Combinatorics, Probability and Computing (2016) 25, 236–268.
doi:10.1017/S0963548315000097

The Satisfiability Threshold for k-XORSAT

BORIS PITTEL[1] and GREGORY B. SORKIN[2†]

[1] Department of Mathematics, Ohio State University, Columbus OH 43210, USA
(e-mail: bgp@math.ohio-state.edu)

[2] Departments of Management and Mathematics, London School of Economics and Political Science,
Houghton Street,
London WC2A 2AE, UK
(e-mail: g.b.sorkin@lse.ac.uk)

Received 1 April 2011; revised 3 March 2015; first published online 31 July 2015

We consider 'unconstrained' random k-XORSAT, which is a uniformly random system of m linear non-homogeneous equations in $\mathbb{F}_2$ over n variables, each equation containing $k \geqslant 3$ variables, and also consider a 'constrained' model where every variable appears in at least two equations. Dubois and Mandler proved that $m/n = 1$ is a sharp threshold for satisfiability of constrained 3-XORSAT, and analysed the 2-core of a random 3-uniform hypergraph to extend this result to find the threshold for unconstrained 3-XORSAT.

We show that $m/n = 1$ remains a sharp threshold for satisfiability of constrained k-XORSAT for every $k \geqslant 3$, and we use standard results on the 2-core of a random k-uniform hypergraph to extend this result to find the threshold for unconstrained k-XORSAT. For constrained k-XORSAT we narrow the phase transition window, showing that $m - n \to -\infty$ implies almost-sure satisfiability, while $m - n \to +\infty$ implies almost-sure unsatisfiability.

2010 *Mathematics subject classification*: Primary 68Q87
Secondary 60B20, 05A16

1. Introduction

An instance of k-XORSAT is given by a set of m linear equations in $\mathbb{F}_2$, over n variables, each equation involving k variables and a right-hand side which is either 0 or 1. Equivalently, it is a linear system $Ax = b$ modulo 2 in which A is an $m \times n$ 0–1 matrix each of whose row sums is k, and b is an arbitrary 0–1 vector.

† This research was supported by DIMACS, Center for Discrete Mathematics and Theoretical Computer Science, Rutgers, the State University of New Jersey, funded by the NSF under grant DMS06-02942, Special Focus on Discrete Random Systems, and by the NSF under grants DMS-0805996 and DMS 1101237. The paper was begun when the second author was a researcher in the Department of Mathematical Sciences, IBM T.J. Watson Research Center, Yorktown Heights NY 10598, USA.

Random instances of many problems of this sort undergo phase transitions around some critical ratio c^* of m/n, meaning that for $m, n \to \infty$ with $\lim m/n < c^*$, the probability that a random instance $F_{n,m}$ is satisfiable (or possesses some similar property) approaches 1, while if $\lim m/n > c^*$ the probability approaches 0. (There is no loss of generality in hypothesizing the existence of a limit since, in a broad context, a result as stated implies the same with the weaker hypotheses $\liminf m/n > c^*$ and $\limsup m/n < c^*$.) Friedgut [19] proved that a wide range of problems have such sharp thresholds, but with the possibility that the threshold $c^* = c^*(n)$ does not tend to a constant. The relatively few cases in which c^* is known to be a constant include 2-SAT, by Chvátal and Reed [7], Goerdt [20], and Fernandez de la Vega [18] (with the scaling window detailed by Bollobás, Borgs, Chayes, Kim and Wilson [5]), an extension to Max 2-SAT, by Coppersmith, Gamarnik, Hajiaghayi and Sorkin [10], and the pure-literal threshold for a k-SAT formula, by Molloy [25].

The most natural random model of the k-XORSAT problem is the 'unconstrained' model in which each of the m equations' k variables are drawn uniformly (without replacement) from the set of all n variables, and the right-hand side values are uniformly 0 or 1; equivalently a random instance $Ax = b$ is given by a matrix $A \in \{0, 1\}^{m\times n}$ drawn uniformly at random from the set of all such matrices with each row sum equal to k, and $b \in \{0, 1\}^m$ chosen uniformly at random.

The case $k = 2$ has been extensively studied. As shown by Kolchin [22] and Creignon and Daudé [11], the random instance has a solution with limiting probability $p(2m/n) + o(1)$, where $p(x) \in (0, 1)$ for $x < 1$, $p(1-) = 0$, and $p(x) \equiv 0$ for $x > 1$. Daudé and Ravelomanana [13], and Pittel and Yeum [30], analysed the near-critical behaviour of the solvability probability for $2m/n = 1 + \varepsilon$, $\varepsilon = o(n^{-1/4})$.

For $k > 2$, Kolchin [22] analysed the expected number of non-empty 'critical row sets' (non-empty collections of rows whose sum is all-even), whose presence is necessary and sufficient for the (Boolean) rank of A to be less than m. He determined the thresholds c_k such that the expected number of non-empty critical sets goes to 0 if $\lim m/n < c_k$ and to infinity if $\lim m/n > c_k$; in particular, $c_3 = 0.8894\ldots$. Thus, for $\lim m/n < c_k$, with high probability A is of full rank, so $Ax = b$ is solvable. It follows that the satisfiability threshold c_k^* is at least c_k. It is an easy observation (see Remark 1) that $c_k^* \leqslant 1$. However, Kolchin could not resolve the precise value, or even the existence, of the satisfiability threshold.

Dubois and Mandler [16] (see also [17]) introduced a 'constrained' random k-XORSAT model, where b is still uniformly random, but A is uniformly random over the subset of matrices in which each column sum is at least 2. For $k = 3$ (3-XORSAT) they showed that its threshold for m/n is 1. This is of interest because from the threshold for the constrained model, they were able to derive that for the unconstrained model. Dubois and Mandler suggested that their methods could be extended to the general constrained k-XORSAT, $k \geqslant 3$. However, their approach – the second-moment method for the number of solutions – requires solving a hard maximization problem with $\Theta(k)$ variables, a genuinely daunting task.

Our main result is that 1 continues to be the threshold for all $k > 3$.

Theorem 1.1. *Let $Ax = b$ be a uniformly random constrained k-XORSAT instance with m equations and n variables. Suppose $k \geqslant 4$. If $m, n \to \infty$ with $\lim m/n \in (2/k, 1)$, then $Ax = b$*

https://doi.org/10.1017/S0963548315000097 Published online by Cambridge University Press

is asymptotically almost surely (a.a.s.) satisfiable, with satisfiability probability $1-O(m^{-(k-2)})$*, while if* $m,n\to\infty$ *with* $\lim m/n>1$ *then* $Ax=b$ *is a.a.s. unsatisfiable, with satisfiability probability* $O(2^{-(m-n)})$.

We treat k as fixed, and the constants implicit in the $O(\cdot)$ notation may depend on k. We are also able to treat the case when the gap between m and n is not linear but arbitrarily slowly growing, obtaining the following stronger theorem.

Theorem 1.2. *Let* $Ax=b$ *be a uniformly random constrained* k*-XORSAT instance with* m *equations and* n *variables, with* $k\geqslant 3$ *and* $m,n\to\infty$ *with* $\liminf m/n>2/k$*. Then, for any* $w(n)\to+\infty$*, if* $m\leqslant n-w(n)$ *then* $Ax=b$ *is a.a.s. satisfiable, with satisfiability probability* $1-O(m^{-(k-2)}+\exp(-0.69\,w(n)))$*, while if* $m\geqslant n+w(n)$ *then* $Ax=b$ *is a.a.s. unsatisfiable, with satisfiability probability* $O(2^{-w(n)})$.

Rather than using the second-moment method on the number of solutions, as Dubois and Mandler do, we use the critical-set approach of Kolchin. Remark 2 shows that the two methods are equivalent, but Kolchin's leads us to more tractable calculations, specifically, to a maximization problem with a number of variables that is fixed, independent of k. Using Kolchin's approach, but in the constrained model, we will establish that $c_k^*\geqslant 1$. In the constrained and unconstrained models, a simple argument shows that $c_k^*\leqslant 1$ (again see Remark 1). Thus, for the constrained model (unlike the constrained one), the two bounds coincide, establishing the threshold.

Dubois and Mandler extended the threshold for the constrained 3-XORSAT model to that for the unconstrained model by observing that, in an unconstrained instance, any variable appearing in just one clause (or none), can be deleted along with that clause (if any), to give an equivalent instance, and this process can be repeated. The key observation is that a uniformly random *unconstrained* instance reduces to a uniformly random *constrained* instance with a predictable ratio m/n; the threshold for the unconstrained model is the value for which the corresponding constrained instance has ratio 1. The same approach works for any k, and we capitalize on existing analyses of the 2-core of a random k-uniform hypergraph to establish the unconstrained k-XORSAT threshold in Theorem 7.1.

Other related work

Work on the rank of random matrices over finite fields is not as extensive as that on real random matrices, but nonetheless a survey is beyond our scope. In addition to the work already described, we note that the rank of matrices with independent random 0–1 entries was explored over a decade ago by Blömer, Karp and Welzl [4], and Cooper [8], among others.

In 2003, the k-XORSAT phase transition was determined by Mézard, Ricci-Tersenghi and Zecchina [23], by the non-rigorous 'replica' method of statistical physics and also by a second-moment calculation, with the purpose of showing that the replica method is correct in this instance. The calculational details were omitted from the paper, and the authors acknowledge [24] that they did not rigorously prove negativity of the function

https://doi.org/10.1017/S0963548315000097 Published online by Cambridge University Press

playing the role of our H_k (see (4.2)) nor did they treat the polynomial terms in the sum corresponding to our (4.1) (which are of concern for small and large values of ℓ). Concurrently with and independently from our work, the k-XORSAT phase transition was also studied by Dietzfelbinger, Goerdt, Mitzenmacher, Montanari, Pagh and Rink as part of a study of cuckoo hashing [14, 15], but the work has not yet appeared in journal form.

Recently, Darling, Penrose, Wade and Zabell [12] have explored a random XORSAT model replacing the constant k with a distribution, but the satisfiability threshold has not yet been determined for this generalization.

To translate our result for the constrained model to the unconstrained one, we exploit results on the core of a random hypergraph. For usual graphs, the threshold for the appearance of an r-core was first obtained by Pittel, Spencer and Wormald [29]. For k-uniform hypergraphs, the r-core thresholds were obtained roughly concurrently by Cooper [9], Kim [21], and Molloy [25]. Two aspects of Cooper's treatment are noteworthy. First, he works with a degree-sequence hypergraph model; taking Poisson-distributed degrees reproduces the results for a simple random hypergraph. Also, he observes [9, Section 5.2] that the point at which a random k-uniform hypergraph's core has a (typical) edges-to-vertices ratio of 1 is an upper bound on the satisfiability threshold of unconstrained k-XORSAT; proving that this is the true threshold is the main subject of the present paper.

Outline

The remainder of the paper is organized as follows. Section 2 formalizes our introductory observations about the first- and second-moment methods, the number of solutions, and the number of critical sets. Section 3 shows that for the constrained model, instead of considering random 0–1 matrices A, it is asymptotically equivalent to consider random non-negative *integer* matrices A subject to the same constraints on row sums (equal to k) and column sums (at least 2). Section 4, using generating functions and Chernoff's method, obtains an exponential bound for the expected number of critical sets of any given cardinality. Section 5 uses this bound to show that, for $\lim m/n \in (2/k, 1)$ and $k > 3$, the expected number of non-empty critical sets is $O(m^{-(k-2)})$. Hence, with high probability, there is no such set, A is of full rank, and the instance is satisfiable. We conclude that 1 is a sharp threshold for satisfiability of $Ax = b$ in the constrained case for all $k \geqslant 3$.

Section 6 builds on the earlier results to treat the case $\lim m/n = 1$ and prove Theorem 1.2. Section 7 derives the unconstrained k-XORSAT threshold from the constrained one, using standard results on the 2-core of a random hypergraph.

2. Proof background

Let N be the number of solutions to the system of equations $Ax = b$.

Remark 1. For an arbitrarily distributed $A \in \{0,1\}^{m\times n}$, with b independent and uniformly distributed over $\{0,1\}^m$, $\mathbb{E}[N] = 2^{n-m}$, and the satisfiability threshold is at most 1.

Proof. Given A, there are 2^m systems given by (A, b), and in all they have 2^n solutions since any x uniquely determines $b = Ax$. So $\mathbb{E}[N \mid A] = 2^{n-m}$, and $\mathbb{E}[N] = 2^{n-m}$. By the first-moment method, $\mathbb{P}(Ax = b \text{ is satisfiable}) = \mathbb{P}(N > 0) \leqslant \mathbb{E}[N] = 2^{n-m}$, which tends to 0 if $\lim m/n > 1$. □

Definition 1. Given a matrix, a *critical set* is a collection of rows whose sum is all-even (*i.e.*, the sum is the 0 vector in $\mathbb{F}_2^n$).

Note that the collection of critical sets is sandwiched between the minimal linearly dependent sets of rows, and all linearly dependent sets of rows. It is useful because the minimal sets are hard to characterize, while the collection of all linearly dependent row sets is too large (as it includes all sets containing any linearly dependent sets); the critical sets are a happy medium.

Let X be the number of non-empty critical row subsets of a matrix A. Where the first-moment method establishes the probable absence of solutions, their probable presence can be established in this setting either by the second-moment method on the number of solutions, showing that $\mathbb{E}[N^2]/\mathbb{E}[N]^2 \to 1$, or by the first-moment method on the number of non-empty critical row sets, showing that $\mathbb{E}[X] \to 0$. We will use the second approach (Kolchin's). The two approaches suggest dramatically different calculations, but as the following remark shows, they are equivalent.

Remark 2. Let a distribution on $A \in \{0,1\}^{m\times n}$ be given, and let b be independent of A and uniformly distributed over $\{0,1\}^m$. Then $\mathbb{E}[N^2]/\mathbb{E}[N]^2 = \mathbb{E}[X] + 1$.

Proof. Consider any fixed A, having rank $r(A)$ over $\mathbb{F}_2$. By elementary linear algebra, for each of the $2^{r(A)}$ values of b in $\{Ax : x \in \{0,1\}^n\}$, $Ax = b$ has $2^{n-r(A)}$ solutions, giving $2^{2n-2r(A)}$ ordered pairs of solutions in each such case. For the remaining values of b there are no solutions, so in all there are $2^{2n-r(A)}$ ordered pairs of solutions. Taking the expectation over b uniformly distributed over its 2^m possibilities, $\mathbb{E}[N^2 \mid A] = \mathbb{E}[2^{2n-r(A)-m}]$, thus $\mathbb{E}[N^2] = \mathbb{E}[2^{2n-r(A)-m}]$. Since $\mathbb{E}[N] = 2^{n-m}$ (see Remark 1),

$$\mathbb{E}[N^2]/\mathbb{E}[N]^2 = \mathbb{E}[2^{2n-r(A)-m}]/(2^{n-m})^2 = \mathbb{E}[2^{m-r(A)}] = \mathbb{E}[2^{n(A^\intercal)}],$$

where $n(A^\intercal)$ denotes the nullity of the transpose of A.

