Ann. Inst. Henri Poincaré Comb. Phys. Interact. 3 (2016), 349–362
DOI 10.4171/AIHPD/31

The phase transition in random regular exact cover

Cristopher Moore

Abstract. A k-uniform, d-regular instance of Exact Cover is a family of m sets $F_{n,d,k} = \{S_j \subseteq \{1,\dots,n\}\}$, where each subset has size k and each $1 \le i \le n$ is contained in d of the S_j. It is satisfiable if there is a subset $T \subseteq \{1,\dots,n\}$ such that $|T \cap S_j| = 1$ for all j. Alternately, we can consider it a d-regular instance of Positive 1-in-k SAT, i.e., a Boolean formula with m clauses and n variables where each clause contains k variables and demands that exactly one of them is true. We determine the satisfiability threshold for random instances of this type with $k > 2$. Letting

$$d^\star = \frac{\ln k}{(k-1)(-\ln(1-1/k))} + 1\,,$$

we show that $F_{n,d,k}$ is satisfiable with high probability if $d < d^\star$ and unsatisfiable with high probability if $d > d^\star$. We do this with a simple application of the first and second moment methods, boosting the probability of satisfiability below $d^\star$ to $1 - o(1)$ using the small subgraph conditioning method.

Mathematics Subject Classification (2010). 68Q87, 05C80, 82B26.

Keywords. Random structures, phase transitions, Boolean formulas, satisfiability, NP-complete problems, second moment method, small subgraph conditioning.

1. Introduction

A k-uniform d-regular instance of Exact Cover, or equivalently a Positive 1-in-k SAT formula, has n variables and m clauses where $dn = km$. We can treat it as a bipartite multigraph, with n variables of degree d on one side connected to m clauses of degree k on the other. A satisfying assignment is a subset T of the variables such that exactly one variable in each clause is true.

We choose random formulas $F_{n,d,k}$ according to the configuration model: that is, we make d copies of each variable and k copies of each clause, and choose a

uniformly random bipartite matching of the resulting $dn = km$ copies with each other. We assume that $d, k = O(1)$ so that $m = \Theta(n)$.

Note that the configuration model allows repetitions where some variable appears in a clause more than once. However, the number of such clauses is asymptotically Poisson with mean $O(1)$, and the formula is simple (i.e., with no repetitions) with constant probability. Thus any event that holds with high probability in the configuration model also holds with high probability in the uniform distribution over simple formulas with n variables and m clauses.

We determine the satisfiability threshold for these formulas. Namely, we prove the following.

Theorem 1. *Let*

$$d_k^\star = \frac{\ln k}{(k-1)(-\ln(1-1/k))} + 1. \tag{1}$$

Then for any $k > 2$ and any integer d,

$$\lim_{n\to\infty} \Pr[F_{n,d,k} \text{ is satisfiable}] = \begin{cases} 0 & d > d_k^\star, \\ 1 & d < d_k^\star. \end{cases}$$

Note that when k is large, the threshold given by Theorem 1 is $d_k^\star \approx (\ln k) + 1$. Note also that $d_k^\star$ is never an integer if $k > 2$, since then k would be a rational power of $k-1$. Finally, when $k = 2$ we have $d_k^\star = 2$, and the formula corresponds to a d-regular graph whose vertices are variables and whose edges are clauses. The formula is satisfiable if and only if this graph is bipartite; this is obviously the case if $d = 1$, but is false with high probability if $d \geq 2$. Thus Theorem 1 holds for $k = 2$ as well.

Our proof begins with an easy application of the first and second moment method gives unsatisfiability with high probability for $d > d_k^\star$, and satisfiability with positive probability for $d < d_k^\star$. We boost the latter to high probability with the small subgraph conditioning method [1, 2].

The fact that the second moment method is exact suggests that, at least in the d-regular case, this problem does not have a condensation transition. In contrast, for Graph Coloring, NAE-k-SAT and k-SAT, at a certain density condensation occurs [3, 4, 5, 6]: the set of satisfying assignments becomes dominated by a constant number of clusters, and since the sizes of these clusters fluctuates the number of satisfying assignments becomes much less concentrated. Thus while the second moment method gives fairly good bounds for these problems [7, 8, 9, 10], pushing it beyond this point requires much more sophisticated methods that count clusters

of solutions, and further reduce the variance by carefully conditioning on the distribution of neighborhood structures throughout the formula [11, 12, 13]. This line of work recently culminated in a proof of the threshold conjecture for k-SAT for sufficiently large k [14], although many open questions still remain.

