2

RANDOM GRAPHS: DYNAMICAL PROCESSES AND REPLICA METHOD

2.1 The solution space of random 3-XORSAT

2.1.1 *Numerical simulations for the threshold*

Figure 2.1 shows the probability that a random 3-XORSAT formula is satisfiable as a function of α for increasing sizes N. It appears that formulas with ratio $\alpha < \alpha_c \simeq 0.92$ are very likely to be satisfiable in the large N limit, while formulas with ratios beyond this critical value are almost surely unsatisfiable. This behaviour is different from the 2-XORSAT case (Figure 1.4) in that P_{SAT} seems to tend to unity below threshold.

It is important to realize that, contrary to the 2-XORSAT case, the Sat/Unsat transition is not related to connectivity percolation. Consider indeed a variable, say, x_1. This variable appear, on average, in 3α equations. Each of those equations contain other 2 variables. Hence the 'connectivity' of x_1 is $c = 6\alpha$, which is larger than unity for $\alpha_p = \frac{1}{6}$. In the range $[\alpha_p, \alpha_c]$ the formula is percolating but still satisfiable with high probability. The reason is that cycles do not hinder satisfiability as much as in the 2-XORSAT case.

2.1.2 *Space of solutions and clustering*

We start from a simple observation. Assume we have a formula F of 3-XORSAT where a variable, say, x, appears only once, that is, in one equation, say, E : $x + y + z = 0$. Let us call F' the subformula obtained from F after removal of equation E. Then the following statement is true: *F is satisfiable if and only if F' is satisfiable.* The proof is obvious: whatever the values of y, z required to satisfy F' equation E can be satisfied by an adequate choice of x, and so can be the whole formula F.

In a random 3-XORSAT formula F with ratio α there are about $N \times 3\alpha\, e^{-3\alpha}$ variables appearing only once in the formula. Removal of those variables (and their equations) produces a shorter formula with $O(N)$ less equations. Furthermore it may happen that variables with multiple occurrences in the original formula have disappeared from the output formula, or appear only once. Hence the procedure can be iterated until no single-occurrence variables are present. We are left with F_2, the largest subformula (of the original formula) where every variable appears at least twice.

Many questions can be asked: how many equations are left in F_2? how many variables does it involve? how many solutions does it have? Giving the answers requires a thorough analysis of the removal procedure, with the techniques exposed

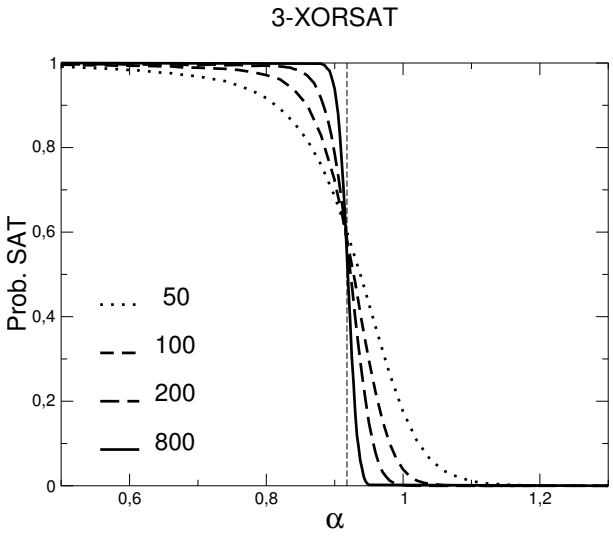

FIG. 2.1. Probability that a random 3-XORSAT formula is satisfiable as a function of the ratio α of equations per variable, and for various sizes N. The dotted line locates the threshold $\alpha_c \simeq 0.918$.

