Available online at www.sciencedirect.com

ScienceDirect

Theoretical Computer Science 393 (2008) 260–279

Theoretical Computer Science

www.elsevier.com/locate/tcs

Pairs of SAT-assignments in random Boolean formulæ

Hervé Daudé[a], Marc Mézard[b], Thierry Mora[b,*], Riccardo Zecchina[c]

[a] LATP, UMR 6632 CNRS et Université de Provence, 13453 Marseille Cedex, France
[b] LPTMS, UMR 8626 CNRS et Université Paris-Sud, 91405 Orsay Cedex, France
[c] Physics Department, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino, Italy

Received 1 June 2005; received in revised form 19 September 2007; accepted 5 January 2008

Communicated by G. Ausiello

Abstract

We investigate geometrical properties of the random K-satisfiability problem using the notion of x-satisfiability: a formula is x-satisfiable is there exist two SAT-assignments differing in Nx variables. We show the existence of a sharp threshold for this property as a function of the clause density. For large enough K, we prove that there exists a region of clause density, below the satisfiability threshold, where the landscape of Hamming distances between SAT-assignments experiences a gap: pairs of SAT-assignments exist at small x, and around $x = \frac{1}{2}$, but they do not exist at intermediate values of x. This result is consistent with the clustering scenario which is at the heart of the recent heuristic analysis of satisfiability using statistical physics analysis (the cavity method), and its algorithmic counterpart (the survey propagation algorithm). Our method uses elementary probabilistic arguments (first and second moment methods), and might be useful in other problems of computational and physical interest where similar phenomena appear.

Keywords: Satisfiability; Clustering

1. Introduction and outline

Consider a string of Boolean variables – or equivalently a string of *spins* – of size N: $\vec{\sigma} = \{\sigma_i\} \in \{-1, 1\}^N$. Call a K-clause a disjunction binding K of these Boolean variables in such a way that one of their 2^K joint assignments is set to FALSE, and all the others to TRUE. A formula in a conjunctive normal form (CNF) is a conjunction of such clauses. The satisfiability problem is stated as: does there exist a truth assignment $\vec{\sigma}$ that satisfies this formula? A CNF formula is said to be *satisfiable* (SAT) if this is the case, and *unsatisfiable* (UNSAT) otherwise.

The satisfiability problem is often viewed as the canonical constraint satisfaction problem (CSP). It is the first problem to have been shown NP-complete [1], i.e. at least as hard as any problem for which a solution can be checked in polynomial time.

* Corresponding address: Princeton University, Carl Icahn Laboratory, 08544 Princeton, NJ, United States. Tel.: +1 609 258 7194; fax: +1 609 258 8004.

E-mail address: tmora@princeton.edu (T. Mora).

0304-3975/$ - see front matter
doi:10.1016/j.tcs.2008.01.005

The $P \neq NP$ conjecture states that no general polynomial-time algorithm exists that can decide whether a formula is SAT or UNSAT. However formulae which are encountered in practice can often be solved easily. In order to understand properties of some typical families of formulae, one introduces a probability measure on the set of instances. In the random K-SAT problem, one generates a random K-CNF formula $F_K(N, M)$ as a conjunction of $M = N\alpha$ K-clauses, each of them being uniformly drawn from the $2^K \binom{N}{K}$ possibilities. In the recent years the random K-satisfiability problem has attracted much interest in computer science and in statistical physics [3–7]. Its most striking feature is certainly its sharp threshold.

Throughout this paper, 'with high probability' (w.h.p.) means with a probability which goes to one as $N \to \infty$.

Conjecture 1.1 (*Satisfiability Threshold Conjecture*). *For all $K \geq 2$, there exists $\alpha_c(K)$ such that:*

- *if $\alpha < \alpha_c(K)$, $F_K(N, N\alpha)$ is satisfiable w.h.p.*
- *if $\alpha > \alpha_c(K)$, $F_K(N, N\alpha)$ is unsatisfiable w.h.p.*

The random K-SAT problem, for N large and α close to $\alpha_c(K)$, provides instances of very hard CNF formulae that can be used as benchmarks for algorithms. For such hard ensembles, the study of the typical complexity could be crucial for the understanding of the usual 'worst-case' complexity.

Although Conjecture 1.1 remains unproved, Friedgut established the existence of a non-uniform sharp threshold [8].

Theorem 1.2 (*Friedgut*). *For each $K \geq 2$, there exists a sequence $\alpha_N(K)$ such that for all $\epsilon > 0$:*

$$\lim_{N\to\infty} \mathbf{P}(F_K(N, N\alpha) \textit{is satisfiable}) = \begin{cases} 1 & \textit{if } \alpha = (1-\epsilon)\alpha_N(K) \\ 0 & \textit{if } \alpha = (1+\epsilon)\alpha_N(K). \end{cases} \tag{1}$$

A lot of efforts have been devoted to finding tight bounds for the threshold. The best upper bounds so far were derived using first moment methods [9,10], and the best lower bounds were obtained by second moment methods [11, 12]. Using these bounds, it was shown that $\alpha_c(K) = 2^K \ln(2) - O(K)$ as $K \to \infty$.

On the other hand, powerful, self-consistent, but non-rigorous tools from statistical physics were used to predict specific values of $\alpha_c(K)$, as well as heuristical asymptotic expansions for large K [14–19]. The *cavity method* [13], which provides these results, relies on several unproven assumptions motivated by spin-glass theory, the most important of which is the partition of the space of SAT-assignments into many *states* or *clusters* far away from each other (with Hamming distance greater than cN as $N \to \infty$), in the so-called hard-SAT phase.

So far, the existence of such a clustering phase has been shown rigorously in the simpler case of the random XORSAT problem [27,26,28] in compliance with the prediction of the cavity method, but its existence is predicted in many other problems, such as q-colorability [21,22] or the Multi-Index Matching Problem [23]. At the heuristic level, clustering is an important phenomenon, often held responsible for entrapping local search algorithm into non-optimal metastable states [20]. It is also a limiting feature for the belief propagation iterative decoding algorithms in Low Density Parity Check Codes [24,25].

In this paper we provide a rigorous analysis of some geometrical properties of the space of SAT-assignments in the random K-SAT problem. This study complements the results of [29], and its results are consistent with the clustering scenario. A new characterizing feature of CNF formulae, the 'x-satisfiability', is proposed, which carries information about the spectrum of distances between SAT-assignments. The x-satisfiability property is studied thoroughly using first and second moment methods previously developed for the satisfiability threshold.

The Hamming distance between two assignments $(\vec{\sigma}, \vec{\tau})$ is defined by

$$d_{\vec{\sigma}\vec{\tau}} = \frac{N}{2} - \frac{1}{2}\sum_{i=1}^{N} \sigma_i \tau_i \ . \tag{2}$$

(Throughout the paper the term 'distance' will always refer to the Hamming distance.) Given a random formula $F_K(N, N\alpha)$, we define a 'SAT-x-pair' as a pair of assignments $(\vec{\sigma}, \vec{\tau}) \in \{-1, 1\}^{2N}$, which both satisfy F, and which are at a fixed distance specified by x as follows:

$$d_{\vec{\sigma}\vec{\tau}} \in [Nx - \epsilon(N), Nx + \epsilon(N)]. \tag{3}$$

Here x is the proportion of distinct values between the two configurations, which we keep fixed as N and d go to infinity. The resolution $\epsilon(N)$ has to be ≥ 1 and sub-extensive: $\lim_{N\to\infty}\epsilon(N)/N = 0$, but its precise form is unimportant for our large N analysis. For example we can choose $\epsilon(N) = \sqrt{N}$.

Definition 1.3. A CNF formula is x-satisfiable if it possesses a SAT-x-pair.

Note that for $x = 0$, x-satisfiability is equivalent to satisfiability, while for $x = 1$, it is equivalent to Not-All-Equal satisfiability, where each clause must contain at least one satisfied literal and at least one unsatisfied literal [2].

The clustering property found heuristically in [15,14] suggests the following:

Conjecture 1.4. *For all $K \geq K_0$, there exist $\alpha_1(K)$, $\alpha_2(K)$, with $\alpha_1(K) < \alpha_2(K)$, such that: for all $\alpha \in (\alpha_1(K), \alpha_2(K))$, there exist $x_1(K,\alpha) < x_2(K,\alpha) < x_3(K,\alpha)$ such that:*

- *for all $x \in [0, x_1(K,\alpha)] \cup [x_2(K,\alpha), x_3(K,\alpha)]$, a random formula $F_K(N, N\alpha)$ is x-satisfiable w.h.p.*
- *for all $x \in [x_1(K,\alpha), x_2(K,\alpha)] \cup [x_3(K,\alpha), 1]$, a random formula $F_K(N, N\alpha)$ is x-unsatisfiable w.h.p.*

Let us give a geometrical interpretation of this conjecture. The space of SAT-assignments is partitioned into non-empty regions whose diameter is smaller than x_1; the distance between any two of these regions is at least x_2, while x_3 is the maximum distance between any pair of SAT-assignments. This interpretation is compatible with the notion of clusters used in the statistical physics approach. It should also be mentioned that in a contribution posterior to this work [30], the number of regions was shown to be exponential in the size of the problem, further supporting the statistical mechanics picture.

Conjecture 1.4 can be rephrased in a slightly different way, which decomposes it into two steps. The first step is to state the *Satisfiability Threshold Conjecture* for pairs:

Conjecture 1.5. *For all $K \geq 3$ and for all x, $0 < x < 1$, there exists an $\alpha_c(K,x)$ such that:*

- *if $\alpha < \alpha_c(x)$, $F_K(N, N\alpha)$ is x-satisfiable w.h.p.*
- *if $\alpha > \alpha_c(x)$, $F_K(N, N\alpha)$ is x-unsatisfiable w.h.p.*

The second step conjectures that for K large enough, as a function of x, the function $\alpha_c(K,x)$ is non-monotonic and has two maxima: a local maximum at a value $x_M(K) < 1$, and a global maximum at $x = 0$.

In this paper we prove the equivalent of Friedgut's theorem:

Theorem 1.6. *For each $K \geq 3$ and x, $0 < x < 1$, there exists a sequence $\alpha_N(K,x)$ such that for all $\epsilon > 0$:*

$$\lim_{N\to\infty} \mathbf{P}(F_K(N, N\alpha) \text{ is } x\text{-satisfiable}) = \begin{cases} 1 & \text{if } \alpha = (1-\epsilon)\alpha_N(K,x), \\ 0 & \text{if } \alpha = (1+\epsilon)\alpha_N(K,x), \end{cases} \tag{4}$$

and we obtain two functions, $\alpha_{LB}(K,x)$ and $\alpha_{UB}(K,x)$, such that:

- For $\alpha > \alpha_{UB}(K,x)$, a random K-CNF $F_K(N, N\alpha)$ is x-unsatisfiable w.h.p.
- For $\alpha < \alpha_{LB}(K,x)$, a random K-CNF $F_K(N, N\alpha)$ is x-satisfiable w.h.p.

