, the assertion follows from Proposition 2.1, Corollary 2.6 and Lemma 2.7. □

3. The first moment

We continue to assume that $k \geqslant k_0$ and that d satisfies (1.3).

In this section we prove Proposition 2.1. We begin by calculating $\mathbb{E}[Z]$. By linearity of expectation this comes down to calculating the probability that a fixed truth assignment $\tau : \{x_1, \ldots, x_n\} \to$

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

$\{\pm 1\}$ is satisfying. With the notation introduced in Section 2, we thus aim to calculate the probability that

$$\min_{i\in[m]}\max_{j\in[k]}\operatorname{sign}(i,j)\tau(\partial(i,j))=1.$$

Hence, we need to get a handle on the random ± 1-sequence

$$(\operatorname{sign}(i,j)\tau(\partial(i,j)))_{i\in[m],j\in[k]}.$$

Clearly, because every literal has an equal number of positive and negative occurrences, for *every* assignment τ we have

$$\sum_{i\in[m],j\in[k]}\operatorname{sign}(i,j)\tau(\partial(i,j))=0. \tag{3.1}$$

To compute $\mathbb{E}[Z]$ we merely specialize the first moment computation that was done in [10] in greater generality to the regular k-SAT model.[1] Thus, following [10] we study the sequence $(\operatorname{sign}(i,j)\tau(\partial(i,j)))_{i,j}$ by means of another random ± 1-vector $\chi=(\chi_{ij})_{i\in[m],j\in[k]}$. With q from (1.4) the entries χ_{ij} are mutually independent such that $\mathbb{P}[\chi_{ij}=1]=q$ and $\mathbb{P}[\chi_{ij}=-1]=1-q$. Consider the event $\mathcal{B}=\{\sum_{i\in[m],j\in[k]}\chi_{ij}=0\}$. Then the following is immediate from (3.1) and the definition of the random formula Φ.

Fact 3.1. *Let $\tau:\{x_1,\ldots,x_n\}\to\{\pm 1\}$ be a truth assignment. Then the conditional distribution of χ given $\mathcal{B}$ coincides with the distribution of $(\operatorname{sign}(i,j)\tau(\partial(i,j)))_{i,j}$.*

Hence, to calculate $\mathbb{E}[Z]$ we need to figure out the probability of

$$\mathcal{S}=\{\min_{i\in[m]}\max_{j\in[k]}\chi_{ij}=1\}$$

given $\mathcal{B}$.

Lemma 3.2. *We have*

$$\mathbb{P}[\mathcal{S}|\mathcal{B}]\sim\frac{(1-(1-q)^k)^m(4q(1-q))^{-dn}}{\sqrt{2+2(k-1)q-k}}.$$

We prove Lemma 3.2 by calculating $\mathbb{P}[\mathcal{S}],\mathbb{P}[\mathcal{B}]$ and $\mathbb{P}[\mathcal{B}|\mathcal{S}]$ and applying Bayes' rule.

Claim 3.3. *We have $\mathbb{P}[\mathcal{S}]=(1-(1-q)^k)^m$.*

Proof. The probability that for some $i\in[m]$ we have $\max_{j\in[k]}\chi_{ij}=-1$ equals $(1-q)^k$. Hence, the claim is immediate from the independence of the entries of χ. □

[1] Although it is not included in [10] explicitly, Konstantinos Panagiotou and the first author actually had the proof of Lemma 3.2 on the blackboard. The formula given for the first moment in [22] is equivalent but of a slightly different form.

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Claim 3.4. *We have*

$$\mathbb{P}[\mathcal{B}] = \binom{km}{dn} q^{dn}(1-q)^{dn}.$$

Proof. As $2dn = km$ the assertion follows from the independence of the entries of χ. □

Claim 3.5. *We have* $\mathbb{P}[\mathcal{B}|\mathcal{S}] \sim (\pi km(1-k/2+(k-1)q))^{-1/2}$.

Proof. Let $X = \sum_{i=1}^{m}\sum_{j=1}^{k} 1\{\chi_{ij}=1\}$. Then $\mathcal{B} = \{X = dn\}$. Moreover, the choice (1.4) of q ensures that

$$\mathbb{E}[X|\mathcal{S}] = \frac{kmq}{1-(1-q)^k} = dn. \tag{3.2}$$

Further, given $\mathcal{S}$, X is merely the sum of the independent random variables $X_i = \sum_{j=1}^{k} 1\{\chi_{ij}=1\}$ and

$$\begin{aligned}\mathrm{Var}[X_i|\mathcal{S}] = \mathrm{Var}(\mathrm{Bin}_{\geqslant 1}(k,q)) &= \frac{kq(1-q)+(kq)^2}{1-(1-q)^k} - \left(\frac{kq}{1-(1-q)^k}\right)^2 \\ &= \frac{k}{2}(1-q-k/2+kq).\end{aligned}$$

Consequently, $\mathrm{Var}(X|\mathcal{S}) = km(1-q-k/2+kq)/2$. Thus, the assertion follows from (3.2) and the local limit theorem for sums of independent random variables [13]. □

Proof of Lemma 3.2. By Bayes' rule, Claims 3.3–3.5 and Stirling's formula,

$$\begin{aligned}\mathbb{P}[\mathcal{S}|\mathcal{B}] &\sim \frac{\mathbb{P}[\mathcal{B}|\mathcal{S}]\,\mathbb{P}[\mathcal{S}]}{\mathbb{P}[\mathcal{B}]} = \frac{(1-(1-q)^k)^m}{\sqrt{\pi km(1-q-k/2+kq)}\cdot\binom{km}{km/2}(q(1-q))^{km/2}} \\ &\sim \frac{(1-(1-q)^k)^m(4q(1-q))^{-dn}}{\sqrt{2+2(k-1)q-k}},\end{aligned}$$

as claimed. □

Proceeding to the expectation of Z_μ, we let $M(\sigma)$ be the number of indices $i \in [m]$ such that the random vector χ satisfies $\chi_{ij} = \sigma_j$ for all $j \in [k]$ for $\sigma \in \Sigma = \{\pm 1\}^k \setminus \{(-1,\ldots,-1)\}$. Further, for $\mu \in \mathcal{M}$ let

$$\mathcal{S}_\mu = \{M(\sigma) = m\mu(\sigma) \text{ for all } \sigma \in \Sigma\}. \tag{3.3}$$

Claim 3.6. *For any $\mu \in \mathcal{M}$ we have*

$$\mathbb{P}[\mathcal{S}_\mu|\mathcal{B}\cap\mathcal{S}] = \binom{m}{m\mu}(q(1-q))^{dn}/\mathbb{P}[\mathcal{B}\cap\mathcal{S}].$$

Proof. The definition of the set $\mathcal{M}$ ensures that $\mathcal{S}_\mu \subset \mathcal{S}\cap\mathcal{B}$. Therefore, the lemma follows from the independence of the entries χ_{ij}. □

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Proof of Proposition 2.1. Combining Fact 3.1, Lemma 3.2 and multiplying by the total number of truth assignments, we obtain

$$\mathbb{E}[Z] \sim 2^n \cdot \frac{(1-(1-q)^k)^m (4q(1-q))^{-dn}}{\sqrt{2+2(k-1)q-k}}. \tag{3.4}$$

Further, expanding (1.4), we see that the unique solution $q \in (0,1)$ satisfies

$$q = \frac{1}{2} - 2^{-1-k} + O(k/4^k). \tag{3.5}$$

Hence, recalling (1.3), we obtain

$$\begin{aligned} \ln \mathbb{E}[Z] &= n[\ln 2 + 2k^{-1} d \ln(1-(1-q)^k) - d\ln(4q(1-q))] + O(1) \\ &= 4n(2^{-k} + O(k^2 4^{-k})) = \Omega(n). \end{aligned} \tag{3.6}$$

Finally, (2.7) follows from (3.4) and (3.6).

To complete the proof of Proposition 2.1, fix a number $\omega > 0$. The definition vectors $\mu \in \mathcal{M}_\omega$ must satisfy the two conditions $\sum_{\sigma\in\Sigma} \mu(\sigma) = 1$ and $\sum_{\sigma\in\Sigma} \mu(\sigma)\langle 1, \sigma\rangle = 0$. Therefore,

$$|\mathcal{M}_\omega| = \Theta(m^{-1+|\Sigma|/2}), \tag{3.7}$$

with the number hidden in the $\Theta(\cdot)$ dependent on ω, of course. Further, Claims 3.3, 3.5 and Claim 3.6 and Stirling's formula imply that uniformly for all $\mu \in \mathcal{M}_\omega$,

$$\begin{aligned} \mathbb{P}[\mathcal{S}_\mu | \mathcal{B} \cap \mathcal{S}] &= \Theta(\sqrt{m}) \binom{m}{m\mu} \frac{(q(1-q))^{dn}}{(1-(1-q)^k)^m} \\ &= \Theta(m^{1-|\Sigma|/2}) \frac{(q(1-q))^{dn}}{(1-(1-q)^k)^m} \prod_{\sigma\in\Sigma} \mu(\sigma)^{-m\mu(\sigma)}. \end{aligned}$$

Rewriting the last expression in terms of the distribution $\bar{\mu}$ from (2.6), we obtain

$$\mathbb{P}[\mathcal{S}_\mu | \mathcal{B} \cap \mathcal{S}] = \Theta(m^{1-|\Sigma|/2}) \exp(-m D_{\mathrm{KL}}(\mu \| \bar{\mu})) \quad \text{uniformly for } \mu \in \mathcal{M}_\omega. \tag{3.8}$$

Since the Kullback–Leibler divergence, whose definition we recall from (1.9), attains its global minimum at the point $\mu = \bar{\mu}$ and because its second and third derivative are bounded at this point, (2.9) follows from (3.7), (3.8) and Fact 3.1. Finally, (2.8) follows from (3.8) because the Kullback–Leibler divergence is strictly convex. □

4. Counting cycles

4.1. Proof of Proposition 2.2

Similar results were proved for bipartite graphs in the second author's PhD thesis [25]. (See Proposition 3.5 for example, and Theorem 3.12 more explicitly for biregular bipartite graphs of large girth.) The (minor) difference here is that the sign patterns of the cycles are specified. The key step of the proof is to establish the following lemma.

Lemma 4.1. *Let $S \subset \bigcup_{l\geqslant 1}\{\pm 1\}^{2l}$ be a finite set and let $(c_s)_{s\in S}$ be a non-negative integer vector. Then*

$$\lim_{n\to\infty} \mathbb{E} \prod_{s\in S} C_s^{c_s} = \prod_{s\in S} \lambda_s^{c_s}.$$

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Proposition 2.2 is immediate from Lemma 4.1 and standard results on convergence to the Poisson distribution (*e.g.* [6, Theorem 1.23]). To prove Lemma 4.1 we recall that the random factor graph $G(\Phi)$ is obtained by linking clones of clauses and literals according to the random bijection (2.1).