Here the situation is much simpler. The only source of variance in the number of satisfying assignments is the number of cycles of each length in the formula, so the small subgraph conditioning method reduces the variance enough to prove satisfiability with high probability. It also turns out that that the point corresponding to two independent satisfying assignments is a local maximum of the rate function for the second moment, so there is no need to reweight the assignments as in [8, 17, 18].

The second moment method also owes its success to the fact that, in the d-regular case, Positive 1-in-k SAT is "locked" in the sense that most variables cannot be flipped without also flipping many others, so that satisfying assignments are isolated [15, 16]. Given a set $S \in \{1, \ldots, k-1\}$ let S-SAT be the problem where each clause has k variables, and demands that the number of true variables it contains is an element of S. If S does not contain any adjacent pairs $i, i+1$, and if every variable has degree at least 2, these problems are locked. In [16] the authors wrote the first and second moments for this family of problems, described the resulting bound as a fixed point equation, and conjectured that it is exact. This paper proves the case of their conjecture where $S = \{1\}$.

One can also consider random Positive 1-in-k SAT formulas where clauses appear independently, so that the degrees of the variables are Poisson distributed. A lower bound on the threshold in this model was given in [19] for $k = 3$ using differential equations. Other constraint satisfaction problems for which the threshold can be computed exactly (and where condensation does not appear to occur) include random XOR-SAT [20, 21, 22] as well as 1-in-k SAT [23] where literals are negated with probability $1/2$ as opposed to the positive case we consider here.

We write $f(n) \sim g(n)$ if $\lim_{n\to\infty} f(n)/g(n) = 1$. We say a series of events E_n *holds with high probability* if $\Pr[E_n] \sim 1$, and with positive probability if, for some constant $B > 0$, $\Pr[E_n] \geq B$ for all sufficiently large n.

2. The first and second moments

Throughout the paper, Z denotes the number of satisfying assignments of a random formula chosen according to the configuration model. In this section we bound the first and second moments of Z; we show that $\mathbb{E}[Z]$ is exponentially

small if $d > d_k^\star$, and that $\mathbb{E}[Z^2]/\mathbb{E}[Z]^2$ tends to a constant if $d < d_k^\star$ and $k > 2$. This implies that $F_{n,d,k}$ is unsatisfiable with high probability if $d > d_k^\star$, and satisfiable with positive probability if $d < d_k^\star$ and $k > 2$. We improve the latter to high probability in Section 3.

Lemma 1. *If $d > d_k^\star$ then $\mathbb{E}[Z] = \mathrm{e}^{-\Omega(n)}$.*

Proof. Since there are d copies of each true variable, and each of the $m = dn/k$ clauses must contain exactly one of them, the number of true variables is $|T| = n/k$. Thus the expectation of Z is $\binom{n}{n/k}$ times the fraction of bipartite matchings, for a given T, that connect each clause to exactly one copy of a true variable. Applying Stirling's formula $x! = (1 + o(1))\sqrt{2\pi x}\, x^x \mathrm{e}^{-x}$ gives

$$\begin{aligned} \mathbb{E}[Z] &= \binom{n}{n/k} \frac{m!\, k^m\, ((k-1)m)!}{(km)!} \\ &= k^m \binom{n}{n/k} \Big/ \binom{km}{m} \\ &\sim \sqrt{d}\, k^m\, \mathrm{e}^{(n-km)h(1/k)} \\ &= \sqrt{d}\, \mathrm{e}^{n\phi_1}. \end{aligned} \tag{2}$$

where

$$\begin{aligned} \phi_1 &= \frac{d}{k} \ln k - (d-1)\, h(1/k) \\ &= \frac{\ln k + (d-1)(k-1)\ln(1-1/k)}{k}. \end{aligned} \tag{3}$$

and

$$h(\alpha) = -\alpha \ln \alpha - (1-\alpha)\ln(1-\alpha)$$

denotes the Shannon entropy function. Since $\phi_1 = 0$ when $d = d_k^\star$, and ϕ_1 is a decreasing function of d, we have $\Pr[Z > 0] \le \mathbb{E}[Z] = \mathrm{e}^{-\Omega(n)}$ whenever $d > d_k^\star$. □