The two functions $\alpha_{LB}(K,x)$ and $\alpha_{UB}(K,x)$ are lower and upper bounds for $\alpha_N(K,x)$ as N tends to infinity. Numerical computations of these bounds indicate that $\alpha_N(K,x)$ is non-monotonic as a function of x for $K \geq 8$, as illustrated in Fig. 1. More precisely, we prove

Theorem 1.7. *For all $\epsilon > 0$, there exists K_0 such that for all $K \geq K_0$,*

$$\min_{x\in\left(0,\frac{1}{2}\right)} \alpha_{UB}(K,x) \leq (1+\epsilon)\frac{2^K \ln 2}{2}, \tag{5}$$

$$\alpha_{LB}(K,0) \geq (1-\epsilon)2^K \ln 2, \tag{6}$$

$$\alpha_{LB}(K,1/2) \geq (1-\epsilon)2^K \ln 2. \tag{7}$$

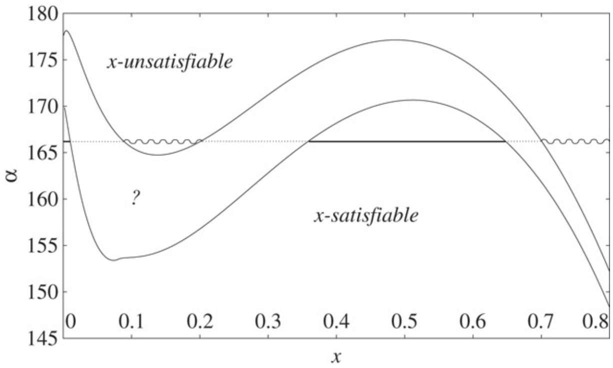

Fig. 1. Lower and Upper Bounds for $\alpha_N(K = 8, x)$. The Upper Bound is obtained by the first moment method. Above this curve there exists no SAT-x-pair, w.h.p. The Lower Bound is obtained by the second moment method. Below this curve there exists a SAT-x-pair w.h.p. For $164.735 < \alpha < 170.657$, these curves confirm the existence of a clustering phase, illustrated here for $\alpha = 166.1$: solid lines represent x-sat regions, and wavy lines x-unsat regions. The x-sat zone near 0 corresponds to SAT-assignments belonging to the same region, whereas the x-sat zone around $\frac{1}{2}$ corresponds to SAT-assignments belonging to different regions. The x-unsat region around .13 corresponds to the inter-cluster gap. We recall that the best refined lower and upper bounds for the satisfiability threshold $\alpha_c(K = 8)$ from [10,12] are respectively 173.253 and 176.596. The cavity prediction is 176.543 [16].

This in turn shows that, for K large enough and in some well chosen interval of α below the satisfiability threshold $\alpha_c \sim 2^K \ln 2$, SAT-x-pairs exist for x close to zero and for $x = \frac{1}{2}$, but they do not exist in the intermediate x region. Note that Eq. (6) was established by [12].

In Section 2 we establish rigorous and explicit upper bounds using the first-moment method. The existence of a gap interval is proven in a certain range of α, and bounds on this interval are found, which imply Eq. (5) in Theorem 1.7. Section 3 derives the lower bound, using a weighted second-moment method, as developed recently in [11,12], and presents numerical results. In Section 4 we discuss the behavior of the lower bound for large K. The case of $x = \frac{1}{2}$ is treated rigorously, and Eq. (7) in Theorem 1.7 is proven. Other values of x are treated at the heuristic level. Section 5 presents a proof of Theorem 1.6. We discuss our results in Section 6.

2. Upper bound: The first moment method

The first moment method relies on Markov's inequality:

Lemma 2.1. *Let X be a non-negative random variable. Then*

$$\mathbf{P}(X \geq 1) \leq \mathbf{E}(X)\,. \tag{8}$$

We take X to be the number of pairs of SAT-assignments at fixed distance:

$$Z(x, F) = \sum_{\vec{\sigma},\vec{\tau}} \delta\left(d_{\vec{\sigma}\vec{\tau}} \in [Nx + \epsilon(N), Nx - \epsilon(N)]\right)\ \delta\left[\vec{\sigma},\ \vec{\tau} \in S(F)\right], \tag{9}$$

where $F = F_K(N, N\alpha)$ is a random K-CNF formula, and $S(F)$ is the set of SAT-assignments to this formula. Throughout this paper $\delta(A)$ is an indicator function, equal to 1 if the statement A is true, equal to 0 otherwise. The expectation $\mathbf{E}$ is over the set of random K-CNF formulae. Since $Z(x, F) \geq 1$ is equivalent to 'F is x-satisfiable', (8) gives an upper bound for the probability of x-satisfiability.

The expected value of the double sum can be rewritten as:

$$\mathbf{E}(Z) = 2^N \sum_{d \in [Nx+\epsilon(N), Nx-\epsilon(N)] \cap \mathbb{N}} \binom{N}{d} \mathbf{E}\left[\delta\left(\vec{\sigma}, \vec{\tau} \in S(F)\right)\right], \tag{10}$$

where $\vec{\sigma}$ and $\vec{\tau}$ are any two assignments with Hamming distance d. We have $\delta\left(\vec{\sigma}, \vec{\tau} \in S(F)\right) = \prod_c \delta\left(\vec{\sigma}, \vec{\tau} \in S(c)\right)$, where c denotes one of the M-clauses. All clauses are drawn independently, so that we have:

$$\mathbf{E}(Z) \leq (2\epsilon(N) + 1) 2^N \max_{d \in [Nx+\epsilon(N), Nx-\epsilon(N)] \cap \mathbb{N}} \left\{ \binom{N}{d} \left(\mathbf{E}\left[\delta\left(\vec{\sigma}, \vec{\tau} \in S(c)\right)\right]\right)^M \right\}, \tag{11}$$

where we have bounded the sum by the maximal term times the number of terms. $\mathbf{E}\left[\delta\left(\vec{\sigma}, \vec{\tau} \in S(c)\right)\right]$ can easily be calculated and its value is: $1 - 2^{1-K} + 2^{-K}(1-x)^K + o(1)$. Indeed there are only two realizations of the clause among 2^K that do not satisfy c unless the two configurations overlap exactly on the domain of c.

Considering the normalized logarithm of this quantity,

$$F(x, \alpha) = \lim_{N\to\infty} \frac{1}{N} \ln \mathbf{E}(Z) = \ln 2 + H_2(x) + \alpha \ln\left(1 - 2^{1-K} + 2^{-K}(1-x)^K\right), \tag{12}$$

where $H_2(x) = -x \ln x - (1-x)\ln(1-x)$ is the two-state entropy function, one can deduce an upper bound for $\alpha_N(K, x)$. Indeed, $F(x, \alpha) < 0$ implies $\lim_{N\to\infty} \mathbf{P}(Z(x, F) \geq 1) = 0$. Therefore:

Theorem 2.2. *For each K and $0 < x < 1$, and for all α such that*

$$\alpha > \alpha_{UB}(K, x) = -\frac{\ln 2 + H_2(x)}{\ln(1 - 2^{1-K} + 2^{-K}(1-x)^K)}, \tag{13}$$

a random formula $F_K(N, N\alpha)$ is x-unsatisfiable w.h.p.

We observe numerically that a 'gap' (x_1, x_2 and α such that $x_1 < x < x_2 \Longrightarrow F(x, \alpha) < 0$) appears for $K \geq 6$. More generally, the following results holds, which implies Eq. (5) in Theorem 1.7:

Theorem 2.3. *Let $\epsilon \in (0, 1)$, and $\{y_K\}_{K\in\mathbb{N}}$ be a sequence verifying $K y_K \to \infty$ and $y_K = o(1)$. Denote by $H_2^{-1}(u)$ the smallest root to $H_2(x) = u$, with $u \in [0, \ln 2]$.*

There exists K_0 such that for all $K \geq K_0$, $\alpha \in [(1+\epsilon)2^{K-1} \ln 2, \alpha_N(K))$ and $x \in [y_K, H_2^{-1}(\alpha 2^{1-K} - \ln 2 - \epsilon)] \cup [1 - H_2^{-1}(\alpha 2^{1-K} - \ln 2 - \epsilon), 1]$, $F_K(N, N\alpha)$ is x-unsatisfiable w.h.p.

Proof. Clearly $(1+\epsilon)2^{K-1} \ln(2) < \alpha_N(K)$ since $\alpha_N(K) = 2^K \ln(2) - O_K(K)$ [12]. Observe that $(1 - y_K)^K = o(1)$. Then for all $\delta > 0$, there exists K_1 such that for all $K \geq K_1$, $x > y_K$:

$$\alpha_{UB}(x) < (1+\delta)2^{K-1}(\ln 2 + H_2(x)). \tag{14}$$

Inverting this inequality yields the theorem. □

The choice (9) of X, although it is the simplest one, is not optimal. The first moment method only requires the condition $X \geq 1$ to be equivalent to the x-satisfiability, and better choices of X exist which allow to improve the bound. Techniques similar to the one introduced separately by Dubois and Boufkhad [10] on the one hand, and Kirousis, Kranakis and Krizanc [9] on the other hand, can be used to obtain two tighter bounds. Quantitatively, it turns out that these more elaborate bounds provide only very little improvement over the simple bound (13) (see Fig. 2). For the sake of completeness, we give without proof the simplest of these bounds:

Theorem 2.4. *The unique positive solution of the equation*

$$\begin{aligned} H_2(x) &+ \alpha \ln\left(1 - 2^{1-K} + 2^{-K}(1-x)^K\right) + (1-x)\ln\left[2 - \exp\left(-K\alpha \frac{2^{1-K} - 2^{-K}(1-x)^{K-1}}{1 - 2^{1-K} + 2^{-K}(1-x)^K}\right)\right] \\ &+ x \ln\left[2 - \exp\left(-K\alpha \frac{2^{1-K} - 2^{1-K}(1-x)^{K-1}}{1 - 2^{1-K} + 2^{-K}(1-x)^K}\right)\right] = 0 \end{aligned} \tag{15}$$

is an upper bound for $\alpha_N(K, x)$. For $x = 0$ we recover the expression of [9].

The proof closely follows that of [9] and presents no notable difficulty. We also derived a tighter bound based on the technique used in [10], gaining only a small improvement over the bound of Theorem 2.4 (less than .001%).

3. Lower bound: The second moment method

The second moment method uses the following consequence of Chebyshev's inequality:

Lemma 3.1. *If X is a non-negative random variable, one has:*

$$\mathbf{P}(X > 0) \geq \frac{\mathbf{E}(X)^2}{\mathbf{E}(X^2)}. \tag{16}$$

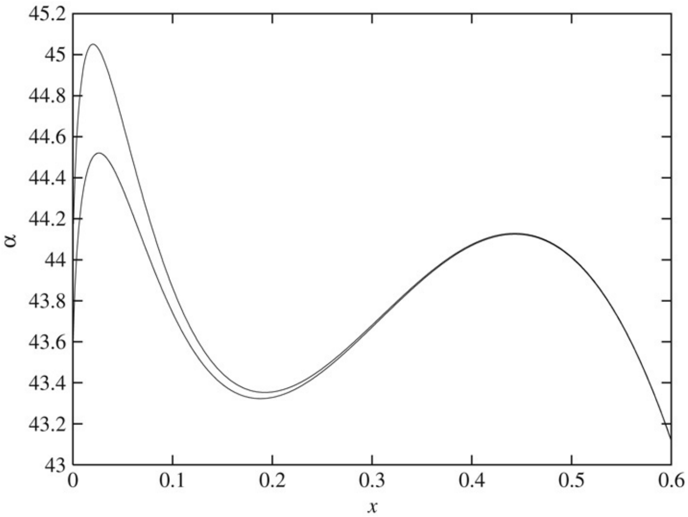

Fig. 2. Comparison between the simple upper bound (13) for $\alpha_N(K = 6, x)$ (top curve) and the refined one (bottom curve), as defined in Theorem 2.4.