Claim 4.2. *Fix an integer $b > 1$. The expected number of sets of at most b vertices that span more than b edges in $G(\Phi)$ is $O(1/n)$.*

Proof. Suppose that $b_1, b_2 > 0$ are integers such that $b_1 + b_2 = b$ and let $b_3 > b$. Let $Y(b_1, b_2, b_3)$ be the number of pairs (A, B) such that $A \subset \{x_1, \ldots, x_n\}$, $|A| = b_1$, $B \subset [m]$ such that $A \cup B$ spans at least b_3 edges in $G(\Phi)$. Then

$$Y(b_1, b_2, b_3) \leqslant \binom{n}{b_1}\binom{m}{b_2}\binom{2db_1}{b_3}\binom{kb_2}{b_3} b_3!(2dn - b_3)!/(2dn)!; \tag{4.1}$$

indeed, the binomial coefficients count the number of ways of choosing b_1 variables, b_2 clauses and b_3 'clones' of the chosen variables and clauses. Then there are $b!$ ways of matching these chosen clones up and $(2dn - b_3)!$ ways of joining the remaining clones. By comparison, the total number of bijections (2.1) equals $(2dn)!$. The right-hand side of (4.1) is $O(1/n)$ because $b_3 > b$. Finally, the assertion follows by summing over all b_1, b_2 such that $b_1 + b_2 = b$ and all b_3 such that $b < b_3 \leqslant \min\{2db_1, kb_2\}$. □

Let $l \geqslant 1$ and let $s \in \{\pm 1\}^{2l}$. As a warm-up we calculate $\mathbb{E}[C_s]$; in the process we introduce a bit of notation that will prove useful in Section 4.2 as well. Each cycle with sign pattern s arises as follows. We start from some clause vertex i of $G(\Phi)$. Then we alternate between variable nodes and clause nodes such that the signs decorating the edges that we walk through are as prescribed by s. Finally, the lth variable loops back to the original clause that we started from. Of course, given the starting clause i, each such walk can be encoded by specifying the clones of the clause/literal clones that we follow at each step. Thus, we let $I(s)$ be the set of all families $(j_h, g_h)_{h=2,\ldots,2l+1}$ with $j_h \in [k]$, $g_h \in [d]$ such that

- $j_2 \neq j_{2l+1}$ and $j_{2h+1} \neq j_{2h+2}$ for all $h < l$,
- $g_{2h} \neq g_{2h+1}$ for all $h \in [l]$ such that $s_{2h}s_{2h+1} = 1$.

See Figure 2 for an illustration. Then

$$|I(s)| = (k(k-1))^{2l} d^l \prod_{h=1}^{l} (d-1)^{(1+s_{2h}s_{2h+1})/2} d^{(1-s_{2h}s_{2h+1})/2}. \tag{4.2}$$

Further, for $i \in [m]$ let $\mathcal{C}_\Phi(s, i, j, g)$ be the event that the cycle prescribed by $(j, g) \in I(s)$ materializes from the starting clause i. That is, if we define $i_2 = i$ and $i_{2t-1} = i_{2t} = \partial(\partial(i_{2t-2}, j_{2t-2}), g_{2t-1})$ for $t \geqslant 2$, then (i, j) satisfies the conditions **CY1–CY5** and

$$\Phi[i_t, j_t] \in \{x_1, \ldots, x_n\} \times \{g_t\} \times \{\pm 1\} \quad \text{for all } t = 2, \ldots, 2l+1.$$

We claim that

$$\mathbb{E}[C_s] = \sum_{i=1}^{m} \sum_{(j,g) \in I(s)} \mathbb{P}[\mathcal{C}_\Phi(s, i, j, g)] \sim \frac{|I(s)|}{2l}(2kd)^{-l} = \lambda_s. \tag{4.3}$$

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

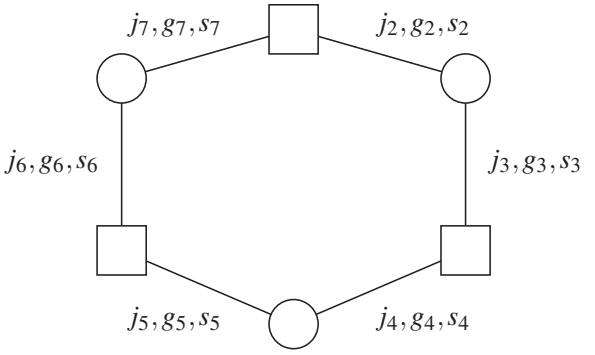

Figure 2. The indices j_h, g_h along a cycle with $l = 3$ clauses, with squares representing clauses and circles variables.

Indeed, because Φ comes from the random bijection (2.1), the probability that for $h \in [2l]$ the j_{2h}th clone of clause i_{2h} is connected to the g_{2h}th clone with sign s_{2h} of some variable is $(2d)^{-1} + o(1)$. Further, the probability that the g_{2h}th clone with sign s_{2h+1} of this variable is connected to the j_{2h+1}th clone of some clause is $k^{-1} + o(1)$. Ultimately, the probability that the g_{2l}th clone of sign s_{2l+1} of the last variable visited is connected to the j_1th clone of the starting clause is $(1 + o(1))(km)^{-1}$. Finally, the factor $1/2l$ in (4.3) comes from **CY4** and the convention that we consider the clauses with the least index the starting point of the cycle.

Proof of Lemma 4.1. It is straightforward to extend the argument from the previous paragraph to the joint factorial moments of the random variables C_s. Hence, let $S \subset \bigcup_l \{\pm 1\}^{2l}$ be finite and let $c = (c_s)_{s \in S}$ be an integer vector with $c_s > 0$ for all s. Then $\prod_{s \in S} C_s^{\underline{c_s}}$ is the number of families that contain precisely c_s distinct cycles of type s for each $s \in S$. By Fact 4.2 we just need to count families of vertex-disjoint cycles. To this end, we choose distinct starting clauses $(i(s,g))_{s \in S, g \in [c_s]}$. Because $\sum_{s \in S} c_s$ remains fixed as $n \to \infty$, the number of choices is $(1 + O(1/m))m^{\sum_{s \in S} c_s}$. Further, for each $s \in S$ and $g \in [c_s]$ we pick $(j_h(s,g), g_h(s,g))_h \in I(s)$. By the same reasoning as in the calculation of $\mathbb{E}[C_s]$, for each $s \in S$, $g \in [c_s]$ the probability that the desired cycle materializes is $(1 + o(1))(2kd)^{-l} m^{-1}$. In fact, these events are asymptotically independent because we only consider vertex-disjoint cycles and $\sum_{s \in S} c_s = O(1)$ as $n \to \infty$. Hence Lemma 4.1 follows. □

4.2. Proof of Proposition 2.3

With respect to Proposition 2.3, we use the random vector χ and the other notation from Section 3. Consider the following experiment for constructing a formula $\hat{\Phi}$ together with an assignment $\hat{\sigma}$, which we call the *planted distribution*; similar constructions have been used previously [5, 9, 10].

PL1 Choose a truth assignment $\hat{\sigma} : \{x_1, \ldots, x_n\} \to \{\pm 1\}$ uniformly at random.
PL2 Choose χ independently of $\hat{\sigma}$ given that $\chi \in \mathcal{S} \cap \mathcal{B}$.
PL3 Choose bijection $\hat{\Phi} : [m] \times [k] \to \{x_1, \ldots, x_n\} \times [d] \times \{\pm 1\}$ uniformly subject to the condition

$$\operatorname{sign}_{\hat{\Phi}}(i,j)\hat{\sigma}(\partial_{\hat{\Phi}}(i,j)) = \chi_{ij} \quad \text{for all } (i,j) \in [m] \times [k].$$

In words, we first choose a truth assignment $\hat{\sigma}$ uniformly at random. Then, we prescribe a random sequence χ of km truth values subject to the condition that for each clause index $i \in [m]$

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

there exists $j \in [k]$ such that $\chi_{ij} = 1$ and such that $\sum_{i,j} \chi_{ij} = 0$. Finally, we randomly match those literal occurrences that the assignment $\hat{\sigma}$ renders true to the precisely dn clause slots (i,j) such that $\chi_{ij} = 1$ and the ones that $\hat{\sigma}$ sets to false to the dn remaining positions. As an immediate consequence of Fact 3.1 we obtain the following.

Fact 4.3. *Let $\mathcal{A}$ be a set of pairs (Φ, σ) of formulas and assignments. Moreover, let $Z_{\mathcal{A}}(\Phi)$ be the number of satisfying assignments σ of Φ such that $(\Phi, \sigma) \in \mathcal{A}$. Then*

$$\mathbb{E}[Z_{\mathcal{A}}(\Phi)] = \mathbb{E}[Z(\Phi)] \cdot \mathbb{P}[(\hat{\Phi}, \hat{\sigma}) \in \mathcal{A}].$$

We are going to use Lemma 4.6 to prove the following statement. Let $I(s)$ be as in the previous section. As before we are going to be interested in the event $\mathcal{C}_{\hat{\Phi}}(i,j,g,s)$ that, for a clause index i and $(j,g) \in I(s)$, a cycle as described by i,j,g,s occurs in the formula $\hat{\Phi}$. Further, for $i \in [m]$ let $\mathcal{C}_{\hat{\Phi}}(i,s)$ be the event that there exists $(j,g) \in I(s)$ such that $\mathcal{C}_{\hat{\Phi}}(i,j,g,s)$ occurs.

Lemma 4.4. *Let $S \subset \bigcup_{l \geqslant 1} \{\pm 1\}^{2l}$ be finite and let $c = (c_s)_{s \in S}$ be a non-negative integer vector. Let $i = (i(s,a))_{s \in S, a \in [c_s]}$ be a random vector whose entries $i(s,a) \in [m]$ are independent and uniformly distributed. Then*

$$\mathbb{P}\left[\bigcap_{s \in S, a \in [c_s]} \mathcal{C}_{\hat{\Phi}}(i(s,a),s)\right] \sim \prod_{s \in S} \left(\frac{(1+\delta_s)\lambda_s}{m}\right)^{c_s}.$$

The proof of Lemma 4.4 is based on the following elementary observation.

Claim 4.5. *Let $\mathcal{I} \subset [m]$ be a set of size $|\mathcal{I}| \leqslant n^{1/3}$ and let $\tau = (\tau_i)_{i \in \mathcal{I}} \in \Sigma^{\mathcal{I}}$. Further, let $\mathcal{E}(\mathcal{I}, \tau)$ be the event that for each $i \in \mathcal{I}$ we have $(\hat{\sigma}(\hat{\Phi}[i,j]))_{j \in [k]} = \tau_i$. Then*

$$\mathbb{P}[\mathcal{E}(\mathcal{I}, \tau)] \sim \prod_{i \in \mathcal{I}} \frac{((1-q)q)^{k/2} \prod_{j=1}^{k} (q/(1-q))^{\tau_{ij}/2}}{2q}. \tag{4.4}$$

Proof. Since $1 - (1-q)^k = 2q$ by the definition of q, the right-hand side of (4.4) is just the probability that $\chi_{ij} = \tau_{ij}$ for all $i \in \mathcal{I}$, $j \in [k]$ given the event $\mathcal{S}$. Moreover, because $|\mathcal{I}| \leqslant n^{1/3}$, a similar application of the local limit theorem as in the proof of Claim 3.5 shows that $\mathbb{P}[\mathcal{B}|\mathcal{S}] \sim \mathbb{P}[\mathcal{B}|\mathcal{S}, \mathcal{E}(\mathcal{I}, \tau)]$. Therefore, the assertion follows from Bayes' rule. □

Proof of Lemma 4.4. A similar calculation as in the proof of Claim 4.2 shows that we only need to consider families of vertex-disjoint cycles. Further, because the total number of vertices involved in the cycles remains bounded as $n \to \infty$, the events $\mathcal{C}(i(s,a))$ are asymptotically independent. Therefore, we are just going to calculate the probability of a single event $\mathcal{C}(i,s)$ for a random $i \in [m]$.

We can write $\mathcal{C}(i,s)$ as a disjoint union of sub-events in which we specify the truth values that $\hat{\sigma}$ assigns to the literals in the order in which they appear along the cycle. Thus, let $\xi = (\xi_2, \ldots, \xi_{2l+1}) \in \{\pm 1\}^{2l}$ be a sequence such that $\xi_{2h}\xi_{2h+1} = s_{2h}s_{2h+1}$ for all h. Further, set $\xi_1 = \xi_{2l+1}$, $j_1 = j_{2l+1}$. Moreover, let $i = (i_1, \ldots, i_l) \in [m]^l$ be a sequence of pairwise distinct clause

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

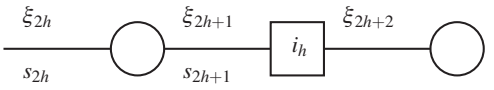

Figure 3. The transition from ξ_{2h} to ξ_{2h+2} along clause i_h.

indices and let $(j,g) \in I(s)$. Thus, $(j_h, g_h)_{h=2,\dots,2l+1}$ are families of indices $j_h \in [k]$, $g_h \in [d]$ such that $j_2 \neq j_{2l+1}$ and $j_{2h+1} \neq j_{2h+2}$ for all $h < l$, and $g_{2h} \neq g_{2h+1}$ for all $h \in [l]$ such that $s_{2h}s_{2h+1} = 1$. Let $\mathcal{D}_h(i,j,g,\xi,s)$ be (just) the event that $\chi_{i_h,j_{2h-1}} = \xi_{2h+1}$ and $\chi_{i_h,j_{2h}} = \xi_{2h+2}$ and let

$$\mathcal{D}(i,j,g,\xi,s) = \bigcap_{h=1}^{l} \mathcal{D}_h(i,j,g,\xi,s).$$

Then the probability

$$M'_{s_{2h}s_{2h+1}}(\xi_{2h}, \xi_{2(h+1)}) = \mathbb{P}[\mathcal{D}_h(i,j,g,\xi,s)]$$

depends on $s_{2h}s_{2h+1}$ and $\xi_{2h}, \xi_{2(h+1)}$ only. In fact, using Claim 4.5 with $\mathcal{I} = \{i_1, \dots, i_l\}$ we can work out the probabilities of the eight possible cases easily. See Figure 3 for an illustration.