in the next Section. The outcome depends on the value of the ratio compared to

$$\alpha_d = \min_b -\frac{\log(1-b)}{3\,b^2} \simeq 0.8184\ldots \tag{2.1}$$

hereafter called clustering threshold. With high probability when $N \to \infty$ F_2 is empty if $\alpha < \alpha_d$, and contains an extensive number of equations, variables when $\alpha > \alpha_d$. In the latter case calculation of the first and second moments of the number of solutions of F_2 shows that this number does not fluctuate around the value $e^{N\,s_{clu}(\alpha)+o(N)}$ where

$$s_{clu}(\alpha) = (b - 3\alpha\,b^2 + 2\alpha\,b^3)\ln 2 \tag{2.2}$$

and b is the strictly positive solution of the self-consistent equation

$$1 - b = e^{-3\,\alpha\,b^2}\ . \tag{2.3}$$

Hence F_2 is satisfiable if and only if $\alpha < \alpha_c$ defined through $s_{clu}(\alpha_c) = 0$, that is,

$$\alpha_c \simeq 0.9179\ldots\ . \tag{2.4}$$

This value is, by virtue of the equivalence between F and F_2 the Sat/Unsat threshold for 3-XORSAT, in excellent agreement with Figure 2.1.

How can we reconstruct the solutions of F from the ones of F_2? The procedure is simple. Start from one solution of F_2 (empty string if $\alpha < \alpha_d$). Then

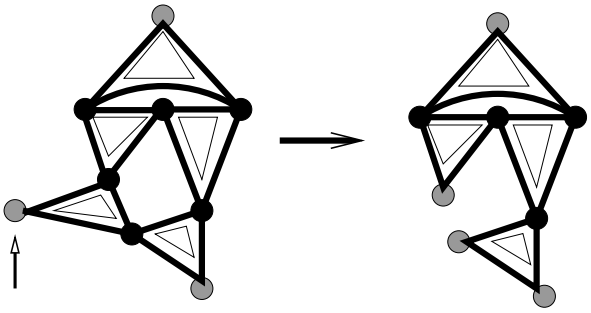

FIG. 2.2. Graph representation of the 3-XORSAT formula. Vertices (variables) are joined by plaquettes (values $0, 1$ of second members are not shown here). A step of decimation consists in listing all 1-variables (appearing only once in the formula, shown by gray vertices), choosing randomly one of them (gray vertex pointed by the arrow), and eliminating this variable and its plaquette. New 1-variables may appear. Decimation is repeated until no 1-variable is left.

introduce back the last equation which was removed since it contained $n \geq 1$ single-occurrence variable. If $n = 1$ we fix the value of this variable in a unique way. If $n = 2$ (respectively $n = 3$) there are 2 (respectively, 4) ways of assigning the reintroduced variables, defining as many solutions from our initial, partial solution. Reintroduction of equations one after the other according to the Last In – First Out order gives us more and more solutions from the initial one, until we get a bunch of solutions of the original formula F. It turns out that the number of solutions created this way is $e^{N\, s_{in}(\alpha)+o(N)}$ where

$$s_{in}(\alpha) = (1-\alpha)\,\ln 2 - s_{cluster}(\alpha)\ . \tag{2.5}$$

The above formula is true for $\alpha > \alpha_d$, and should be intended as $s_{in}(\alpha) = (1-\alpha)\ln 2$ for $\alpha < \alpha_d$. These two entropies are shown in Figure 2.3. The total entropy, $s^*(\alpha) = s_{in}(\alpha) + s_{clu}(\alpha)$, is simply $(1-\alpha)\ln 2$ for all ratios smaller than the Sat/Unsat threshold. It shows no singularity at the clustering threshold. However a drastic change in the structure of the space of solutions takes place, symbolized in the phase diagram of Figure 2.4:

- For ratios $\alpha < \alpha_d$ the intensive Hamming distance between two solutions is, with high probability, equal to $d = 1/2$. Solutions thus differ on $N/2 + o(N)$ variables, as if they were statistically unrelated assignments of the N Boolean variables. In addition the space of solutions enjoys some connectedness property. Any two solutions are connected by a path (in the space of solutions) along which successive solutions differ by a bounded number of variables. Losely speaking one is not forced to cross a big region prived of solutions when going from one solution to another.
- For ratios $\alpha > \alpha_d$ the space of solutions is not connected any longer.