It is well known that the simplest choice of X as the number of SAT-assignments (in our case the number of SAT-x-pairs) is bound to fail. The intuitive reason [11,12] is that this naive choice favors pairs of SAT-assignments with a great number of satisfying literals. It turns out that such assignments are highly correlated, since they tend to agree with each other, and this causes the failure of the second-moment method. In order to deal with *balanced* (with approximately half of literals satisfied) and uncorrelated pairs of assignments, one must consider a weighted sum of all SAT-assignments. Following [11,12], we define:

$$Z(x, F) = \sum_{\vec{\sigma},\vec{\tau}} \delta\left(d_{\vec{\sigma}\vec{\tau}} = \lfloor Nx \rfloor\right) W(\vec{\sigma}, \vec{\tau}, F), \tag{17}$$

where $\lfloor Nx \rfloor$ denotes the integer part of Nx. Note that the condition $d_{\vec{\sigma}\vec{\tau}} = \lfloor Nx \rfloor$ is stronger than Eq. (3). The weights $W(\vec{\sigma}, \vec{\tau}, F)$ are decomposed according to each clause:

$$W(\vec{\sigma}, \vec{\tau}, F) = \prod_c W(\vec{\sigma}, \vec{\tau}, c), \tag{18}$$

$$\text{with} \quad W(\vec{\sigma}, \vec{\tau}, c) = W(\vec{u}, \vec{v}), \tag{19}$$

where $\vec{u}, \vec{v}$ are K-component vectors such that: $u_i = 1$ if the ith literal of c is satisfied under $\vec{\sigma}$, and $u_i = -1$ otherwise (here we assume that the variables connected to c are arbitrarily ordered). $\vec{v}$ is defined in the same way with respect to $\vec{\tau}$. In order to have the equivalence between $Z > 0$ and the existence of pairs of SAT-assignments, we impose the following condition on the weights:

$$W(\vec{u}, \vec{v}) = \begin{cases} 0 & \text{if} \quad \vec{u} = (-1, \ldots, -1) \quad \text{or} \quad \vec{v} = (-1, \ldots, -1), \\ > 0 & \text{otherwise.} \end{cases} \tag{20}$$

Let us now compute the first and second moments of Z:

Claim 3.2.

$$\mathbf{E}(Z) = 2^N \binom{N}{\lfloor Nx \rfloor} f_1(x)^M, \tag{21}$$

where

$$f_1(x) = \mathbf{E}[W(\vec{\sigma}, \vec{\tau}, c)] \tag{22}$$

$$= 2^{-K} \sum_{\vec{u},\vec{v}} W(\vec{u}, \vec{v})(1 - x)^{|\overrightarrow{u \cdot v}|} x^{K - |\overrightarrow{u \cdot v}|}. \tag{23}$$

Here $|\vec{u}|$ is the number of indices i such that $u_i = +1$, and $\overrightarrow{u \cdot v}$ denotes the vector $(u_1 v_1, \ldots, u_K v_K)$.

Writing the second moment is a little more cumbersome:

Claim 3.3.

$$\mathbf{E}(Z^2) = 2^N \sum_{\mathbf{a}\in V_N\cap\{0,1/N,2/N,\dots,1\}^8} \frac{N!}{\prod_{i=0}^{7}(Na_i)!} f_2(\mathbf{a})^M, \tag{24}$$

where

$$\begin{aligned} f_2(\mathbf{a}) &= \mathbf{E}[W(\vec{\sigma},\vec{\tau},c)W(\vec{\sigma},\vec{\tau},c)] \\ &= 2^{-K}\sum_{\vec{u},\vec{v},\vec{u}',\vec{v}'} W(\vec{u},\vec{v})W(\vec{u}',\vec{v}')\prod_{i=1}^{K} a_0^{\delta(u_i=v_i=u_i'=v_i')} a_1^{\delta(u_i=v_i=u_i'\neq v_i')} a_2^{\delta(u_i=v_i=v_i'\neq u_i')} a_3^{\delta((u_i=v_i)\neq(u_i'=v_i'))} \\ &\quad a_4^{\delta(u_i=u_i'=v_i'\neq v_i)} a_5^{\delta((u_i=u_i')\neq(v_i=v_i'))} a_6^{\delta((u_i=v_i')\neq(u_i'=v_i))} a_7^{\delta(u_i'=v_i'=u_i\neq u_i)} \end{aligned} \tag{25}$$

a *is a* 8*-component vector giving the proportion of each type of quadruplets* $(\tau_i,\sigma_i,\tau_i',\sigma_i')$ *–* $\vec{\tau}$ *being arbitrarily (but without losing generality) fixed to* $(1,\dots,1)$ *– as described in the following table:*

	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7
τ_i	+	+	+	+	+	+	+	+
σ_i	+	+	+	+	−	−	−	−
τ_i'	+	+	−	−	+	+	−	−
σ_i'	+	−	+	−	+	−	+	−

The set $V_N \subset [0,1]^8$ *is a simplex specified by:*

$$\begin{cases} \lfloor N(a_4+a_5+a_6+a_7)\rfloor = \lfloor Nx\rfloor \\ \lfloor N(a_1+a_2+a_5+a_6)\rfloor = \lfloor Nx\rfloor \\ \sum_{i=0}^{7} a_i = 1. \end{cases} \tag{26}$$

These three conditions (26) correspond to the normalization of the proportions and to the enforcement of the conditions $d_{\vec{\sigma}\vec{\tau}} = \lfloor Nx\rfloor$, $d_{\vec{\sigma}'\vec{\tau}'} = \lfloor Nx\rfloor$. When $N\to\infty$, $V = \bigcap_{N\in\mathbb{N}} V_N$ defines a five-dimensional simplex described by the three hyperplanes:

$$\begin{cases} a_4+a_5+a_6+a_7 = x \\ a_1+a_2+a_5+a_6 = x \\ \sum_{i=0}^{7} a_i = 1. \end{cases} \tag{27}$$

In order to yield an asymptotic estimate of $\mathbf{E}(Z^2)$ we first use the following lemma, which results from a simple approximation of integrals by sums:

Lemma 3.4. *Let* $\psi(\mathbf{a})$ *be a real, positive, continuous function of* **a**, *and let* V_N, V *be defined as previously. Then there exists a constant* C_0 *depending on* x *such that for sufficiently large* N*:*

$$\sum_{\mathbf{a}\in V_N\cap\{1/N,2/N,\dots,1\}^8} \frac{N!}{\prod_{i=0}^{7}(Na_i)!}\psi(\mathbf{a})^N \le C_0 N^{3/2}\int_V \mathrm{d}\mathbf{a}\, e^{N[H_8(\mathbf{a})+\ln\psi(\mathbf{a})]}, \tag{28}$$

where $\sum_{i=0}^{7} a_i \ln a_i$.

A standard Laplace method[1] used on Eq. (28) with $\psi = 2(f_2)^\alpha$ yields:

[1] The method is carried out on the simplex V, which can be parametrized by the five variables (a_0,a_1,a_2,a_4,a_5). From this point on this parametrization will implicitly be used for calculations.

Claim 3.5. *For each K, x, define:*

$$\Phi(\mathbf{a}) = H_8(\mathbf{a}) - \ln 2 - 2H_2(x) + \alpha \ln f_2(\mathbf{a}) - 2\alpha \ln f_1(x). \tag{29}$$

and let $\mathbf{a}_0 \in V$ be the global maximum of Φ restricted to V. Suppose that $\partial^2_{\mathbf{a}}\Phi(\mathbf{a}_0)$ is definite negative. Then there exists a constant C_1 such that, for N sufficiently large,

$$\frac{\mathbf{E}(Z)^2}{\mathbf{E}(Z^2)} \geq C_1 \exp(-N\Phi(\mathbf{a}_0)). \tag{30}$$

Obviously $\Phi(\mathbf{a}_0) \geq 0$ in general. In order to use Lemma 3.1, one must find the weights $W(\vec{u}, \vec{v})$ in such a way that $\max_{\mathbf{a}\in V} \Phi(\mathbf{a}) = 0$. We first notice that, at the particular point $\mathbf{a}^*$ where the two pairs are uncorrelated with each other,

$$a_0^* = a_3^* = \frac{(1-x)^2}{2}, \quad a_1^* = a_2^* = a_4^* = a_7^* = \frac{x(1-x)}{2}, \quad a_5^* = a_6^* = \frac{x^2}{2}, \tag{31}$$

we have the following properties:

- $H_8(\mathbf{a}^*) = \ln 2 + 2H_2(x)$,
- $\partial_{\mathbf{a}} H_8(\mathbf{a}^*) = 0$, $\partial^2_{\mathbf{a}} H_8(\mathbf{a}^*)$ definite negative,
- $f_1(x)^2 = f_2(\mathbf{a}^*)$ and hence $\Phi(\mathbf{a}^*) = 0$.

(Note that the derivatives $\partial_{\mathbf{a}}$ are taken in the simplex V). So the weights must be chosen in such a way that $\mathbf{a}^*$ be the global maximum of Φ. A necessary condition is that $\mathbf{a}^*$ be a local maximum, which entails $\partial_{\mathbf{a}} f_2(\mathbf{a}^*) = 0$.

Using the fact that the number of common values between four vectors $\vec{u}, \vec{v}, \vec{u}', \vec{v}' \in \{-1, 1\}^K$ can be written as:

$$\frac{1}{8}\left(K + \vec{u}\cdot\vec{v} + \vec{u}\cdot\vec{u}' + \vec{u}\cdot\vec{v}' + \vec{v}\cdot\vec{u}' + \vec{v}\cdot\vec{v}' + \vec{u}'\cdot\vec{v}' + \overrightarrow{u\cdot v}\cdot\overrightarrow{u'\cdot v'}\right) \tag{32}$$

we deduce from $\partial_{\mathbf{a}} f_2(\mathbf{a}^*) = 0$ the condition:

$$\sum_{\vec{u},\vec{v}} W(\vec{u},\vec{v}) \begin{cases}\vec{u}\\ \vec{v}\end{cases} (1-x)^{|\overrightarrow{u\cdot v}|} x^{K-|\overrightarrow{u\cdot v}|} = 0, \tag{33}$$

$$\begin{aligned}0 \;=\; & K(2x-1)^2\left[\sum_{\vec{u},\vec{v}} W(\vec{u},\vec{v})(1-x)^{|\overrightarrow{u\cdot v}|}x^{K-|\overrightarrow{u\cdot v}|}\right]^2 + \left[\sum_{\vec{u},\vec{v}} W(\vec{u},\vec{v})\overrightarrow{u\cdot v}\,(1-x)^{|\overrightarrow{u\cdot v}|}x^{K-|\overrightarrow{u\cdot v}|}\right]^2 \\ & + 2(2x-1)\left[\sum_{\vec{u},\vec{v}} W(\vec{u},\vec{v})\vec{u}\cdot\vec{v}\,(1-x)^{|\overrightarrow{u\cdot v}|}x^{K-|\overrightarrow{u\cdot v}|}\right]\left[\sum_{\vec{u},\vec{v}} W(\vec{u},\vec{v})(1-x)^{|\overrightarrow{u\cdot v}|}x^{K-|\overrightarrow{u\cdot v}|}\right]. \end{aligned} \tag{34}$$

If we suppose that W is invariant under simultaneous and identical permutations of the u_i or of the v_i (which we must, since the ordering of the variables by the label i is arbitrary), the K-components of all vectorial quantities in Eqs. (33) and (34) should be equal. Then we obtain equivalently:

$$\sum_{\vec{u},\vec{v}} W(\vec{u},\vec{v})(2|\vec{u}| - K)\,(1-x)^{|\overrightarrow{u\cdot v}|}x^{K-|\overrightarrow{u\cdot v}|} = 0 \quad \text{and} \quad \vec{u} \leftrightarrow \vec{v}, \tag{35}$$

$$\sum_{\vec{u},\vec{v}} W(\vec{u},\vec{v})(K(2x-1) + \vec{u}\cdot\vec{v})(1-x)^{|\overrightarrow{u\cdot v}|}x^{K-|\overrightarrow{u\cdot v}|} = 0, \tag{36}$$

We choose the following simple form for $W(\vec{u}, \vec{v})$:

$$W(\vec{u},\vec{v}) = \begin{cases} 0 & \text{if } \vec{u} = (-1,\ldots,-1) \quad \text{or} \quad \vec{v} = (-1,\ldots,-1), \\ \lambda^{|\vec{u}|+|\vec{v}|}\nu^{|\overrightarrow{u\cdot v}|} & \text{otherwise.}\end{cases} \tag{37}$$

Although this choice is certainly not optimal, it turns out particularly tractable. Eqs. (35) and (36) simplify to:

$$\begin{aligned}[\nu(1-x)]^{K-1} &= (\lambda^2 + 1 - 2\lambda\nu)\big(2\lambda x + \nu(1-x)(1+\lambda^2)\big)^{K-1} \\ (\nu(1-x) + \lambda x)^{K-1} &= (1-\lambda\nu)\big(2\lambda x + \nu(1-x)(1+\lambda^2)\big)^{K-1}.\end{aligned} \tag{38}$$

We found numerically a unique solution $\lambda > 0$, $\nu > 0$ to these equations for any value of $K \geq 2$ that we checked.