Case 1. $s_{2h}s_{2h+1} = 1$. There are four sub-cases depending on the truth values $\xi_{2h}, \xi_{2(h+1)}$.

Case 1a. $\xi_{2h} = \xi_{2(h+1)} = 1$. Clause i_h is satisfied because $\xi_{2h} = 1$. Therefore, the probability that $\xi_{2(h+1)} = \xi_{2h+1} = 1$ comes to

$$M'_1(1,1) \sim q^2/(2q) = q/2.$$

Case 1b. $\xi_{2h} = -\xi_{2(h+1)} = 1$. Clause i_h is satisfied due to $\xi_{2h} = 1$. Hence,

$$M'_1(1,-1) \sim (1-q)/2.$$

Case 1c. $\xi_{2h} = -\xi_{2(h+1)} = -1$. Clause i_h is satisfied as $\xi_{2h+1} = 1$. Hence,

$$M'_1(-1,1) \sim (1-q)/2.$$

Case 1d. $\xi_{2h} = \xi_{2(h+1)} = -1$. One of the $k-2$ remaining literals of clause i_h has to take the value 1 to satisfy the clause. Since $(1-q)^k = 1-2q$ and thus $(1-q)^{k-2} = (1-2q)/(1-q)^2$, we get

$$M'_1(-1,-1) \sim (1-q)^2(1-(1-q)^{k-2})/(2q) = q/2.$$

Case 2. $s_{2h}s_{2h+1} = -1$. Once more there are four sub-cases.

Case 2a. $\xi_{2h} = \xi_{2(h+1)} = 1]$. Clause i_h is satisfied because $\xi_{2h+2} = 1$. Therefore,

$$M'_{-1}(1,1) \sim q(1-q)/(2q) = (1-q)/2.$$

Case 2b. $\xi_{2h} = -\xi_{2(h+1)} = 1$. For clause i_h to be satisfied one of the $k-2$ literals in the clause that do not belong to the cycle has to be true. Thus,

$$M'_{-1}(-1,1) \sim \frac{(1-q)^2(1-(1-q)^{k-2})}{2q} = \frac{q((1-q)^2-(1-q)^k)}{2q(1-q)} = \frac{q}{2}.$$

Case 2c. $\xi_{2h} = -\xi_{2(h+1)} = -1$. Clause i_h is satisfied due to $\xi_{2h+1} = 1$. Hence,

$$M'_{-1}(1,-1) \sim q/2.$$

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Case 2d. $\xi_{2h} = \xi_{2(h+1)} = -1$. Clause i_h is satisfied as $\xi_{2h+1} = 1$. Therefore,

$$M'_{-1}(-1,-1) \sim q(1-q)/(2q) = (1-q)/2.$$

Taking the union over all possible truth values ξ, we obtain (following similar arguments in [17, Section 4])

$$\mathbb{P}\left[\bigcup_{\xi} \mathcal{D}(i,j,g,\xi,s)\right] \sim \sum_{\xi} \prod_{h=1}^{l} M'_{s_{2h}s_{2h+1}}(\xi_{2h},\xi_{2(h+1)}) = \operatorname{tr}\prod_{i=1}^{l} M'_{s_{2i}s_{2i+1}}. \tag{4.5}$$

Additionally, we claim that

$$\mathbb{P}[\mathcal{C}_{\hat{\Phi}}(s,i,j,g) \mid \mathcal{D}(i,j,g,\xi,s)] = 2^l\,\mathbb{P}[\mathcal{C}_{\Phi}(s,i,j,g)]. \tag{4.6}$$

Indeed, in the probability term on the right-hand side the literals that are matched to the clauses $i_1,\ldots,i_l$ are chosen uniformly at random from the set of all $2n$ literals. By contrast, in the experiment on the left-hand side we condition on the truth values of the literals on the cycle, which are prescribed by the vector ξ, and thus they are chosen from the n literals with the correct truth value under $\hat{\sigma}$.

Finally, with $M_{\pm 1}$ the matrices from (2.12), we see that $M'_{\pm 1} \sim \frac{1}{2}M_{\pm 1}$. Hence, (4.5) and (4.6) yield

$$\mathbb{P}[\mathcal{C}_{\hat{\Phi}}(i,s)] \sim 2^l\,\mathbb{P}[\mathcal{C}_{\Phi}(i,s)]\operatorname{tr}\prod_{i=1}^{l} M'_{s_{2i}s_{2i+1}} = \mathbb{P}[\mathcal{C}_{\Phi}(i,s)]\operatorname{tr}\prod_{i=1}^{l} M_{s_{2i}s_{2i+1}}.$$

Thus, the assertion follows from Lemma 4.1. □

While Lemma 4.4 puts us in a position to calculate the covariance of Z and the cycle counts C_s, Proposition 2.3 deals with the covariance of Z_μ and the C_s. Hence, we need to consider a variant of the planted distribution that fixes the clause marginal μ. We recall the event $\mathcal{S}_\mu$ from (3.3).

Lemma 4.6. *For any $\omega > 0$ the following is true. Let $S \subset \bigcup_{l\geqslant 1}\{\pm 1\}^{2l}$ be finite and let $c = (c_s)_{s\in S}$ be a non-negative integer vector. Let $i = (i(s,a))_{s\in S, a\in[c_s]}$ be a random vector whose entries $i(s,a) \in [m]$ are independent and uniformly distributed. Further, let*

$$\mathcal{C} = \bigcap_{s\in S, a\in[c_s]} \mathcal{C}_{\hat{\Phi}}(i(s,a),s).$$

Then

$$\mathbb{P}[\mathcal{S}_\mu \mid \mathcal{S}\cap\mathcal{C}] \sim \mathbb{P}[\mathcal{S}_\mu \mid \mathcal{S}] \quad \textit{uniformly for all } \mu \in \mathcal{M}_\omega.$$

Proof. Suppose that the event $\mathcal{S}\cap\mathcal{C}$ occurs. Let $J \subset [m]$ be the set of all indices of clauses that participate in the cycles corresponding to $\mathcal{C}$. Then $m' = |J| = m - O(1)$. Further, for each $\sigma \in \Sigma$ let $m\mu''(\sigma)$ be the number of clauses $i \in [m]\setminus J$ that are satisfied according to $\sigma \in \Sigma$. Additionally, let $m\mu'(\sigma)$ be such that $m(\mu'(\sigma)+\mu''(\sigma)) = \mu(\sigma)$. Finally, let $\mathcal{S}'_\mu$ be the event that the empirical distribution of patterns on the clauses $\bar{J} = [m]\setminus J$ works out to be precisely μ'. Then given $\mathcal{C}$ the

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

event $\mathcal{S}_\mu$ occurs if and only if $\mathcal{S}'_\mu$ occurs. Hence, in analogy to Claim 3.6 we have

$$\begin{aligned}\mathbb{P}[\mathcal{S}_\mu|\mathcal{S}\cap\mathcal{C}] &= \binom{m'}{m'\mu'}\frac{(q(1-q))^{dn}}{\mathbb{P}[\mathcal{S}]}\\ &\sim (2\pi m)^{1-2^{k-1}}\left[\prod_{\sigma\in\Sigma}\mu'(\sigma)\right]^{-1/2}\exp[-|J|D_{\mathrm{KL}}(\mu'\|\bar{\mu})]\\ &\sim \frac{(2\pi m)^{1-2^{k-1}}}{\prod_{\sigma\in\Sigma}\sqrt{\bar{\mu}(\sigma)}}\exp[-(m-O(1))D_{\mathrm{KL}}(\mu'\|\bar{\mu})] \quad \text{uniformly for } \mu\in\mathcal{M}_\omega. \quad (4.7)\end{aligned}$$

Further, since $|J| = O(1)$ we have $\|\mu-\mu'\|_2 = O(1/m)$, whence

$$D_{\mathrm{KL}}(\mu'\|\bar{\mu}) - D_{\mathrm{KL}}(\mu\|\bar{\mu}) = o(m^{-1}).$$

Moreover, as $\|\mu-\bar{\mu}\|_2 = O(m^{-1/2})$, we have $D_{\mathrm{KL}}(\mu\|\bar{\mu}) = O(1/m)$. Therefore, (4.7) implies that uniformly for $\mu\in\mathcal{M}_\omega$,

$$\mathbb{P}[\mathcal{S}_\mu|\mathcal{S}\cap\mathcal{C}] \sim \frac{(2\pi m)^{1-2^{k-1}}}{\prod_{\sigma\in\Sigma}\sqrt{\bar{\mu}(\sigma)}}\exp[-mD_{\mathrm{KL}}(\mu\|\bar{\mu})] \sim \mathbb{P}[\mathcal{S}_\mu|\mathcal{S}],$$

as claimed. □

Combining Lemmas 4.4 and 4.6 gives the following.

Corollary 4.7. *Let $\omega > 0$. With the notation from Lemma 4.4 we have*

$$\mathbb{P}\left[\bigcap_{s\in S,a\in[c_s]}\mathcal{C}_{\hat{\Phi}}(i(s,a),s)\middle|\mathcal{S}_\mu\right] \sim \prod_{s\in S}\left(\frac{(1+\delta_s)\lambda_s}{m}\right)^{c_s} \quad \textit{uniformly for all } \mu\in\mathcal{M}_\omega.$$

Now, (2.15) follows from Fact 4.3, Corollary 4.7 and the standard result on convergence to the Poisson distribution (*e.g.* [6, Theorem 1.23]). Hence, the following completes the proof of Proposition 2.3.

Lemma 4.8. *The series $\sum_{l,s}\delta_s^2\lambda_s$ converges and satisfies* (2.16).

Proof. Being the solution to (1.4), q satisfies $q = 1/2 + O(2^{-k})$. Hence, our assumption that $d \leqslant k2^k$ ensures that

$$|(2d-1)(k-1)(1-4q(1-q))| < 1.$$

Therefore, merely substituting in the expressions from (2.10) and (2.14), we obtain

$$\begin{aligned}\sum_{l\geqslant 1}\sum_{s\in\{\pm1\}^{2l}}\delta_s^2\lambda_s &= \sum_{l\geqslant 1}\frac{1}{2l}[(2d-1)(k-1)(1-4q(1-q))]^l\\ &= -\frac{1}{2}\ln(1-(2d-1)(k-1)(1-4q(1-q))) < \infty,\end{aligned}$$

as claimed. □

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

5. The second moment

5.1. Outline

In this section we prove Proposition 2.4. Let $Z^{\otimes}_{\alpha,\mu}$ be the number of pairs (τ_1,τ_2) of satisfying assignments such that $\mu=\mu(\Phi,\tau_1)=\mu(\Phi,\tau_2)$ and such that $\sum_{i=1}^{n}1\{\tau_1(x_i)=\tau_2(x_i)\}=\alpha$. Then by the linearity of expectation

$$\mathbb{E}[Z_\mu^2]=\sum_{\alpha=0}^{n}\mathbb{E}[Z^{\otimes}_{\mu,\alpha}]. \tag{5.1}$$

We will evaluate the sum on the right-hand side of (5.1) in two steps. The main step is to calculate the contribution of α close to $n/2$.