Lemma 2. *If $k > 2$ and $d < d_k^\star$ then*

$$\frac{\mathbb{E}[Z^2]}{\mathbb{E}[Z]^2} \sim \sqrt{\frac{k-1}{k-d}}. \tag{4}$$

Proof. The second moment $\mathbb{E}[Z^2]$ is the expected number of pairs of assignments T, T' that are both satisfying. This depends on the size of their difference. For a

given $w \in [0,1]$, let $Z_w^{(2)}$ denote the expected number of satisfying pairs with $|T \setminus T'| = |T' \setminus T| = wn/k$. For a given such pair, $(1-w)m$ of the clauses must be satisfied by a variable in $T \cap T'$, and the remaining wm clauses must be satisfied both by a variable in $T \setminus T'$ and one in $T' \setminus T$. The number of such matchings is

$$\binom{m}{wm}((1-w)m)!\,k^{(1-w)m}\,(wm)!^2\,(k(k-1))^{wm}\,((k-(1-w)-2w)m)!$$
$$= k^m\,(k-1)^{wm}\,m!\,(wm)!\,((k-1-w)m)!\,.$$

Thus

$$\mathbb{E}[Z_w^{(2)}] = k^m\,(k-1)^{wm}\binom{n}{n/k}\binom{n/k}{wn/k}\binom{(1-1/k)n}{wn/k}\frac{m!(wm)!((k-1-w)m)!}{(km)!} \tag{5}$$
$$= \mathbb{E}[Z](k-1)^{wm}\binom{n/k}{wn/k}\binom{(1-1/k)n}{wn/k}\Big/\binom{(k-1)m}{wm}.$$

For $0 < w < 1$, applying Stirling's formula to (5) gives

$$\mathbb{E}[Z_w^{(2)}] \sim \frac{1}{\sqrt{2\pi n}}\,f(w)\,\mathrm{e}^{n\phi_2(w)}\,,$$

where

$$f(w) = d\sqrt{\frac{k}{w(1-w)}} \tag{6}$$

and

$$\phi_2(w) = \phi_1 + \frac{wd}{k}\ln(k-1) + \frac{1}{k}\,h(w) - (d-1)\Big(1-\frac{1}{k}\Big)h\Big(\frac{w}{k-1}\Big). \tag{7}$$

As in [7], we can approximate the second moment by an integral, which we evaluate asymptotically using Laplace's method. If $\phi_2(w)$ has a unique maximum $w_{\max} \in [0,1]$ where $0 < w_{\max} < 1$ and $\phi_2''(w_{\max}) < 0$, then

$$\mathbb{E}[Z^2] = \sum_{w=0,k/n,2k/n,\ldots} \mathbb{E}[Z_w^{(2)}]$$
$$\sim \frac{1}{\sqrt{2\pi n}}\frac{n}{k}\int_0^1 \mathrm{d}w\; f(w)\,\mathrm{e}^{n\phi_2(w)} \tag{8}$$
$$\sim \frac{1}{k}\frac{f(w_{\max})}{\sqrt{-\phi_2''(w_{\max})}}\,\mathrm{e}^{n\phi_2(w_{\max})}.$$

In particular, suppose $w_{\max} = 1 - 1/k$. We have

$$\phi_2(1 - 1/k) = 2\phi_1 \,,$$

which corresponds to the fact that $1 - 1/k$ is the typical value of w if the two sets T, T' are chosen independently. Thus if ϕ_2 is maximized at $1 - 1/k$, and if $\phi_2'' < 0$ there, we have $\mathbb{E}[Z^2] \sim C\,\mathbb{E}[Z]^2$ for some constant C.

The following lemma shows that this is in fact the case whenever $d < d_k^\star$.

Lemma 3. *Let $k > 2$ and $d < d_k^\star$. Then $w_{\max} = 1 - 1/k$ is the unique maximum of $\phi_2(w)$ in the unit interval, and $\phi_2''(w_{\max}) < 0$.*