Fixing (λ, ν) to a solution of (38), we seek the largest value of α such that the local maximum $\mathbf{a}^*$ is a global maximum, i.e. such that there exists no $\mathbf{a} \in V$ with $\Phi(\mathbf{a}) > 0$. To proceed one needs analytical expressions for $f_1(x)$ and $f_2(\mathbf{a})$. f_1 simply reads:

$$f_1(x) = 2^{-K}\left((1-x)\nu(1+\lambda^2) + 2x\lambda\right)^K - 2\cdot 2^{-K}(x\lambda + (1-x)\nu)^K + 2^{-K}((1-x)\nu)^K \tag{39}$$

f_2 is calculated by Sylvester's formula, but its expression is long and requires preliminary notations. We index the 16 possibilities for (u_i, v_i, u_i', v_i') by a number $r \in \{0, \ldots, 15\}$ defined as:

$$r = 8\frac{1-u_i}{2} + 4\frac{1-v_i}{2} + 2\frac{1-u_i'}{2} + \frac{1-v_i'}{2}. \tag{40}$$

For each index r, define

$$l(r) = \delta(u_i = 1) + \delta(v_i = 1) + \delta(u_i' = 1) + \delta(v_i' = 1), \tag{41}$$

$$n(r) = \delta(u_i v_i = 1) + \delta(u_i' v_i' = 1), \tag{42}$$

and

$$z_r = \lambda^{l(r)}\nu^{n(r)} \times \begin{cases} a_r & \text{if } r \leq 7 \\ a_{15-r} & \text{if } r \geq 8. \end{cases} \tag{43}$$

Also define the four following subsets of $\{0, \ldots, 15\}$: A_0 is the set of indices r corresponding to quadruplets of the form $(-1, v_i, u_i', v_i')$. $A_0 = \{r \in \{0, \ldots, 15\} \mid u_i = -1\}$. Similarly, $A_1 = \{r \mid v_i = -1\}$, $A_2 = \{r \mid u_i' = -1\}$ and $A_3 = \{r \mid v_i' = -1\}$.

Then f_2 is given by:

$$2^K f_2(\mathbf{a}) = \left(\sum_{j=0}^{15} z_j\right)^K - \sum_{k=0}^{3}\left(\sum_{j\in A_k} z_j\right)^K + \sum_{0\leq k<k'\leq 3}\left(\sum_{j\in A_k\cap A_{k'}} z_j\right)^K - \sum_{0\leq k<k'<k''\leq 3}\left(\sum_{j\in A_k\cap A_{k'}\cap A_{k''}} z_j\right)^K + \left(\sum_{j\in A_0\cap A_1\cap A_2\cap A_3} z_j\right)^K. \tag{44}$$

We can now state our lower-bound result:

Lemma 3.6. *Let $\alpha_+ \in (0, +\infty]$ be the smallest α such that $\partial^2_{\mathbf{a}}\Phi(\mathbf{a}^*)$ is not definite negative. For each K and $x \in (0, 1)$, and for all $\alpha \leq \alpha_{LB}(K, x)$, with*

$$\alpha_{LB}(K, x) = \min\left[\alpha_+, \inf_{\mathbf{a}\in V_+} \frac{\ln 2 + 2H_2(x) - H_8(\mathbf{a})}{\ln f_2(\mathbf{a}) - 2\ln f_1(x)}\right], \tag{45}$$

where $V_+ = \{\mathbf{a} \in V \mid f_2(\mathbf{a}) > f_1^2(1/2)\}$, and where (λ, ν) is chosen to be a positive solution of (38), the probability that a random formula $F_K(N, N\alpha)$ is x-satisfiable is bounded away from 0 as $N \to \infty$.

This is a straightforward consequence of the expression (29) of $\Phi(\mathbf{a})$. Note that $\alpha_{LB}(K, x)$ could be trivial. We rule this out numerically for general x, and rigorously for $x = \frac{1}{2}$.

Theorem 1.6 and Lemma 3.6 immediately imply:

Theorem 3.7. *For all $\alpha < \alpha_{LB}(K, x)$ defined in Lemma 3.6, a random K-CNF formula $F_K(N, N\alpha)$ is x-satisfiable w.h.p.*

We devised several numerical strategies to evaluate $\alpha_{LB}(K, x)$. The implementation of Powell's method on each point of a grid of size $\mathcal{N}^5$ ($\mathcal{N} = 10, 15, 20$) on V turned out to be the most efficient and reliable. The results are given by Fig. 1 for $K = 8$, the smallest K such that the picture given by Conjecture 1.4 is confirmed. We found a clustering phenomenon for all the values of $K \geq 8$ that we checked. In the following we shall provide a rigorous estimate of $\alpha_{LB}\left(K, \frac{1}{2}\right)$ at large K.

4. Large K analysis

4.1. Asymptotics for $x = \frac{1}{2}$

The main result of this section is contained in the following theorem, which implies Eq. (7) in Theorem 1.7:

Theorem 4.1. *The large K asymptotics of $\alpha_{LB}(K, x)$ at $x = 1/2$ is given by:*

$$\alpha_{LB}(K, 1/2) \sim 2^K \ln 2. \tag{46}$$

The proof primarily relies on the following results:

Claim 4.2. *Let $\nu = 1$ and λ be the unique positive root of:*

$$(1-\lambda)(1+\lambda)^{K-1} - 1 = 0. \tag{47}$$

Then (λ, ν) is solution to (38) with $x = \frac{1}{2}$ and one has, at large K:

$$\lambda - 1 \sim -2^{1-K}. \tag{48}$$

Lemma 4.3. *Let $x = \frac{1}{2}$. There exist $K_0 > 0$, $C_1 > 0$ and $C_2 > 0$ such that for all $K \geq K_0$, and for all $\mathbf{a} \in V$ s.t. $|\mathbf{a} - \mathbf{a}^*| < 1/8$,*

$$|\ln f_2(\mathbf{a}) - 2 \ln f_1(1/2)| \leq K^2 C_1 |\mathbf{a} - \mathbf{a}^*|^2 2^{-2K} + C_2 |\mathbf{a} - \mathbf{a}^*|^3 2^{-K}. \tag{49}$$

Lemma 4.4. *Let $x = \frac{1}{2}$. There exist $K_0 > 0$, $C_0 > 0$ such that for $K \geq K_0$, for all $\mathbf{a} \in V$,*

$$\begin{aligned} |\ln f_2(\mathbf{a}) - 2 \ln f_1(1/2)| \leq 2^{-K} \Big[&(a_0 + a_1 + a_4 + a_5)^K + (a_0 + a_2 + a_4 + a_6)^K \\ &+ (a_0 + a_1 + a_6 + a_7)^K + (a_0 + a_2 + a_5 + a_7)^K \Big] + C_0 K 2^{-2K}. \end{aligned} \tag{50}$$

The proofs of these lemmas are deferred to Sections 4.3 and 4.4.

4.2. Proof of Theorem 4.1

We first show that $\partial^2_{\mathbf{a}} \Phi(\mathbf{a}^*)$ is definite negative for all $\alpha < 2^K$, when K is sufficiently large. Indeed $\partial^2_{\mathbf{a}} H_8(\mathbf{a}^*)$ is definite negative and its largest eigenvalue is -4. Using Lemma 4.3, for $\mathbf{a} \in V$ close enough to $\mathbf{a}^*$:

$$\Phi(\mathbf{a}) \leq -2|\mathbf{a} - \mathbf{a}^*|^2 + \alpha C_1 |\mathbf{a} - \mathbf{a}^*|^2 K^2 2^{-2K} + \alpha C_2 |\mathbf{a} - \mathbf{a}^*|^3 2^{-K}. \tag{51}$$

Therefore

$$\Phi(\mathbf{a}) \leq -|\mathbf{a} - \mathbf{a}^*|^2 \quad \text{for } K \text{ large enough, } |\mathbf{a} - \mathbf{a}^*| < \frac{1}{2C_2} \text{ and } \alpha < 2^K. \tag{52}$$

Using Theorem 3.6, we need to find the minimum, for $a \in V_+$, of

$$G(K, \mathbf{a}) \equiv \frac{3 \ln 2 - H_8(\mathbf{a})}{\ln f_2(\mathbf{a}) - 2 \ln f_1(1/2)}. \tag{53}$$

We shall show that

$$\inf_{\mathbf{a} \in V_+} G(K, \mathbf{a}) \sim 2^K \ln 2. \tag{54}$$

We divide this task in two parts. The first part states that there exists $R > 0$ and K_1 such that for all $K \geq K_1$, and for all $\mathbf{a} \in V_+$ such that $|\mathbf{a} - \mathbf{a}^*| < R$, $G(K, \mathbf{a}) > 2^K$. This is a consequence of Lemma 4.3; using the fact that $3 \ln 2 - H_8(\mathbf{a}) \geq |\mathbf{a} - \mathbf{a}^*|^2$ for $\mathbf{a}$ close enough to $\mathbf{a}^*$, one obtains:

$$G(K, \mathbf{a}) \geq \frac{2^K}{C_1 K^2 2^{-K} + C_2 |\mathbf{a} - \mathbf{a}^*|} \tag{55}$$

which, for K large enough and $\mathbf{a}$ close enough to $\mathbf{a}^*$, is greater than 2^K.

The second part deals with the case where $\mathbf{a}$ is far from $\mathbf{a}^*$, i.e. $|\mathbf{a}-\mathbf{a}^*| > R$. First we put a bound on the numerator of $G(\mathbf{a})$: There exists a constant $C_3 > 0$ such that for all $\mathbf{a} \in V$ s.t. $|\mathbf{a}-\mathbf{a}^*| > R$, one has $3\ln 2 - H_8(\mathbf{a}) > C_3$.

Looking at Eq. (50), it is clear that, in order to minimize $G(K, \mathbf{a})$, $\mathbf{a}$ should be 'close' to at least one the four hyperplanes defined by

$$a_0 + a_1 + a_4 + a_5 = 1, \qquad a_0 + a_2 + a_4 + a_6 = 1,$$
$$a_0 + a_1 + a_6 + a_7 = 1, \qquad a_0 + a_2 + a_5 + a_7 = 1. \tag{56}$$

More precisely, we say for instance that $\mathbf{a}$ is *close to* the first hyperplane defined above iff

$$a_0 + a_1 + a_4 + a_5 > 1 - K^{-1/2}. \tag{57}$$

Now suppose that $\mathbf{a}$ is *not* close to that hyperplane. Then the corresponding term goes to 0:

$$(a_0 + a_1 + a_4 + a_5)^K \le \left(1 - K^{-1/2}\right)^K \sim \exp(-\sqrt{K}) \quad \text{as } K \to \infty. \tag{58}$$

We classify all possible cases according to the number of hyperplanes $\mathbf{a} \in V_+$ is close to:

- $\mathbf{a}$ is close to none of the hyperplanes. Then

$$G(K, \mathbf{a}) \ge \frac{2^K C_3}{4\exp(-\sqrt{K}) + C_0 K 2^{-K}} > 2^K \qquad \text{for } K \text{ large enough.} \tag{59}$$

- $\mathbf{a}$ is close to one hyperplane only, e.g. the first hyperplane $a_0 + a_1 + a_4 + a_5 = 1$ (the other hyperplanes are treated equivalently). As $\sum_{i=0}^{7} a_i = 0$, one has

$$a_2 < K^{-1/2}, \quad a_3 < K^{-1/2}, \quad a_6 < K^{-1/2}, \quad a_7 < K^{-1/2}. \tag{60}$$

  This implies $H_8(\mathbf{a}) < 2\ln 2 + 2\ln K/\sqrt{K}$, and we get:

$$G(K, \mathbf{a}) \ge \frac{2^K[\ln 2 - 2\ln K/\sqrt{K}]}{1 + C_0 K 2^{-K} + 3\,\mathrm{e}^{-\sqrt{K}}} \ge 2^K(\ln 2)\left[1 - 3\ln K/\sqrt{K}\right] \tag{61}$$

  for sufficiently large K.
- $\mathbf{a}$ is close to two hyperplanes. It is easy to check that these hyperplanes must be either the first and the fourth ones, or the second and the third ones. In the first case we have $a_0 + a_5 > 1 - 3/\sqrt{K}$ and in the second case $a_0 + a_6 > 1 - 3/\sqrt{K}$. Both cases imply: $H_8(\mathbf{a}) < \ln 2 + 3\ln K/\sqrt{K}$. One thus obtains:

$$G(K, \mathbf{a}) \ge \frac{2^K[2\ln 2 - 3\ln K/\sqrt{K}]}{2 + C_0 K 2^{-K} + 2\,\mathrm{e}^{-\sqrt{K}}} \ge 2^K(\ln 2)\left[1 - 3\ln K/\sqrt{K}\right]. \tag{62}$$

- One can check that $\mathbf{a}$ cannot be close to more than two hyperplanes.