Lemma 5.1. *Uniformly for $\mu\in\mathcal{M}_\omega$ we have*

$$\lim_{a\to\infty}\lim_{n\to\infty}\sum_{\alpha:|\alpha-n/2|\leqslant a\sqrt{n}}\frac{\mathbb{E}[Z^{\otimes}_{\mu,\alpha}]}{\mathbb{E}[Z_\mu]^2}=(1-(2d-1)(k-1)(1-4q(1-q)))^{-1/2}.$$

The proof of Lemma 5.1 is based on the following lemma, which we derive from the central limit theorem for random permutations [8] in Section 5.2. The motivation for the definition of $y^{\otimes}$ in this lemma will become clear very soon, in the proof of Lemma 5.1.

Lemma 5.2. *The following holds uniformly for all $\mu\in\mathcal{M}_\omega$. Let*

$$y^{\otimes}=(y^{(1)}_{ij},y^{(2)}_{ij})_{(i,j)\in[m]\times[k]}$$

be chosen uniformly at random from the set of all $m\times k$ $\{\pm1\}^2$-arrays. Let $\mathcal{S}^{\otimes}_\mu$ be the event that

$$\sum_{i=1}^{m}\prod_{j=1}^{k}1\{y^{(1)}_{ij}=\sigma_j\}=\sum_{i=1}^{m}\prod_{j=1}^{k}1\{y^{(2)}_{ij}=\sigma_j\}=m\mu(\sigma)\quad\text{for all }\sigma\in\Sigma. \tag{5.2}$$

Further, let

$$A=\sum_{i=1}^{m}\sum_{j=1}^{k}1\{y^{(1)}_{ij}=y^{(2)}_{ij}=1\},\quad \nu^2=\frac{k}{16}(k-4(k-1)q(1-q)).$$

Then uniformly for all reals $a<b$ we have

$$\mathbb{P}[m^{-1/2}(A-dn/2)\in(a,b)|\mathcal{S}^{\otimes}_\mu]=\frac{1}{\sqrt{2\pi}\nu}\int_a^b\exp(-z^2/(2\nu^2))dz+o(1).$$

Proof of Lemma 5.1. Fix $\omega>0$ and let $\mu\in\mathcal{M}_\omega$. There are $2^n\binom{n}{\alpha}$ pairs (τ_1,τ_2) of truth assignments with overlap $\sum_{i=1}^{n}1\{\tau_1(x_i)=\tau_2(x_i)\}=\alpha$; to see this, start by choosing a truth assignment τ_1 out of the set of all 2^n possible assignments, then obtain τ_2 by selecting α variables on which both assignments agree. Suppose we fix one such pair (τ_1,τ_2). What is the probability that $\mu(\Phi,\tau_1)=\mu(\Phi,\tau_2)=\mu$? To determine this we need information on the distribution of the

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

string

$$\tilde{y}^{\otimes} = (\tilde{y}_{ij}^{(1)}, \tilde{y}_{ij}^{(2)})_{(i,j)\in[m]\times[k]} \in \{(-1,-1),(-1,1),(1,-1),(1,1)\}^{km} \quad \text{where}$$
$$\tilde{y}_{ij}^{(t)} = \operatorname{sign}(i,j)\tau^{(t)}(\partial(i,j)) \quad (i \in [m], j \in [k], t \in \{1,2\}).$$

Recalling that $\partial(i,j)$ is the variable that occurs in the jth position of the ith clause, and that $\operatorname{sign}(i,j)$ is the sign with which the variable occurs, we see that $\tilde{y}^{\otimes}$ comprises the truth value combinations that emerge if we assign the variables of the random formula Φ according to $\tau^{(1)}, \tau^{(2)}$. Thus, with $\mathcal{S}_{\mu}^{\otimes}$ the event from Lemma 5.2 we obtain

$$\mathbb{E}[Z_{\mu,\alpha}^{\otimes}] = 2^n \binom{n}{\alpha} \mathbb{P}[\mu(\Phi,\tau_1) = \mu(\Phi,\tau_2) = \mu] = 2^n \binom{n}{\alpha} \mathbb{P}[\tilde{y}^{\otimes} \in \mathcal{S}_{\mu}^{\otimes}]. \tag{5.3}$$

We study the distribution of $\tilde{y}^{\otimes}$ by way of the uniformly random string

$$y^{\otimes} \in \{(-1,-1),(-1,1),(1,-1),(1,1)\}^{km}$$

from Lemma 5.2. To this end, with the notation of Lemma 5.2 define the two events

$$\mathcal{A}_{\alpha} = \{A = d\alpha\}, \quad \mathcal{B}^{\otimes} = \left\{\sum_{i=1}^{m}\sum_{j=1}^{k} y_{ij}^{(1)} = \sum_{i=1}^{m}\sum_{j=1}^{k} y_{ij}^{(2)} = 0\right\}.$$

Then the distribution of $\tilde{y}^{\otimes}$ coincides with the distribution of $y^{\otimes}$ given $\mathcal{A}_{\alpha} \cap \mathcal{B}^{\otimes}$. Indeed, we have $\tilde{y}^{\otimes} \in \mathcal{A}_{\alpha}$ because τ_1, τ_2 have overlap α, and $\tilde{y}^{\otimes} \in \mathcal{B}^{\otimes}$ because there are precise dn true and dn false literals occurrences. In particular,

$$\mathbb{P}[\tilde{y}^{\otimes} \in \mathcal{S}_{\mu}^{\otimes}] = \mathbb{P}[y^{\otimes} \in \mathcal{S}_{\mu}^{\otimes} \mid \mathcal{A}_{\alpha} \cap \mathcal{B}^{\otimes}]. \tag{5.4}$$

As a next step we will prove that, uniformly for all α such that $|\alpha - n/2| \leqslant n^{0.6}$ and all $\mu \in \mathcal{M}_{\omega}$,

$$\mathbb{P}[y^{\otimes} \in \mathcal{S}_{\mu}^{\otimes} \mid \mathcal{A}_{\alpha} \cap \mathcal{B}^{\otimes}] \sim \frac{\sqrt{\pi dn}\,\mathbb{E}[Z_{\mu}]^2}{2^{2n+1}} \exp\left(4dn\left(\frac{\alpha}{n} - \frac{1}{2}\right)^2\right) \mathbb{P}[y^{\otimes} \in \mathcal{A}_{\alpha} | \mathcal{S}_{\mu}^{\otimes}]. \tag{5.5}$$

Indeed, since $\mathcal{S}_{\mu}^{\otimes} \subset \mathcal{B}^{\otimes}$, Bayes' rule gives

$$\mathbb{P}[y^{\otimes} \in \mathcal{S}_{\mu}^{\otimes} | \mathcal{A}_{\alpha} \cap \mathcal{B}^{\otimes}] = \frac{\mathbb{P}[y^{\otimes} \in \mathcal{S}_{\mu}^{\otimes} | \mathcal{B}^{\otimes}]}{\mathbb{P}[y^{\otimes} \in \mathcal{A}_{\alpha} | \mathcal{B}^{\otimes}]} \cdot \mathbb{P}[y^{\otimes} \in \mathcal{A}_{\alpha} | \mathcal{S}_{\mu}^{\otimes}]. \tag{5.6}$$

Hence, we need to calculate $\mathbb{P}[y^{\otimes} \in \mathcal{S}_{\mu}^{\otimes} | \mathcal{B}^{\otimes}]$ and $\mathbb{P}[y^{\otimes} \in \mathcal{A}_{\alpha} | \mathcal{B}^{\otimes}]$. With respect to the latter, there are $\binom{2dn}{dn}$ strings in $\{\pm 1\}^{km}$ with as many $+1$s as -1s. Therefore,

$$|\mathcal{B}^{\otimes}| = \binom{2dn}{dn}^2. \tag{5.7}$$

Furthermore, we have

$$|\mathcal{A}_{\alpha} \cap \mathcal{B}^{\otimes}| = \binom{2dn}{\alpha d, (n-\alpha)d, (n-\alpha)d, \alpha d}; \tag{5.8}$$

for any string in $\mathcal{A}_{\alpha} \cap \mathcal{B}^{\otimes}$ contains exactly α many $(1,1)$ entries and $(n-\alpha)d$ many entries $(-1,1)$ and $(1,-1)$ entries. Hence, combining (5.7) and (5.8) and applying Stirling's formula,

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

we obtain, uniformly for all α such that $|\alpha - n/2| \leqslant n^{0.6}$ and all $\mu \in \mathcal{M}_\omega$,

$$\mathbb{P}[y^\otimes \in \mathcal{A}_\alpha | \mathcal{B}^\otimes] = \binom{2dn}{\alpha d, (n-\alpha)d, (n-\alpha)d, \alpha d} \binom{2dn}{dn}^{-2} = \binom{dn}{d\alpha}^2 / \binom{2dn}{dn}$$
$$\sim \frac{2}{\sqrt{\pi dn}} \exp\left(-4dn\left(\frac{\alpha}{n} - \frac{1}{2}\right)^2\right). \tag{5.9}$$

Additionally, we claim that

$$\mathbb{P}[y^\otimes \in \mathcal{S}_\mu^\otimes | \mathcal{B}^\otimes] = 4^{-n}\,\mathbb{E}[Z_\mu]^2. \tag{5.10}$$

Indeed, if we fix a truth assignment τ, then the random matching Φ of literals to clause slots induces a uniformly random string of length km comprising dn many $+1$ entries and dn many -1 entries. The probability that the resulting empirical distribution of truth value patterns on the m clauses matches μ is precisely equal to $2^{-n}\,\mathbb{E}[Z_\mu]$ (because we fixed the truth assignment τ upfront). Furthermore, given $\mathcal{B}^\otimes$ the two components $(y_{ij}^{(1)})_{i,j}$, $(y_{ij}^{(2)})_{i,j}$ are independent, whence we obtain (5.10). Finally, combining (5.6), (5.9) and (5.10), we obtain (5.5).

Combining (5.3), (5.4) and (5.5), we get

$$\frac{\mathbb{E}[Z_{\mu,\alpha}^\otimes]}{\mathbb{E}[Z_\mu]^2} \sim 2^n \binom{n}{\alpha} \frac{\sqrt{\pi dn}}{2^{2n+1}} \exp\left(4dn\left(\frac{\alpha}{n} - \frac{1}{2}\right)^2\right) \mathbb{P}[y^\otimes \in \mathcal{A}_\alpha | \mathcal{S}_\mu^\otimes], \tag{5.11}$$

uniformly for all α such that $|\alpha - n/2| \leqslant n^{0.6}$ and all $\mu \in \mathcal{M}_\omega$. Moreover, uniformly for all α such that $|\alpha - n/2| \leqslant n^{0.6}$,

$$2^{-n}\binom{n}{\alpha n} \sim \sqrt{\frac{2}{\pi n}} \exp\left[-2n\left(\frac{\alpha}{n} - \frac{1}{2}\right)^2\right]. \tag{5.12}$$

Hence, combining (5.11) and (5.12) with Lemma 5.2, we find

$$\sum_{\alpha:|\alpha-n/2|\leqslant a} \frac{\mathbb{E}[Z_{\mu,\alpha}^\otimes]}{\mathbb{E}[Z_\mu]^2} = o(1) + \sqrt{\frac{d}{2}} \sum_{\alpha:|\alpha-n/2|\leqslant a\sqrt{n}} \exp\left((4d-2)\left(\frac{\alpha}{n} - \frac{1}{2}\right)^2 n\right) \mathbb{P}[y^\otimes \in \mathcal{A}_\alpha | \mathcal{S}_\mu^\otimes]$$
$$= o(1) + \sqrt{\frac{dn}{4\pi\nu^2 m}} \int_{-\infty}^{\infty} \exp\left[\left(4d - 2 - \frac{dk}{4\nu^2}\right) z^2\right] dz.$$

Taking $a \to \infty$, we thus obtain

$$\lim_{a\to\infty} \lim_{n\to\infty} \sum_{\alpha:|\alpha-n/2|\leqslant a} \frac{\mathbb{E}[Z_{\mu,\alpha}^\otimes]}{\mathbb{E}[Z_\mu]^2} = \sqrt{\frac{k}{8\pi\nu^2}} \int_{-\infty}^{\infty} \exp\left[\left(4d - 2 - \frac{dk}{4\nu^2}\right) z^2\right] dz$$
$$= \sqrt{\frac{k}{2dk - 16(2d-1)\nu^2}}.$$

Substituting in the expression for ν^2 and simplifying completes the proof. □

Building upon ideas from [10], in Section 5.3 we prove the following bound on the contribution of α far from $n/2$.