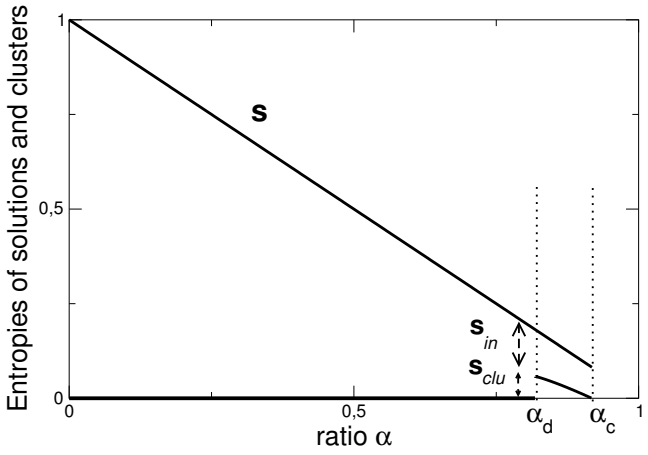

FIG. 2.3. Entropies (base 2 logarithms divided by size N) of the numbers of solutions and clusters as a function of the ratio α. The entropy of solutions equals $1-\alpha$ for $\alpha < \alpha_c \simeq 0.918$. For $\alpha < \alpha_d \simeq 0.818$, solutions are uniformly scattered on the N-dimensional hypercube. At α_d the solution space discontinuously breaks into disjoint clusters. The entropies of clusters, $s_{cluster}$, and of solutions in each cluster, s_{in}, are such that $s_{cluster} + s_{in} = s$. At α_c the number of clusters stops being exponentially large ($s_{cluster} = 0$). Above α_c there is almost surely no solution.

It is made of an exponentially large (in N) number $\mathcal{N}_{clu} = e^{N\, s_{cluster}}$ of connected components, called clusters, each containing an exponentially large number $\mathcal{N}_{in} = e^{N\, s_{in}}$ of solutions. Two solutions belonging to different clusters lie apart at a Hamming distance $d_{clu} = 1/2$ while, inside a cluster, the distance is $d_{in} < d_{clu}$. b given by (2.3) is the fraction of variables having the same value in all the solutions of a cluster (defined as the backbone).

We present in Section 2.3 the statistical physics tools developed to deal with the scenario of Figure 2.4.

2.2 Analysis of the decimation dynamical process

We now sketch how the above results may found back rigorously. The techniques used are borrowed from probability theory, and the analysis of algorithms. Let us call ℓ-variable a variable which appears in ℓ distinct equations (plaquettes, see Figure 2.2) of the 3-XORSAT formula. Plaquettes containing at least a 1-variable are never frustrated. Our decimation procedure consists in a recursive elimination of these plaquettes and attached 1-variables, until no 1-variable is left. We define the numbers $N_\ell(T)$ of ℓ–variables after T steps of the decimation algorithm, *i.e.* once T plaquettes have been removed, and their set $\mathcal{N}(T) = \{N_\ell(T), \ell \geq 0\}$. The variations of the N_ℓs during the $(T+1)^{th}$ step of the algorithm are stochastic

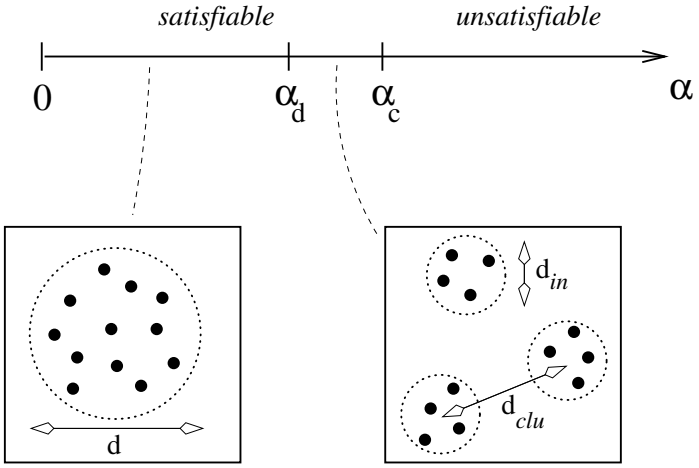

FIG. 2.4. Phase diagram of 3-XORSAT. A 'geometrical' phase transition takes place in the satisfiable phase at $\alpha_d \simeq 0.818$. At small ratios $\alpha < \alpha_d$ solutions are uniformely scattered on the N-dimensional hypercube, with a typical normalized Hamming distance $d = \frac{1}{2}$. At α_d the solution space discontinuously breaks into disjoint clusters: the Hamming distance $d_{in} \simeq 0.14$ between solutions inside a cluster is much smaller than the typical distance $d_{clu} = \frac{1}{2}$ between two clusters.