To sum up, we have proved that for K large enough, for all $\mathbf{a} \in V_+$,

$$G(K, \mathbf{a}) \ge 2^K(\ln 2)\left[1 - 3\ln K/\sqrt{K}\right], \tag{63}$$

Clearly, $\alpha_{LB}(K, 1/2) = \inf_{\mathbf{a}\in V_+} G(K, \mathbf{a}) < \alpha_{UB}(K, 1/2)$. Since from Theorem 2.2 we know that $\alpha_{UB}(K, 1/2) \sim 2^K \ln 2$, this proves Eq. (54).

4.3. *Proof of Lemma* 4.3

Let $x = \frac{1}{2}$ and choose $\nu = 1$ and λ the unique positive root of Eq. (47). Let $\epsilon_i = a_i - 1/8$, and $\boldsymbol{\epsilon} = (\epsilon_0, \ldots, \epsilon_7)$. We expand $f_2(\mathbf{a})$ in series of $\boldsymbol{\epsilon}$. The zeroth order term is $f_2(1/8, \ldots, 1/8) = f_1^2(1/2)$. The first order term vanishes. We thus get:

$$f_2(\mathbf{a}) = f_1^2(1/2) + B_0 - B_1 + B_2 - B_3 + B_4, \tag{64}$$

with

$$B_0 = \sum_{q=2}^{K} \binom{K}{q} \left(\frac{1}{2} \sum_{i=0}^{7} p_i(\lambda)\epsilon_i \right)^q \left[\frac{1+\lambda}{2} \right]^{4(K-q)}, \tag{65}$$

$$B_1 = 2^{-K} \sum_{a=1}^{4} \sum_{q=2}^{K} \binom{K}{q} \left[\sum_{i=0}^{7} \left(\lambda^{\ell_{ai}} - 1 \right) \epsilon_i \right]^q \left[\frac{1+\lambda}{2} \right]^{3(K-q)}, \tag{66}$$

$$B_2 = 2^{-2K} \sum_{a=1}^{6} \sum_{q=2}^{K} \binom{K}{q} [2r_a(\lambda, \boldsymbol{\epsilon})]^q \left[\frac{1+\lambda}{2} \right]^{2(K-q)}, \tag{67}$$

$$B_3 = 2^{-3K} \sum_{a=1}^{4} \sum_{q=2}^{K} \binom{K}{q} [4s_a(\lambda, \boldsymbol{\epsilon})]^q \left[\frac{1+\lambda}{2} \right]^{K-q}, \tag{68}$$

$$B_4 = 2^{-4K} \sum_{k=2}^{K} (8\epsilon_0)^q. \tag{69}$$

In B_0, $p_i(\lambda) = \lambda^{l(i)} + \lambda^{l(15-i)} - 2 - 4(\lambda - 1)$. We have used the fact that $\sum_{i=0}^{7} \epsilon_i = 0$. Using $l(i) + l(15-i) = 4$, one obtains $|p_i(\lambda)| \le 11(\lambda - 1)^2 \le 11 \cdot 2^{4-2K}$, since $|\lambda - 1| \le 2^{2-K}$ for K large enough, by virtue of Lemma 4.2.

In B_1, we have used again $\sum_{i=0}^{7} \epsilon_i = 0$. ℓ_{ai} is either $l(i)$ or $l(15-i)$, depending on a. In both cases $|\lambda^{\ell_{ai}} - 1| \le 4|\lambda - 1| \le 2^{4-K}$. In B_2 and B_3, the expressions of $r_a(\lambda, \boldsymbol{\epsilon})$ and $s_a(\lambda, \boldsymbol{\epsilon})$ are given by:

$$\begin{aligned} &r_1 = \epsilon_0 + \lambda(\epsilon_1 + \epsilon_2) + \lambda^2\epsilon_3, \qquad r_2 = \epsilon_0 + \lambda(\epsilon_1 + \epsilon_4) + \lambda^2\epsilon_5, \\ &r_3 = \epsilon_0 + \lambda(\epsilon_2 + \epsilon_4) + \lambda^2\epsilon_6, \qquad r_4 = \epsilon_0 + \lambda(\epsilon_1 + \epsilon_7) + \lambda^2\epsilon_6, \\ &r_5 = \epsilon_0 + \lambda(\epsilon_2 + \epsilon_7) + \lambda^2\epsilon_5, \qquad r_6 = \epsilon_0 + \lambda(\epsilon_4 + \epsilon_7) + \lambda^2\epsilon_3, \end{aligned} \tag{70}$$

$$s_1 = \epsilon_0 + \lambda\epsilon_1, \qquad s_2 = \epsilon_0 + \lambda\epsilon_2, \qquad s_3 = \epsilon_0 + \lambda\epsilon_4, \qquad s_4 = \epsilon_0 + \lambda\epsilon_7. \tag{71}$$

In order to prove Lemma 4.3 we will use the following fact:

Claim 4.5. *Let y be a real variable such that $|y| \le 1$. Then*

$$\left| \sum_{k=2}^{K} \binom{K}{k} y^k \right| \le \frac{K(K-1)}{2} y^2 + 2^K |y|^3. \tag{72}$$

One has $|2r_a| \le 8|\boldsymbol{\epsilon}|$, $|4s_a| \le 8|\boldsymbol{\epsilon}|$, and $|8\epsilon_0| \le 8|\boldsymbol{\epsilon}|$. Therefore, for $|\boldsymbol{\epsilon}| < 1/8$, one can write:

$$|B_0| \le \frac{K(K-1)}{2} (11 \cdot 2^6)^2 2^{-4K} |\boldsymbol{\epsilon}|^2 + (11 \cdot 2^6)^3 2^{-5K} |\boldsymbol{\epsilon}|^3 \tag{73}$$

$$|B_1| \le 4 \frac{K(K-1)}{2} 2^{14} 2^{-3K} |\boldsymbol{\epsilon}|^2 + 2^{21} 2^{-3K} |\boldsymbol{\epsilon}|^3 \tag{74}$$

$$|B_i| \le \binom{4}{i} \frac{K(K-1)}{2} 2^6 2^{-iK} |\boldsymbol{\epsilon}|^2 + 2^9 2^{-(i-1)K} |\boldsymbol{\epsilon}|^3 \quad \text{for } 2 \le i \le 4. \tag{75}$$

Observe that

$$f_1(1/2) = \left[\left(\frac{1+\lambda}{2} \right)^K - 2^{-K} \right]^2 = 1 + O(K 2^{-K}) \tag{76}$$

and that for K large enough,

$$\left| \ln \frac{f_2(\mathbf{a})}{f_1^2(1/2)} \right| \le \frac{2}{f_1(1/2)^2} \sum_{i=0}^{4} |B_i|, \tag{77}$$

which proves Lemma 4.3.

4.4. Proof of Lemma 4.4

Note that the bounds on B_0 and B_1 (73), (74) remain valid for any $\boldsymbol{\epsilon}$. Therefore $B_0 = O(2^{-2K})$ and $B_1 = O(2^{-2K})$ uniformly. We bound B_3 by observing that:

$$B_3 = 2^{-K}\left[(a_0+\lambda a_1)^K + (a_0+\lambda a_2)^K + (a_0+\lambda a_4)^K + (a_0+\lambda a_7)^K\right] - 2^{-3K}\sum_{a=1}^{4}\left[\frac{1+\lambda}{2}\right]^K\left[1+K\left(\frac{8s_a(\lambda,\boldsymbol{\epsilon})}{1+\lambda}\right)\right]. \tag{78}$$

Since $(a_0+\lambda a_1) \le a_0 + a_1 \le 1/2$ and likewise for the three other terms, one has $B_3 = O(2^{-2K})$ uniformly in $\mathbf{a}$. A similar argument yields $B_4 = O(2^{-2K})$. There remains B_2, which we write as:

$$B_2 = 2^{-K}\sum_{0\le k<k'\le 3}\left(\sum_{j\in A_k\cap A_{k'}} z_j\right)^K - 2^{-2K}\sum_{a=1}^{6}\left[\frac{1+\lambda}{2}\right]^{2K}\left[1+K\left(\frac{8r_a(\lambda,\boldsymbol{\epsilon})}{(1+\lambda)^2}\right)\right]. \tag{79}$$

The second term of the sum is $O(K2^{-2K})$. The first term is made of six contributions. Two of them, namely $2^{-K}(a_0+\lambda(a_1+a_2)+\lambda^2 a_3)$ and $2^{-K}(a_0+\lambda(a_4+a_7)+\lambda^2 a_3)$, are $O(2^{-2K})$, because of the condition on distances. Among the four remaining contributions, we show how to deal with one of them, the others being handled similarly. This contribution can be written as:

$$(a_0+\lambda(a_1+a_4)+\lambda^2 a_5)^K = (a_0+a_1+a_4+a_5)^K\left(1+\frac{(\lambda-1)(a_1+a_4)+(\lambda^2-1)a_5}{a_0+a_1+a_4+a_5}\right)^K. \tag{80}$$

We distinguish two cases. Either $a_0+a_1+a_4+a_5 \le 1/2$, and we get trivially:

$$(a_0+\lambda(a_1+a_4)+\lambda^2 a_5)^K - (a_0+a_1+a_4+a_5)^K = O(2^{-K}), \tag{81}$$

since both terms are $O(2^{-K})$; or $a_0+a_1+a_4+a_5 \ge 1/2$, and then:

$$\left|(a_0+\lambda(a_1+a_4)+\lambda^2 a_5)^K - (a_0+a_1+a_4+a_5)^K\right| \le \left|\left(1+\frac{(\lambda-1)(a_1+a_4)+(\lambda^2-1)a_5}{a_0+a_1+a_4+a_5}\right)^K - 1\right| = O(K2^{-K}). \tag{82}$$

Using again Eq. (76) finishes the proof of Lemma 4.4. □

4.5. Heuristics for arbitrary x

For arbitrary x, the function to minimize in (45) is hard to study analytically. Here we present what we believe to be the correct asymptotic expansion of $\alpha_{LB}(K,x)$ at large K. Hopefully this temptative analysis could be used as a starting point towards a rigorous analytical treatment for any x.

A careful look at the numerics suggests the following Ansatz on the position of the global maximum, at large K:

$$a_0 = 1-x+o(1), \quad a_6 = x+o(1)$$
$$a_i = o(1) \quad \text{for } i \ne 0, 6. \tag{83}$$

A second, symmetric, maximum also exists around $a_0 = 1-x$, $a_5 = x$. Plugging this locus into Eq. (45) leads to the following conjecture:

Conjecture 4.6. *For all $x \in (0,1]$, the asymptotics of $\alpha_{LB}(x)$ is given by:*

$$\lim_{K\to\infty} 2^{-K}\alpha_{LB}(K,x) = \frac{\ln 2 + H(x)}{2}, \tag{84}$$

and the limit is uniform on any closed sub-interval of $(0,1]$.