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Lemma 5.3. *Uniformly for $\mu \in \mathcal{M}_\omega$ we have*

$$\lim_{a\to\infty}\lim_{n\to\infty}\sum_{\alpha:|\alpha-(n/2)|>a\sqrt{n}}\frac{\mathbb{E}[Z_{\mu,\alpha}^{\otimes}]}{\mathbb{E}[Z_\mu]^2}=0.$$

Finally, Proposition 2.4 is immediate from Lemmas 5.3 and 5.1.

5.2. Proof of Lemma 5.2

We begin by calculating the expectation and the variance of A given $\mathcal{S}_\mu^{\otimes}$ as defined in (5.2). This is the number of 1s in common between the arrays $\mathbf{y}^{(1)}$ and $\mathbf{y}^{(2)}$, conditional on both arrays having row frequencies specified by μ. To simplify the notation we let

$$\hat{y}=(\hat{y}_{ij}^{(1)},\hat{y}_{ij}^{(2)})_{i,j}$$

denote the random vector $y^{\otimes}$ given that $\mathcal{S}_\mu^{\otimes}$ occurs.

Lemma 5.4. *We have $\mathbb{E}[A(\hat{y})]=dn/2+O(1)$ and $\mathrm{Var}(A(\hat{y}))\sim \nu^2 m$, where*

$$\nu^2=\frac{k}{16}(k-4(k-1)q(1-q)).$$

The proof will show that ν^2 is $\mathrm{Var}(A(\hat{y}))$ in the case that $\mu=\bar{\mu}$.

Proof. Let $A_{ij}=1\{\hat{y}_{ij}^{(1)}=\hat{y}_{ij}^{(2)}=1\}$ so that $A=\sum_{i,j}A_{ij}$. To calculate the expectation, set

$$A_j=\sum_{i\in[m]}1\{\hat{y}_{ij}^{(1)}=\hat{y}_{ij}^{(2)}=1\},$$
$$a_j=\sum_{\sigma\in\Sigma}1\{\sigma_j=1\}\mu(\sigma)=\frac{1}{m}\sum_{i\in[m]}1\{\hat{y}_{ij}^{(1)}=1\}=\frac{1}{m}\sum_{i\in[m]}1\{\hat{y}_{ij}^{(2)}=1\}.$$

Thus, a_j is the fraction of clauses whose jth literal is 'true' in a truth assignment that contributes to Z_μ. Then it is clear that $\mathbb{E}[A]=\sum_{j=1}^k\mathbb{E}[A_j]$ and $\mathbb{E}[A_j]=ma_j^2$. Furthermore, because $\mu\in\mathcal{M}_\omega$ we have

$$\begin{aligned}a_j-\frac{1}{2}&=a_j-\sum_{\sigma\in\Sigma}1\{\sigma_j=1\}\bar{\mu}(\sigma)\quad\text{(by (1.4) and (2.6))}\\&=\sum_{\sigma\in\Sigma}1\{\sigma_j=1\}(\mu(\sigma)-\bar{\mu}(\sigma))\leqslant 2^k\|\mu-\bar{\mu}\|_2\leqslant 2^k\omega m^{-1/2}.\end{aligned}$$

Finally, since $\sum_j a_j=1/2$ by (2.4), for any fixed $\omega>0$ we have

$$\mathbb{E}[A]-\frac{dn}{2}=m\sum_{j=1}^k\left(a_j^2-\frac{1}{4}\right)=m\sum_{j=1}^k\left(a_j-\frac{1}{2}\right)^2\leqslant 4^k\omega^2=O(1).$$

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Moving on to the variance, we expand $\mathbb{E}[A^2]$ to obtain

$$\begin{aligned}\mathbb{E}[A^2] &= \sum_{i,s=1}^{m}\sum_{j,t=1}^{k}\mathbb{E}[A_{ij}A_{st}]\\ &= \mathbb{E}[A] + \sum_{i,j,s,t:i=s,t\neq j}\mathbb{E}[A_{ij}A_{st}] + \sum_{i,j,s,t:i\neq s,j=t}\mathbb{E}[A_{ij}A_{st}] + \sum_{i,j,s,t:i\neq s,j\neq t}\mathbb{E}[A_{ij}A_{st}]\\ &= \mathbb{E}[A] + \sum_{i,j,t:t\neq j}\mathbb{E}[A_{ij}A_{it}] + \sum_{i,j,s,t:i\neq s}\mathbb{E}[A_{ij}A_{st}].\mathbb{E}[X_{ij}X_{st}].\end{aligned}$$

Further, for $\sigma,\tau\in\Sigma$ and $j\in[k]$ let

$$\zeta_j(\sigma,\tau) = 1\{\sigma_j=\tau_j=1\} \quad\text{and}\quad \zeta(\sigma,\tau) = \sum_{j\in[k]}\zeta_j(\sigma,\tau) = (k+\langle\sigma,\tau\rangle)/2.$$

Then

$$\begin{aligned}\sum_{i,j,t:t\neq j}\mathbb{E}[A_{ij}A_{it}] &= m^{-1}\sum_{\sigma,\tau}\mu(\sigma)\mu(\tau)\sum_{j\neq t}\zeta_j(\sigma,\tau)\zeta_t(\sigma,\tau)\\ &= m^{-1}\sum_{\sigma,\tau}\mu(\sigma)\mu(\tau)(\zeta(\sigma,\tau)^2-\zeta(\sigma,\tau))\\ &= -\mathbb{E}[A]+m^{-1}\sum_{\sigma,\tau}\mu(\sigma)\mu(\tau)\zeta(\sigma,\tau)^2.\end{aligned}$$

Additionally,

$$\begin{aligned}\sum_{i,j,s,t:i\neq s}\mathbb{E}[A_{ij}A_{st}] &= \sum_{\sigma,\tau}\sum_{\sigma',\tau'}\frac{\mu(\sigma)\mu(\tau)(\mu(\sigma')-1\{\sigma=\sigma'\})(\mu(\tau')-1\{\tau=\tau'\})}{m(m-1)}\zeta(\sigma,\tau)\zeta(\sigma',\tau')\\ &= \frac{[\sum_{\sigma,\tau}\mu(\sigma)\mu(\tau)\zeta(\sigma,\tau)]^2}{m(m-1)} - 2\frac{\sum_{\sigma,\tau,\sigma'}\mu(\sigma)\mu(\tau)\mu(\sigma')\zeta(\sigma,\tau)\zeta(\sigma,\sigma')}{m(m-1)}\\ &\quad+\frac{\sum_{\sigma,\tau}\mu(\sigma)\mu(\tau)\zeta(\sigma,\tau)^2}{m(m-1)}\\ &= \frac{m\mathbb{E}[A]^2}{m-1} - \frac{2}{m(m-1)}\sum_{\sigma,\tau,\sigma'}\mu(\sigma)\mu(\tau)\mu(\sigma')\zeta(\sigma,\tau)\zeta(\sigma,\sigma')\\ &\quad+\frac{1}{m(m-1)}\sum_{\sigma,\tau}\mu(\sigma)\mu(\tau)\zeta(\sigma,\tau)^2.\end{aligned}$$

Combining the above, we see that uniformly for $\mu\in\mathcal{M}_\omega$

$$\begin{aligned}\mathrm{Var}(A) \sim \frac{1}{m}\sum_{\sigma,\tau}\bar{\mu}(\sigma)\bar{\mu}(\tau)\zeta(\sigma,\tau)^2 - \frac{2}{m^2}\sum_{\sigma,\tau,\sigma'}\bar{\mu}(\sigma)\bar{\mu}(\tau)\bar{\mu}(\sigma')\zeta(\sigma,\tau)\zeta(\sigma,\sigma')\\ +\frac{1}{m}\left[\sum_{\sigma,\tau}\bar{\mu}(\sigma)\bar{\mu}(\tau)\zeta(\sigma,\tau)\right]^2.\end{aligned}$$

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Substituting in the definition of $\bar{\mu}$ and using (1.4), we obtain

$$\begin{aligned}
m^{-2}\sum_{\sigma,\tau}\bar{\mu}(\sigma)\bar{\mu}(\tau)\zeta(\sigma,\tau) &= (1-(1-q)^k)^{-2}\,\mathbb{E}[\mathrm{Bin}(k,q^2)] = k/4,\\
m^{-2}\sum_{\sigma,\tau}\bar{\mu}(\sigma)\bar{\mu}(\tau)\zeta(\sigma,\tau)^2 &= (1-(1-q)^k)^{-2}\,\mathbb{E}[\mathrm{Bin}(k,q^2)^2]\\
&= \frac{kq^2((k-1)q^2+1)}{(1-(1-q)^k)^2} = \frac{k}{4}((k-1)q^2+1),\\
m^{-3}\sum_{\sigma,\tau,\tau'}\mu(\sigma)\mu(\tau)\mu(\tau')\zeta(\sigma,\tau)\zeta(\sigma,\tau') &= (1-(1-q)^k)^{-3}\\
&\quad\times\sum_{j=1}^{k}\binom{k}{j}q^j(1-q)^j\Bigg(\sum_{l=1}^{j}lq^l(1-q)^{j-l}\Bigg)^2\\
&= \frac{kq^3((k-1)q+1)}{(1-(1-q)^k)^3} = \frac{k}{8}((k-1)q+1).
\end{aligned}$$

Hence,

$$\begin{aligned}
m^{-1}\mathrm{Var}(A) &\sim \frac{k}{16}[k-4((k-1)q+1)+4((k-1)q^2+1)]\\
&= \frac{k}{16}(k-4(k-1)q(1-q)),
\end{aligned}$$

as claimed. □

Finally, Lemma 5.2 follows from Lemma 5.4 and Bolthausen's central limit theorem for random permutations from [8]; this result can be viewed as an extension of the Berry–Esseen inequality to certain dependent random variables, and as such provides a uniform estimate for our purposes. To be precise, due to our conditioning on the event $\mathcal{S}_\mu^{\otimes}$ the distribution of the random vector $\hat{y} = (\hat{y}_{ij}^{(1)}, \hat{y}_{ij}^{(2)})_{i,j}$ can be described as follows. Fix any vector $\tilde{u} = (\tilde{u}_{ij})_{i,j} \in \{\pm 1\}^{km}$ such that

$$\sum_{i=1}^{m} 1\{(u_{i1},\ldots,u_{ik}) = \sigma\} = m\mu(\sigma) \quad \text{for every } \sigma \in \Sigma.$$

Moreover, let $\pi^{(1)}, \pi^{(2)} : [m] \to [m]$ be two independent uniformly random permutations and let $\tilde{u}^{(t)} = (u_{\pi^{(t)}(i),j})_{i,j}$ for $t = 1,2$. In words, $\tilde{u}^{(t)}$ is obtained from $\tilde{u}$ by permuting the m blocks of length k that represent the individual clauses randomly. Then $\hat{y}$ has the same distribution as $(u_{\pi^{(1)}(i),j}, u_{\pi^{(2)}(i),j})_{i,j}$. Hence, A is distributed as

$$\sum_{i=1}^{m}\sum_{j=1}^{k} 1\{u_{\pi^{(1)}(i),j} = u_{\pi^{(2)}(i),j} = 1\} = \sum_{i=1}^{m}\sum_{j=1}^{k} 1\{u_{i,j} = u_{\pi^{(2)-1}\circ\pi^{(1)}(i),j} = 1\},$$

which is precisely the type of random sum for which [8] establishes convergence to the normal distribution.