On the other hand, a critical row set is precisely one given by an indicator vector $y \in \{0,1\}^m$ for which $y^\intercal A = 0$. For a given A the number of critical sets is thus $2^{n(A^\intercal)}$, and the expected number of non-empty critical row subsets is $\mathbb{E}[X] = \mathbb{E}[2^{n(A^\intercal)}] - 1$. □

In fact, if $m \leqslant n$ and $\mathbb{E}[X] \to 0$, then with high probability $N = 2^{n-m}$ (rather than merely $N/2^{n-m} \to 1$ in probability as given by the second-moment method). This follows because $X = 0$ implies $r(A) = m$, in which case $N = 2^{n-m}$ for every b. Thus,

$$\mathbb{P}(N = 2^{n-m}) \geqslant \mathbb{P}(X = 0) = 1 - \mathbb{P}(X > 0) \geqslant 1 - \mathbb{E}[X] \to 1.$$

The work in Sections 3–5 is to count the critical row subsets. We will show that indeed $\mathbb{E}[X] \to 0$ for the constrained random model with $k \geqslant 4$ and $m, n \to \infty$ with $\lim m/n \in (2/k, 1)$.

3. Probability spaces

This section will establish Corollary 3.3, showing that the uniform distribution over constrained k-XORSAT matrices $A \in \mathcal{A}_{m,n}$ (see below) is for our purposes equivalent to a model $C \in \mathcal{C}_{m,n}$ allowing a variable to appear more than once within an equation.

Let $\mathcal{A}_{m,n}$ denote the set of all $m \times n$ matrices with 0–1 entries, such that all m row sums are k, and all n column sums are at least 2. For $\mathcal{A}_{m,n}$ to be non-empty it is necessary that $km \geqslant 2n$, and we will assume that $m, n \to \infty$ with $\lim m/n \in (2/k, \infty)$.

A matrix $A \in \mathcal{A}_{m,n}$ may be interpreted as an outcome of the following allocation scheme. We have an $m \times n$ array of cells with k *indistinguishable* chips assigned to each of the m rows. For each row, the k chips are put in k distinct cells (so there is at most one chip per cell), subject to the constraint that each column gets at least two chips.

Let us consider an alternative model, with the same constraints but where the chips in each row are *distinguishable*, giving allocations $B \in \mathcal{B}_{m,n}$. Then each allocation in $\mathcal{A}_{m,n}$ is obtained from $(k!)^m$ allocations in $\mathcal{B}_{m,n}$, and the uniform distribution on $\mathcal{A}_{m,n}$ is equivalent to that on $\mathcal{B}_{m,n}$.

Let $\mathcal{C}_{m,n}$ be a relaxed version of $\mathcal{B}_{m,n}$, without the requirement that each of the mn cells gets at most one chip. Let B and C be distributed uniformly on $\mathcal{B}_{m,n}$ and $\mathcal{C}_{m,n}$, respectively. Crucially, and obviously, B is equal in distribution to C, conditioned on $C \in \mathcal{B}_{m,n}$.

To state a key lemma on $|\mathcal{A}_{m,n}|$, $|\mathcal{B}_{m,n}|$, and $|\mathcal{C}_{m,n}|$ we need some notation, much of which will recur throughout the paper.

Introduce

$$f(x) = \sum_{j \geqslant 2} \frac{x^j}{j!} = e^x - 1 - x, \quad \psi(x) = \frac{x f'(x)}{f(x)}, \tag{3.1}$$

with $\psi(0) = 2$ defined by continuity, and the *truncated* Poisson random variable $Z = Z(\lambda)$,

$$\mathbb{P}(Z(\lambda) = j) = \frac{\lambda^j / j!}{f(\lambda)}, \quad j \geqslant 2. \tag{3.2}$$

Then

$$\mathbb{E}[Z(\lambda)] = \sum_j \frac{j \cdot \lambda^j / j!}{f(\lambda)} = \frac{\lambda f'(\lambda)}{f(\lambda)} = \psi(\lambda). \tag{3.3}$$

Also, $\mathbb{E}[Z(\lambda)(Z(\lambda) - 1)] = \lambda^2 f''(\lambda)/f(\lambda)$, leading to

$$\begin{aligned} \operatorname{Var}[Z(\lambda)] &= \mathbb{E}[Z(Z-1)] + \mathbb{E}[Z] - (\mathbb{E}[Z])^2 \\ &= \lambda^2 f''(\lambda)/f(\lambda) + \psi(\lambda) - (\psi(\lambda))^2 = \lambda \psi'(\lambda). \end{aligned} \tag{3.4}$$

(With $\psi = x f'(x)/f(x)$, (3.3) and (3.4) hold for f and Z defined by any series $a_j x^j$, not just $x^j/j!$, assuming convergence.)

From (3.4) it is immediate that $\psi'(\lambda) > 0$ for any $\lambda > 0$. (See also a general formulation in [31, Chapter 4, problem 6, p. 77].) The next claim shows that ψ is convex as well as increasing, and establishes both facts for all λ (though we only require them for positive λ).

Claim 3.1. *$\psi(x)$ is strictly increasing, and convex.*

https://doi.org/10.1017/S0963548315000097 Published online by Cambridge University Press

Proof. We begin with convexity. From (3.1) it is easy to check that $\psi(x) = x + x^2/f(x)$, which in turn eases the calculation of $\psi''(x)$, showing that $\psi''(x) = g(x)/f^3(x)$, where

$$g = 2f^2 - 4xf'f - x^2 f''f + 2x^2(f')^2. \tag{3.5}$$

Write $g(x) = \sum_{j\geqslant 0} g_j x^j$. Expanding (3.5), substituting

$$x^a e^{bx} = \sum_{j\geqslant 0} \frac{b^j x^{a+j}}{j!},$$

and collecting like terms, we find that $g_j = 0$ for $j \leqslant 5$, while for all $j \geqslant 6$,

$$g_j = \frac{j-1}{j!}\left[2^{j-2}(j-8) + j^2 - j + 4\right] > 0.$$

Positivity is trivial for $j \geqslant 8$ and easily checked for $j = 6$ and 7. This establishes that $g(x) > 0$ for $x > 0$. Substituting $x = -y$ in $g(x)$, writing $g(x) = e^{-2y}\sum_{j\geqslant 0} g'_j y^j$, and using the same method yields $g'_j = 0$ for $j \leqslant 5$, while for $j \geqslant 6$,

$$g'_j = \frac{1}{j!}(2^{j+1} - j^3 + 4j^2 - 7j - 4) > 0.$$

This establishes that $g(x) > 0$ for $x < 0$. Finally, $\psi''(0) = 1/9$. Therefore $\psi''(x) > 0$ for all x.

That $\psi'(x) > 0$ follows from $\lim_{x\to-\infty}\psi'(x) = 0$ and $\psi'' > 0$. □

Under our assumption that $m/n > 2/k$, the equation $\psi(x) = km/n$ has a unique root, and it is positive. This follows from the facts that $\psi(x)$ is strictly increasing (see Claim 3.1), $\psi(0) = 2$, and $\psi(x) \to \infty$ as $x \to \infty$. Henceforth, let

$$\lambda = \lambda(km/n) := \psi^{-1}(km/n) \tag{3.6}$$

be this root. Since by Claim 3.1 ψ is strictly increasing, so is $\lambda = \psi^{-1}$.

From (3.3) and (3.6),

$$\mathbb{E}[Z(\lambda)] = \psi(\lambda) = \frac{km}{n}. \tag{3.7}$$

From Claim 3.1, for $\lambda > 0$, $\psi'(\lambda)$ lies between $\psi'(0) = 1/3$ and $\lim_{x\to\infty}\psi'(x) = 1$, and thus

$$\mathrm{Var}[Z(\lambda)] = \lambda\psi'(\lambda) = \Theta(\lambda). \tag{3.8}$$

With these preliminaries done, we focus on asymptotics of $|\mathcal{A}_{m,n}|$, $|\mathcal{B}_{m,n}|$ and $|\mathcal{C}_{m,n}|$.

Lemma 3.2. *Suppose $m, n \to \infty$ with $\lim m/n \in (2/k, \infty)$. Then, with λ as in (3.6),*

$$|\mathcal{C}_{m,n}| = \frac{1 + O(n^{-1})}{\sqrt{2\pi n\,\mathrm{Var}[Z(\lambda)]}}(km)!\frac{f(\lambda)^n}{\lambda^{km}}, \tag{3.9}$$

$$\frac{|\mathcal{B}_{m,n}|}{|\mathcal{C}_{m,n}|} = \exp\left(-\frac{k-1}{2}\,\frac{\lambda e^\lambda}{e^\lambda - 1}\right) + o(1), \tag{3.10}$$

https://doi.org/10.1017/S0963548315000097 Published online by Cambridge University Press

so that the fraction $|\mathcal{B}_{m,n}|/|\mathcal{C}_{m,n}|$ *is bounded away from zero. Consequently*

$$|\mathcal{A}_{m,n}| = \frac{|\mathcal{B}_{m,n}|}{(k!)^m} = \frac{1+o(1)}{\sqrt{2\pi n \operatorname{Var}[Z(\lambda)]}} \frac{(km)!}{(k!)^m} \frac{f(\lambda)^n}{\lambda^{km}} \exp\left(-\frac{k-1}{2}\frac{\lambda e^\lambda}{e^\lambda - 1}\right). \tag{3.11}$$

Corollary 3.3. *Under the hypotheses of Lemma 3.2, uniformly for all non-negative, matrix-dependent functions r,*

$$\mathbb{E}[r(A)] = \mathbb{E}[r(B)] = O(\mathbb{E}[r(C)]).$$

Proof. The first equality is trivial. To show the second, for any $S \subseteq \mathcal{B}_{m,n}$,

$$\begin{aligned} \mathbb{P}(B \in S) &= \mathbb{P}(C \in S \mid C \in \mathcal{B}_{m,n}) \\ &= \frac{\mathbb{P}(C \in S,\, C \in \mathcal{B}_{m,n})}{|\mathcal{B}_{m,n}|\,/\,|\mathcal{C}_{m,n}|} \leqslant \frac{|\mathcal{C}_{m,n}|}{|\mathcal{B}_{m,n}|}\,\mathbb{P}(C \in S) = O(1)\,\mathbb{P}(C \in S) \end{aligned} \tag{3.12}$$

by (3.10). □

Proof of Lemma 3.2. Equation (3.11) is immediate from (3.9) and (3.10). Proving (3.9) and (3.10) will occupy the rest of this section.

(3.9) To determine $|\mathcal{C}_{m,n}|$, recall that each row $i \in m$ is given its own k, mutually distinguishable, chips, so we may think of all km chips as distinguishable. An allocation $C \in \mathcal{C}_{m,n}$ thus corresponds uniquely to choosing some $j_1 \geqslant 2$ chips for column 1 (the chips' rows are determined by their identities), some $j_2 \geqslant 2$ chips for column 2, and so on, with $j_1 + \cdots + j_n = km$. Given $j_1, \ldots, j_n$, the number of such allocations is the multinomial coefficient $(km)!/(j_1! \cdots j_n!)$, so $|\mathcal{C}_{m,n}|$ is the sum of these coefficients.

This sum is conveniently expressed through the distribution of the sum of independent copies of the truncated Poisson random variable $Z(\lambda)$ defined in (3.2). The probability generating function (p.g.f) of $Z(\lambda)$ is given by

$$\mathbb{E}[z^{Z(\lambda)}] = \frac{f(z\lambda)}{f(\lambda)}. \tag{3.13}$$

Following the notational convention that for $h(z) = \sum_j h_j z^j$, $[z^j]\,h(z) := h_j$, we have

$$\begin{aligned} |\mathcal{C}_{m,n}| &= \sum_{\substack{j_1+\cdots+j_n=km \\ j_1,\ldots,j_n \geqslant 2}} \frac{(km)!}{j_1! \cdots j_n!} \\ &= (km)!\,[z^{km}]\left(\sum_{j \geqslant 2} \frac{z^j}{j!}\right)^n = (km)!\,[z^{km}] f(z)^n \qquad (3.14) \\ &= (km)! \frac{f(\lambda)^n}{\lambda^{km}}\,[z^{km}]\left(\frac{f(z\lambda)}{f(\lambda)}\right)^n \\ &= (km)! \frac{f(\lambda)^n}{\lambda^{km}}\,[z^{km}]\big(\mathbb{E}[z^{Z(\lambda)}]\big)^n \quad \text{(see (3.13))} \\ &= (km)! \frac{f(\lambda)^n}{\lambda^{km}}\,\mathbb{P}\left(\sum_{j=1}^n Z_j(\lambda) = km\right), \qquad (3.15) \end{aligned}$$

https://doi.org/10.1017/S0963548315000097 Published online by Cambridge University Press

where $Z_1(\lambda), \dots, Z_n(\lambda)$ are independent copies of $Z(\lambda)$. Now, since $\mathrm{Var}[Z(\lambda)] = \Theta(\lambda)$ (by (3.8)) and $\liminf \lambda > 0$ (by $\lambda = \lambda(km/n)$ and the hypothesis that $\lim m/n > 2/k$), we have $\liminf \mathrm{Var}[Z(\lambda)] > 0$. So, by a local limit theorem (Aronson, Frieze and Pittel [2, equation (5)]),

$$\mathbb{P}\bigg(\sum_{j=1}^{n} Z_j(\lambda) = km\bigg) = \mathbb{P}\bigg(\sum_{j=1}^{n} Z_j(\lambda) = n\mathbb{E}[Z(\lambda)]\bigg) = \frac{1+O(n^{-1})}{\sqrt{2\pi n \mathrm{Var}[Z(\lambda)]}},$$

which proves (3.9).

(3.10) Let $C = \{c_{i,j}\}$ be distributed uniformly on $\mathcal{C}_{m,n}$. Let M denote the number of cells that house two or more chips, that is, $M = |\{(i,j) : c_{i,j} \geqslant 2\}|$. Let $\overline{M}$ be the number of pairs of chips hosted by the same cell, that is,

$$\overline{M} = \sum_{(i,j)\,:\, c_{i,j} \geqslant 2} \binom{c_{i,j}}{2} = \sum_{(i,j)} \binom{c_{i,j}}{2}.$$

$\overline{M} = M$ if and only if there are no cells hosting more than two chips. Clearly

$$\frac{|\mathcal{B}_{m,n}|}{|\mathcal{C}_{m,n}|} = \mathbb{P}(C \in \mathcal{B}_{m,n}) = \mathbb{P}(\overline{M} = 0).$$

Of course, $\mathbb{P}(\overline{M} = 0) = \mathbb{P}(M = 0)$, but, unlike M, $\overline{M}$ is amenable to moment calculations.