This conjecture is consistent with both our numerical simulations and our result at $x = \frac{1}{2}$.

5. Proof of Theorem 1.6

Starting with the sharpness criterion for monotone properties of the hypercube given by E. Friedgut and J. Bourgain, we will prove Theorem 1.6 by using techniques and tools developed by N. Creignou and H. Daudé for proving the sharpness of monotone properties in random CSPs.

First we make precise some notations for this study on random K-CNF formula over N Boolean variables $\{x_1, \ldots, x_N\}$. A K-clause C is given in disjunctive form: $C = x_1^{\varepsilon_1} \vee \cdots \vee x_K^{\varepsilon_K}$ where $\varepsilon_i \in \{0, 1\}$ (x_i^0 is the positive literal x_i and x_i^1 is the negative one $\overline{x_i}$). A K-CNF formula F is a finite conjunction of K-clauses, $\Omega(F)$ will denote the set of distinct variables occurring in F, $\Omega(F) \subset \{x_1, \ldots, x_N\}$. In this Boolean framework, $S(F)$ the set of satisfying assignments to F, becomes a subset of $\{0, 1\}^N$.

Now, let us recall how a slight change of our probability measure on formulæ gives a convenient product probability space for studying x-satisfiability.

5.1. x-unsatisfiability as a monotone property

In our case the number of clauses in a random formula $F_K(N, N\alpha)$ is fixed to $M = N\alpha$. We define another kind of random formula $G_K(N, N\alpha)$ by allowing each of the $\mathcal{N} = 2^K \binom{N}{K}$ possible clauses to be present with probability $p = \alpha N/\mathcal{N}$. Then, assigning 1 to each clause if it is present and 0 otherwise, the hypercube $\{0, 1\}^{\mathcal{N}}$ stands for the set of all possible formulæ, endowed with the so-called product measure μ_p, where p is the probability for 1, and $1 - p$ for 0.

More generally, let $\mathcal{N}$ be a positive integer, a property $Y \subset \{0, 1\}^{\mathcal{N}}$ is called monotone if , for any $y, y' \in \{0, 1\}^{\mathcal{N}}$, $y \leq y'$ and $y \in Y$ implies $y' \in Y$. In that case $\mu_p(y \in Y)$ is an increasing function of $p \in [0, 1]$ where

$$\mu_p(y_1, \ldots, y_{\mathcal{N}}) = p^{|y|} \cdot (1 - p)^{\mathcal{N}-|y|} \quad \text{where } |y| = \sharp\{1 \leq i \leq \mathcal{N} \;/\; y_i = 1\}.$$

For any non-trivial Y we can define for every $\beta \in]0, 1[$ the unique $p_\beta \in]0, 1[$ such that:

$$\mu_{p_\beta}(y \in Y) = \beta.$$

In our case Y will be the property of being x-unsatisfiable. If we put:

$$\mathcal{D} = \left\{(\vec{\sigma}, \vec{\tau}) \in \{0, 1\}^N \times \{0, 1\}^N \; s.t. \; d_{\vec{\sigma}\vec{\tau}} \in [Nx - \varepsilon(N), Nx + \varepsilon(N)]\right\} \tag{85}$$

then x-unsatisfiability can be read:

$$F \in Y \iff S(F) \times S(F) \quad \cap \quad \mathcal{D} = \emptyset.$$

Observe that the number of clauses in $G_K(N, N\alpha)$ is distributed as a binomial law $\text{Bin}(\mathcal{N}, p = \alpha N/\mathcal{N})$ peaked around its expected value $p \cdot \mathcal{N} = \alpha N$. Therefore, from well known results on monotone property of the hypercube, [37, page 21 and Corollary 1.16 page 19], our Theorem 1.6 is equivalent to the following result, which establishes the sharpness of the monotone property Y under μ_p.

Theorem 5.1. *For each $K \geq 3$ and x, $0 < x < 1$, there exists a sequence $\alpha_N(K, x)$ such that for all $\eta > 0$:*

$$\lim_{N\to\infty} \mu_p(F \textit{ is } x\textit{-unsatisfiable}) = \begin{cases} 1 & \textit{if } \; p \cdot \mathcal{N} = (1 - \eta)\alpha_N(K, x)N, \\ 0 & \textit{if } \; p \cdot \mathcal{N} = (1 + \eta)\alpha_N(K, x)N. \end{cases} \tag{86}$$

This theorem will be proved using general results on monotone properties of the hypercube. We state these results below without proof.

5.2. General tools

The main tool used to prove the existence of a sharp threshold will be a sharpness criterion stemming from Bourgain's result [8] and from a remark by Friedgut on the possibility to strengthen his criterion [36, Remark following Theorem 2.2]. Thus, a slight strengthening of Bourgain's proof in the appendix of [8] combined with an observation made in [33, Theorem 2.3, page 130] gives the following sharpness criterion:

Theorem 5.2. *Let $Y_{\mathcal{N}} \subset \{0,1\}^{\mathcal{N}}$ be a sequence of monotone properties, then Y has a sharp threshold as soon as there exists a sequence $T_{\mathcal{N}}$ with $T_{\mathcal{N}} \supset Y_{\mathcal{N}}$ such that for any $\beta \in]0,1[$ and every $D \geq 1$ the three following conditions are satisfied:*

$$p_\beta = o(1), \tag{87}$$

$$\mu_{p_\beta}(y \text{ s.t. } \exists z \in T,\ z \subset y,\ |z| \leq D) = o(1), \tag{88}$$

$$\forall z_0 \notin T,\ |z_0| \leq D \quad \mu_{p_\beta}(y \in Y,\ y \setminus z_0 \notin Y \quad | \quad y \supset z_0\ ) = o(1). \tag{89}$$

We end this subsection by recalling two general results on monotone properties defined on finite sets, established in [34].

Lemma 5.3 *([34, Lemma A.1, Page 236]). Let $U = \{1,\dots,\mathcal{N}\}$ be partitioned into two sets U' and U'' with $\#U' = \mathcal{N}', \#U'' = \mathcal{N}''$ and $\mathcal{N} = \mathcal{N}' + \mathcal{N}''$. For any $u \subset U$ let us denote $u' = u \cap U'$ and $u'' = u \cap U''$. Let $Y \subset \{0,1\}^{\mathcal{N}}$ be a monotone property. For any element u, let $\mathcal{A}(u)$ be the set of elements from U' that are essential for property Y at u: $\mathcal{A}(u) = \left\{i \in U' \text{ s.t. } u \cup \{i\} \in Y\right\}$. Then, for any $a > 0$ the following holds*

$$\mu_p(u \in Y, u'' \notin Y) \leq \frac{1}{(1-p)^{\mathcal{N}'}} \cdot \mu_p(u \notin Y, \#\mathcal{A}(u) \geq a) + \frac{a \cdot p}{(1-p)^{\mathcal{N}'}}.$$

For the second result we consider a sequence of monotone properties $Y_{\mathcal{N}} \subset \{0,1\}^{\mathcal{N}}$. For any fixed $u \in \{0,1\}^{\mathcal{N}}$, $\mathcal{B}_j(u)$ will be the set of collections of j elements such that one can reach property Y from u by adding this collection, thus $\#\mathcal{B}_j(u) \leq \binom{\mathcal{N}}{j}$.

Lemma 5.4 *([34, Lemma A.2, Page 237]). Let $Y_{\mathcal{N}} \subset \{0,1\}^{\mathcal{N}}$ be a sequence of monotone properties. For any integer $j \geq 1$, for any $b > 0$ and as soon as $\mathcal{N} \cdot p$ tends to infinity, the following estimate holds*

$$\mu_p\Big(u \notin Y, \#\mathcal{B}_j(u) \geq b \cdot \binom{\mathcal{N}}{j}\Big) = o(1),$$

$$\mathcal{B}_j(u) = \Big\{\{i_1,\dots,i_j\}, 1 \leq i_1 < \cdots < i_j \leq \mathcal{N},\ \text{such that } u \cup \{i_1,\dots,i_j\} \in Y\Big\}.$$

5.3. Proof of Theorem 5.1 (main steps)

As usual, the first two conditions (87) and (88) are easy to verify for the x-unsatisfiability property. For the first one we have:

$$\mu_p(F \text{ is } x\text{-satisfiable}) \leq \mu_p(F \text{ is satisfiable}) \leq 2^N (1-p)^{\binom{N}{K}}.$$

This shows that $p_\beta \leq \dfrac{N\ln(2) - \ln(1-\beta)}{\binom{N}{K}}$, thus for x-unsatisfiability we get:

$$\forall \beta \in]0,1[\quad p_\beta(N) = O(N^{1-K}). \tag{90}$$

For the second condition, let $H(F)$ be the K-uniform hypergraph associated to a formula F: its vertices are the $\Omega(F)$ variables occurring in F, each index set of a clause C in F corresponds to an hyperedge. Let us recall, see [38], that a K-uniform connected hypergraph with v vertices and w edges is called a *hypertree* when $(K-1)w - v = -1$; it is said to be *unicyclic* when $(K-1)w - v = 0$, and *complex* when $(K-1)w - v \geq 1$. Let T be the set of formulæ F such that $H(F)$ has at least one complex component. We will rule out (88) (and also (89)) by using the following result on non-complex formulæ, the proof of which is deferred to the next subsection:

Lemma 5.5. *Let $K \geq 3$. If G is a K-CNF-formula on v variables whose associated hypergraph is an hypertree or unicyclic then for all integer $d \in \{0,\dots,v\}$ there exits $(\vec{\sigma},\vec{\tau}) \in S(G) \times S(G)$ such that $d_{\vec{\sigma}\vec{\tau}} = d$.*

In particular, this result shows that any x-unsatisfiable formula has at least one complex component, i. e. $T \supset Y$. Then observe that there is $O(N^{(K-1)s-1})$ distinct complex components of size s with N vertices. Thus we get for all p : $\mu_p(F \text{ s.t. } \exists G \in T,\ G \subset F,\ |G| \leq D) \leq \sum_{s \leq D} O(N^{(K-1)s-1}) \cdot p^s$, and (88) follows from (90)

In order to prove (89), let us introduce some tools inspired of [34].

For each positive integer t and $\Delta = (\Delta_1, \dots, \Delta_t) \in \{0,1\}^t$, a Δ-assignment is an assignment for which the t first values of the variables are equal to $\Delta_1, \dots, \Delta_t$. Then $S_\Delta(F)$ will denote the set of satisfying Δ-assignments to F: $S_\Delta(F) \subset S(F) \subset \{0,1\}^N$.

For any pair of t-tuples $(\Delta, \Delta') \in \{0,1\}^t \times \{0,1\}^t$ we define $Y^{\Delta,\Delta'}$:

$$F \in Y^{\Delta,\Delta'} \iff S_\Delta(F) \times S_{\Delta'}(F) \quad \cap \quad \mathcal{D}_x = \emptyset.$$

Observe that $Y^{\Delta,\Delta'}$ is a monotone property containing Y.

Now we come back to (89) with $F_0 \notin T$, so that the hypergraph associated to the booster formula F_0 has no complex components. $S(F_0) \neq \emptyset$ and w.l.o.g. we can suppose that $\Omega(F_0) = \{1, \dots, t\}$. Then, for $F \in Y$ such that $F \supset F_0$ with $F \setminus F_0 \notin Y$, let F'' denote the largest subformula of F such that $\Omega(F'') \cap \{1, \dots, t\} = \emptyset$. We have the two following claims whose proof is postponed to the next subsection.