variables due to the randomness in the formula and the choice of the 1-variable to be removed, with conditional expectations with respect to $\mathcal{N}(T)$ given by

$$\mathbf{E}[N_\ell(T+1) - N_\ell(T)|\mathcal{N}(T)] = 2\,p_{\ell+1}(T) - 2\,p_\ell(T) + \delta_{\ell,0} - \delta_{\ell,1} \quad , \tag{2.6}$$

where δ denotes the Kronecker function. When a plaquette is removed, a 1-variable disappears (-$\delta_{\ell,1}$ term in (2.6)) to become a 0–variable ($\delta_{\ell,0}$). The plaquette contains two other variables. The number of occurrences ℓ of each of these two variables is distributed with probability $p_\ell(T) = \ell\, N_\ell(T)/3/(M-T)$, and is diminished by one once the plaquette is taken away. For large sizes N, the densities $n_\ell = N_\ell/N$ of ℓ–variables becomes self–averaging, and evolve on a long time scale of the order of N. Defining the reduced time $t = T/N$, the densities obey a set of coupled differential equations which can be deduced from (2.6),

$$\frac{dn_\ell}{dt} = \frac{2\,[(\ell+1)\,n_{\ell+1}(t) - \ell\, n_\ell(t)]}{3(\alpha - t)} + \delta_{\ell,0} - \delta_{\ell,1}\ . \tag{2.7}$$

Initially, densities are Poisson distributed: $n_\ell(0) = e^{-3\alpha}\,(3\alpha)^\ell/\ell!$. Equation (2.7) may be solved, with the result

$$n_\ell(t) = e^{-3\,\alpha\, b(t)^2}\ \frac{(3\,\alpha\, b(t)^2)^\ell}{\ell!} \qquad (\ell \geq 2)\ , \tag{2.8}$$