Denoting the indicator of an event E by $\mathbf{1}(E)$, we write

$$\overline{M} = \sum_{i \in [m],\, j \in [n]} \sum_{1 \leqslant u < v \leqslant k} \mathbf{1}\big(E(i,j;u,v)\big), \tag{3.16}$$

where $E(i,j;u,v)$ is the event that, of the k chips owned by row i, at least the two chips u and v were put into cell (i,j). Each of these $mn\binom{k}{2}$ event indicators has the same expected value,

$$\mathbb{E}[\mathbf{1}(E(i,j;u,v))] = (km-2)!\, \frac{[x^{km-2}] f(x)^{n-1} e^x}{|\mathcal{C}_{m,n}|}. \tag{3.17}$$

To see why (3.17) is so, compare with (3.14) and note that once we have put two selected chips into a cell (i,j) we allocate the remaining $(km-2)$ chips amongst n columns, at least two per column, with the exception (hence the sole e^x factor) that the jth column receives an unconstrained number of additional chips (as it already has two). Arguing as for (3.15),

$$[x^{km-2}] f(x)^{n-1} e^x = \frac{f(\lambda)^{n-1} e^{\lambda}}{\lambda^{km-2}}\, \mathbb{P}\bigg(\sum_{j=1}^{n-1} Z_j(\lambda) + X(\lambda) = km-2\bigg), \tag{3.18}$$

where $X(\lambda)$ stands for an independent, usual (not truncated) Poisson(λ) random variable. This last probability equals

$$\sum_r \bigg[\mathbb{P}(\mathrm{Po}(\lambda) = r) \cdot \mathbb{P}\bigg(\sum_{j=1}^{n-1} Z_j(\lambda) = km-2-r\bigg)\bigg].$$

By the local limit theorem for $\sum_{j=1}^{n-1} Z_j(\lambda)$, for $r \leqslant \ln n$ the second probability in the rth term of the sum is again asymptotic to $(2\pi n \operatorname{Var}[Z(\lambda)])^{-1/2}$. Then so is the probability in (3.18), since $\mathbb{P}(X(\lambda) > \ln n) = O(n^{-K})$, for every $K > 0$. From this, (3.16), (3.17), (3.18) and (3.9),

$$\mathbb{E}[\overline{M}] = (1 + o(1)) \frac{mn\binom{k}{2}}{(km)_2} \frac{\lambda^2 e^{\lambda}}{f(\lambda)}$$

with the usual falling-factorial notation $(a)_b := a(a-1)\cdots(a-b+1)$. Recalling (3.6) and setting

$$\gamma := \frac{k-1}{2} \frac{\lambda e^{\lambda}}{e^{\lambda}-1} \tag{3.19}$$

gives

$$\mathbb{E}[\overline{M}] = \gamma + o(1).$$

More generally, we now show that for every fixed $t \geqslant 1$ we have

$$\mathbb{E}[(\overline{M})_t] = \gamma^t + o(1). \tag{3.20}$$

Let $\boldsymbol{T}$ be the set of all 4-tuples (i, j, u, v) as before, with $i \in [m]$, $j \in [n]$, and $1 \leqslant u < v \leqslant k$. Now let $(\boldsymbol{T})_t$ denote the collection of t-tuples of such 4-tuples with all the 4-tuples distinct. Where $((i_\tau, j_\tau, u_\tau, v_\tau))_{\tau=1}^t \in (\boldsymbol{T})_t$, in a slight abuse of notation we will write $(\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{u}, \boldsymbol{v}) \in (\boldsymbol{T})_t$, where $\boldsymbol{i} = (i_1, \ldots, i_t)$, $\boldsymbol{j} = (j_1, \ldots, j_t)$, $\boldsymbol{u} = (u_1, \ldots u_t)$, $\boldsymbol{v} = (v_1, \ldots, v_t)$. Then we have

$$(\overline{M})_t = \sum_{(\boldsymbol{i},\boldsymbol{j},\boldsymbol{u},\boldsymbol{v}) \in (\boldsymbol{T})_t} \mathbf{1}\left(\bigcap_{s=1}^{t} E(i_t, j_t; u_t, v_t)\right),$$

hence

$$\mathbb{E}[(\overline{M})_t] = \sum_{(\boldsymbol{i},\boldsymbol{j},\boldsymbol{u},\boldsymbol{v}) \in (\boldsymbol{T})_t} \mathbb{P}\left(\bigcap_{s=1}^{t} E(i_t, j_t; u_t, v_t)\right).$$

We break the sum into two parts, Σ_1 and the remainder Σ_2, where Σ_1 is the restriction to $\boldsymbol{i}$ and $\boldsymbol{j}$ each having all its components distinct. In Σ_1 the number of summands is $(m)_t (n)_t \binom{k}{2}^t$, and each summand is

$$(km-2t)! \, \frac{[x^{km-2t}] \, f(x)^{n-t} (e^x)^t}{|\mathcal{C}_{m,n}|};$$

see the explanation following (3.17). Analogously to (3.18),

$$[x^{km-2t}] f(x)^{n-t} (e^x)^t = \frac{f(\lambda)^{n-t} (e^{\lambda})^t}{\lambda^{km-2t}} \, \mathbb{P}\left(\sum_{j=1}^{n-t} Z_j(\lambda) + \sum_{s=1}^{t} X_s(\lambda) = km - 2t\right),$$

where the n truncated and ordinary Poisson random variables $Z_j(\lambda)$ and $X_s(\lambda)$ are mutually independent. Since t is fixed, the probability remains asymptotic to $(2\pi n \operatorname{Var}[Z(\lambda)])^{-1/2}$.

So, using (3.9) and recalling (3.19) and as ever (3.6), we have

$$\begin{aligned}\Sigma_1 &\sim \frac{(m)_t(n)_t\binom{k}{2}^t}{(km)_{2t}}\left(\frac{\lambda^2 e^\lambda}{f(\lambda)}\right)^t\\ &\sim \left[\frac{mn\binom{k}{2}}{(km)^2}\,\frac{\lambda^2 e^\lambda}{f(\lambda)}\right]^t = \gamma^t. \end{aligned} \tag{3.21}$$

In the case of Σ_2, letting $I = \{i_1, \ldots, i_t\}$, $J = \{j_1, \ldots, j_t\}$, we have $|I| + |J| \leqslant 2t - 1$. So the number of attendant pairs (I, J) is at most $(m+n)^{2t-1} = O\big(m^{2t-1}\big)$. The number of pairs $(\boldsymbol{i}, \boldsymbol{j})$ inducing a given pair (I, J) is bounded above by a constant $s(t)$. For every one of those $s(t)$ choices, we select pairs of chips for each of the chosen t cells; there are at most $\binom{k}{2}^t$ ways of doing so. Lastly, we allocate the remaining $(km-2t)$ chips in such a way that every column $j \in [n] \setminus J$ gets at least two chips. As in the case of Σ_1, this can be done in

$$\begin{aligned}&(km-2t)!\,[x^{km-2t}]\,f(x)^{n-|J|}(e^x)^{|J|}\\ &\quad= (km-2t)!\,\frac{f(\lambda)^{n-|J|}(e^\lambda)^{|J|}}{\lambda^{km-2t}}\;\mathbb{P}\Bigg(\sum_{j=1}^{n-|J|} Z_j(\lambda) + \sum_{s=1}^{|J|}\mathrm{Po}_s(\lambda) = km-2t\Bigg)\end{aligned}$$

ways. Again, the probability is asymptotic to $\big(2\pi n \mathrm{Var}[Z(\lambda)]\big)^{-1/2}$. So, as $e^\lambda > f(\lambda)$, the sum Σ_2 is of order

$$m^{2t-1}\,\frac{(km-2t)!}{(km)!}\left(\frac{e^\lambda\lambda^2}{f(\lambda)}\right)^t = O(m^{2t-1}/m^{2t}) = O(m^{-1}). \tag{3.22}$$

Combining (3.21) and (3.22), and recalling (3.19), we conclude that for each fixed $t \geqslant 1$,

$$\mathbb{E}[(\overline{M})_t] = \gamma^t + o(1).$$

Therefore $\overline{M}$ is asymptotic, with all its moments and in distribution, to $\mathrm{Po}(\gamma)$. In particular,

$$\mathbb{P}(\overline{M} = 0) = \mathbb{P}(\mathrm{Po}(\gamma) = 0) + o(1) = e^{-\gamma} + o(1).$$

This completes the proof of Lemma 3.2. □

4. Counting critical row subsets, and the main result

This section will prove Theorem 1.1. Remark 1 already dealt with the case $\lim m/n > 1$. It suffices, then, to show that with $\lim m/n \in (2/k, 1)$, the expected number of non-empty critical row sets goes to 0: then with high probability there is no such set, A is of full rank, and the instance is satisfiable.

In the model $\mathcal{C}_{m,n}$, Lemma 4.1 gives an upper bound on the expected number of critical row sets of each cardinality $\ell \in \{1, \ldots, m\}$ as a function of $c = m/n$, k, n, and ℓ, minimized over two additional variables ζ_1 and ζ_2. Lemma 4.2 shows that, for $c \in (2/k, 1)$, there exist values for ζ_1 and ζ_2 making this bound small, in particular making its exponential dependence on n decreasing rather than increasing. Corollary 4.3 uses Lemma 4.2 to show that in the model $\mathcal{A}_{m,n}$ the total expected number of non-empty critical row sets is of order $O\big(m^{-(k-2)}\big)$, proving Theorem 1.1.

Lemma 4.2 is established by several claims deferred to Section 5, and Section 7 extends Theorem 1.1 to the unconstrained k-XORSAT model (Theorem 7.1).

Lemma 4.1. *Suppose $k \geqslant 3$ and $m, n \to \infty$ with $\lim m/n \in (2/k, \infty)$, and let C be chosen uniformly at random from $\mathcal{C}_{m,n}$. For $\ell \in \{1, \dots, m\}$, let $Y_{m,n}^{(\ell)}$ denote the number of critical row sets of C of cardinality ℓ. Then, with $c = m/n$, $\alpha = \ell/m$, $\bar{\alpha} = 1 - \alpha$, $\lambda = \lambda(ck)$ as given by* (3.6), *and $\boldsymbol{\zeta} = (\zeta_1, \zeta_2) > \mathbf{0}$,*

$$\mathbb{E}\big[Y_{m,n}^{(\ell)}\big] \leqslant O(1)\sqrt{\frac{1}{\zeta_2}}\exp\big[nH_k(\alpha, \boldsymbol{\zeta}\,; c)\big], \quad \textit{for all } \boldsymbol{\zeta} > 0, \tag{4.1}$$

where

$$\begin{aligned} H_k(\alpha, \boldsymbol{\zeta}\,; c) = {} & cH(\alpha) + ck\alpha \ln(\alpha/\zeta_1) + ck\bar{\alpha}\ln(\bar{\alpha}/\zeta_2) \\ & + \ln \frac{f(\lambda\cdot(\zeta_2+\zeta_1)) + f(\lambda\cdot(\zeta_2-\zeta_1))}{2f(\lambda)}, \end{aligned} \tag{4.2}$$

by continuity we define $x \ln x = 0$ at $x = 0$, and $H(\alpha)$ is the usual entropy function

$$H(\alpha) := -\alpha \ln \alpha - (1-\alpha)\ln(1-\alpha).$$

Proof. By symmetry,

$$\mathbb{E}[Y_{m,n}^{(\ell)}] = \binom{m}{\ell}\mathbb{P}(\mathcal{D}_\ell); \quad \mathcal{D}_\ell := \bigcap_{j=1}^{n}\left\{\sum_{i=1}^{\ell} c_{i,j} \text{ is even}\right\}. \tag{4.3}$$

By symmetry again,

$$\mathbb{P}(\mathcal{D}_\ell) = \sum_{v=1}^{n}\binom{n}{v}\mathbb{P}(\mathcal{D}_{\ell,v}), \tag{4.4}$$

where

$$\mathcal{D}_{\ell,v} := \bigcap_{j=1}^{v}\left\{\sum_{i=1}^{\ell} c_{i,j} \text{ is even, positive}\right\} \bigcap \bigcap_{j=v+1}^{n}\left\{\sum_{i=1}^{\ell} c_{i,j} = 0\right\}. \tag{4.5}$$

Recalling that $\sum_{i\in[m]} c_{i,j} \geqslant 2$, we see that on the event $\mathcal{D}_{\ell,v}$,

$$\sum_{i\leqslant\ell} c_{i,j} = \begin{cases} \text{even } > 0, & j \leqslant v, \\ 0, & j > v, \end{cases} \qquad \sum_{i>\ell} c_{i,j} \geqslant \begin{cases} 0, & j \leqslant v, \\ 2, & j > v. \end{cases} \tag{4.6}$$

Thus on $\mathcal{D}_{\ell,v}$ the column sums of the two complementary submatrices,

$$\{c_{i,j}\}_{i\leqslant\ell, j\in[n]}, \quad \{c_{i,j}\}_{i>\ell, j\in[n]},$$

are subject to independent constraints.

Let $\mathcal{C}_{m,n}(\ell, v)$ denote the set of all matrices C with row sums k which meet the constraints (4.6). Then $\mathbb{P}(\mathcal{D}_{\ell,v})$ is given by

$$p(\ell, v) := \mathbb{P}(\mathcal{D}_{\ell,v}) = \frac{|\mathcal{C}_{m,n}(\ell, v)|}{|\mathcal{C}_{m,n}|}. \tag{4.7}$$

https://doi.org/10.1017/S0963548315000097 Published online by Cambridge University Press

By the independence of constraints on column sums for the upper and the lower submatrices of the matrices C in question,

$$|\mathcal{C}_{m,n}(\ell, v)| = a(\ell, v) \cdot b(m-\ell, v), \tag{4.8}$$

where (paralleling our definition of $\mathcal{C}_{m,n}$ in Section 3) $a(\ell, v)$ is the number of ways to assign $k\ell$ chips among the first v columns so that each of those columns gets a positive even number of chips, and $b(m-\ell, v)$ is the number of ways to assign $k(m-\ell)$ chips among all n columns so that each of the last $(n-v)$ columns gets at least two chips.

As in (3.15),

$$\begin{aligned} a(\ell, v) &= \sum_{\substack{j_1+\cdots+j_v=k\ell \\ j_s>0,\text{ even}}} \frac{(k\ell)!}{j_1!\cdots j_v!} \\ &= (k\ell)!\,[z^{k\ell}]\biggl(\sum_{j>0,\text{ even}} \frac{z^j}{j!}\biggr)^v \\ &= (k\ell)!\,[z^{k\ell}](\cosh z - 1)^v, \end{aligned} \tag{4.9}$$

and

$$\begin{aligned} b(m-\ell, v) &= \sum_{\substack{j_1+\cdots+j_n=k(m-\ell) \\ j_1,\ldots,j_v\geqslant 0;\; j_{v+1},\ldots,j_n\geqslant 2}} \frac{(k(m-\ell))!}{j_1!\cdots j_n!} \\ &= (k(m-\ell))!\,[z^{k(m-\ell)}](e^z)^v f(z)^{n-v}. \end{aligned} \tag{4.10}$$

Since the coefficients of the Taylor expansion around $z=0$ of $e^{zv}f(z)^{n-v}$ are non-negative, we use these identities in a standard (Chernoff) way to bound

$$a(\ell, v) \leqslant (k\ell)!\,\frac{(\cosh z_1 - 1)^v}{z_1^{k\ell}}, \quad \text{for all } z_1 > 0. \tag{4.11}$$

We could control $b(m-\ell, v)$ similarly, but we need a stronger bound, namely

$$b(m-\ell, v) \leqslant O(1)\,(nz_2)^{-1/2}(k(m-\ell))!\,\frac{(e^{z_2})^v f(z_2)^{n-v}}{z_2^{k(m-\ell)}}, \quad \text{for all } z_2 > 0. \tag{4.12}$$

The bound (4.12) follows from three components: the Cauchy integral formula

$$b(m-\ell, v) = \frac{(k(m-\ell))!}{2\pi} \oint_{\substack{z=z_2e^{i\theta}: \\ \theta\in(-\pi,\pi]}} \frac{(e^z)^v f(z)^{n-v}}{z^{k(m-\ell)+1}}\,dz,$$

and (with $z = z_2e^{i\theta}$) the identity $|e^z| = e^{z_2}\exp[-z_2(1-\cos\theta)]$ and the less obvious inequality

$$|f(z)| \leqslant |f(z_2)|\exp[-z_2(1-\cos\theta)/3]. \tag{4.13}$$

(See Pittel [26, Appendix] for the inequality, and Aronson, Frieze and Pittel [2, inequality (A2)] for how it works in combination with the Cauchy formula.)