Claim 5.6. *For any $(\Delta, \Delta') \in S(F_0) \times S(F_0)$, $F \setminus F_0 \in Y^{\Delta,\Delta'}$.*

Claim 5.7. *There exits $(\Delta, \Delta') \in S(F_0) \times S(F_0)$ such that $F'' \notin Y^{\Delta,\Delta'}$.*

Thus (89) is proved as soon as for any $\beta \in]0,1[$ and $(\Delta, \Delta') \in \{0,1\}^t \times \{0,1\}^t$:

$$\mu_{p_\beta}(F \setminus F_0 \in Y^{\Delta,\Delta'}, F'' \notin Y^{\Delta,\Delta'} \quad | \quad F \supset F_0) = o(1). \tag{91}$$

The two first events in the R.H.S. of (91) do not depend on the set of clauses in F_0 thus by independence under the product measure and recalling that $Y^{\Delta,\Delta'}$ is a monotone property we are led to prove that:

$$\mu_{p_\beta}(F \in Y^{\Delta,\Delta'}, F'' \notin Y^{\Delta,\Delta'}) = o(1).$$

From (90) we know that $p_\beta(N) = O(N^{1-K})$. Let $\mathcal{N}' = \Theta(N^{K-1})$ be the number of clauses having at least one variable in $\{1, \dots, t\}$, then Lemma 5.3, applied to the monotone property $Y^{\Delta,\Delta'}$, shows that the above assertion is true as soon as we are able to prove that for all $\gamma > 0$:

$$\mu_{p_\beta}(F \notin Y^{\Delta,\Delta'}, \#\mathcal{A}_{\Delta,\Delta'}(F) \geq \gamma \cdot N^{K-1}) = o(1). \tag{92}$$

where $\mathcal{A}_{\Delta,\Delta'}(F)$ is the set of K-clauses C on N variables having at least one variable in $\{x_1, \dots, x_t\}$ and such that $F \wedge C \in Y^{\Delta,\Delta'}$.

Then let $\mathcal{B}_{\Delta,\Delta'}(F)$ be the set of collections of $(K-1)$ K-clauses $\{C_1, \dots, C_{K-1}\}$ such that $F \wedge C_1 \wedge \cdots \wedge C_{K-1} \in Y^{\Delta,\Delta'}$. From Lemma 5.3 we deduce that (92) is true as soon as the following result is proved:

Lemma 5.8. *For all $t, K \geq 3, \gamma > 0$ and $(\Delta, \Delta') \in \{0,1\}^t \times \{0,1\}^t$, there exits $\theta > 0$ such that for all N, the following holds:*

$$\#\mathcal{A}_{\Delta,\Delta'}(F) \geq \gamma \cdot N^{K-1} \Longrightarrow \#\mathcal{B}_{\Delta,\Delta'}(F) \geq \theta \cdot N^{K\cdot(K-1)}. \tag{93}$$

Again the proof of this last result is deferred to the next subsection that furnishes a detailed and complete proof of Theorem 5.1.

5.4. Detailed proofs

5.4.1. Lemma 5.5

Proof. When G has a leaf-clause, that is a clause $C = x_1^{\varepsilon_1} \vee \cdots \vee x_K^{\varepsilon_K}$ having only one variable, say x_1, in common with $G \setminus C$, the assertion can be proved by induction on the number of clauses in G. Indeed from a pair of satisfying assignments $(\vec{\sigma}, \vec{\tau}) \in S(G \setminus C) \times S(G \setminus C)$ with $d_{\vec{\sigma}\vec{\tau}} = d$ and a pair of satisfying assignments at distance $d' \in \{0, \dots, K-1\}$ for $C' = x_2^{\varepsilon_2} \vee \cdots \vee x_K^{\varepsilon_K}$, one gets a pair of satisfying assignments at distance $d + d'$. But C' is a $K-1$-clause, thus for any $d' \in \{0, \dots, K-1\}$ C' has a pair of satisfying assignments at distance d'.

When any K-clause C_i of $G = C_1 \wedge \cdots \wedge C_l$ has exactly two variables in common with $G \setminus C_i$ then we can write $C_1 = x_1^{\mu_1} \vee x_2^{\nu_2} \vee C'_1, C_2 = x_2^{\mu_2} \vee x_3^{\nu_3} \vee C'_2, \ldots, C_l = x_l^{\mu_l} \vee x_1^{\nu_1} \vee C'_l$ where the C'_j are $(K-2)$-clauses. A variable in C'_j occurs exactly once in formula G and the set of variables in these C'_j is equal to $\{x_{l+1}, \ldots, x_v\}$. In particular this set is disjoint from the set of variables of the 2-CNF formula $(x_1^{\mu_1} \vee x_2^{\nu_2}) \wedge (x_2^{\mu_2} \vee x_3^{\nu_3}) \wedge \cdots \wedge (x_l^{\mu_l} \vee x_1^{\nu_1})$. First observe that this 2-CNF cyclic formula has always a satisfying assignment $(\sigma_1, \ldots, \sigma_l)$ and together with any truth value for the $(x_j, j > l)$ it gives a satisfying assignment for G. Thus, for G, one gets a pair of satisfying assignments at distance d for any $d \leq v - l$. Second, as $\Omega(C'_j) \cap \Omega(C'_k) = \emptyset$ when $j \neq k$ a satisfying assignment $\sigma_{l+1}, \ldots, \sigma_v$ can easily be found for $C'_1 \wedge \cdots \wedge C'_l$. Together with any truth values of the $(x_i, i \leq l)$ it gives a satisfying assignment for G. Then, from the satisfying assignment $(\sigma_1, \ldots, \sigma_l, 1-\sigma_{l+1}, \ldots, 1-\sigma_v)$ one gets, for any $d \geq v - l$, a pair of satisfying assignments at distance d. □

5.4.2. Claims 5.6 *and* 5.7

Proof. Observe that any SAT-x-pair $(\vec{\sigma}, \vec{\tau})$ for $F \setminus F_0$ with $(\sigma_1, \ldots, \sigma_t) \in S(F_0)$ and $(\tau_1, \ldots, \tau_t) \in S(F_0)$ is also a SAT-x-pair for F. This proves the first claim by contradiction.

For the second claim, $F \setminus F_0 \notin Y$ so there exits a SAT-x-pair $(\vec{\sigma}, \vec{\tau}) \in S(F \setminus F_0) \times S(F \setminus F_0)$. By construction, the set of satisfying assignment of F'' does not depend on the first t coordinates. Let d_t be the Hamming distance between $(\sigma_1, \ldots \sigma_t)$ and $(\tau_1, \ldots \tau_t)$. We know that all components of the hypergraph associated to formula F_0 are simple and Lemma 5.5 shows that there exits $(\sigma'_1, \ldots \sigma'_t) \in S(F_0)$ and $(\tau'_1, \ldots \tau'_t) \in S(F_0)$ such that $d_{\vec{\sigma}'\vec{\tau}'} = d_t$. Hence $(\sigma'_1, \ldots \sigma'_t, \sigma_{t+1}, \ldots, \sigma_N)$ and $(\tau'_1, \ldots \tau'_t, \tau_{t+1}, \ldots, \tau_N)$ form now a SAT-x-pair for F'', thus proving the second claim. □

5.4.3. Lemma 5.8

Proof. In [35], Erdös and Simonovits proved that any sufficiently dense uniform hypergraph always contains specific subhypergraphs. In particular they considered a generalization of the complete bipartite graph specified by two integers $h \geq 2$ and $m \geq 1$. Let us denote by $K_h(m)$ the h-uniform hypergraph with $h \cdot m$ vertices partitioned into h classes $V_1, \ldots, V_h$ with $\#V_i = m$ and whose hyperedges are those h-tuples, which have exactly one vertex in each V_i. Thus $K_h(m)$ has m^h hyperedges, for $h = 2$ it is a complete bipartite graph $K(m, m)$.

For proving Lemma 5.8, we need a small variation on a result of Erdös and Simonovits which differs only in that it deals with ordered h-tuples as opposed to sets of size h. More precisely, let us consider hypergraphs on n vertices, say $\{x_1, \ldots, x_n\}$, we will say that two disjoint subsets of vertices A and B verify $A < B$ if for all x_i in A and all x_j in B we have $i < j$. Let H be an h-uniform hypergraph with vertex set $\{x_1, \ldots, x_n\}$, then any h-uniform subhypergraph $K_h(m)$ with $V_1 < \cdots < V_h$ is called an *ordered copy of* $K_h(m)$ *in* H. Thus, the ordered version of the theorem from Erdös and Simonovits about supersaturated uniform hypergraphs [35, Corollary 2, page 184] can be stated as follows.

Theorem 5.9 (*Ordered Erdös–Simonovits*). *Given $c > 0$ and two integers $h \geq 2$ and $m \geq 1$, there exist $c' > 0$ and N such that for all integers $n \geq N$, if H is a h-uniform hypergraph over n vertices having at least $c \cdot \binom{n}{h}$ hyperedges then H contains at least $c'n^{hm}$ ordered copies of $K_h(m)$.*

We will also use the following observation made when one consider an assignment of two colors, say 0 and 1, to the hyperedges of $K_h(m)$. First let's say that a vertex s is c-marked if s belongs to at least one c-colored hyperedge. A subset of vertices S is said c-marked if any s in S is c-marked.

Claim 5.10. *Let $h \geq 2$, $m \geq 1$, and $V_1, \ldots, V_h$ the partition associated to $K_h(m)$. Consider an assignment of two colors to the m^h hyperedges of $K_h(m)$, then at least one of the V_i is marked.*

Indeed, suppose that $V_1, \ldots, V_h$ are not c-marked. Now consider a vertex $s \in V_1$ then s is $(1-c)$ marked else by construction of $K_h(m)$, V_i would be c-marked for all $i \geq 2$. Hence V_1 becomes $(1-c)$-marked.

Now let us show (93), in other words that for any K-CNF formula F such that $\mathcal{A}_{\Delta,\Delta'}(F)$ is dense then $\mathcal{B}_{\Delta,\Delta'}(F)$ is also dense. For more readability we will restrict our attention to the special case $K = 3$, in using the above fact the proof will be easily extendable to any $K \geq 3$. Suppose there exist $\Theta(N^2)$ clauses in $\mathcal{A}_{\Delta,\Delta'}(F)$ then, by the pigeon hole principle, at least for one of the eight types of clause we can find $\Theta(N^2)$ clauses of this type in $\mathcal{A}_{\Delta,\Delta'}(F)$. Suppose, for example, that

$$\#\{C = \overline{x_{i_1}} \vee x_{i_2} \vee \overline{x_{i_3}},\ 1 \leq i_1 < i_2 < i_3 \leq N, i_1 \leq t,\ F \wedge C \in Y^{\Delta,\Delta'}\} = \Theta(N^2).$$

From well chosen elements in $\mathcal{A}_{\Delta,\Delta'}(F)$ we now exhibit an element in $\mathcal{B}_{\Delta,\Delta'}(F)$. We consider the graph $H(F)$ associated to formula F: The set of vertices is $\{1,\dots,N\}$ and for each $C = \overline{x_{i_1}} \vee x_{i_2} \vee \overline{x_{i_3}} \in \mathcal{A}_{\Delta,\Delta'}(F)$ we create an edge $\{i_2, i_3\}$. Let $(\vec{\sigma}, \vec{\tau})$ be a SAT-x-pair for F, then either $\sigma \notin S(C)$ or $\tau \notin S(C)$. Now, following a fixed ordering on the set of pairs of truth assignments we put the color 0 on the non-colored edge $\{i_2, i_3\}$ if $\sigma_{i_2} = 0$ and $\sigma_{i_3} = 1$ else we put the color 1, having in this case $\tau_{i_2} = 0$ and $\tau_{i_3} = 1$. Now, let's take an ordered copy of $K(3,3)$ in $H(F)$ with partition $A = \{j_1, j_2, j_3\}$ and $B = \{j_4, j_5, j_6\}$. From Fact 5.10 we know that one part, say A, is marked. In such a case we have $\sigma_{j_1} = 0, \sigma_{j_2} = 0, \sigma_{j_3} = 0$ (A is 0-marked) or $\tau_{j_1} = 0, \tau_{j_2} = 0, \tau_{j_3} = 0$ (A is 1-marked) hence $(\vec{\sigma}, \vec{\tau})$ is no longer a SAT-x-pair for $F \wedge (x_{j_1} \vee x_{j_2} \vee x_{j_3})$. If B is marked then $(\vec{\sigma}, \vec{\tau})$ is no longer a SAT-x-pair for $F \wedge (\overline{x_{j_4}} \vee \overline{x_{j_5}} \vee \overline{x_{j_6}})$. Thus in any case $\{(x_{j_1} \vee x_{j_2} \vee x_{j_3}), (\overline{x_{j_4}} \vee \overline{x_{j_5}} \vee \overline{x_{j_6}})\} \in \mathcal{B}_{\Delta,\Delta'}(F)$.