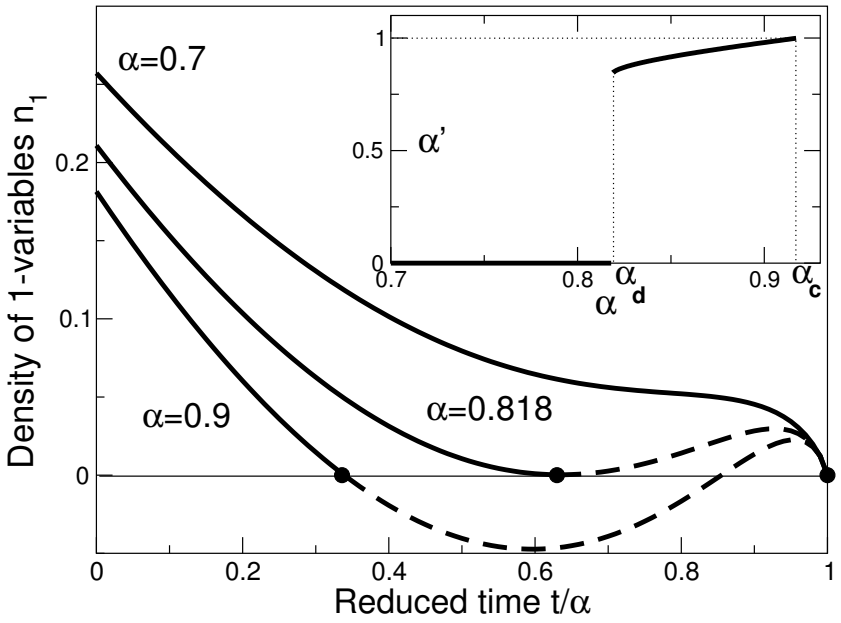

FIG. 2.5. Evolution of the density of 1-variables $n_1(t)$ generated by the decimation procedure. For $\alpha < \alpha_d \simeq 0.818$, $n_1(t)$ remains positive until all the plaquettes are eliminated at $t^* = \alpha$. For $\alpha > \alpha_d$ the decimation procedure stops at the time t^* for which n_1 vanishes (black dots), and the solution of eqn. (2.7) is non physical for $t > t^*$ (dashed part of the curves). Notice that t^* discontinuously jumps down at $\alpha = \alpha_d$ (first order transition). Inset: plaquette density α' for the reduced formula F_2 vs. α. At $\alpha = \alpha_d$, α' discontinuously jumps to a positive value; the threshold $\alpha' = 1$ for the disappearance of solution is reached for $\alpha_s \simeq 0.918$.

and

$$n_1(t) = 3\,\alpha\,b(t)^2\,\left(e^{-3\,\alpha\,b(t)^2} + b(t) - 1\right)\,, \tag{2.9}$$

where

$$b(t) \equiv \left(1 - \frac{t}{\alpha}\right)^{1/3}\,. \tag{2.10}$$

The density of 1–variables is showed on Fig. 2.5 for various initial plaquettes per variable ratios c. The algorithm stops at the time t^* for which n_1 vanishes, that is, when no 1-variable is left. From eqn. (2.9), $b(t^*)$ coincides with b defined in eqn. (2.3).

What does the reduced formula F_2 look like once the decimation has stopped? For $\alpha < \alpha_d$, $t^* = \alpha$, and no variable and plaquette is left. The entropy s of solutions of F_2 can be computed recursively. Each time a plaquette containing $v(\geq 1)$ 1-variables and these v vertices are removed (Fig. 2.2), the number of

solutions gets divided by 2^{v-1}, and the average entropy (base 2 logarithm) of solutions decreased by $\mathbf{E}[v-1|\mathcal{N}(T)] = 2\,p_1(T)$. As no variable is left when the algorithm stops, the final value for the entropy vanishes, giving

$$s = \int_0^{t^*} dt\, \frac{2\,n_1(t)}{3\,(\alpha - t)} + e^{-3c}\ , \tag{2.11}$$

where the last term comes from the contribution $n_0(0)$ of 0-variables. Using eqn. (2.9) and $t^* = c$, we find back $s = 1 - \alpha$.

When $\alpha_d < \alpha < \alpha_c$, the decimation procedure stops at $t^* < \alpha$, and has not succeeded in eliminating all plaquettes and variables. The remaining fraction of plaquettes per variable, $\alpha' = (\alpha - t^*)/\sigma$ where $\sigma = \sum_{\ell \geq 2} n_\ell(t^*)$, is plotted as a function of α in the Inset of Fig. 2.5. Each solution of F_2 can be seen as a 'seed' from which a cluster of solution of F in the original configuration space can be reconstructed. To do so, plaquettes which were eliminated during decimation are reintroduced, one after the other, and the variables they contain are assigned all possible values that leave the plaquettes unfrustrated. Combining any of these partial variable assignments with (free) 0-variables assignments, all the solutions in a cluster are obtained. Repeating the argument leading to the calculation of the entropy in the $\alpha < \alpha_d$ case, we find that the average entropy s_{in} of solutions in a cluster is given by the r.h.s. of eqn. (2.11).

To complete the description of clusters, some statistical knowledge about their seeds is required. The average value of the number $\mathcal{U}'$ of solutions of F_2 can be easily computed: $\langle \mathcal{U}' \rangle = 2^{N'(1-\alpha')}$. As the average number of solutions is an upper bound to the probability of existence of at least one solution we conclude that $\mathcal{U}'$ almost surely vanishes when $\alpha' > 1$. The calculation of the second moment is harder and will not be done here. The result is that $\mathcal{U}'$ show weak fluctuations around its average value. Hence the entropy of solutions is, with high probability, given by $\frac{1}{N} \log \langle \mathcal{U}' \rangle = \frac{N'}{N}(1-\alpha') \log 2$. This entropy is precisely the logarithm of the number of clusters s_{clu} defined above. In addition we obtain the value of the threshold α_c through the condition $\alpha'(\alpha_c) = 1$.