Using (4.7), (4.8), (4.11), (4.12), with $|\mathcal{C}_{m,n}|$ from (3.9) and $\operatorname{Var} Z(\lambda)$ from (3.8), we obtain that, for all $z_1, z_2 > 0$,

$$p(\ell, v) \leqslant O(1)\sqrt{\frac{\lambda}{z_2}}\binom{km}{k\ell}^{-1}\frac{\lambda^{km}}{z_1^{k\ell}\, z_2^{k(m-\ell)}}\,\frac{[e^{z_2}(\cosh z_1 - 1)]^{v} f(z_2)^{n-v}}{f(\lambda)^{n}}. \tag{4.14}$$

Now, it is immediate from (4.3), (4.4) and (4.7) that

$$\mathbb{E}\big[Y_{m,n}^{(\ell)}\big] = \binom{m}{\ell}\sum_{v=1}^{n}\binom{n}{v} p(\ell, v). \tag{4.15}$$

If we restrict to z_1 and z_2 depending only on ℓ, m and n (not on v), then on substituting (4.14) into (4.15) we may simplify the sum using the binomial formula to obtain

$$\begin{aligned}\mathbb{E}\big[Y_{m,n}^{(\ell)}\big] &\leqslant O(1)\sqrt{\frac{\lambda}{z_2}}\binom{m}{\ell}\binom{km}{k\ell}^{-1}\lambda^{km}\\ &\quad\times\frac{1}{z_1^{k\ell}\, z_2^{k(m-\ell)}}\left(\frac{f(z_2)+e^{z_2}(\cosh z_1 - 1)}{f(\lambda)}\right)^{n}, \quad \text{for all } z_1, z_2 > 0.\end{aligned} \tag{4.16}$$

Observe that

$$f(z_2) + e^{z_2}(\cosh z_1 - 1) = \frac{f(z_1+z_2) + f(z_2 - z_1)}{2}.$$

Inequality (4.1), and thus the lemma, are established by substituting this and the Stirling-based approximation

$$\binom{n}{pn} = O(1)\frac{1}{\sqrt{np(1-p)}}\exp(nH(p))$$

into (4.16), recalling that $m = cn$, $\alpha = \ell/m$ and $\bar{\alpha} = 1-\alpha$, substituting $z_1 = \zeta_1\lambda$ and $z_2 = \zeta_2\lambda$, and observing that $\sqrt{k} = O(1)$. For $\ell = m$ the Stirling-based approximation is inapplicable, but consistency of (4.1) with (4.16) is easily checked. □

Recall the definition of $H_k(\alpha, \zeta; c)$ from (4.2). Roughly speaking, the following lemma establishes the existence of ζ making $H_k(\alpha, \zeta; c)$ negative. An intuitive description of the behaviour of $H_k(\alpha, \zeta; c)$ is given at the start of the next section.

Lemma 4.2. *Let*

$$\alpha_k = ek^{-k/(k-2)}. \tag{4.17}$$

For all $k \geqslant 4$ and $c \in (2/k, 1)$, there exist $\varepsilon = \varepsilon(c,k) > 0$ and $\zeta_0 = \zeta_0(c,k) > 0$, both functions continuous in c, such that

$$\big(\forall\alpha \in (0, \alpha_k]\big)(\exists\zeta) : H_k(\alpha, \zeta; c) \leqslant (c\alpha)\big(\tfrac{k}{2} - 1\big)\ln(\alpha/\alpha_k) \text{ and } \zeta_2 \geqslant \zeta_0 \tag{4.18}$$

$$\big(\forall\alpha \in [\alpha_k/3, 1]\big)(\exists\zeta) : H_k(\alpha, \zeta; c) \leqslant -\varepsilon \text{ and } \zeta_2 \geqslant \zeta_0. \tag{4.19}$$

Proof. The lemma follows immediately from Claims 5.1, 5.2 and 5.3, all stated and proved in Section 5, treating α in the ranges $(0, 0.99\alpha_k]$, $[0.99\alpha_k, 1/2]$ and $(1/2, 1]$ respectively. A suitable function ζ is given explicitly in each case. □

https://doi.org/10.1017/S0963548315000097 Published online by Cambridge University Press

The lemma yields the following corollary.

Corollary 4.3. *For $k \geqslant 4$ and $m,n \to \infty$ with $\lim m/n \in (2/k,1)$,*

$$\sum_{\ell=2}^{m} \mathbb{E}\big[Y_{m,n}^{(\ell)}\big] = O\big(m^{-(k-2)}\big).$$

Proof. Since $\lim m/n \in (2/k,1)$, there exists a closed interval $I \subset (2/k,1)$ such that, for all but finitely many cases, $c = m/n \in I$. Where $\varepsilon(c,k)$ and $\zeta_0(c,k)$ satisfy the conditions of Lemma 4.2 define $\varepsilon = \varepsilon(I) = \min\{\varepsilon(c,k) : c \in I\}$, and $\zeta_0 = \zeta_0(I)$ likewise; the minima exist by continuity of ε and ζ_0 in c. Then, for all but finitely many pairs m,n, inequalities (4.18) and (4.19) hold true.

Letting $\ell_k = \alpha_k m = \Theta(n)$, for $\ell \leqslant \ell_k/2$, recalling that $\alpha c n = \alpha m = \ell$, (4.1) and (4.18) give

$$\mathbb{E}\big[Y_{m,n}^{(\ell)}\big] = O(1)\,\exp\big[\big(\tfrac{k}{2}-1\big)\ell\ln(\ell/\ell_k)\big], \tag{4.20}$$

where we have incorporated $\sqrt{1/\zeta_0}$ in the leading $O(1)$. By convexity of $\ell\ln(\ell/\ell_k)$, interpolating for $\ell \in [2,\ell_k/2]$ from the endpoints of this interval,

$$\begin{aligned}\ell\ln(\ell/\ell_k) &\leqslant 2\ln(2/\ell_k) + \frac{\ell-2}{\ell_k/2-2}\big((\ell_k/2)\ln(1/2) - 2\ln(2/\ell_k)\big)\\ &= 2\ln(2/\ell_k) + (\ell-2)(-\ln 2 + o(1)),\\ &\leqslant 2\ln(2/\ell_k) - 0.6(\ell-2)\end{aligned}$$

for n sufficiently large, where we have used $\ell_k = \Theta(n)$ and $0.6 < \ln 2$. Thus, for $\ell \in [2,\ell_k/2]$,

$$\begin{aligned}\mathbb{E}\big[Y_{m,n}^{(\ell)}\big] &\leqslant O(1)\,\exp\big(\big(\tfrac{k}{2}-1\big)[2\ln(2/\ell_k) - 0.6(\ell-2)]\big)\\ &= O(1)\,m^{-(k-2)}\exp\big(-0.6\big(\tfrac{k}{2}-1\big)(\ell-2)\big),\end{aligned}$$

where the last line incorporates $(2/\alpha_k)^{k-2}$ in the $O(1)$. Given this upper bound that is geometrically decreasing in ℓ, summing gives

$$\sum_{\ell=2}^{\lfloor(\alpha_k/2)m\rfloor} \mathbb{E}\big[Y_{m,n}^{(\ell)}\big] = O\big(m^{-(k-2)}\big).$$

For $\ell > (\alpha_k/2)m$, by (4.19), we have $\mathbb{E}\big[Y_{m,n}^{(\ell)}\big] = O(1)\exp(-\varepsilon n)$, giving

$$\sum_{\ell=\lceil(\alpha_k/2)m\rceil}^{m} \mathbb{E}\big[Y_{m,n}^{(\ell)}\big] = O(m)\exp(-\varepsilon n) = \exp(-\Omega(n)).$$

Adding the two partial sums yields Corollary 4.3. □

Proof of Theorem 1.1. By the remarks at the start of this section, we need only consider the case $\lim m/n \in (2/k,1)$. Under the hypotheses of Corollary 4.3, let $A \in \mathcal{A}_{m,n}$ and $C \in \mathcal{C}_{m,n}$ be uniformly random, and let $X_{m,n}$ and $Y_{m,n}$ denote the numbers of non-empty critical row sets of A and C respectively, and $X_{m,n}^{(\ell)}$ and $Y_{m,n}^{(\ell)}$ those of cardinality ℓ. $X_{m,n}^{(1)} = 0$

https://doi.org/10.1017/S0963548315000097 Published online by Cambridge University Press

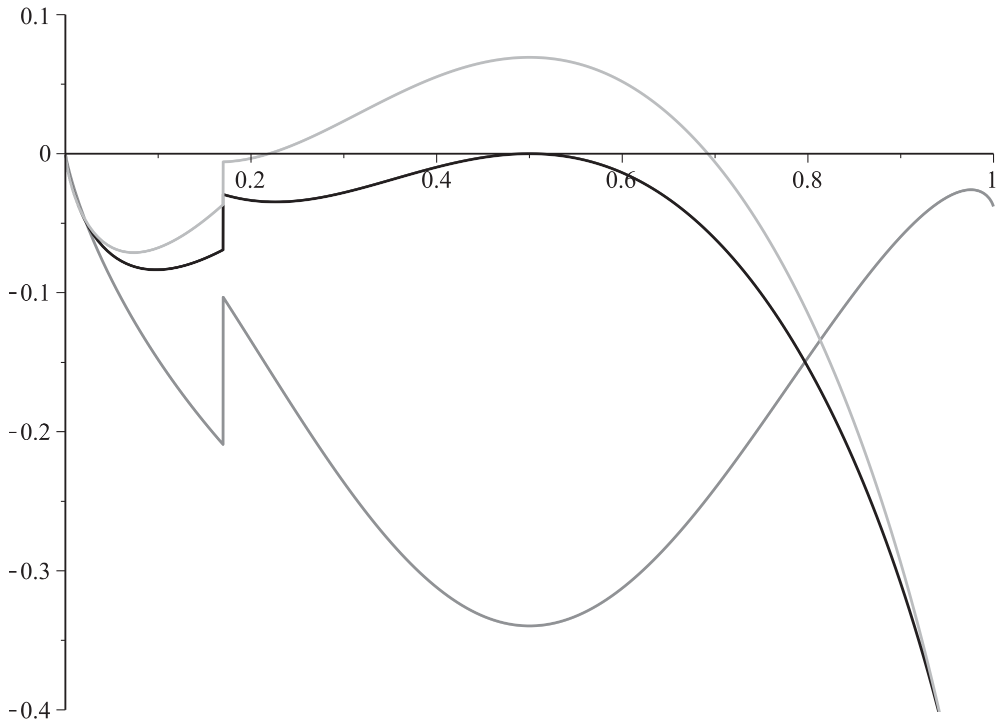

Figure 1. Plot of $H_k(\alpha,\zeta;c)$ versus α, for $k=4$ and c values of 0.51, 1.0, 1.1 (from bottom to top). The kinks occur at α_k, where we switch functional forms for $\zeta(c,k,\alpha)$.

since every row of A has k ones. (The bound on $Y^{(1)}_{m,n}$ from (4.20) is $O(m^{-(k/2-1)})$, whose use would weaken the corollary's conclusion. $Y^{(1)}_{m,n}$ is not necessarily 0 since a row of C can be 0, for example if all the ones in its defining configuration lie in a single cell.) Then

$$\mathbb{E}\big[X_{m,n}\big] = 0 + \sum_{\ell=2}^{m} \mathbb{E}\big[X^{(\ell)}_{m,n}\big] = O(1)\sum_{\ell=2}^{m} \mathbb{E}\big[Y^{(\ell)}_{m,n}\big] = O\big(m^{-(k-2)}\big),$$

the last two equalities coming from Corollaries 4.3 and 3.3. Then $\mathbb{P}(A$ is not of full rank$) \leqslant \mathbb{E}[X_{m,n}] = O(m^{-(k-2)})$, so with probability $1-O(m^{-(k-2)})$, A is of full rank and any system $Ax=b$ is satisfiable. □

5. Analysis of the function $H_k(\alpha,\zeta;c)$ to prove Lemma 4.2

Recall the notation $\bar{\alpha} = 1-\alpha$ and $\boldsymbol{\zeta} = (\zeta_1,\zeta_2)$ as well as the definition of $H_k(\alpha,\boldsymbol{\zeta};c)$ from (4.2). In this section we use an explicit function $\boldsymbol{\zeta} = \boldsymbol{\zeta}(c,k,\alpha)$, taking different forms in different ranges of α, to establish Claims 5.1, 5.2 and 5.3 and thus Lemma 4.2.

For intuition about $H_k(\alpha,\boldsymbol{\zeta};c)$, the case $k=4$ is indicative. Figure 1 shows a graph of the function value against α, for a few choices of c, with $\boldsymbol{\zeta}$ given by (5.1) for small α, and by $\boldsymbol{\zeta} = (\alpha,\bar{\alpha})$ otherwise. Numerical experiments suggest that the optimal choice of $\boldsymbol{\zeta}$ leads

https://doi.org/10.1017/S0963548315000097 Published online by Cambridge University Press

to qualitatively similar results, though of course without the kinks where we change from one functional form for ζ to another. As shown, $H_k(\alpha,\zeta;c)$ tends to 0 at $\alpha = 0$ (treated in Claim 5.1), but the dependence on c here is not critical: an analogue of the claim, with different parameters, could be obtained as long as c is bounded away from 0 and infinity. At $\alpha = 1/2$ (treated in Claim 5.2), the function tends to 0 as c tends to 1, so this is where $c < 1$ is required. Claim 5.2 also covers values of α between 0 and 1/2 but bounded away from them; here the function value is bounded away from 0 (for $c \leqslant 1$) and could be dealt with by cruder means, such as that by interval arithmetic in [28]. Function values for $\alpha > 1/2$ (treated in Claim 5.3) are dominated by their symmetric counterparts at $1-\alpha$, except for some special treatment required near 1.