By hypothesis $H(F)$ is a dense graph so from Theorem 5.9 we can find $\Theta(N^6)$ copies of $K(3,3)$ in $H(F)$. The above construction provide $\Theta(N^6)$ elements in $\mathcal{B}_{\Delta,\Delta'}(F)$ thus proving that this set is also dense. □

5.5. A general sharpness result

Note that the above proof does not use any information about the shape of the set $\mathcal{D}$ defining the x-unsatisfiability in terms of a subset of $\{0,\dots,N\}$, namely the interval $[Nx - \varepsilon(N), Nx + \varepsilon(N)]$ (see (85)). Actually we can consider properties defined by a non-empty proper subset of $\{0,\dots,N\}$ and we have proved the following general result:

Theorem 5.11. *Let J_N be a non-empty subset of $\{0,\dots,N\}$ and consider*

$$\mathcal{D}_J = \left\{(\vec{\sigma}, \vec{\tau}) \in \{0,1\}^N \times \{0,1\}^N \ s.t.\ d_{\vec{\sigma}\vec{\tau}} \in J_N\right\}.$$

Let $K \geq 3$ and Y_J be the set of K-CNF formula defined as:

$$F \in Y_J \iff S(F) \times S(F) \quad \cap \quad \mathcal{D}_J = \emptyset.$$

Then, Y_J is a monotone property exhibiting a sharp threshold.

On one hand, any upper bound for the satisfiability threshold, for instance (90), is an upper bound for all Y_J threshold. On the other hand, Lemma 5.5 tells us that a non-complex formula does not belongs to Y_J. Then, from [38], we know that w.h.p a formula whose ratio between the number of clauses and the number of variables is less than $1/K(K-1)$, has no complex component. Thus it provides a lower bound for all Y_J threshold.

6. Discussion and conclusion

We have developed a simple and rigorous probabilistic method which is a first step towards a complete characterization of the clustered hard-SAT phase in the random satisfiability problem. Our result is consistent with the clustering picture and supports the validity of the one-step replica symmetry breaking scheme of the cavity method for $K \geq 8$.

The study of x-satisfiability has the advantage that it does not rely on a precise definition of clusters. Indeed, it is important to stress that the "appropriate" definition for clusters may vary according to the problem at hand. The natural choice seems to be the connected components of the space of SAT-assignments, where two adjacent assignments have by definition Hamming distance 1. However, although this naive definition seems to work well on the satisfiability problem, it raises major difficulties on some other problems. For instance, in q-colorability, it is useful to permit color exchanges between two adjacent vertices in addition to single-vertex color changes. In XORSAT, the naive definition is inadequate, since jumps from solution to solution can involve a large, yet finite, Hamming distance due to the hard nature of linear Boolean constraints [31].

On the other hand, the existence of a gap in the x-satisfiability property is stronger than the original clustering hypothesis. Clusters are expected to have a typical size, and to be separated by a typical distance. However, even for typical formulae, there exist atypical clusters, the sizes and separations of which may differ from their typical values. Because of this variety of cluster sizes and separations, a large range of distances is available to pairs of SAT-assignments, which our x-satisfiability analysis takes into account. What we have shown suggests that, for typical formulae, the maximum size of all clusters is smaller than the minimum distance between two clusters (for a certain range of α and $K \geq 8$). This is a sufficient condition for clustering, but by no means a necessary one. As a matter of fact, our large K analysis conjectures that $\alpha_1(K)$ (the smaller α such that Conjecture 1.4 is verified) scales as $2^{K-1}\ln 2$, whereas $\alpha_d(K)$ (where the replica symmetry breaking occurs) and $\alpha_s(K)$ (where the one-step RSB Ansatz is supposed to be valid) scale as $2^K \ln K/K$ [16]. According to the physics interpretation, in the range $\alpha_s(K) < a < \alpha_1(K)$, there exist clusters, but they are not detected by the x-satisfiability approach. This limitation might account for the failure of our method for small values of K — even though more sophisticated techniques for evaluating the x-satisfiability threshold $\alpha_c(K, x)$ might yield some results for $K < 8$. Still, the conceptual simplicity of our method makes it a useful tool for proving similar phenomena in other systems of computational or physical interest.

A better understanding of the structure of the space of SAT-assignments could be gained by computing the average configurational entropy of pairs of clusters at fixed distance, which contains details about how intra-cluster sizes and inter-cluster distances are distributed. This would yield the value of the x-satisfiability threshold. Such a computation was carried out at a heuristic level within the framework of the cavity method for the random XORSAT problem [32], and should be extendable to the satisfiability problem or to other CSPs.

Acknowledgements

This work has been supported in part by the EC through the network MTR 2002-00319 'STIPCO' and the FP6 IST consortium 'EVERGROW'. This paper, signed in alphabetic order, is based on previous work by Mora Mézard and Zecchina reported in Sections 1–4 and 6. The proof in Section 5 is due to Daudé. We thank an anonymous referee for pointing out a mistake in an early version of the paper.

References

[1] Stephen Cook, The complexity of theorem proving procedures, in: Proceedings of the Third Annual ACM Symposium on Theory of Computing, 1971, pp. 151–158.
[2] M.R. Garey, D.S. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness, W.H. Freeman, 1979.
[3] R. Monasson, R. Zecchina, Statistical mechanics of the random K-satisfiability model, Phys. Rev. E 56 (1997) 1357–1370.
[4] T. Hogg, B.A. Huberman, C.P. Williams, Phase transitions and the search problem, Artificial Intelligence 81 (1996) 1–15.
[5] O. Dubois, R. Monasson, B. Selman, R. Zecchina (Eds.), NP-hardness and Phase transitions, Theoret. Comput. Sci. 265 (1–2) (2001) (special issue).
[6] S. Kirkpatrick, B. Selman, Critical behavior in the satisfiability of random Boolean expressions, Science 264 (1994) 1297–1301.
[7] R. Monasson, R. Zecchina, S. Kirkpatrick, B. Selman, L. Troyanski, Computational complexity from 'characteristic' phase transitions, Nature 400 (1999) 133–137.
[8] E. Friedgut, Sharp Thresholds of Graph Properties, and the k-sat Problem, J. Amer. Math. Soc. 12 (4) (1999) 1017–1054. An appendix by J. Bourgain.
[9] L.M. Kirousis, E. Kranakis, D. Krizanc, A better upper bound for the unsatisfiability threshold, Technical Report TR-96-09, School of Computer Science, Carleton University, 1996.
[10] O. Dubois, Y. Boufkhad, A general upper bound for the satisfiability threshold of random r-sat formulae, J. Algorithms 24 (2) (1997) 395–420.
[11] D. Achlioptas, C. Moore, The asymptotic order of the random k-SAT threshold, Proc. Found. Comput. Sci. (2002) 779–788.
[12] D. Achlioptas, Y. Peres, The threshold for random k-SAT is $2^k \log 2 - O(k)$, J. AMS 17 (2004) 947–973.
[13] M. Mézard, G. Parisi, The Bethe lattice spin glass revisited, Eur. Phys. J. B 20 (2001) 217–233; The cavity method at zero temperature, J. Stat. Phys. 111 (2003) 1–34.
[14] M. Mézard, R. Zecchina, Random K-satisfiability problem: From an analytic solution to an efficient algorithm, Phys. Rev. E 66 (2002) 056126.
[15] M. Mézard, G. Parisi, R. Zecchina, Analytic and algorithmic solution of random satisfiability problems, Science 297 (2002) 812–815.
[16] S. Mertens, M. Mézard, R. Zecchina, Threshold values of Random K-SAT from the cavity method, Random Structures Algorithms 28 (2006) 340–373.
[17] A. Braunstein, M. Mezard, R. Zecchina, Survey propagation: an algorithm for satisfiability, Random Structures Algorithms 27 (2005) 201–226.
[18] A. Montanari, F. Ricci-Tersenghi, On the nature of the low-temperature phase in discontinuous mean-field spin glasses, Eur. Phys. J. B 33 (2003) 339–346.
[19] A. Montanari, G. Parisi, F. Ricci-Tersenghi, Instability of one-step replica-symmetry-broken phase in satisfiability problems, J. Phys. A 37 (2004) 2073–2091.
[20] G. Semerjian, R. Monasson, A study of pure random walk on random satisfiability problems with "physical" methods, in: E. Giunchiglia, A. Tacchella (Eds.), Proceedings of the SAT 2003 Conference, in: Lecture Notes in Computer Science, vol. 2919, Springer, 2004, pp. 120–134.
[21] R. Mulet, A. Pagnani, M. Weigt, R. Zecchina, Coloring random graphs, Phys. Rev. Lett. 89 (2002) 268701.
[22] A. Braunstein, R. Mulet, A. Pagnani, M. Weigt, R. Zecchina, Polynomial iterative algorithms for coloring and analyzing random graphs, Phys. Rev. E 68 (2003) 036702.
[23] O.C. Martin, M. Mézard, O. Rivoire, Frozen glass phase in the multi-index matching problem, Phys. Rev. Lett. 93 (2004) 217205.

[24] A. Montanari, The glassy phase of Gallager codes, Eur. Phys. J. B 23 (2001) 121–136.
[25] S. Franz, M. Leone, A. Montanari, F. Ricci-Tersenghi, Dynamic phase transition for decoding algorithms, Phys. Rev. E 66 (2002) 046120.
[26] M. Mézard, F. Ricci-Tersenghi, R. Zecchina, Two solutions to diluted p-spin models and XORSAT problems, J. Stat. Phys. 111 (2003) 505–533.
[27] S. Cocco, O. Dubois, J. Mandler, R. Monasson, Rigorous decimation-based construction of ground pure states for spin-glass models on random lattices, Phys. Rev. Lett. 90 (2003) 047205.
[28] O. Dubois, J. Mandler, The 3-XORSAT threshold, Proceedings of the 43th Annual IEEE Symposium on Foundations of Computer Science, Vancouver, 2002, pp. 769–778.
[29] M. Mézard, T. Mora, R. Zecchina, Clustering of solutions in the random satisfiability problem, Phys. Rev. Lett. 94 (2005) 197205.
[30] D. Achlioptas, F. Ricci-Tersenghi, On the solution-space geometry of random constraint satisfaction problems, in: Proc. 38th Annual ACM Symposium on Theory of Computing, 2006, p. 130.
[31] A. Montanari, G. Semerjian, On the dynamics of the glass transition on Bethe lattices, J. Stat. Phys. 124 (2006) 103.
[32] T. Mora, M. Mézard, Geometrical organization of solutions to random linear Boolean equations, J. Stat. Mech. (2006) P10007.
[33] N. Creignou, H. Daudé, Coarse and sharp thresholds for random k-YOR-CNF satisfiability, Inform. Théor. Appl./Theoret. Inform. Appl. 37 (2) (2003) 127–147.
[34] N. Creignou, H. Daudé, Combinatorial sharpness criterion and phase transition classification for random CSPs, Inform. Comput. 190 (2) (2004) 220–238.
[35] P. Erdös, M. Simonovits, Supermarked graphs and hypergraphs, Combinatorica 3 (2) (1982) 181–192.
[36] E. Friedgut, Hunting for sharp thresholds, Random Structures Algorithms 26 (1–2) (2005) 27–51.
[37] S. Janson, T. Luczak, A. Rucinski, Random Graphs, John Wiley, New York, 1999.
[38] M. Karonski, T. Luczak, The phase transition in a random hypergraph, J. Comput. Appl. Math. 142 (2002) 125–135.