Proof. By direct calculation we have $\phi_2'(1 - 1/k) = 0$ and

$$\phi_2''(1 - 1/k) = -\frac{k(k-d)}{(k-1)^2} \,,$$

which is negative since $d_k^\star < k$ for all $k > 2$. Thus $1 - 1/k$ is a local maximum. To show that it is unique, note that ϕ_2 has a unique inflection point w_0 where $\phi_2'' = 0$, namely

$$w_0 = \frac{(d-2)(k-1)}{dk - d - k} \,.$$

This implies that $1-1/k$ is the only local maximum. Thus we just have to eliminate the possibility that the maximum of ϕ_2 in the unit interval is at $w = 0$ or $w = 1$. But this is easy: since $d < d_k^\star$ we have $\phi_1 > 0$, so $\phi_2(0) = \phi_1 < 2\phi_1 = \phi_2(1 - 1/k)$, and as $w \to 1$. At the other end of the interval, as $w \to 1$ we have $\phi_2(w) \to -\infty$ due to the $h(w)$ term in (7). △

Plugging Lemma 3 into the Laplace method (8) gives

$$\mathbb{E}[Z^2] \sim d \sqrt{\frac{k-1}{k-d}}\, \mathrm{e}^{2n\phi_1} \,,$$

and combining this with (2) gives

$$\frac{\mathbb{E}[Z^2]}{\mathbb{E}[Z]^2} \sim \sqrt{\frac{k-1}{k-d}} = C \,.$$

In particular, since $\Pr[Z > 0] \geq \mathbb{E}[Z]^2/\mathbb{E}[Z^2] \sim 1/C$, this shows that $F_{n,d,k}$ is satisfiable with constant probability. □

3. Small subgraph conditioning

When there are strong correlations between the events that a pair of assignments are both satisfying, the variance $\mathbb{E}[Z^2] - \mathbb{E}[Z]^2$ is a constant times $\mathbb{E}[Z]^2$, and the second moment method can only prove satisfiability with positive probability. However, in some cases we can show that the variance is much smaller if we condition on the number of small subgraphs in the formula—in particular, the number of cycles of each constant length. This technique was introduced in [1], where it was used to show that random 3-regular graphs possess a Hamiltonian cycle with high probability; other applications include [24], showing that random 5-regular graphs are 3-colorable with high probability, and [6], proving k-colorability for $G(n, m)$ up to the condensation threshold for sufficiently large k. (Note that this last case is for non-regular graphs, making the calculation more complicated than ours.)

Let X_i be the number of cycles of length $2i$ in the formula, i.e., cycles alternating between i distinct variables and i distinct clauses. Our goal is to compute the correlation between Z and X_i and its higher moments, and hence to learn to what extent X_i affects the number of satisfying assignments. Our goal is to explain almost all of the variance in Z with the variance in the X_i.

Let $(x)_r$ denote the falling factorial $x(x-1)(x-2)\cdots(x-r+1)$; thus $(X_i)_r$ is the number of ordered lists of r cycles of length $2i$. If X is Poisson with mean λ, we have $\mathbb{E}[(X)_r] = \lambda^r$. We use the following "plug and play" version of the subgraph conditioning method from [2].

Theorem 2. *Let Z and $X_1, X_2, \ldots$ be nonnegative integer-valued random variables. Suppose that $\mathbb{E}[Z] > 0$, and that for each $i \geq 0$ there are constants $\lambda_i > 0$, $\delta_i > -1$ such that*

(1) *for any j, the variables $X_1, \ldots, X_j$ are asymptotically independent and Poisson distributed, with $\mathbb{E}[X_i] \sim \lambda_i$,*

(2) *for any sequence $m_1, \ldots, m_j$ of nonnegative integers,*

$$\frac{\mathbb{E}[Z \prod_{i=1}^{j} (X_i)_{m_i}]}{\mathbb{E}[Z]} \sim \prod_{i=1}^{j} \mu_i^{m_i} \quad \text{where } \mu_i = \lambda_i(1+\delta_i), \tag{9}$$

(3) *$\sum_{i=1}^{\infty} \lambda_i \delta_i^2$ is finite, and*

$$\frac{\mathbb{E}[Z^2]}{\mathbb{E}[Z]^2} \sim \exp\Big(\sum_{i=1}^{\infty} \lambda_i \delta_i^2\Big). \tag{10}$$

Then $\Pr[Z > 0] = 1 - o(1)$.

Applying this technology to prove the following theorem, and thus complete the proof of Theorem 1, is an enjoyable exercise in combinatorics.