Lemma 4.2 only considers $k > 3$. The lemma can be extended to $k = 3$, but this case was already treated by [16] and the proof poses additional difficulties for us; see further discussion after the proof of Claim 5.2, and in Section 6, specifically at (6.4).

Claim 5.1. *For all $k \geqslant 3$ and all $c \in (2/k, 1]$, taking*

$$\zeta_1 = (ck)^{-1/2}\alpha^{1/2}, \quad \zeta_2 = \bar{\alpha} \tag{5.1}$$

yields

$$H_k(\alpha,\zeta;c) \leqslant (c\alpha)\left(\frac{k}{2}-1\right)\ln(\alpha/\alpha_k) \quad \textit{for all } \alpha \in (0,\alpha_k].$$

Also, for any $\delta = \delta(k) > 0$ there exists $\varepsilon = \varepsilon(k) > 0$ such that $H_k(\alpha,\zeta;c) < -\varepsilon$ for all $\alpha \in [\delta, 0.99\alpha_k]$. In both cases, $\zeta_2 \geqslant \zeta_0(k) := 1-\alpha_k > 0$.

The first part of the claim establishes (4.18), and the second part, with $\delta = \alpha_k/3$, establishes (4.19) for $\alpha \in [\alpha_k/3, 0.99\alpha_k]$. As both ε and ζ_0 depend only on k they are automatically continuous (constant) with respect to c, thus satisfying the hypothesis of Lemma 4.2.

Proof. Trivially, $\zeta_2 = \bar{\alpha} \geqslant 1-\alpha_k > 0$, since $\alpha_k = ek^{-k/(k-2)} < e/k < 1$. The issue in this range of α is to control the final logarithmic term of $H_k(\alpha,\zeta;c)$ when the two summands within the logarithm are nearly equal. Note that $\ln f(x)$ is concave on either side of 0 (diverging to $-\infty$ at 0, it is not concave as a whole), as

$$[\ln f(x)]'' = \frac{e^x(1-x-e^{-x})}{f^2(x)} < 0. \tag{5.2}$$

Since

$$\frac{d}{d\Delta}\ln f(\lambda(1+\Delta))\bigg|_{\Delta=0} = \frac{\lambda f'(\lambda)}{f(\lambda)},$$

if λ and $\lambda\cdot(1+\Delta)$ are on the same side of 0 (*i.e.*, if $1+\Delta \geqslant 0$) then concavity gives

$$\ln f(\lambda(1+\Delta)) \leqslant \ln f(\lambda) + \Delta\frac{\lambda f'(\lambda)}{f(\lambda)}.$$

Or, with $\zeta = 1+\Delta$, if $\zeta \geqslant 0$ then

$$\frac{f(\lambda\zeta)}{f(\lambda)} \leqslant \exp\left((\zeta-1)\frac{\lambda f'(\lambda)}{f(\lambda)}\right) = \exp\big((\zeta-1)ck\big), \tag{5.3}$$

recalling from (3.6) that $\lambda f'(\lambda)/f(\lambda) = ck$. It is easily checked that (4.17) gives $\alpha_k < 0.2$, hence from (5.1) $\zeta_2 > 0.8$ and $\zeta_1 < 0.4$, so $\zeta_2 - \zeta_1 \geqslant 0$ and of course $\zeta_2+\zeta_1 \geqslant 0$. Thus for the final term of $H_k(\alpha,\boldsymbol{\zeta};c)$, from (5.3) we have

$$\begin{aligned}
\ln & \frac{f(\lambda\cdot(\zeta_2+\zeta_1)) + f(\lambda\cdot(\zeta_2-\zeta_1))}{2f(\lambda)} \\
&\leqslant \ln\left(\frac{\exp(ck(\zeta_2+\zeta_1-1))}{2} + \frac{\exp(ck(\zeta_2-\zeta_1-1))}{2}\right) \\
&= \ln\left(\exp(ck(\zeta_2-1))\left[\frac{\exp(ck\zeta_1)+\exp(-ck\zeta_1)}{2}\right]\right) \\
&= ck(\zeta_2-1) + \ln\cosh(ck\zeta_1) \\
&\leqslant ck(\zeta_2-1) + (ck\zeta_1)^2/2,
\end{aligned}$$

using the well-known inequality $\cosh x \leqslant e^{x^2/2}$. Now also using $-\bar{\alpha}\ln\bar{\alpha} \leqslant \alpha$ for all $\bar{\alpha} \in [0,1)$, substituting $\boldsymbol{\zeta}$ from (5.1) into $H_k(\alpha,\boldsymbol{\zeta};c)$,

$$\begin{aligned}
H_k(\alpha,\boldsymbol{\zeta};c) &\leqslant -c\alpha\ln\alpha + c\alpha + ck\alpha\ln((ck\alpha)^{1/2}) + 0 + ck(-\alpha) + \sqrt{ck\alpha}^{\,2}/2 \\
&= c\alpha\big[\big(\tfrac{k}{2}-1\big)\ln\alpha + \big(1-\tfrac{k}{2}\big) + \tfrac{k}{2}\ln(ck)\big] \\
&= (c\alpha)\big(\tfrac{k}{2}-1\big)\ln\big[\alpha\,\tfrac{1}{e}(ck)^{k/(k-2)}\big].
\end{aligned}$$

Pessimistically taking $c=1$ within the logarithm and recalling α_k from (4.17),

$$H_k(\alpha,\boldsymbol{\zeta};c) \leqslant (c\alpha)\big(\tfrac{k}{2}-1\big)\ln(\alpha/\alpha_k). \tag{5.4}$$

(A different upper bound for c would simply call for a different value for α_k.) This proves the first part of the claim.

Clearly, for all $\alpha \in (0,\alpha_k)$, $\alpha\ln(\alpha/\alpha_k)$ is negative. Therefore, for any $\delta = \delta(k) > 0$, over $\alpha \in [\delta, 0.99\alpha_k]$ it is bounded away from 0. By hypothesis, $c \geqslant 2/k$ (any positive constant would do), thus $H_k(\alpha,\boldsymbol{\zeta};c)$ is also bounded away from 0, that is, there is some $\varepsilon = \varepsilon(k) > 0$ for which $H_k(\alpha,\boldsymbol{\zeta};c) \leqslant -\varepsilon$. This proves the second part of the claim. □

Claim 5.2. *For all $k \geqslant 4$ and all $c \in (2/k, 1)$, there exists $\varepsilon = \varepsilon(c,k) > 0$, with $\varepsilon(c,k)$ continuous in c, such that for all $\alpha \in [0.99\alpha_k, 1/2]$, taking*

$$\zeta_1 = \alpha, \quad \zeta_2 = \bar{\alpha} \tag{5.5}$$

yields $H_k(\alpha,\boldsymbol{\zeta};c) < -\varepsilon$ and (trivially) $\zeta_2 \geqslant \zeta_0 := 1/2$.

Proof. Recall the definition of $H_k(\alpha,\boldsymbol{\zeta};c)$ in (4.2), including its use of $\lambda = \lambda(kc) = \psi^{-1}(kc)$, *i.e.*, $\psi(\lambda) = kc$ (see (3.6)). If we let

$$g(\alpha;\lambda) := \frac{f(\lambda\cdot(1-2\alpha))}{f(\lambda)} \tag{5.6}$$

https://doi.org/10.1017/S0963548315000097 Published online by Cambridge University Press

then we have

$$H_k(\alpha,\zeta(\alpha;c);c) = cH(\alpha) + \ln\frac{f(\lambda)+f(\lambda\cdot(1-2\alpha))}{2f(\lambda)} \tag{5.7}$$

$$= \frac{\psi(\lambda)}{k}H(\alpha) + \ln\frac{1+g(\alpha;\lambda)}{2} =: H_k(\alpha;\lambda). \tag{5.8}$$

The advantage of $H_k(\alpha;\lambda)$ over $H_k(\alpha,\zeta;c)$ is that the former is an explicit function of the 'hidden' parameter $\lambda = \lambda(ck)$, while the latter depends on c both explicitly, and implicitly via $\lambda(ck)$. (To put it another way, λ appears repeatedly in $H_k(\alpha,\zeta;c)$ and is only implicitly defined as ψ^{-1} (see (3.6)), where ψ appears just once in $H_k(\alpha;\lambda)$ and is explicitly defined (see (3.1)).)

Since $\lambda(\cdot)$ is increasing (see after (3.6)) and $c \in (2/k,1)$,

$$\lambda := \lambda(ck) \in (\lambda(2),\lambda(ck)] \subset (0,\lambda_k), \quad \text{where } \lambda_k := \lambda(k). \tag{5.9}$$

We now argue that it suffices to consider only the largest possible value of c, namely $c=1$, or correspondingly of λ, namely $\lambda=\lambda_k$. Referring back to the original question about the k-XORSAT phase transition, in the unconstrained model such a form of monotonicity is obvious: if random instances of given constraint-to-variable density are a.a.s. satisfiable, the same is true of sparser instances, as there is a coupling in which we simply eliminate some constraints. But in the constrained model in which we are now working, monotonicity is not obvious: it is not clear that sparser instances are more likely to be satisfiable than denser ones. We attempted unsuccessfully to show this by converting to and from the unconstrained model.

In the next part we prove a more limited form of monotonicity, in a short following section we show as a consequence that it suffices to show that $H_k(\alpha;\lambda_k) \leqslant 0$, and in a third part we do so.

Monotonicity

For $k \geqslant 4$, there exists a $\sigma_k > 0$ such that for all $\alpha \in [0.99\alpha_k, 1/2]$ and $\lambda \in [0,\lambda_k]$,

$$\text{if } H_k(\alpha;\lambda) \geqslant 0 \quad \text{then } \frac{\partial H_k(\alpha;\lambda)}{\partial\lambda} \geqslant \sigma_k. \tag{5.10}$$

In words, as a function of λ, $H_k(\alpha;\lambda)$ is strictly increasing when it is non-negative.

By (5.8), the condition $H_k(\alpha;\lambda) \geqslant 0$ is equivalent to

$$H(\alpha) \geqslant \frac{k}{\psi(\lambda)}\ln\frac{2}{1+g(\alpha;\lambda)}. \tag{5.11}$$

Also,

$$\begin{aligned}\frac{\partial \ln g(\alpha;\lambda)}{\partial\lambda} &= \frac{\partial g(\alpha;\lambda))/\partial\lambda}{g(\alpha;\lambda)} = \frac{\partial \ln f(\lambda\cdot(1-2\alpha))}{\partial\lambda} - \frac{\partial \ln f(\lambda)}{\partial\lambda}\\ &= (1-2\alpha)f'(\lambda\cdot(1-2\alpha))/f(\lambda\cdot(1-2\alpha)) - f'(\lambda)/f(\lambda)\\ &= \frac{1}{\lambda}\psi(\lambda\cdot(1-2\alpha)) - \frac{1}{\lambda}\psi(\lambda),\end{aligned}$$

https://doi.org/10.1017/S0963548315000097 Published online by Cambridge University Press

from which

$$\frac{\partial g(\alpha;\lambda))}{\partial\lambda} = \lambda^{-1} g(\alpha;\lambda)\big[\psi(\lambda\cdot(1-2\alpha)) - \psi(\lambda)\big]. \tag{5.12}$$

Differentiating (5.8), under the assumption that $H_k(\alpha;\lambda) \geqslant 0$ and using (5.11) and (5.12) in the first inequality,

$$\begin{aligned}\frac{\partial H_k(\alpha;\lambda)}{\partial\lambda} &= k^{-1}\psi'(\lambda)H(\alpha) + \frac{\partial g(\alpha;\lambda)/\partial\lambda}{1+g(\alpha;\lambda)}\\ &\geqslant \frac{\psi'(\lambda)}{\psi(\lambda)}\ln\frac{2}{1+g(\alpha;\lambda)} + \lambda^{-1}\frac{g(\alpha;\lambda)}{1+g(\alpha;\lambda)}\big[\psi(\lambda(1-2\alpha)) - \psi(\lambda)\big]\\ &\geqslant \frac{\psi'(\lambda)}{\psi(\lambda)}\left[\ln\frac{2}{1+g(\alpha;\lambda)} - 2\alpha\psi(\lambda)\frac{g(\alpha;\lambda)}{1+g(\alpha;\lambda)}\right],\end{aligned} \tag{5.13}$$

where the second inequality uses that $\psi'(\lambda) > 0$ and, by convexity of ψ (see Claim 3.1 for both), that $\psi(\lambda(1-2\alpha)) - \psi(\lambda) \geqslant -2\lambda\alpha\psi'(\lambda)$.

Now, regarding $g(\alpha;\lambda)$ as an independent quantity, the right-hand side of (5.13) is decreasing with $g(\alpha;\lambda)$, and for $\lambda \leqslant 1/2$

$$g(\alpha;\lambda) \leqslant \exp[-2\alpha\psi(\lambda)], \tag{5.14}$$

since concavity of $\ln f(x)$ for $x > 0$ (see (5.2)) means that

$$\ln g(\alpha;\lambda) \leqslant -2\alpha\lambda\frac{d}{d\lambda}(\ln f(\lambda)) = -2\alpha\lambda\frac{f'(\lambda)}{f(\lambda)} = -2\alpha\psi(\lambda).$$

It follows then from (5.13) that

$$\frac{\partial H_k(\alpha;\lambda)}{\partial\lambda} \geqslant \frac{\psi'(\lambda)}{\psi(\lambda)} F(2\alpha\psi(\lambda)), \tag{5.15}$$

where

$$F(x) := \ln\frac{2}{1+e^{-x}} - \frac{xe^{-x}}{1+e^{-x}}.$$

Using $\ln(x) \leqslant x-1$ we can confirm that

$$\ln\frac{2}{1+e^{-x}} = -\ln\left(\frac{1}{2}+\frac{1}{2}e^{-x}\right) \geqslant -\left(\frac{1}{2}e^{-x}-\frac{1}{2}\right) = \frac{\sinh(x)}{1+e^{x}},$$

from which

$$F(x) \geqslant \frac{\sinh x - x}{1+e^{x}} \geqslant \frac{x^3}{6(1+e^{x})}. \tag{5.16}$$

By definition (see (3.6)), $\psi(\lambda) = ck$, and here, $x = 2\alpha\psi(\lambda) = 2\alpha ck \leqslant k$. With this, (5.15) and (5.16),

$$\frac{\partial H_k(\alpha;\lambda)}{\partial\lambda} \geqslant \frac{\psi'(\lambda)}{\psi(\lambda)}\,\frac{(2\alpha\psi(\lambda))^3}{6(1+e^{k})} = \frac{\psi'(\lambda)(2\alpha)^3(\psi(\lambda))^2}{6(1+e^{k})} > 1.7\alpha_k^3/(1+e^{k}).$$

For the final inequality, calling again on Claim 3.1, ψ' is increasing, so $\psi'(\lambda) \geqslant \psi'(0) = 1/3$. Here we are in the range $\alpha \geqslant 0.99\alpha_k$, and again $\psi(\lambda) = ck$, which by hypothesis is > 2. This establishes (5.10) with $\sigma_k := 1.7\alpha_k^3/(1+e^{k})$.