The reconstruction process allows a complete characterization of solutions, in terms of an extensive number of (possibly overlapping) blocks made of few variables, each block being allowed to flip as a whole from a solutions to another. When $\alpha < \alpha_d$, with high probability, two randomly picked solutions differ over a fraction $d = 1/2$ of variables, but are connected through a sequence of $O(N)$ successive solutions differing over $O(1)$ variables only. For $\alpha_d < \alpha < \alpha_c$, flippable blocks are juxtaposed to a set of seed-dependent frozen variables. To prove the existence of clustering (Fig. 2.4), one can check that the largest Hamming distance d_1^{max} between two solutions associated to the same seed is lower than the smallest possible distance d_0^{min} between solutions reconstructed from two different seeds.

2.3 The replica method

2.3.1 *From moments to large deviations for the entropy*

Let us define the intensive entropy s through $\mathcal{N} = e^{N\,s}$. As $\mathcal{N}$ is random (at fixed α, N) so is s. We assume that the distribution of s can be described, in the large size limit, by a rate function $\omega(s)$ (which depends on α). Hence,

$$\langle \mathcal{N}^q \rangle = \int ds\; e^{-N\,\omega(s)} \times \left(e^{N\,s}\right)^q \sim \exp\left[N \max_s \left(q\,s - \omega(s)\right)\right] \tag{2.12}$$

using the Laplace method. If we are able to estimate the leading behaviour of the q^{th} moment of the number of solutions when N gets large at fixed α,

$$\langle \mathcal{N}^q \rangle \sim e^{N\,g(q)}\ , \tag{2.13}$$

then ω can be easily calculated by taking the Legendre transform of g. In particular the typical entropy is obtained by $s^* = \frac{dg}{dq}(q \to 0)$. This is the road we will follow below. We will show how $g(q)$ can be calculated when q takes integer values, and then perform an analytic continuation to non integer q. The continuation leads to substantial mathematical difficulties, but is not uncommon in statistical physics e.g. the $q \to 1$ limit of the q-state Potts model to recover percolation, or the $n \to 0$ limit of the $O(n)$ model to describe self-avoiding walks.

To calculate the q^{th} moment we will have to average over the random components of formulas F, that is, the K-uplets of index variables in the first members and the $v = 0, 1$ second members. Consider now homogeneous formulas F_h whose first members are randomly drawn in the same way as for F, but with all second members $v = 0$. The number $\mathcal{N}_h$ of solutions of a homogeneous formula is always larger or equal to one. It is a simple exercise to show that

$$\langle \mathcal{N}^{q+1} \rangle = 2^{N(1-\alpha)} \times \langle \left(\mathcal{N}_h\right)^q \rangle \quad , \tag{2.14}$$

valid for any positive integer q[14]. Therefore it is sufficient to calculate the moments of $\mathcal{N}_h = e^{N\,g_h(q)}$ since (2.14) gives a simple identity between $g(q+1)$ and $g_h(q)$.

2.3.2 *Free energy for replicated variables*

The q^{th} power of the number of solutions to a homogeneous system reads

$$\left(\mathcal{N}_h\right)^q = \left[\sum_X \prod_{\ell=1}^{M} e_\ell(X)\right]^q = \sum_{X^1, X^2, \ldots, X^q} \prod_{\ell=1}^{M} \prod_{a=1}^{q} e_\ell(X^a)\ , \tag{2.15}$$

where $e_\ell(X)$ is 1 if equation ℓ is satisfied by assignment X, and 0 otherwise. The last sum runs over q assignments X^a, with $a = 1, 2, \ldots, q$ of the Boolean

[14] Actually the identity holds for $q = 0$ too, and is known under the name of harmonic mean formula.