5.3. Proof of Lemma 5.3

We build upon the following result on the *total* number of satisfying assignments, which is implicit in prior work [10]; for the sake of completeness we give a self-contained proof in

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Appendix 5.3. Let $Z_\alpha^\otimes$ be the number of pairs (σ,τ) of satisfying assignments of Φ such that $\sum_{i=1}^n 1\{\tau_1(x_i)=\tau_2(x_i)\}=\alpha$.

Lemma 5.5. *There exists a number $t_0=t_0(k)$ such that for every $t>t_0$ we have*

$$\limsup_{n\to\infty}\sum_{\alpha:|\alpha-n/2|>tn^{1/2}}\mathbb{E}[Z_\alpha^\otimes]/\mathbb{E}[Z]^2\leqslant\exp(-t^2/17).$$

Moreover,

$$\sum_{\rho:|\alpha-n/2|>n^{1/2}\ln n}\mathbb{E}[Z_\alpha^\otimes]\leqslant O(n^{-\ln\ln n})\,\mathbb{E}[Z]^2.$$

In the following it will be convenient to replace the parameter α by another overlap parameter to represent the four possible truth value combinations. Define $\rho=(\rho_{s,t})_{s,t=\pm1}$ such that

$$\rho_{1,1}+\rho_{1,-1}=\rho_{1,1}+\rho_{-1,1}=\frac{1}{2},\quad \rho_{1,1}+\rho_{1,-1}+\rho_{-1,1}+\rho_{-1,-1}=1. \tag{5.13}$$

In particular, ρ is a probability distribution on $\{\pm1\}^2$ such that $\rho_{1,1}=\rho_{-1,-1}$ and $\rho_{1,-1}=\rho_{-1,1}$. Hence, (5.13) demonstrates that we can view $\rho_{1,-1},\rho_{-1,1},\rho_{-1,-1}$ as affine functions of $\rho_{1,1}$. The relationship between ρ and α is going to be $2d\alpha=km(\rho_{1,1}+\rho_{-1,-1})=2km\rho_{1,1}$. Indeed, let us introduce the symbols

$$Z_\rho^\otimes=Z_{km\rho_{11}/d}^\otimes,\quad Z_{\mu,\rho}^\otimes=Z_{\mu,km\rho_{11}/d}^\otimes. \tag{5.14}$$

We need to obtain a result similar to Lemma 5.5 for $Z_{\mu,\rho}^\otimes$ rather than $Z_\alpha^\otimes$. Slightly extending the argument from [10], we tackle the second moment computation by way of an auxiliary probability space as in Section 3. To unclutter the notation we write $f(k)=\tilde{O}(g(k))$ if there exists $c>0$ such that $|f(k)|\leqslant k^c g(k)$ for all $k>c$.

Lemma 5.6. *For any ρ there exists a unique probability distribution $(q_{z_1,z_2})_{z_1,z_2\in\{\pm1\}}$ on $\{\pm1\}^2$ such that*

$$\frac{q_{1,1}}{1-2(q_{-1,-1}+q_{-1,1})^k+q_{-1,-1}^k}=\rho_{1,1},\quad \frac{q_{1,-1}(1-(q_{-1,-1}+q_{1,-1})^{k-1})}{1-2(q_{-1,-1}+q_{-1,1})^k+q_{-1,-1}^k}=\rho_{1,-1},\quad q_{-1,1}=q_{1,-1}. \tag{5.15}$$

The derivatives satisfy

$$\frac{\partial q_{1,1}}{\partial\rho_{1,1}}=1+\tilde{O}(2^{-k}),\quad \frac{\partial q_{1,-1}}{\partial\rho_{1,1}}=-1+\tilde{O}(2^{-k}),\quad \frac{\partial^2 q_{1,1}}{\partial\rho_{1,1}^2}=\tilde{O}(2^{-k}),\quad \frac{\partial^2 q_{1,-1}}{\partial\rho_{1,1}^2}=\tilde{O}(2^{-k}). \tag{5.16}$$

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Proof. Let $\mathcal{Q}$ be the set of all probability distributions $(q_{\pm1\pm1})$ such that $q_{1,-1} = q_{-1,1}$. Further, set

$$s = 1 - 2(q_{-1,-1} + q_{1,-1})^k + q_{-1,-1}^k, \quad Q_{1,1} = \frac{q_{1,1}}{s},$$
$$Q_{1,-1} = \frac{q_{1,-1}(1 - (q_{-1,-1} + q_{1,-1})^{k-1})}{s}.$$

Then we aim to study the function $q \mapsto (Q_{1,1}, Q_{1,-1})$ on the two-dimensional compact convex set $\mathcal{Q}$. Since $q_{1,-1} = q_{-1,1}$ we have $q_{1,-1} \leqslant 1/2$ on $\mathcal{Q}$. Similarly, $q_{1,1} \leqslant 1/2$ and $q_{1,1} + q_{1,-1} \leqslant 1/2$. Consequently, $s = 1 - O(2^{-k})$ and $Q_{1,1}, Q_{1,-1}$ are well-defined. The derivatives of s work out to be

$$\frac{\partial s}{\partial q_{1,1}} = 2k(q_{-1,-1} + q_{1,-1})^{k-1} - kq_{-1,-1}^{k-1}, \qquad \frac{\partial s}{\partial q_{1,-1}} = 2k(q_{-1,-1} + q_{1,-1})^{k-1} - 2kq_{-1,-1}^{k-1}.$$

Further,

$$\frac{\partial Q_{1,1}}{\partial q_{1,1}} = \frac{1}{s} - \frac{q_{1,1}}{s^2}\frac{\partial s}{\partial q_{1,1}}, \quad \frac{\partial Q_{1,1}}{\partial q_{1,-1}} = \frac{q_{11}}{s^2}\frac{\partial s}{\partial q_{1,-1}},$$
$$\frac{\partial Q_{1,-1}}{\partial q_{1,1}} = \frac{(k-1)q_{1,-1}(q_{-1,-1} + q_{1,-1})^{k-2}}{s} - \frac{Q_{1,-1}}{s^2}\frac{\partial s}{\partial q_{1,1}},$$
$$\frac{\partial Q_{1,-1}}{\partial q_{1,-1}} = \frac{1 - (q_{-1,-1} + q_{1,-1})^{k-1} + (k-1)q_{1,-1}(q_{-1,-1} + q_{1,-1})^{k-2}}{s} - \frac{Q_{1,-1}}{s^2}\frac{\partial s}{\partial q_{1,-1}}.$$

Since $q_{1,-1} \leqslant 1/2, q_{1,1} \leqslant 1/2, q_{1,1} + q_{1,-1} \leqslant 1/2$ on $\mathcal{Q}$, we see that

$$\frac{\partial Q_{1,1}}{\partial q_{1,1}} = 1 + O(k2^{-k}), \quad \frac{\partial Q_{1,1}}{\partial q_{1,-1}} = O(k2^{-k}),$$
$$\frac{\partial Q_{1,-1}}{\partial q_{1,1}} = O(k2^{-k}), \qquad \frac{\partial Q_{1,-1}}{\partial q_{1,-1}} = 1 + O(k2^{-k}).$$

Consequently, the Jacobi matrix is invertible on $\mathcal{Q}$. Further, for any value $q_{1,-1} \in [0, 1/2]$ we have $\lim_{q_{1,1}\to 0} Q_{1,1} = 0$ and $\lim_{q_{1,1}\to 1/2} Q_{1,1} > 1/2$. Similarly, for $q_{1,1} \in [0, 1/2]$, $\lim_{q_{1,-1}\to 0} Q_{1,-1} = 0$ and $\lim_{q_{1,-1}\to 1/2} Q_{1,-1} > 1/2$. Therefore, the assertion follows from the inverse function theorem. □

Define a random vector

$$\chi^{\otimes} = \chi^{\otimes}(q) = (\chi_{ij}^{(1)}, \chi_{ij}^{(2)})_{i\in[m], j\in[k]}$$

such that

$$\mathbb{P}[(\chi_{ij}^{(1)}, \chi_{ij}^{(2)}) = (z_1, z_2)] = q_{z_1,z_2} \quad (z_1, z_2 \in \{\pm 1\})$$

independently for all $i \in [m]$, $j \in [k]$. Let

$$b_{z_1,z_2} = \frac{1}{km}\sum_{i,j} 1\{\chi_{ij}^{(1)} = z_1, \chi_{ij}^{(2)} = z_2)\} \quad \text{for all } z_1, z_2 \in \{\pm 1\}.$$

Further, let $\mathcal{B}^{\otimes}(\rho)$ be the event that $b = \rho$. The following is analogous to Fact 3.1.

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Fact 5.7. *Let $\tau_1, \tau_2 : \{x_1, \ldots, x_n\} \to \{\pm 1\}$ be truth assignments with overlap ρ. Then the conditional distribution of $\chi^{\otimes}$ given $\mathcal{B}^{\otimes}(\rho)$ coincides with the distribution of the vector*

$$(\mathrm{sign}(i,j)\tau_1(\partial(i,j)), \mathrm{sign}(i,j)\tau_2(\partial(i,j)))_{i\in[m],j\in[k]}.$$

Fact 5.7 as well as the following three claims already appear in [10]; we include the short proofs for the sake of completeness.

Claim 5.8. *Uniformly for all ρ, q such that $\rho_{s,t}, q_{s,t} \in [1/8, 3/8]$ for all $s,t \in \{\pm 1\}$ we have*

$$\ln \mathbb{P}[\mathcal{B}^{\otimes}(\rho)] = -\frac{3}{2}\ln n - kmD_{\mathrm{KL}}(\rho\|q) + O(1).$$

Furthermore, uniformly for all ρ we have

$$\ln \mathbb{P}[\mathcal{B}^{\otimes}(\rho)] \leqslant -kmD_{\mathrm{KL}}(\rho\|q) + O(1).$$

Proof. We have

$$\mathbb{P}[\mathcal{B}^{\otimes}(\rho)] = \binom{km}{\rho km} \prod_{z_1,z_2\in\{\pm 1\}} q_{z_1,z_2}^{km\rho_{z_1,z_2}}.$$

The claim follows by applying Stirling's formula. □

Further, consider the event

$$\mathcal{S}^{\otimes} = \{\forall i \in [m]\, \exists j, j' \in [k] : \chi^{(1)}_{ij} = \chi^{(1)}_{ij'} = 1\}.$$

If we think of the k-tuples $(\chi^{(1)}_{ij})_{j\in[k]}, (\chi^{(2)}_{ij})_{j\in[k]}$ as the truth value combinations induced on a clause by a pair (τ_1, τ_2) of Boolean assignments, then $\mathcal{S}^{\otimes}$ corresponds to the event that both τ_1, τ_2 are satisfying.