Theorem 3. *If $k > 2$ and $d < d_k^\star$ then $F_{n,d,k}$ is satisfiable with high probability.*

Proof. Standard arguments for sparse random graphs [25] show that the X_i are asymptotically independent and Poisson distributed. To compute the asymptotic expectation λ_i, note that there are $(m)_i (n)_i$ sequences of clauses and variables that C could visit; since there are i variables where we could start a cycle and two directions in which we could go, this overcounts by a factor of $2i$. There are $(k(k-1)d(d-1))^i$ choices of copies with which to wire each variable to the clause before and after it in the sequence, and the number of matchings that include a given such wiring is $(km-2i)!$. Thus

$$\begin{aligned} \mathbb{E}[X_i] &= \frac{1}{2i}(m)_i (n)_i (k(k-1)d(d-1))^i \, \frac{(km-2i)!}{(km)!} \\ &\sim \frac{((k-1)(d-1))^i}{2i} \\ &= \lambda_i . \end{aligned} \tag{11}$$

In order to establish (9), we first warm up by computing $\mathbb{E}[ZX_i]$. This is the sum over all pairs (T, C), where T is an assignment and C is a cycle of length $2i$, of the fraction of matchings containing C for which T is satisfying.

We start by choosing one of the $\binom{n}{n/k}$ possible satisfying assignments T. We then choose C. First, we choose $t = |C \cap T|$, the number of true variables in C. Let us think of C as a cycle of i variables, where the edges between them correspond to their shared clauses. Since each clause must contain exactly one true variable, none of C's true variables can be adjacent; in particular, $t \le \lfloor i/2 \rfloor$. (This is similar to [1], where no two adjacent edges of C can belong to a Hamiltonian cycle.) Let $N_{i,t}$ be the number of ordered, labeled cycles with t true variables, where no two true variables are adjacent; for instance, $N_{6,0} = 1$, $N_{6,1} = 6$, $N_{6,2} = 9$, and $N_{6,3} = 2$.

Now that we have chosen t, and chosen one of the $N_{i,t}$ arrangements of true variables in it, we choose what variables and clauses C contains and how they are matched to each other. There are $(m)_i$ ordered sets of i clauses, and $(n/k)_t \left((1-1/k)n\right)_{i-t}$ choices of which true and false variables appear in C and in what order. As before, there are $(k(k-1)d(d-1))^i$ ways to wire each variable to the clause before and after it, and all this overcounts by a factor of $2i$.

At this point in the process, we have already satisfied $2t$ clauses in C, so there are $m-2t$ clauses waiting to be satisfied. Happily, we have $dn/k-2t=m-2t$ unmatched copies of true variables with which to satisfy them. The $m-i$ clauses outside C have k unmatched copies each, and the $i-2t$ clauses in C that are not yet satisfied each have $k-2$ unmatched copies. Thus there are $(m-2t)!$ orders in which we can assign copies of true variables to clauses, and $k^{m-i}\,(k-2)^{i-2t}$ ways to match them with these clauses' copies. After all this, there are $(k-1)m-2(i-t)$ unmatched copies of false variables, which can be matched with the remaining clause copies arbitrarily. Finally, we divide by $(km)!$ to obtain

$$\mathbb{E}[ZX_i]=\binom{n}{n/k}\sum_{t=0}^{\lfloor i/2\rfloor}\Big[\frac{N_{i,t}}{2i}(m)_i(n/k)_t((1-1/k)n)_{i-t}(k(k-1)d(d-1))^i \\ \frac{(m-2t)!\,k^{m-i}(k-2)^{i-2t}((k-1)m-2(i-t))!}{(km)!}\Big].$$

Dividing by $\mathbb{E}[Z]$ and using $(m)_i\sim m^i$, $m!/(m-2t)!\sim m^{2t}$ and so on gives

$$\begin{aligned}\frac{\mathbb{E}[ZX_i]}{\mathbb{E}[Z]}&=\sum_{t=0}^{\lfloor i/2\rfloor}\Big[\frac{N_{i,t}}{2i}(m)_i(n/k)_t((1-1/k)n)_{i-t}(k(k-1)d(d-1))^i \\ &\qquad\frac{(m-2t)!\,k^{m-i}(k-2)^{i-2t}((k-1)m-2(i-t))!}{m!k^m((k-1)m)!}\Big] \\ &\sim\frac{((k-2)(d-1))^i}{2i}\sum_{t=0}^{\lfloor i/2\rfloor}N_{i,t}\Big(\frac{k-1}{(k-2)^2}\Big)^t \\ &=\mu_i=\lambda_i(1+\delta_i),\end{aligned}$$

where

$$\delta_i=\Big(\frac{k-2}{k-1}\Big)^i\sum_{t=0}^{\lfloor i/2\rfloor}N_{i,t}\Big(\frac{k-1}{(k-2)^2}\Big)^t-1. \tag{12}$$