Application of monotonicity

For $c \in (2/k, 1)$ as hypothesized in the claim, we will show that

$$m_k(c) := \sup\{H_k(\alpha;\lambda) : \alpha \in [0.99\alpha_k, 1/2],\ \lambda \in [0, \lambda(ck)]\} < 0. \tag{5.17}$$

By continuity of $H_k(\alpha;\lambda)$, the supremum is attained at some $(\hat{\alpha}, \hat{\lambda})$. Recall from (5.9) that $\lambda(ck) < \lambda_k$. By (5.10), if $H_k(\hat{\alpha};\hat{\lambda}) \geqslant 0$ then $\partial H_k(\hat{\alpha};\lambda)/\partial\lambda \geqslant \sigma_k$ for all $\lambda \in [\hat{\lambda}, \lambda_k]$, implying that $H(\hat{\alpha}, \lambda_k) > 0$. In the next part we will show that this is impossible – that $H(\alpha, \lambda_k) \leqslant 0$ – and thus that $m_k(c) < 0$. For Claim 5.2 we may thus take $\varepsilon(c, k) = -m_k(c)$. That this is continuous in c is immediate from continuity of $H_k(\alpha;\lambda)$.

Analysis of the extreme case

The proof of the claim is complete except for treatment of the extreme case, $c = 1$ or equivalently $\lambda = \lambda_k$, namely showing that

$$H_k(\alpha) := H_k(\alpha;\lambda_k) \leqslant 0 \tag{5.18}$$

for all $\alpha \in [0.99\alpha_k, 1/2]$. (Observe, for example from (5.19) below, that $H_k(1/2) = 0$.) We begin with

$$H_k(\alpha) = H(\alpha) + \ln \frac{f(\lambda_k) + f(\lambda_k(1-2\alpha))}{2f(\lambda_k)} \tag{5.19}$$

$$= H(\alpha) - \ln 2 + \ln\left(1 + \frac{f(\lambda_k \cdot (1-2\alpha))}{f(\lambda_k)}\right)$$

$$\leqslant -\frac{(1-2\alpha)^2}{2}\left(1 - \frac{\lambda_k^2 e^{\lambda_k(1-2\alpha)}}{f(\lambda_k)}\right), \tag{5.20}$$

where inequality (5.20) uses that, as $H''(\alpha) \leqslant -4$,

$$H(\alpha) - H(1/2) \leqslant -\tfrac{1}{2}(1-2\alpha)^2, \tag{5.21}$$

and that

$$\ln(1+x) \leqslant x \quad \text{and} \quad f(x) = \frac{x^2}{2}\sum_{j\geqslant 0} \frac{2x^j}{(j+2)!} \leqslant \frac{x^2 e^x}{2}. \tag{5.22}$$

Case α near 1/2. It is immediate from (5.20) that $H_k(\alpha) \leqslant 0$ for α sufficiently close to 1/2, namely for $\alpha \in [\alpha_k^*, 1/2]$, where

$$\alpha_k^* := \frac{1}{2}\left(1 - \frac{1}{\lambda_k} \ln \frac{f(\lambda_k)}{\lambda_k^2}\right). \tag{5.23}$$

Let us confirm that $\alpha_k^* \in (0, 1/2)$, that is, that

$$\frac{1}{\lambda_k} \ln\left(f(\lambda_k)/\lambda_k^2\right) \in (0,1).$$

First, we show that for all $k \geqslant 3$, $\lambda_k > k-1$. This is equivalent to $k > \psi(k-1)$, or explicitly to $e^{k-1} > 1 + k(k-1)$, which follows for $k \geqslant 7$ by use of $e^x > 1 + \frac{1}{6}x^3$, and simply by checking for $k < 7$. Then, by definition, $k = \psi(\lambda_k) = \lambda_k + \lambda_k^2/f(\lambda_k)$, so $\lambda_k > k-1$ implies that $\lambda_k^2/f(\lambda_k) < 1$, giving

$$\frac{1}{\lambda_k}\ln\left(f(\lambda_k)/\lambda_k^2\right) > 0.$$

Also, $\lambda_k > k-1$ implies $\lambda_k \geqslant 1$, from which $f(\lambda_k)/\lambda_k^2 \leqslant f(\lambda_k) < e_k^{\lambda}$, and

$$\frac{1}{\lambda_k}\ln(f(\lambda_k)/\lambda_k^2) < 1.$$

Case α away from 1/2. We now treat $\alpha \in [0.99\alpha_k, \alpha_k^*]$ through two subcases.

Subcase $k \geqslant 7$. Since

$$\frac{f(\lambda_k \cdot (1-2\alpha))}{f(\lambda_k)} = g(\alpha;\lambda_k) \leqslant e^{-2\alpha k}$$

(by (5.6) and (5.14), the latter relying on $\alpha \leqslant \alpha_k^* \leqslant 1/2$), we have from (5.19) that

$$H_k(\alpha) < H(\alpha) + \ln\frac{1+e^{-2\cdot\alpha k}}{2} \leqslant H(\alpha_k^*) + \ln\frac{1+e^{-2\cdot 0.99\alpha_k k}}{2}. \tag{5.24}$$

Let us show that α_k^* decreases with k, implying that $H(\alpha_k^*) \leqslant H(\alpha_7^*)$. Since $\lambda(\cdot)$ is increasing (see after (3.6)), it suffices to show that $\frac{1}{x}\ln(f(x)/x^2)$ increases with x for $x \geqslant \lambda_3$; we will show it for all $x > 0$. Differentiating,

$$\frac{d}{dx}\left(\frac{1}{x}\ln\frac{f(x)}{x^2}\right) = -\frac{1}{x^2}G(x) \quad \text{where } G(x) := \ln\frac{f(x)}{x^2} + 2 - \frac{xf'(x)}{f(x)},$$

so we must show that $G(x) < 0$ for $x > 0$. Now, $\lim_{x\downarrow 0} G(x) = -\ln 2 < 0$, so it suffices to show that $G'(x) = \left(\psi(x) - 2 - x\psi'(x)\right)/x \leqslant 0$, or equivalently $\psi(x) - 2 - x\psi'(x) \leqslant 0$. This is true, since this expression is 0 at $x = 0$ and its derivative is simply $-\psi''(x)$, which is $\leqslant 0$ by convexity of ψ (see Claim 3.1).

Also, recalling the definition of α_k from (4.17), differentiation immediately shows that $\alpha_k k = ek^{-2/(k-1)}$ increases with k, so that $\alpha_k k \geqslant 7\,\alpha_7$.

So, for $k \geqslant 7$ and $\alpha \in [0.99\alpha_k, \alpha_k^*]$, (5.24) yields the cruder bound

$$H_k(\alpha) < H(\alpha_7^*) + \ln\frac{1+e^{-2\cdot 0.99\cdot 7\,\alpha_7}}{2} < -0.019. \tag{5.25}$$

Subcase $k = 4, 5, 6$. Notice that, for $\alpha \in [0, 1/2]$, the entropy term $H(\alpha)$ in (5.19) for $H_k(\alpha)$ is increasing, while the logarithmic term is decreasing. Consequently, if $0 < x < x' \leqslant 1/2$ are such that

$$H(x') + \ln\frac{f(\lambda_k) + f(\lambda_k \cdot (1-2x))}{2f(\lambda_k)} < 0, \tag{5.26}$$

then $H_k(\alpha) < 0$ for all $\alpha \in [x, x']$. A collection of such intervals $[x, x']$ covering $[0.99\alpha_k, \alpha_k^*]$ gives an 'interval arithmetic' proof that $H_k(\alpha) \leqslant 0$ on $[0.99\alpha_k, \alpha_k^*]$, and there is an elegant iterative procedure for finding such a cover.

The left-hand side of (5.26) is equal to

$$H_k(x) + H(x') - H(x) < H_k(x) + (x'-x)H'(x) \tag{5.27}$$

https://doi.org/10.1017/S0963548315000097 Published online by Cambridge University Press

by convexity of H. Thus, inequality (5.26) is satisfied if the right-hand side of (5.27) is 0, that is, if

$$x' = x - \frac{H_k(x)}{H'(x)}. \tag{5.28}$$

(Note that $H_k(x) < 0$, so $x' > x$.) We apply (5.28), reminiscent of Newton–Raphson, as an iterative update rule, with $x_i = x$ and $x_{i+1} = x'$, to cover the interval $[0.99\alpha_k, \alpha_k^*]$.

For $k = 6$, taking $x_0 = x = 0.99\alpha_k \approx 0.1831$ gives $x_1 = x' \approx 0.2620$, showing that $H_6(\alpha) \leqslant 0$ on $[x_0, x_1]$. Then, taking $x = x_1$ gives $x_2 = x' \approx 0.3421$, showing that $H_6(\alpha) \leqslant 0$ on $[x_1, x_2]$. Since $\alpha_6^* < 0.3024 < x_2$, for $k = 6$ these two intervals suffice to prove negativity of $H_k(\alpha)$ over $[0.99\alpha_k, \alpha_k^*]$.

For $k = 5$, following the same procedure covers $[0.99\alpha_k, \alpha_k^*]$ with three intervals. Likewise, for $k = 4$, $[0.99\alpha_k, \alpha_k^*]$ is covered with eight intervals.

In fact, (5.25) and a check of the intervals for $k = 4, 5, 6$ yields that, for $k \geqslant 4$,

$$H_k(\alpha) < -0.0012 \quad \text{for all } \alpha \in [0.99\alpha_k, \alpha_k^*]. \tag{5.29}$$

This completes the proof of Claim 5.2. □

We have not addressed $k = 3$, already treated by [17], and indeed with ζ as above, $H_3(\frac{1}{2}, \zeta; 1)$ is positive. We remark that we can extend Claim 5.2 to $k = 3$ by choosing ζ differently, notably as given by (6.4). The motivation is that equations (6.4) hold for the optimal $z = \lambda\zeta$ at the stationary points $(\hat{\alpha}, \hat{k})$ of the function $\min_z H_k(\alpha, z/\lambda; \psi^{-1}(ck))$, assuming (without justification) that the implicit-differentiation rules apply. The monotonicity condition (the equivalent of (5.10)) then applies for all $\alpha \in (0, 1/2]$. For details, see [27, Appendix (b)]. An interval arithmetic argument verifies that this choice makes $H_3(\alpha, \zeta; 1) < 0$ for $\alpha \in [0.99\alpha_3, \alpha_3^*]$, as we will show after (6.4), where this is needed to treat the phase transition more precisely. If we make this extension, Claim 5.3 also extends immediately to $k = 3$.

We also remark that if we alter the hypotheses of Claim 5.2 to exclude α near $1/2$ then we may allow $c = 1$, as formalized below (where the choice of 0.49 is arbitrary). This will be used when we narrow the phase transition window in Section 6.

Remark 3. For all $k \geqslant 4$ there exists $\varepsilon = \varepsilon(k) > 0$, such that for all $\alpha \in [0.99\alpha_k, 0.49]$ and all $c \in [2/k, 1]$, taking $\zeta_1 = \alpha, \zeta_2 = \bar{\alpha}$ yields $H_k(\alpha, \zeta; c) < -\varepsilon$ and (trivially) $\zeta_2 \geqslant \zeta_0 := 1/2$.

Proof. The substitution gives $H_k(\alpha, \zeta; c) = H_k(\alpha; \lambda)$ (see (5.8)), the range $c \in [2/k, 1]$ corresponds to $\lambda \in [0, \lambda_k]$, and it suffices to show that

$$\sup\{H_k(\alpha; \lambda) : \alpha \in [0.99\alpha_k, 0.49],\ \lambda \in [0, \lambda_k]\} < 0.$$

In analogy with (5.17), by continuity, the supremum over this closed domain is achieved at some $(\hat{\alpha}, \hat{\lambda})$. We prove by contradiction that $H_k(\hat{\alpha}, \hat{\lambda}) < 0$. If not, $H_k(\hat{\alpha}, \hat{\lambda}) \geqslant 0$. If $\hat{\lambda} < \lambda_k$ then as argued previously this implies $H_k(\hat{\alpha}, \lambda_k) = H_k(\hat{\alpha}) > 0$, while if $\hat{\lambda} = \lambda_k$ then, directly, $H_k(\hat{\alpha}) \geqslant 0$. We now show that $H_k(\alpha) < 0$ for $\alpha \in [0.99\alpha_k, 0.49]$, by modifying the previous argument that $H_k(\alpha) \leqslant 0$ for $\alpha \in [0.99\alpha_k, 1/2]$. Referring to (5.23), for any α_k^+ with $\alpha_k^* <$

https://doi.org/10.1017/S0963548315000097 Published online by Cambridge University Press

$\alpha_k^+ < 0.49$, inequality (5.20) shows that $H_k(\alpha) < 0$ for $\alpha \in [\alpha_k^+, 0.49]$. (Recall that α_k^* is decreasing in k – see after (5.24) – so for all $k \geqslant 3$, $\alpha_k^* \leqslant \alpha_3^* < 0.4630$.) And from (5.25), continuity shows that for some α_7^+ slightly larger than α_7^* we have $H_k(\alpha) < -0.018$ for all $\alpha \in [0.99\alpha_k, \alpha_7^+]$ and $k \geqslant 7$. Likewise, for the numerically treated cases $k = 4, 5, 6$, (5.29) extends by continuity to show that, for some α_k^+ slightly larger than α_k^*, $H_k(\alpha) < -0.0011$ for all $\alpha \in [0.99\alpha_k, \alpha_k^+]$. □

Claim 5.3. *For all $k \geqslant 4$ and all $c \in (2/k, 1)$, there exist $\varepsilon = \varepsilon(c,k) > 0$, $\zeta_0 = \zeta_0(c,k) > 0$, both functions being continuous in c, such that for all $\alpha \in (1/2, 1]$ there exists $\boldsymbol{\zeta}$ for which $H_k(\alpha, \boldsymbol{\zeta}; c) < -\varepsilon$ and $\zeta_2 \geqslant \zeta_0$.*

Proof. For any $x > 0$, $f(x) > f(-x)$; this follows from

$$f(x) - f(-x) = e^x - e^{-x} - 2x = 2(\sinh(x) - x) > 0,$$

the last inequality well known. This gives

$$\lim_{\alpha \to 1} H_k(\alpha, (\alpha, \bar{\alpha}); c) = \ln \frac{f(\lambda) + f(-\lambda)}{2f(\lambda)} < 0,$$

the equality immediate from (5.7) and the inequality from $ck > 2$ and thus $\lambda = \lambda(ck) > 0$. By continuity of $H_k(\alpha, (\zeta_1, \zeta_2); c)$ with respect to α, ζ_1 and ζ_2, there exist functions $\delta = \delta(c,k) > 0$ and $\varepsilon = \varepsilon(c,k) > 0$, both continuous in c, for which

$$\sup_{\alpha \in [1-\delta, 1]} H_k(\alpha, (1-\delta, \delta); c) \leqslant -\varepsilon. \tag{5.30}$$

This establishes the claim for $\alpha \in [1-\delta, 1]$.