Claim 5.9. *We have $\mathbb{P}[\mathcal{S}^{\otimes}] = (1 - 2(q_{-1,-1} + q_{-1,1})^k + q^k_{-1,-1})^m$.*

Proof. By inclusion–exclusion, for any $i \in [m]$ we have

$$\begin{aligned}\mathbb{P}[\exists h \in \{1,2\} : \forall j \in [k] : \chi^{(h)}_{ij} = -1] &= (q_{-1,-1} + q_{-1,1})^k + (q_{-1,-1} + q_{1,-1})^k - q^k_{-1,-1} \\ &= 2(q_{-1,-1} - q_{-1,1})^k + q^k_{-1,-1}.\end{aligned}$$

The assertion follows from the independence of the entries of $\chi^{\otimes}$. □

Claim 5.10. *Uniformly for all ρ, q such that $\rho_{s,t}, q_{s,t} \in [1/8, 3/8]$ for all $s,t \in \{\pm 1\}$ we have*

$$\ln \mathbb{P}[\mathcal{B}^{\otimes}(\rho) | \mathcal{S}^{\otimes}] = -\frac{3}{2}\ln n + O(1).$$

Proof. This follows from the local limit theorem for sums of independent bounded random variables (*e.g.* [13]). □

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Departing from the argument in [10], we are now going to accommodate the additional constraint that the clause marginals follow some specific distribution μ on Σ. Hence, let $\mathcal{M}_m(\rho)$ be the set of all probability distributions $\nu = (\nu(\sigma,\tau))_{\sigma,\tau\in\Sigma}$ such that $m\nu(\sigma,\tau)$ is an integer for all $\sigma,\tau\in\Sigma$ and

$$\sum_{i=1}^{k}\sum_{\sigma,\tau\in\Sigma}\nu(\sigma,\tau)1\{\sigma_i=s,\tau_i=t\}=\rho_{s,t}\quad\text{for all } s,t\in\{\pm1\}.$$

Additionally, for a given probability distribution $\mu=(\mu(\sigma))_{\sigma\in\Sigma}$ let $\mathcal{M}_m(\rho,\mu)$ be the set of all $\nu\in\mathcal{M}_m(\rho)$ such that

$$\sum_{\tau\in\Sigma}\nu(\sigma,\tau)=\sum_{\tau\in\Sigma}\nu(\tau,\sigma)=\mu(\sigma)\quad\text{for all }\sigma\in\Sigma.$$

Clearly, the vector $\chi^{\otimes}$ induces a distribution $\nu_{\chi^{\otimes}}$ by

$$\nu_{\chi^{\otimes}}(\sigma,\tau)=\frac{1}{m}\sum_{i=1}^{m}\prod_{j=1}^{k}1\{\chi_{ij}^{(1)}=\sigma_i,\chi_{ij}^{(2)}=\tau_i\}.$$

Letting $p(\nu)=\mathbb{P}[\nu_{\chi^{\otimes}}=\nu|\mathcal{B}^{\otimes}(\rho)\cap\mathcal{S}^{\otimes}]$ for $\nu\in\mathcal{M}_m(\rho)$, recalling (5.14) and using Fact 5.7, we find

$$\mathbb{E}[Z_{\mu,\rho}^{\otimes}]=\mathbb{E}[Z_{\rho}^{\otimes}]\sum_{\nu\in\mathcal{M}_m(\rho,\mu)}p(\nu).$$

Let $\bar\nu(\rho)=(\bar\nu_{\sigma,\tau}(\rho))_{\sigma,\tau\in\Sigma}$ with

$$\bar\nu_{\sigma,\tau}(\rho)=\frac{1}{s}\prod_{i=1}^{k}q_{\sigma(i),\tau(i)}.\tag{5.17}$$

Then Fact 5.7 shows that $\bar\nu(\rho)$ describes the expected statistics of the 'clause overlaps' given overlap ρ. More precisely, if we fix two truth assignments with overlap ρ and then generate a random formula subject to the condition that both assignments are satisfying, then we expect to see $\bar\nu_{\sigma,\tau}(\rho)m$ clauses that are satisfied according to the truth value pattern σ under the first assignment and according to the truth value pattern τ under the second one. By Stirling's formula,

$$p(\nu)=\frac{1}{\mathbb{P}[\mathcal{B}^{\otimes}(\rho)|\mathcal{S}^{\otimes}]}\binom{m}{m\nu}\prod_{s,t\in\{\pm1\}}q_{s,t}^{km\rho_{s,t}}=\frac{r(\nu)}{\mathbb{P}[\mathcal{B}^{\otimes}(\rho)|\mathcal{S}^{\otimes}]}\exp(-mD_{\mathrm{KL}}(\nu\|\bar\nu(\rho))),\tag{5.18}$$

where

$$r(\nu)\sim(2\pi m)^{(1-|\Sigma|^2)/2}\prod_{\sigma,\tau\in\Sigma}\bar\nu_{\sigma,\tau}(\rho)^{-1/2}\tag{5.19}$$

uniformly for ν such that $|\nu_{\sigma,\tau}-\bar\nu_{\sigma,\tau}|\leqslant m/\ln m$ for all σ,τ and $r(\nu)=O(1)$ for all ν.

Claim 5.11. *If $|\rho_{1,1}-1/4|\leqslant\ln n/\sqrt{n}$, then $|\bar\nu_{\sigma,\tau}(\bar\rho)-\nu_{\sigma,\tau}(\rho)|\leqslant\ln^2 n/\sqrt{n}$.*

Proof. This follows from (5.17) and the fact that the derivatives of the implicit parameter q are bounded. □

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Claim 5.12. *Uniformly for ρ such that $|\rho_{1,1} - 1/4| \leqslant \ln n/\sqrt{n}$ we have*

$$\mathbb{E}[Z^{\otimes}_{\mu,\rho}] \sim \mathbb{E}[Z^{\otimes}_{\mu,\rho}] \sum_{\nu \in \mathcal{M}_m(\rho): \|\nu - \bar{\nu}(\rho)\|_\infty \leqslant m^{-1/3}} p(\nu).$$

Proof. This follows from (5.18) and the fact that the Kullback–Leibler divergence is strictly convex. □

Proof of Lemma 5.3. Let $a > 0$. By (3.8) we have

$$\mathbb{E}[Z_\mu]/\mathbb{E}[Z] = \Theta(m^{1-|\Sigma|/2}) \tag{5.20}$$

uniformly for all $\mu \in \mathcal{M}_\Omega$. Therefore, letting

$$S = \sum_{\rho: a < |\rho_{1,1} - 1/4| \leqslant n^{-1/2} \ln n} \mathbb{E}[Z^{\otimes}_{\mu,\rho}],$$

we obtain from Lemma 5.5 and Claim 5.12 that

$$S \sim S' = \sum_{\rho: a < |\rho_{1,1} - 1/4| \leqslant n^{-1/2} \ln n} \mathbb{E}[Z^{\otimes}_{\rho}] \sum_{\nu \in \mathcal{M}_m(\rho,\mu): \|\nu - \bar{\nu}(\rho)\|_\infty \leqslant m^{-1/3}} p(\nu).$$

Hence, (5.18) and (5.19) yield

$$S' \sim S'' = \frac{(2\pi m)^{(1-|\Sigma|^2)/2}}{\prod_{\sigma,\tau \in \Sigma} \bar{\nu}_{\sigma,\tau}(\bar{\rho})^{1/2}} \sum_{\rho: a < |\rho_{1,1} - 1/4| \leqslant n^{-1/2} \ln n} \frac{\mathbb{E}[Z^{\otimes}_{\rho}]}{\mathbb{P}[\mathcal{B}^{\otimes} | \mathcal{S}^{\otimes}]} \cdot \sum_{\nu \in \mathcal{M}_m(\rho,\mu): \|\nu - \bar{\nu}(\rho)\|_\infty \leqslant m^{-1/3}} \exp[-m D_{\mathrm{KL}}(\nu \| \bar{\nu}(\rho))].$$

Estimating the last sum via the Laplace method and using Claim 5.11 once more, we see that uniformly for all ρ, μ (again using convexity of the Kullback–Leibler divergence)

$$\sum_{\nu \in \mathcal{M}_m(\rho,\mu): \|\nu - \bar{\nu}(\rho)\|_\infty \leqslant m^{-1/3}} \exp[-m D_{\mathrm{KL}}(\nu \| \bar{\nu}(\rho))] \leqslant O(m^{(|\Sigma|^2 - 2|\Sigma|)/2}).$$

Consequently, Claim 5.10 yields

$$S'' \leqslant O(m^{2-|\Sigma|})\, \mathbb{E}[Z]^2 \exp(-a^2/16),$$

provided that a is sufficiently large. Therefore, the assertion follows from (5.20). □

Appendix: Proof of Lemma 5.5

We continue to use the notation from Section 5.3.

Claim A.1. *There exists a number $t_0 = t_0(k)$ such that for every $t > t_0$ we have*

$$\sum_{\rho: t_0 n^{-1/2} < |\rho_{11} - 1/4| < 2^{-0.49k}} \mathbb{E}[Z^{\otimes}_{\rho}(\Phi)] \leqslant \exp(-t^2/4)\, \mathbb{E}[Z]^2.$$

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Proof. The proof is based on the Laplace method. Specifically, let $q = q(\rho)$ be the vector from Lemma 5.6. Then at the point $\rho = \bar{\rho} = \frac{1}{4}1$ we can express the vector $(q_{\pm 1,\pm 1})$ in terms of the solution q to (1.4). Indeed, letting $q_1 = q$, $q_{-1} = 1-q$, we verify that the probability distribution $(q_s q_t)_{s,t=\pm 1}$ satisfies (5.15). Hence, Lemma 5.6 implies that $q_{s,t} = q_s q_t$ for $s,t = \pm 1$ at the point $\rho = \bar{\rho}$. Substituting this distribution in and using Fact 5.7, Claim 5.9, Claim 5.10, Stirling's formula and Bayes' rule, we find

$$\frac{\mathbb{E}[Z_\rho^{\otimes}(\Phi)]}{\mathbb{E}[Z^2]} \leqslant O(n^{-1/2})\exp[n(H(\rho)-2\ln 2)+m(f(\rho)-f(\bar{\rho}))], \quad \text{where} \tag{A.1}$$
$$f(\rho) = \ln(1-2(q_{-1,-1}+q_{-1,1})^k + q_{-1,-1}^k) + kD_{\mathrm{KL}}(\rho\|q).$$

We are going to prove that

$$Df(\bar{\rho}) = 0, \tag{A.2}$$
$$D^2 f(\rho) \preceq \frac{n}{km}\mathrm{id} \quad \text{for all } \rho \text{ such that } |\rho_{11}-1/4| \leqslant 2^{-0.49k}. \tag{A.3}$$

Since the entropy satisfies $DH(\bar{\rho}) = 0$ and $D^2H(\rho) \preceq -\mathrm{id}$ if $|\rho_{11}-1/4| \leqslant 2^{-0.49k}$, the assertion follows from (A.1)–(A.3) and a Gaussian summation.

To prove (A.2)[2] we set

$$f_1(\rho) = \ln(1-2(q_{-1,-1}+q_{-1,1})^k + q_{-1,-1}^k), \quad f_2(\rho) = kD_{\mathrm{KL}}(\rho\|q).$$

Further, let $s = 1-2(q_{-1,-1}+q_{-1,1})^k + q_{-1,-1}^k$. Then

$$\frac{\partial f_1}{\partial q_{1,1}} = \frac{2k(q_{-1,-1}+q_{-1,1})^{k-1} - kq_{-1,-1}^{k-1}}{s}, \quad \frac{\partial f_1}{\partial q_{1,-1}} = \frac{2k(q_{-1,-1}+q_{-1,1})^{k-1} - q_{-1,-1}^{k-1}}{s}. \tag{A.4}$$

Moreover, the partial derivatives of the generic term $z\ln(z/y)$ of the Kullback–Leibler divergence work out to be

$$\frac{\partial}{\partial z} z\ln\frac{z}{y} = \ln\frac{z}{y}, \quad \frac{\partial}{\partial y} z\ln\frac{z}{y} = -\frac{z}{y} = -1-\frac{z-y}{y}. \tag{A.5}$$

Hence,

$$\frac{\partial}{\partial q_{1,1}} D_{\mathrm{KL}}(\rho\|q) = -\frac{\rho_{1,1}}{q_{1,1}} + \frac{\rho_{-1,-1}}{q_{-1,-1}}, \quad \frac{\partial}{\partial q_{1,-1}} D_{\mathrm{KL}}(\rho\|q) = -\frac{2\rho_{1,-1}}{q_{1,-1}} + \frac{2\rho_{-1,-1}}{q_{-1,-1}}. \tag{A.6}$$

Using the relations $q_{s,t} = q_s q_t$ and $(1-q)^k = 1-2q$, at the point $\rho = \bar{\rho}$ we obtain $s = 4q^2$ and

$$\frac{2k(q_{-1,-1}+q_{-1,1})^{k-1} - kq_{-1,-1}^{k-1}}{s} = \frac{k(1-2q)}{4q^2(1-q)^2}, \tag{A.7}$$
$$\frac{2k(q_{-1,-1}+q_{-1,1})^{k-1} - q_{-1,-1}^{k-1}}{s} = \frac{k(1-2q)}{2q(1-q)^2},$$
$$-\frac{\rho_{1,1}}{q_{1,1}} + \frac{\rho_{-1,-1}}{q_{-1,-1}} = \frac{1}{4(1-q)^2} - \frac{1}{4q^2},$$
$$-\frac{2\rho_{1,-1}}{q_{1,-1}} + \frac{2\rho_{-1,-1}}{q_{-1,-1}} = \frac{1}{2(1-q)^2} - \frac{1}{2q(1-q)}. \tag{A.8}$$

[2] The following fairly simple way of calculating $Df(\bar{\rho})$ was pointed out to the first author by Victor Bapst.