We can evaluate this sum with a generating function. The requirement that no two true variables are adjacent can be expressed as a transition matrix between two states, true and false, where the matrix element corresponding to the true-true transition is zero. Moreover, since there are a total of $2t$ true-false and false-true transitions, we can think of each one as giving us a factor $\sqrt{z}$ where

$$z=\frac{k-1}{(k-2)^2}\,. \tag{13}$$

Thus

$$\sum_{t=0}^{\lfloor i/2 \rfloor} N_{i,t} \Big(\frac{k-1}{(k-2)^2}\Big)^t = g\Big(\frac{k-1}{(k-2)^2}\Big)$$

where

$$g(z) = \sum_{t=0}^{\lfloor i/2 \rfloor} N_{i,t} z^t = \operatorname{tr} \begin{pmatrix} 0 & \sqrt{z} \\ \sqrt{z} & 1 \end{pmatrix}^i .$$

The trace of the tth power of a matrix is the sum of the tth powers of its eigenvalues. These are the roots $\lambda_\pm =$ of the quadratic equation $\lambda(\lambda - 1) - z = 0$. Thus

$$g(z) = \lambda_+^i + \lambda_-^i = \Big(\frac{1 + \sqrt{1+4z}}{2}\Big)^i + \Big(\frac{1 - \sqrt{1+4z}}{2}\Big)^i$$

Plugging in the value (13) for z and combining with (12) finally gives

$$\begin{aligned} \delta_i &= \Big(\frac{k-2}{k-1}\Big)^i g\Big(\frac{k-1}{(k-2)^2}\Big) - 1 \\ &= \Big(\frac{k-2}{k-1}\Big)^i \Big(\Big(\frac{k-1}{k-2}\Big)^i + \Big(\frac{-1}{k-2}\Big)^i\Big) - 1 \\ &= \Big(-\frac{1}{k-1}\Big)^i . \end{aligned} \tag{14}$$

Generalizing this calculation to show that (9) holds is a matter of bookkeeping. Let $\ell = \sum_{s=1}^j m_s$, and let $i_1, \ldots, i_\ell$ be a sorted list where each s appears m_s times. Then $\mathbb{E}[Z \prod_{i=1}^j (X_i)_{m_i}]$ is the expected number of tuples $(T, C_1, \ldots, C_\ell)$ where T is a satisfying assignment and $C_1, \ldots, C_\ell$ are disjoint cycles, where C_s is of length $2i_s$. Counting as before gives

$$\begin{aligned} \frac{\mathbb{E}[Z \prod_{i=1}^j (X_i)_{m_i}]}{\mathbb{E}[Z]} &= \sum_{t_1=0}^{\lfloor i_1/2 \rfloor} \sum_{t_2=0}^{\lfloor i_2/2 \rfloor} \cdots \sum_{t_\ell=0}^{\lfloor i_\ell/2 \rfloor} \Big[\Big(\prod_{s=1}^{\ell} \frac{N_{i_s,t_s}}{2i_s}\Big) \mathfrak{S}\mathfrak{S}'\Big] \\ &\sim \prod_{s=1}^{\ell} \frac{((k-2)(d-1))^{i_s}}{2i_s} \sum_{t_s=0}^{\lfloor i_s/2 \rfloor} N_{i_s,t_s} \Big(\frac{k-1}{(k-2)^2}\Big)^{t_s} \\ &= \prod_{s=1}^{\ell} \mu_{i_s} \\ &= \prod_{i=1}^{j} \mu_i^{m_i} , \end{aligned}$$

where

$$\mathfrak{S} = (m)_{\sum_s i_s}(n/k)_{\sum_s t_s}((1-1/k)n)_{\sum_s (i_s - t_s)}(k(k-1)d(d-1))^{\sum_s i_s}$$

and

$$\mathfrak{S}' = \frac{(m - 2\sum_s t_s)!\, k^{m-\sum_s i_s}(k-2)^{\sum_s (i_s - 2t_s)}((k-1)m - 2\sum_s (i_s - t_s))!}{m!\, k^m ((k-1)m)!}.$$