For $\alpha \in (1/2, 1-\delta)$, let $\boldsymbol{\zeta} = (\zeta_1, \zeta_2)$ be given by $\zeta_1(\alpha) = \zeta_2(\bar{\alpha})$, the latter determined by Claims 5.1–5.2, and likewise $\zeta_2(\alpha) = \zeta_1(\bar{\alpha})$. Then,

$$\begin{aligned} H_k(\alpha, \boldsymbol{\zeta}(\alpha); c) &= H_k(\alpha, (\zeta_2(\bar{\alpha}), \zeta_1(\bar{\alpha})); c) \\ &\leqslant H_k(\bar{\alpha}, (\zeta_1(\bar{\alpha}), \zeta_2(\bar{\alpha})); c) \\ &= H_k(\bar{\alpha}, \boldsymbol{\zeta}(\bar{\alpha}); c). \end{aligned}$$

The inequality follows from (4.2): for the first three terms of its right-hand side by symmetry, and for its last term by applying the inequality $f(x) \geqslant f(-x)$, with $x := \zeta_2(\bar{\alpha}) - \zeta_1(\bar{\alpha}) \geqslant 0$ (in the proofs of Claims 5.1–5.2, $\zeta_2 \geqslant \zeta_1$). It follows that

$$H_k(\alpha, \boldsymbol{\zeta}(\alpha); c) \leqslant -\varepsilon,$$

where ε is chosen as the minimum of corresponding values in Claims 5.1–5.2. (Actually, here we need the value of $\delta(c,k)$ chosen for (5.30) rather than the $\delta(k)$ used in Claim 5.1. This goes through without difficulty since $\delta(c,k)$ is continuous in c, and the corresponding $\varepsilon(c,k)$ needed in the last paragraph of the proof of Claim 5.1 is continuous in δ, and has no dependence on c other than through δ.)

Finally, for $\zeta_0(c,k) > 0$ suitably chosen, we have $\zeta_2 \geqslant \zeta_0(c,k) > 0$. This follows because for $\alpha \geqslant 1-\delta$ we have $\zeta_2 = \delta$, while for $\alpha \in (1/2, 1-\delta)$ we have $\zeta_2(\alpha) = \zeta_1(\bar{\alpha})$, which by Claims 5.1–5.2 is variously of order $\Theta(\bar{\alpha}^{1/2})$ or $\Theta(\bar{\alpha})$, and in either case bounded away from 0 since $\bar{\alpha} \geqslant \delta$. □

This completes the claims used in proving Lemma 4.2.

6. More precise threshold behaviour

With relatively little additional work, we can prove the finer-grained threshold behaviour given by Theorem 1.2.

Proof of Theorem 1.2. By a standard and general argument we may assume that m/n has a limit. (Any hypothetical sequence of counterexamples has a subsequence where m/n converges.) The case $\lim m/n \neq 1$ was already treated by Theorem 1.1, so we assume henceforth that $\lim m/n = 1$, that is, $w(n) = o(n)$.

The unsatisfiable part of the theorem is immediate from Remark 1.

For satisfiability, we have $c = m/n < 1$ and $c \to 1$. We follow the outline of the proof of Theorem 1.1. Claim 5.1 already treats $m/n = c$ in a closed interval including 1 and all $k \geqslant 3$. (As Dubois and Mandler did not derive this sharper threshold, here we must treat $k = 3$.) So does Claim 5.3, in its treatment of α near 1 and the symmetry argument elsewhere, contingent upon Claim 5.2. That is, the previous analysis (encapsulated in the proof of Corollary 4.3) continues to apply to all terms in the sum $\sum_{\ell=2}^{m} \mathbb{E}\big[Y_{m,n}^{(\ell)}\big]$ *except* those with $\ell/m = \alpha \in [\alpha_k^+, 1/2]$, so that, in the current setting,

$$\sum_{\ell=2}^{m} \mathbb{E}\big[Y_{m,n}^{(\ell)}\big] = O(m^{-(k-2)}) + 2 \sum_{\ell=0.99\alpha_k m}^{m/2} \mathbb{E}\big[Y_{m,n}^{(\ell)}\big].$$

To prove Theorem 1.2 we split the final summand above into two ranges, and we will show that

$$\sum_{\ell=0.99\alpha_k m}^{0.4630m} \mathbb{E}\big[Y_{m,n}^{(\ell)}\big] = O(n)e^{-\Omega(n)} \tag{6.1}$$

(this will be immediate from (6.3)) and

$$\sum_{\ell=0.4630m}^{m/2} \mathbb{E}\big[Y_{m,n}^{(\ell)}\big] = O(1)\exp(-0.69\, w(n)) \tag{6.2}$$

(shown in (6.10)). Both of these require extending Claim 5.2 to the case where $c \to 1$ (no longer bounded away from 1), deriving fresh bounds for $\alpha \in [0.99\alpha_k, 1/2]$, $k \geqslant 3$. The second requires additionally an extension of Lemma 4.1 through an improvement, for ζ_1 bounded away from 0, to inequality (4.11) and in turn to (4.16) and (4.1).

The monotonicity approach used to prove Claim 5.2, allowing us to focus on $c = 1$ (correspondingly, $\lambda = \lambda_k$) no longer applies because, with a vanishingly small gap between λ and λ_k, the argument no longer bounds $H_k(\alpha; \lambda)$ away from 0 (indeed we already remarked that $H_k(1/2, \lambda_k) = 0$). In lieu of the use of monotonicity, though, as noted above, we can assume that c is less than but arbitrarily close to 1 (correspondingly, $\lambda < \lambda_k$ is arbitrarily close to λ_k). We now consider the two ranges of α corresponding to the sums in (6.1) and (6.2).

Case α away from 1/2. We will show that, for $k \geqslant 3$ and suitable $\zeta = \zeta(\alpha; c)$, $H_k(\alpha, \zeta; c)$ is bounded below 0 for c sufficiently close to 1 and for α in a range extending above α_k^*. Specifically, we will show that for all $k \geqslant 3$ there exist $c^- < 1$ and $\varepsilon(k) > 0$ such that

$$\big(\forall\alpha \in [0.99\alpha_k, 0.4630]\big)\,\big(\forall c \in [c^-, 1]\big): \quad H_k(\alpha, \zeta; c) \leqslant -\varepsilon(k). \tag{6.3}$$

For $k \geqslant 4$ this was established in Remark 3. For $k = 3$ we set

$$\zeta_1 = \exp\big(-H(\alpha)/k\big)\, \alpha^{(k-1)/k}, \quad \zeta_2 = \exp\big(-H(\alpha)/k\big)\, \bar{\alpha}^{(k-1)/k}. \tag{6.4}$$

(For more on this choice see the discussion after (5.29).) We have $0.0990 < 0.99\alpha_3$ and $\alpha_3^* < 0.4630$, and using interval arithmetic we verify that for sub-intervals on integral multiples of 0.0001, that is, $[0.0990, 0.0991]$, …, $[0.4629, 0.4630]$, the value of $H_k(\alpha, \zeta; 1)$ on each sub-interval is < -0.0004. The interval arithmetic verification consists of defining ζ according to the interval's first endpoint, then considering the extreme values of the possible results in each monotone component calculation for $H_k(\alpha, \zeta; 1)$ (see (4.2)) to get rigorous lower and upper bounds on the true value anywhere in the interval. Continuity in c then gives (6.3) for some c^- sufficiently close to 1.

Inequality (6.1) is immediate from (6.3) and (4.1).

Case α near 1/2. For the remaining interval $[0.4630, 1/2]$, $H_k(\alpha, \zeta; c)$ is not bounded away from 0, but we will establish a sufficient bound. We again take $\zeta = (\alpha, \bar{\alpha})$, so that $H_k(\alpha, \zeta; c) = H_k(\alpha; \lambda)$ (including for $k = 3$). Then, for all $k \geqslant 3$, for some $c^- < 1$,

$$\begin{aligned}&\big(\forall\alpha \in [0.4630, 1/2]\big)\,\big(\forall c \in [c^-, 1]\big):\\ &\qquad H_k(\alpha, \zeta; c) = H_k(\alpha; \lambda) \leqslant (c-1)H(0.4630) - 0.001(1-2\alpha)^2.\end{aligned} \tag{6.5}$$

To see this we follow the same reasoning as for (5.20), including use of (5.21) and (5.22) for the first inequality below:

$$\begin{aligned} H_k(\alpha; \lambda) &= cH(\alpha) + \ln \frac{f(\lambda) + f(\lambda(1-2\alpha))}{2f(\lambda)} \\ &= (c-1)H(\alpha) + (H(\alpha) - H(1/2)) + \ln\left(1 + \frac{f(\lambda(1-2\alpha))}{f(\lambda)}\right) \\ &\leqslant (c-1)H(0.4630) - \frac{(1-2\alpha)^2}{2}\left(1 - \frac{\lambda^2 e^{\lambda(1-2\alpha)}}{f(\lambda)}\right). \end{aligned}$$

Since the derivative of

$$\frac{\lambda^2 e^{\lambda(1-2\alpha)}}{f(\lambda)}$$

is bounded uniformly over α, and making no assumption about the sign of the $O(\cdot)$ term, we have

$$H_k(\alpha; \lambda) \leqslant (c-1)H(0.4630) - \frac{(1-2\alpha)^2}{2}\left(1 - \frac{\lambda_k^2 e^{\lambda_k(1-2\alpha)}}{f(\lambda_k)} + O(\lambda - \lambda_k)\right). \tag{6.6}$$

https://doi.org/10.1017/S0963548315000097 Published online by Cambridge University Press

Now observe that for $\alpha \in [0.4630, 1/2]$, using the definition (5.23) of α_k^*,

$$\frac{\lambda_k^2 e^{\lambda_k(1-2\alpha)}}{f(\lambda_k)} = \frac{\lambda_k^2 e^{\lambda_k(1-2\alpha_k^*)}}{f(\lambda_k)}\, e^{2\lambda_k(\alpha_k^*-\alpha)} = e^{2\lambda_k(\alpha_k^*-\alpha)}$$
$$\leqslant e^{2\lambda_3(\alpha_3^*-0.4630)} \leqslant 0.9977.$$

This and (6.6) yield (6.5).

Improved bound on $a(\ell, v)$. We will need bounds on $a(\ell, v)$ and $\mathbb{E}[Y_{m,n}^{(\ell)}]$ better than those in (4.11) and (4.16). Reasoning as for (4.12), from (4.9) we have

$$\begin{aligned} a(\ell, v) &= \frac{(k\ell)!}{2\pi} \oint\limits_{\substack{z=z_1 e^{i\vartheta}:\\ \vartheta\in(-\pi,\pi]}} \frac{(\cosh z - 1)^v}{z^{k\ell+1}}\, dz \\ &\leqslant 2\,\frac{(k\ell)!}{2\pi\, z_1^{k\ell+1}} \int_{-\pi/2}^{\pi/2} \exp\big(v\ \ln|\cosh(z_1 e^{i\vartheta}) - 1|\big)\, d\vartheta \\ &= O(1/\sqrt{v})\,(k\ell)!\,\frac{(\cosh z_1 - 1)^v}{z_1^{k\ell+1}}. \end{aligned} \tag{6.7}$$

The final equality follows from the Laplace method for integrals; see for example de Bruijn [6]. Roughly, the Laplace method says that if $f(x)$ is maximized on $[a, b]$ by x_0 then, asymptotically in n,

$$\int_a^b e^{nf(x)} dx = (1 + o(1)) e^{nf(x_0)} \sqrt{\frac{2\pi}{n(-f''(x_0))}}.$$

The maximum of $|\cosh(z_1 e^{i\vartheta}) - 1|$ occurs if and only if ϑ is a multiple of π, as is clear from the Taylor series expansion

$$\cosh(z_1 e^{i\vartheta}) - 1 = \sum_{j=1}^{\infty} \frac{1}{(2j)!} {z_1}^{2j} e^{i\cdot 2j\vartheta}.$$

The modulus of this expression is

$$\sum_{j=1}^{\infty} \frac{1}{(2j)!} {z_1}^{2j}$$

when ϑ is a multiple of π, and only then (for this to be the case all the arguments $2j\vartheta$ must be equal modulo 2π, requiring ϑ to be a multiple of π). In the range $[-\pi/2, \pi/2]$, then, the unique maximum is at $\vartheta = 0$. Letting

$$s(\vartheta) := \ln|\cosh(z_1 e^{i\vartheta}) - 1| = \ln(\cosh(z_1 \cos\vartheta) - \cos(z_1 \sin\vartheta)),$$

the second derivative at the maximum is

$$\left.\frac{d^2 s}{d\vartheta^2}\right|_{\vartheta=0} = -\frac{z_1(\sinh(z_1) - z_1)}{\cosh(z_1) - 1} = -\Theta(1),$$

since $z_1 = \Theta(1)$.

Improved bound on $\mathbb{E}[Y^{(\ell)}_{m,n}]$. Note that the bound on $a(\ell, v)$ in (6.7) is $O(1/(\zeta_1\sqrt{v}))$ times the previous bound given by (4.11), since $z_1 = \zeta_1\lambda$ and we assume throughout that λ is bounded away from 0, which represents an improvement when $\zeta_1 = \Theta(1)$. This gives a corresponding improvement to the bound on $p(\ell, v)$ from (4.14). Let $T(v)$ represent the right-hand side of (4.14), excluding the $O(1)$ term: this notation focuses on the parameter of interest, but $T(v)$ also depends on z_1, z_2, λ, k, m and ℓ. We now have

$$p(\ell, v) = O(1/(\zeta_1\sqrt{v}))\,T(v). \tag{6.8}$$

This improves the summands of (4.15), but the $1/\sqrt{v}$ stops us from applying the binomial theorem to obtain an analogue of (4.16); one additional step is needed.