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Substituting (A.7)–(A.8) into (A.4) and (A.6) and simplifying, we obtain

$$\frac{\partial}{\partial q_{1,1}} f(\rho) = \frac{\partial}{\partial q_{1,-1}} f(\rho) = 0. \tag{A.9}$$

Further, combining (A.5) and (A.9) and using the chain rule, we get

$$\frac{\partial}{\partial \rho_{1,1}} f_2(\rho) = \frac{\partial f(\rho)}{\partial q_{1,1}} \frac{\partial q_{1,1}}{\partial \rho_{1,1}} + \frac{\partial f(\rho)}{\partial q_{1,-1}} \frac{\partial q_{1,-1}}{\partial \rho_{1,1}} + \ln \frac{1}{4q^2} - 2\ln \frac{1}{4q(1-q)} + \ln \frac{1}{4(1-q)^2} = 0. \tag{A.10}$$

Thus, (A.2) follows from (A.9), (A.10) and the chain rule.

With respect to the second derivative, letting

$$u = \frac{2k(k-1)(q_{-1,-1}+q_{-1,1})^{k-2}s - 4k^2(q_{-1,-1}+q_{-1,1})^2}{s^2},$$

we find

$$\frac{\partial f_1}{\partial q_{1,1}}, \frac{\partial f_1}{\partial q_{1,-1}} = \tilde{O}(2^{-k}), \quad \frac{\partial^2 f_1}{\partial q_{1,\pm 1} \partial q_{1,\pm 1}} = u + \tilde{O}(4^{-k}). \tag{A.11}$$

Combining (A.11) with (5.16) and using the chain rule, we obtain

$$\frac{\partial^2 f_1}{\partial \rho_{11}^2} = \tilde{O}_k(4^{-k}). \tag{A.12}$$

Proceeding to f_2, we recall that the second differentials of the generic term $z\ln(z/y)$ of the Kullback–Leibler divergence read

$$\frac{\partial^2}{\partial z^2} z\ln\frac{z}{y} = \frac{1}{z}, \quad \frac{\partial^2}{\partial y^2} z\ln\frac{z}{y} = \frac{z}{y^2}, \quad \frac{\partial^2}{\partial y \partial z} z\ln\frac{z}{y} = -\frac{1}{y}. \tag{A.13}$$

We verify that in the case $|\rho_{11} - 1/4| \leqslant 2^{-0.49k}$ the implicit parameters satisfy $q_{\pm 1,\pm 1} - \rho_{\pm 1,\pm 1} = \tilde{O}_k(2^{-k})$. Moreover, $q_{-1,1} = q_{1,-1}$ and $q_{-1,-1} = 1 - q_{-1,1} - q_{1,-1} - q_{1,1}$. Therefore, (A.5) yields

$$\frac{\partial f_2}{\partial q_{1,1}}, \frac{\partial f_2}{\partial q_{1,-1}} = \tilde{O}_k(2^{-k}).$$

Hence, by (5.16) and the chain rule,

$$\frac{\partial f_2}{\partial q_{1,1}} \frac{\partial^2 q_{1,1}}{\partial \rho_{11}^2} + \frac{\partial f_2}{\partial q_{1,-1}} \frac{\partial^2 q_{1,-1}}{\partial \rho_{11}^2} = \tilde{O}_k(4^{-k}). \tag{A.14}$$

Further, using (A.13) and (5.16) and recalling that $q_{\pm 1,\pm 1} = 1/4 + O(2^{-0.49k})$ if $|\rho_{11} - 1/4| \leqslant 2^{-0.49k}$, we obtain

$$\frac{\partial^2 f_2}{\partial^2 q_{1,1}} \left(\frac{\partial q_{1,1}}{\partial \rho_{1,1}}\right)^2 + \frac{\partial^2 f_2}{\partial^2 q_{1,-1}} \left(\frac{\partial q_{1,-1}}{\partial \rho_{1,1}}\right)^2 + 2\frac{\partial^2 f_2}{\partial q_{1,1} \partial q_{1,-1}} \frac{\partial q_{1,1}}{\partial \rho_{1,1}} \frac{\partial q_{1,-1}}{\partial \rho_{1,1}} = \tilde{O}_k(4^{-k}). \tag{A.15}$$

Combining (A.14) and (A.15), we get

$$\frac{\partial^2 f_2}{\partial \rho_{1,1}^2} = \tilde{O}_k(4^{-k}). \tag{A.16}$$

Finally, since $m/n = \tilde{O}_k(2^{-k})$, (A.3) follows from (A.12) and (A.16). □

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

Claim A.2. *We have*

$$\sum_{\rho:|\rho_{11}-1/4|>2^{-0.49k}} \mathbb{E}[Z_\rho^{\otimes}(\Phi)] \leqslant \exp(-\Omega(n))\,\mathbb{E}[Z]^2.$$

Proof. We observe that Fact 5.7 holds for *any* choice of the auxiliary variables $(q_{\pm1,\pm1})$ that define the random vector $\chi^{\otimes}$. Hence, choosing $q=\rho$ and applying Bayes' rule, we find

$$\mathbb{E}[Z_\rho^{\otimes}] \leqslant \exp\left[n\left(H(\rho)+\frac{2d}{k}\ln(1-2^{1-k}+\rho_{11}^k)\right)+o(n)\right].$$

We claim that

$$g(\rho_{1,1}) = H(\rho)+\frac{2d}{k}\ln(1-2^{1-k}+\rho_{1,1}^k)$$

attains its maximum at the boundary point $\rho_{11}=1/4+2^{-0.49k}$. Indeed, we read off that $g(\rho_{1,1}) > g(1/2-\rho_{1,1})$ if $\rho_{11}>1/4$. Hence, the maximum occurs in the interval $\rho_{1,1}\in[1/4+2^{-0.49k},1/2)$. Further, since $g(\rho)$ is a sum of the concave $\rho_{11}\mapsto H(\rho)$ and a multiple of the convex $\rho_{11}\mapsto \ln(1-2^{1-k}+\rho_{11}^k)$, it suffices to prove this claim for the maximum value of $2d/k$ that (1.3) allows. Hence, for this d we need to study the zeros of

$$\frac{\partial}{\partial\rho_{11}}g(\rho) = 2\ln\frac{1-2\rho_{11}}{2\rho_{11}}+\frac{2d\rho_{11}^{k-1}}{1-2^{1-k}+\rho_{11}^k}.$$

Setting

$$x=\frac{1-2\rho_{11}}{2\rho_{11}}\in(0,1)$$

and taking exponentials, we transform this problem into finding the solutions to

$$x=\exp\left(-\frac{2d(1+x)}{(2^k-2)(1+x)^k+1}\right)$$

for $x\in(0,1/2-2^{-0.49k})$. A bit of elementary calculus shows that there are just two solutions, namely

$$x_1=(1+O(k^{-1}))2^{-k}\quad\text{and}\quad x_2=\Theta(\ln k/k).$$

The first solution x_1 is indeed a local maximum, but a direct calculation yields $g((1+x_1)/2) < g(1/4+2^{-0.49k})$. Moreover, x_2 is a local minimum. Finally, the assertion follows from the observation that $g(1/4+2^{-0.49k}) < f(\bar\rho)$. □

References

[1] Achlioptas, D. and Coja-Oghlan, A. (2008) Algorithmic barriers from phase transitions. In *FOCS 2008: 49th Annual IEEE Symposium on Foundations of Computer Science*, IEEE, pp. 793–802.

[2] Achlioptas, D. and Moore, C. (2006) Random k-SAT: Two moments suffice to cross a sharp threshold. *SIAM J. Comput.* **36** 740–762.

[3] Achlioptas, D., Naor, A. and Peres, Y. (2005) Rigorous location of phase transitions in hard optimization problems. *Nature* **435** 759–764.

https://doi.org/10.1017/S0963548318000263 Published online by Cambridge University Press

[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** 947–973.
[5] Bapst, V. and Coja-Oghlan, A. (2016) The condensation phase transition in the regular k-SAT model. In *RANDOM 2016: 20th International Workshop on Approximation, Randomization, and Combinatorial Optimization*, Springer, #22.
[6] Bollobás, B. (2001) *Random Graphs*, second edition, Cambridge University Press.
[7] Békéssy, A., Békéssy, P. and Komlós, J. (1972) Asymptotic enumeration of regular matrices. *Studia Sci. Math. Hungar.* **7** 343–353.
[8] Bolthausen, E. (1984) An estimate of the remainder in a combinatorial central limit theorem. *Z. Wahr. Verw. Gebiete* **66** 379–386.
[9] Coja-Oghlan, A. and Panagiotou, K. (2016) The asymptotic k-SAT threshold. *Adv. Math.* **288** 985–1068.
[10] Coja-Oghlan, A. and Panagiotou, K. (2013) Going after the k-SAT threshold. In *STOC 2013: 45th Annual ACM Symposium on Theory of Computing*, ACM, pp. 705–714.
[11] Coja-Oghlan, A. and Vilenchik, D. (2013) Chasing the k-colorability threshold. In *FOCS 2013: IEEE 54th Annual Symposium on Foundations of Computer Science*, IEEE, pp. 380–389.
[12] Coja-Oghlan, A. and Zdeborová, L. (2012) The condensation transition in random hypergraph 2-coloring. In *SODA 2012: 23rd Annual ACM–SIAM Symposium on Discrete Algorithms*, SIAM, pp. 241–250.
[13] Davis, B. and McDonald, D. (1995) An elementary proof of the local central limit theorem. *J. Theoret. Probab.* **8** 693–701.
[14] Ding, J., Sly, A. and Sun, N. (2014) Satisfiability threshold for random regular NAE-SAT. In *STOC 2014: 46th Annual ACM Symposium on Theory of Computing*, ACM, pp. 814–822.
[15] Ding, J., Sly, A. and Sun, N. (2015) Proof of the satisfiability conjecture for large k. In *STOC 2015: Proc. 47th Annual ACM Symposium on Theory of Computing*, ACM, pp. 59–68.
[16] Frieze, A. and Wormald, N. C. (2005) Random k-Sat: A tight threshold for moderately growing k. *Combinatorica* **25** 297–305.
[17] Janson, S. (1995) Random regular graphs: Asymptotic distributions and contiguity. *Combin. Probab. Comput.* **4** 369–405.
[18] Kirousis, L., Kranakis, E., Krizanc, D. and Stamatiou, Y. (1998) Approximating the unsatisfiability threshold of random formulas. *Random Struct. Alg.* **12** 253–269.
[19] Mézard, M., Parisi, G. and Zecchina, R. (2002) Analytic and algorithmic solution of random satisfiability problems. *Science* **297** 812–815.
[20] Molloy, M., Robalewska, H., Robinson, R. W. and Wormald, N. C. (1997) 1-factorisations of random regular graphs. *Random Struct. Alg.* **10** 305–321.
[21] Rassmann, F. (2016) On the number of solutions in random hypergraph 2-colouring. *Electron. J. Combin.* **24** 3.11.
[22] Rathi, V., Aurell, E., Rasmussen, L. K. and Skoglund, M. (2010) Bounds on threshold of regular random k-SAT. In *SAT 2010: 12th International Conference on Theory and Applications of Satisfiability Testing*, Springer, pp. 264–277.
[23] Robinson, R. W. and Wormald, N. C. (1992) Almost all cubic graphs are Hamiltonian. *Random Struct. Alg.* **3** 117–125.
[24] Sly, A., Sun, N. and Zhang, Y. (2016) The number of solutions for random regular NAE-SAT. *Proc. 57th FOCS* 724–731.
[25] Wormald, N. C. (1978) Some problems in the enumeration of labelled graphs. Doctoral thesis, Newcastle University.