Finally, we establish (10). Using the Taylor series $-\log(1-z) = \sum_{i=1}^{\infty} z^i/i$ gives

$$\sum_{i=1}^{\infty} \lambda_i \delta_i^2 = \frac{1}{2}\sum_{i=1}^{\infty} \frac{1}{i}\Big(\frac{d-1}{k-1}\Big)^i = \frac{1}{2}\log\frac{k-1}{k-d},$$

and comparing with (4) shows that this is indeed the logarithm of the asymptotic ratio $C \sim \mathbb{E}[Z^2]/\mathbb{E}[Z]^2$. This completes the proof. □

Acknowledgments

This work was supported by NSF grants CCF-1117426 and CCF-1219117. I am grateful to Allan Sly, Lenka Zdeborová, and Amin Coja-Oghlan for helpful conversations. I am also grateful to the Bellairs Research Institute of McGill University where part of this work was carried out.

References

[1] R. W. Robinson and N. C. Wormald, Almost all cubic graphs are Hamiltonian. *Random Structures Algorithms* **3** (1992), no. 2, 117–125. MR 1151355 Zbl 0755.05075

[2] N. C. Wormald, Models of random regular graphs. In J. D. Lamb and D. A. Preece (eds.), *Surveys in combinatorics, 1999.* Papers from the British Combinatorial Conference held at the University of Kent at Canterbury, Canterbury, 1999. London Mathematical Society Lecture Note Series, 267. Cambridge University Press, Cambridge, 1999, 239–298. MR 1725006 Zbl 0935.05080

[3] F. Krzakala, A. Montanari, F. Ricci-Tersenghi, G. Semerjian, and L. Zdeborová, Gibbs states and the set of solutions of random constraint satisfaction problems. *Proc. Natl. Acad. Sci. USA* **104** (2007), no. 25, 10318–10323. MR 2317690 Zbl 1190.68031

[4] A. Coja-Oghlan and L. Zdeborová, The condensation transition in random hypergraph 2-coloring. In Y. Rabani (ed.), *Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms.* Proceedings of the symposium (SODA, 2012) held in Kyoto, January 17–19, 2012. Association for Computing Machinery (ACM), New York, 2012, 241–250. MR 3205212

[5] V. Bapst, A. Coja-Oghlan, S. Hetterich, F. Raßmann, and D. Vilenchik, The condensation phase transition in random graph coloring. In K. Jansen, J. D. P. Rolim, N. R. Devanur, and C. Moore (eds.), *Approximation, randomization, and combinatorial optimization. Algorithms and techniques.* Proceedings of the 17th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX 2014) and the 18th International Workshop on Randomization and Computation (RANDOM 2014) held at the Universitat Politècnica de Catalunya, Barcelona, September 4–6, 2014. LIPIcs. Leibniz International Proceedings in Informatics, 28. Schloss Dagstuhl. Leibniz-Zentrum für Informatik, Wadern, 2014, 449–464. MR 3319009 Zbl 06544482

[6] V. Bapst, A. Coja-Oghlan, and Ch. Efthymiou, Planting colourings silently. Preprint 2014. arXiv:1411.0610 [cs.DM]

[7] D. Achlioptas and C. Moore, Two moments suffice to cross a sharp threshold. *SIAM J. Comput.* **36** (2006), no. 3, 740–762. MR 2263010 Zbl 1120.68096

[8] D. Achlioptas and Y. Peres, The threshold for random k-SAT is $2^k(\ln 2 - O(k))$. In *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing.* Held in San Diego, CA, 2003 (STOC 2003). Association for Computing Machinery (ACM), New York, 2003, 223–231. MR 2121043 Zbl 1192.68333

[9] D. Achlioptas and A. Naor, The two possible values of the chromatic number of a random graph. In *Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing.* Held in Chicago, IL, June 13–15, 2004 (STOC 2004). Association for Computing Machinery (ACM), New York, 2004, 587–593. MR 2121647 Zbl 1192.05140

[10] D. Achlioptas and C. Moore, The Chromatic Number of Random Regular Graphs. In K. Jansen, S. Khanna, J. D. P. Rolim, and D. Ron (eds.), *Approximation, randomization, and combinatorial optimization. Algorithms and techniques.* Proceedings of the 7th international workshop on approximation algorithms for combinatorial optimization problems, (APPROX 2004) and the 8th international workshop on randomization and computation, (RANDOM 2004) Cambridge, MA, USA, August 22-24, 2004. Lecture Notes in Computer Science, 3122. Springer, Berlin, 219–228. Zbl 1105.05063