As we did for (4.16), restrict z_1 and z_2 to depend only on ℓ, m and n (not on v). Then the maximum of $(1/(\zeta_1\sqrt{v}))\,T(v)$ can be seen to occur where the ratio of consecutive terms,

$$\frac{(1/\sqrt{v+1}\,)\,T(v+1)}{(1/\sqrt{v}\,)\,T(v)} = \sqrt{\frac{v}{v+1}}\,\frac{n-v}{v+1}\,\frac{e^{z_2}(\cosh z_1 - 1)}{f(z_2)},$$

is 1, which occurs at some $v_0 = \Theta(n)$. Terms before $v_0/2$ are exponentially smaller than the maximum, while later terms $(1/(\zeta_1\sqrt{v}))\,T(v)$ are of order $O(1/(\zeta_1\sqrt{n}))\,T(v)$. Thus,

$$\begin{aligned}\sum_{v=1}^{n}\binom{n}{v}p(\ell,v) &= O(1)\sum_{v=1}^{v_0/2}\binom{n}{v}(1/(\zeta_1\sqrt{v}))\,T(v) + O(1)\sum_{v=v_0/2}^{n}\binom{n}{v}(1/(\zeta_1\sqrt{v}))\,T(v)\\ &= O(n)\exp(-\Theta(n))T(v_0) + O(1/(\zeta_1\sqrt{n}))\sum_{v=1}^{n}\binom{n}{v}\,T(v)\\ &= O(1/(\zeta_1\sqrt{n}))\sum_{v=1}^{n}\binom{n}{v}\,T(v),\end{aligned}$$

an analogue of (4.15) but smaller by $O(1/(\zeta_1\sqrt{n}))$. To this we can apply the binomial theorem, as we did to (4.15), giving a corresponding improvement to (4.16) and in turn (4.1), namely

$$\mathbb{E}\big[Y^{(\ell)}_{m,n}\big] \leqslant O(1)\frac{1}{\zeta_1\sqrt{n\zeta_2}}\exp\big[nH_k(\alpha,\boldsymbol{\zeta};c)\big], \quad \text{for all } \boldsymbol{\zeta} > 0. \tag{6.9}$$

From (6.5) and (6.9),

$$\begin{aligned}\sum_{\ell=0.4630m}^{m/2}\mathbb{E}[Y^{(\ell)}_{m,n}] &\leqslant \sum_{\ell=0.4630m}^{m/2} O\left(\frac{1}{\sqrt{n}}\right)\exp\big(nH_k(\alpha,\boldsymbol{\zeta};c)\big)\\ &\leqslant O\left(\frac{1}{\sqrt{n}}\right)\sum_{\ell=0.4630m}^{m/2}\exp\big((c-1)\,n\,H(0.4630) - 0.001(1-2\ell/m)^2 n\big)\\ &\leqslant O\left(\frac{1}{\sqrt{n}}\right)\exp\big((m-n)H(0.4630)\big)\sum_{x=0}^{\infty}\exp\big(-0.001(x/m)^2 n\big)\end{aligned}$$

$$= O\left(\frac{1}{\sqrt{n}}\right) \exp(-H(0.4630)\, w(n))\, O(\sqrt{n})$$
$$= O(1) \exp(-0.69\, w(n)). \tag{6.10}$$

This establishes (6.2) and concludes the proof of Theorem 1.2. □

7. Satisfiability threshold for unconstrained k-XORSAT

If a variable appears in at most one equation, then deleting that variable, along with the corresponding equation if any, yields a linear system that is clearly solvable if and only if the original system was. Stop this process when each variable appears in at least two equations, or when the system is empty. Dubois and Mandler analysed unconstrained 3-XORSAT by analysing this process, which ends with a (possibly empty) constrained 3-XORSAT instance.

Regarding each variable as a vertex and each equation as a hyperedge on its k variables yields the k-uniform 'constraint hypergraph' underlying a k-XORSAT instance. The process described simply restricts the instance to the 2-core of its hypergraph. The analysis by Dubois and Mandler for 3-XORSAT is easily generalized to k-XORSAT using the (later) analyses of the 2-core of a random k-uniform hypergraph, and we take this approach.

Note that the our (unconstrained) k-XORSAT model really corresponds to a random k-uniform *multi*-hypergraph. However, the probability that a random matrix corresponds to a simple graph is

$$\binom{n}{k}_{(m)} \Big/ \binom{n}{k}^m = 1 - O(n^{-(k-2)}) = 1 - o(1).$$

Thus any a.a.s. property of a simple random hypergraph is also an a.a.s. property for random k-XORSAT, and we shall proceed with the simple random hypergraph model.

It is well known that the 2-core of a uniformly random k-uniform hypergraph is, conditioned on its size and order, uniformly random among all such k-uniform hypergraphs with minimum degree 2. (One short and simple proof is identical to that for conditioning on the core's degree sequence in [25, Claim 1].) Also, the 'core' of a random k-XORSAT instance is an instance uniformly random on its underlying hypergraph: the (uniform) hypergraph core determines the core A matrix, while the core b is simply the restriction of its uniformly random initial value to the surviving rows of A, a process oblivious to b.

Thus, satisfiability of a random unconstrained instance hinges on the edge-to-vertex ratio of the core of its constraint hypergraph.

Recall the definition of λ from (3.6).

Theorem 7.1. *Let $Ax = b$ be a uniformly random unconstrained uniform random k-XORSAT system with m equations and n variables. Suppose that $k \geqslant 3$ and $m, n \to \infty$ with*

$\lim m/n = c$. Define

$$g_k(x) := \frac{x}{k(1-e^{-x})^{k-1}}.$$

With $c_k^* = g_k(\lambda(k))$, if $c < c_k^*$ then $Ax = b$ is a.a.s. satisfiable, and if $c > c_k^*$ then $Ax = b$ is a.a.s. unsatisfiable.

Proof. We treat k as fixed. Restricting consideration to $x > 0$, from Molloy [25, proof of Lemma 4], $g_k(x)$ has a unique minimum $\hat{c}$, with $g_k(x) = c$ having no solutions for any $c < \hat{c}$, and two solutions for any $c > \hat{c}$. Simple calculus confirms that for $k \geqslant 3$, g_k is unimodal (indeed, convex).

Let H be a random k-uniform hypergraph with m edges and n vertices. Molloy [25, Theorem 1] shows that if $\lim m/n < \hat{c}$ then the 2-core is a.a.s. empty, while if $\lim m/n = c > \hat{c}$, then with μ the larger solution of $g_k(\mu) = c$, the order N and size M of the 2-core a.a.s. satisfy

$$N = n\frac{e^\mu - 1 - \mu}{e^\mu} + o(n), \quad M = n\frac{\mu(e^\mu - 1)}{ke^\mu} + o(n);$$

see also Achlioptas and Molloy [1, Proposition 30]. In fact Molloy works in the Bernoulli model where the number of edges of the hypergraph H_p is $\mathrm{Bin}(\binom{n}{k}, p)$, but the result translates to the above by standard arguments. Specifically, choose p so that the expected number of edges of H_p is m. Generate a random H with exactly m edges as follows: generate H_p; if it has m edges or more, which with constant probability it does, then randomly subsample H_p to give H; otherwise repeat. The core of H is contained in that of H_p, so M and N will not be larger than the bounds given for the Bernoulli model, with failure probability a constant times the failure probability of that for the Bernoulli model. Similarly, generating H by randomly augmenting an H_p having m edges or fewer shows that M and N will not be smaller than the bounds given.

It follows for the core that, a.a.s.,

$$\frac{M}{N} = \frac{\mu(e^\mu - 1)}{k(e^\mu - 1 - \mu)} + o(1) = \frac{1}{k}\psi(\mu) + o(1). \tag{7.1}$$

Define $\mu^* = \lambda(k)$ so that $\psi(\mu^*) = k$; remember from (3.6) that for $k > 2$ this is well defined, with $\mu^* > 0$. We claim that μ^* is the larger of the two values of μ for which $g_k(\mu) = g_k(\mu^*)$. Given that g_k is unimodal, this is true if and only if $g_k'(\mu^*) > 0$. Now,

$$g_k'(\mu^*) = \frac{1 + e^{-\mu^*}(\mu^* - \mu^* k - 1)}{k(1 - e^{-\mu^*})^k}.$$

Focusing on the numerator, multiplying through by e^{μ^*}, and replacing $k = \psi(\mu^*)$, this means showing that

$$e^{\mu^*} + \mu^* - 1 - \mu^*\left(\frac{\mu^*(e^{\mu^*} - 1 - \mu^*)}{e^{\mu^*} - 1}\right) > 0.$$

Multiplying the expression by $e^{\mu^*} - 1$ gives

$$(e^{\mu^*} + \mu^* - 1)(e^{\mu^*} - 1) - \mu^{*2}(e^{\mu^*} - 1 - \mu^*)$$
$$= \left(e^{\mu^*} - 1 - \mu^* - \tfrac{1}{2}\mu^{*2}\right)^2 + 3\mu^*\left(e^{\mu^*} - 1 - \tfrac{1}{3}\mu^* - \tfrac{1}{12}\mu^{*3}\right) > 0$$

as desired. The inequality is immediate from the Taylor series for e^{μ^*}, as $\mu^* > 0$.

Let $c_k^* = g_k(\mu^*)$. Because μ^* is the larger of the two values μ for which $g_k(\mu) = g_k(\mu^*)$, we may apply (7.1), concluding that a random k-uniform hypergraph with $\lim m/n = c_k^* = g_k(\mu^*)$ has a core where, a.a.s.,

$$M/N = \frac{1}{k}\psi(\mu^*) + o(1) = 1 + o(1).$$

For any $c > c_k^*$, the larger solution μ of $g_k(\mu) = c$ has $\mu > \mu^*$ (by the unimodality of g_k), and $\psi(\mu) > \psi(\mu^*) = k$ (by Claim 3.1). Thus, a random k-uniform hypergraph with $\lim m/n = c > c_k^*$ has a core where, a.a.s.,

$$M/N = \frac{1}{k}\psi(\mu) + o(1) > 1.$$

By this section's introductory remarks, a random k-XORSAT instance with $\lim m/n = c > c_k^*$ reduces to a random constrained k-XORSAT instance with M/N converging in probability to a value greater than 1, the reduced instance is a.a.s. unsatisfiable, and thus so is the original instance.

By the same token, if $c < c_k^*$ then either $g_k(\mu) = c$ has no solution (if $c < \hat{c}$), or its larger solution has $\mu < \mu^*$ and $\psi(\mu) < \psi(\mu^*) = k$. Thus, a random k-XORSAT instance with $\lim m/n = c < c_k^*$ reduces to a constrained k-XORSAT instance that either is a.a.s. empty (and trivially satisfied), or has M/N converging in probability to a value less then 1, and thus is a.a.s. satisfiable by Theorem 1.1. Thus the original instance is a.a.s. satisfiable. □

Acknowledgements

We are most grateful to Paul Balister: our proof that the critical exponent can be made negative owes a great deal to his detailed suggestions on using patchwork functional approximations to get finitely away from critical points, and interval arithmetic elsewhere [3]. We sincerely thank the anonymous referees, and Paul, for their careful reading and constructive comments. Additionally, we are grateful to Mike Molloy for helpful thoughts, to Colin Cooper, Alan Frieze and Federico Ricci-Tersenghi for pointing out related work, and to Noga Alon for suggesting we aim for Theorem 1.2.

References

[1] Achlioptas, D. and Molloy, M. (2015) The solution space geometry of random linear equations. *Random Struct. Alg.* **46** 197–231.

[2] Aronson, J., Frieze, A. and Pittel, B. (1998) On maximum matching in sparse random graphs: Karp–Sipser revisited. *Random Struct. Alg.* **12** 111–177.

[3] Balister, P. (2012) Personal communication.

[4] Blömer, J., Karp, R. and Welzl, E. (1997) The rank of sparse random matrices over finite fields. *Random Struct. Alg.* **10** 407–419.
[5] Bollobás, B., Borgs, C., Chayes, J. T., Kim, J.-H. and Wilson, D. B. (2001) The scaling window of the 2-SAT transition. *Random Struct. Alg.* **18** 201–256.
[6] de Bruijn, N. G. (1981) *Asymptotic Methods in Analysis*, Dover.
[7] Chvátal, V. and Reed, B. (1992) Mick gets some (the odds are on his side). In *33rd Annual Symposium on Foundations of Computer Science*, IEEE Computer Society, pp. 620–627.
[8] Cooper, C. (2000) On the rank of random matrices. *Random Struct. Alg.* **16** 209–232.
[9] Cooper, C. (2004) The cores of random hypergraphs with a given degree sequence. *Random Struct. Alg.* **25** 353–375.
[10] Coppersmith, D., Gamarnik, D., Hajiaghayi, M. T. and Sorkin, G. B. (2004) Random MAX SAT, random MAX CUT, and their phase transitions. *Random Struct. Alg.* **24** 502–545.
[11] Creignon, N. and Daudé, H. (2003) Smooth and sharp thresholds for random k-XOR-CNF satisfiability. *Theor. Inform. Appl.* **37** 127–147.
[12] Darling, R. W. R., Penrose, M. D., Wade, A. R. and Zabell, S. L. (2014) Rank deficiency in sparse random GF[2] matrices. *Electron. J. Probab.* **19**, 2458 (Paper 83).
[13] Daudé, H. and Ravelomanana, V. (2008) Random 2-XORSAT at the satisfiability threshold. In *LATIN 2008: Theoretical Informatics*, Vol. 4957 of *Lecture Notes in Computer Science*, Springer, pp. 12–23.
[14] Dietzfelbinger, M., Goerdt, A., Mitzenmacher, M., Montanari, A., Pagh, R. and Rink, M. (2010) Tight thresholds for cuckoo hashing via XORSAT. In *Proc. 37th International Colloquium on Automata, Languages and Programming: ICALP'10* (S. Abramsky *et al.*, eds), Springer, pp. 213–225.
[15] Dietzfelbinger, M., Goerdt, A., Mitzenmacher, M., Montanari, A., Pagh R. and Rink, M. (2010) Tight thresholds for cuckoo hashing via XORSAT. `arXiv:0912.0287v3`
[16] Dubois, O. and Mandler, J. (2002) The 3-XORSAT threshold. In *Proc. 43rd Annual IEEE Symposium on Foundations of Computer Science: FOCS 2002*, IEEE Computer Society, pp. 769–778.
[17] Dubois, O. and Mandler, J. (2002) The 3-XORSAT threshold. *CR Acad. Sci. Paris, Ser. I* **335** 963–966.
[18] Fernandez de la Vega, W. (1992) On random 2-SAT. Manuscript.
[19] Friedgut, E. (1999) Necessary and sufficient conditions for sharp thresholds of graph properties, and the k-SAT problem. *J. Amer. Math. Soc.* **12** 1017–1054.
[20] Goerdt, A. (1996) A threshold for unsatisfiability. *J. Comput. System Sci.* **53** 469–486.
[21] Kim, J. H. (2006) Poisson cloning model for random graphs, International Congress of Mathematicians. Vol. III, *Eur. Math. Soc.*, Zürich, 873–897.
[22] Kolchin, V. F. (1999) *Random Graphs*, Vol. 53 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press.
[23] Mézard, M., Ricci-Tersenghi, F. and Zecchina, R. (2003) Two solutions to diluted p-spin models and XORSAT problems. *J. Statist. Phys.* **111** 505–533.
[24] Mézard, M., Ricci-Tersenghi, F. and Zecchina, R. (2014) Personal communication.
[25] Molloy, M. (2005) Cores in random hypergraphs and Boolean formulas. *Random Struct. Alg.* **27** 124–135.
[26] Pittel, B. (1986) Paths in a random digital tree: Limiting distributions. *Adv. Appl. Probab.* **18** 139–155.
[27] Pittel, B. and Sorkin, G. B. (2012) The satisfiability threshold for k-XORSAT. `arXiv:1212.1905v1`
[28] Pittel, B. and Sorkin, G. B. (2012) The satisfiability threshold for k-XORSAT, using an alternative proof. `arXiv:1212.3822`

[29] Pittel, B., Spencer, J. and Wormald, N. (1996) Sudden emergence of a giant k-core in a random graph. *J. Combin. Theory Ser B* **67** 111–151.
[30] Pittel, B. and Yeum, J.-A. (2010) How frequently is a system of 2-linear equations solvable? *Electron. J. Combin.* **17** R92.
[31] Thompson, C. J. (1972) *Mathematical Statistical Mechanics*, Macmillan.