[11] A. Coja-Oghlan and K. Panagiotou, Catching the k-NAESAT threshold. In H. J. Karloff and T. Pitassi (eds.), *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing.* Held in New York, N.Y., May 19–22, 2012 (STOC 2012). Association for Computing Machinery (ACM), New York, 2012, 899–908. MR 2961553 Zbl 1286.68185

[12] A. Coja-Oghlan, The asymptotic k-SAT threshold. In *Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing.* Held in New York, N.Y., USA, May 31– June 3, 2014 (STOC 2014). Association for Computing Machinery (ACM), New York, 2014, 804–813. Zbl 1315.68146

[13] J. Ding, A. Sly, and N. Sun, Satisfiability threshold for random regular NAE-SAT. In *Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing*. Held in New York, N.Y., USA, May 31– June 3, 2014 (STOC 2014). Association for Computing Machinery (ACM), New York, 2014, 814–822. Zbl 1315.68148

[14] J. Ding, A. Sly, and N. Sun, Proof of the satisfiability conjecture for large k. In *Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing*. Held in Portland, OR, June 15–17, 2015 (STOC 2015). Association for Computing Machinery (ACM), New York, 2015, 59–68. MR 3388183 Zbl 1321.68304

[15] L. Zdeborová and M. Mézard, Locked constraint satisfaction problems. *Phys. Rev. Lett.* **101** (2008), article id. 078702.

[16] L. Zdeborová and M. Mézard, Constraint satisfaction problems with isolated solutions are hard. *J. Stat. Mech.* **2008**, article id. P12004.

[17] D. Achlioptas, A. Naor, and Y. Peres, On the maximum satisfiability of random formulas. *J. ACM* **54** (2007), no. 2, Art. 10, 21 pp. MR 2295994 Zbl 1291.68175

[18] V. Dani and C. Moore, Independent sets in random graphs from the weighted second moment method. In L. A. Goldberg, K. Jansen, R. Ravi, and J. D. P. Rolim (eds.), *Approximation, randomization, and combinatorial optimization.* Algorithms and techniques. Proceedings of the 14th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX 2011) and the 15th International Workshop on Randomization and Computation (RANDOM 2011) held at Princeton University, Princeton, N.J., August 17–19, 2011. Springer, Berlin etc., 2011, 472–482. MR 2863283 Zbl 05940176

[19] V. Kalapala and C. Moore, The phase transition in exact cover. *Chic. J. Theoret. Comput. Sci.* **2008**, Article 5. MR 2448778 Zbl 1286.68236

[20] O. Dubois and J. Mandler, The 3-XORSAT threshold. *C. R. Math. Acad. Sci. Paris* **335** (2002), no. 11, 963–966. MR 1952558 Zbl 1038.68052

[21] M. Mézard, F. Ricci-Tersenghi, and R. Zecchina. Two solutions to diluted p-spin models and XORSAT problems. *J. Statist. Phys.* **111** (2003), no. 3-4, 505–533. MR 1972120 Zbl 1049.82073

[22] B. Pittel and G. B. Sorkin, The satisfiability threshold for k-XORSAT. *Combin. Probab. Comput.* **25** (2016), no. 2, 236–268. MR 3455676

[23] D. Achlioptas, A. Chtcherba, G. Istrate, and C. Moore, The phase transition in 1-in-k SAT and NAE 3-SAT. In D. Kosaraju (ed), *Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms.* Held in Washington, D.C., January 7–9, 2001 (SODA 2001). Society for Industrial and Applied Mathematics (SIAM), New York, and Association for Computing Machinery (ACM), New York, 721–722. Zbl 0991.68032

[24] J. Díaz, A. C. Kaporis, G. D. Kemkes, L. M. Kirousis, X. Pérez, and N. C. Wormald (eds.), On the chromatic number of a random 5-regular graph. *J. Graph Theory* **61** (2009), no. 3, 157–191. MR 2527637 Zbl 1190.05069

[25] B. Bollobás, *Random graphs.* Academic Press, London etc., 1985. MR 0809996 Zbl 0567.05042

Communicated by Andrea Montanari

Received March 4, 2015; accepted February 15, 2016

Cristopher Moore, Santa Fe Institute, 1399 Hyde Park Road, Santa Fe, NM 87501, US
e-mail: moore@santafe.edu