variables, called replicas of the original assignment X. It will turn useful to denote by $\vec{x}_i = (x_i^1, x_i^2, \ldots, x_i^q)$ the q-dimensional vector whose components are the values of variable x_i in the q replicas. To simplify notations we consider the case $K = 3$ only here, but extension to other values of K is straightforward. Averaging over the instance, that is, the triplets of integers labelling the variables involved in each equation ℓ, leads to the following expression for the q^{th} moment,

$$\begin{aligned}\langle \big(\mathcal{N}_h\big)^q \rangle &= \sum_{X^1, X^2, \ldots, X^q} \langle \prod_{a=1}^{q} e(X^a) \rangle^M \\ &= \sum_{X^1, X^2, \ldots, X^q} \left[\frac{1}{N^3} \sum_{1 \le i,j,k \le N} \delta_{\vec{x}_i + \vec{x}_j + \vec{x}_k} + O\left(\frac{1}{N}\right) \right]^M \end{aligned} \tag{2.16}$$

where $\delta_{\vec{x}} = 1$ if the compoments of $\vec{x}$ are all null mod. 2, and 0 otherwise. We now procede to some formal manipulations of the above equation (2.16).

First step. Be $\mathcal{X} = \{X^1, X^2, \ldots, X^q\}$ one of the 2^{qN} replica assignment. Focus on variable i, and its attached assignment vector, $\vec{x}_i$. The latter may be any of the 2^q possible vectors e.g. $\vec{x}_i = (1, 0, 1, 0, 0, \ldots, 0)$ if variable x_i is equal to 0 in all but the first and third replicas. The histogram of the assignments vectors given replica assignment $\mathcal{X}$,

$$\rho\big(\vec{x}|\mathcal{X}\big) = \frac{1}{N} \sum_{i=1}^{N} \delta_{\vec{x} - \vec{x}_i} \quad , \tag{2.17}$$

counts the fraction of assignments vectors $\vec{x}_i$ having value $\vec{x}$ when i scans the whole set of variables from 1 to N. Of course, this histogram is normalised to unity,

$$\sum_{\vec{x}} \rho\big(\vec{x}\big) = 1 \quad , \tag{2.18}$$

where the sum runs over all 2^q assignment vectors. An simple but essential observation is that the r.h.s. of (2.16) may be rewritten in terms of the above histogram,

$$\frac{1}{N^3} \sum_{1 \le i,j,k \le N} \delta_{\vec{x}_i + \vec{x}_j + \vec{x}_k} = \sum_{\vec{x}, \vec{x}'} \rho\big(\vec{x}\big)\ \rho\big(\vec{x}'\big)\ \rho\big(\vec{x} + \vec{x}'\big)\ . \tag{2.19}$$

Keep in mind that ρ in (2.17,2.19) depends on the replica assignement $\mathcal{X}$ under consideration.

Second step. According to (2.19), two replica assignments $\mathcal{X}_1$ and $\mathcal{X}_2$ defining the same histogram ρ will give equal contributions to $\langle \big(\mathcal{N}_h\big)^q \rangle$. The sum over replica assignments $\mathcal{X}$ can therefore be replaced over the sum over possible histograms provided the multiplicity $\mathcal{M}$ of the latter is taken properly into account.

This multiplicity is also equal to the number of combinations of N elements (the $\vec{x}_i$ vectors) into 2^q sets labelled by $\vec{x}$ and of cardinalities $N\,\rho(\vec{x})$. We obtain

$$\langle \big(\mathcal{N}_h\big)^q \rangle = \sum_{\{\rho\}}^{(norm)} e^{\,N\,\mathcal{G}_h\big(\{\rho\},\alpha\big)+o(N)} \quad , \tag{2.20}$$

where the $(norm)$ subscript indicates that the sum runs over histograms ρ normalized according to (2.18), and

$$\mathcal{G}_h\big(\{\rho\},\alpha\big) = -\sum_x \rho(x)\,\ln\rho(x) + \alpha\,\ln\left[\sum_{\vec{x},\vec{x}'} \rho\big(\vec{x}\big)\,\rho\big(\vec{x}'\big)\,\rho\big(\vec{x}+\vec{x}'\big)\right] . \tag{2.21}$$

In the large N limit, the sum in (2.20) is dominated by the histogram ρ^* maximizing the functional $\mathcal{G}_h$.

Third step. Maximisation of function $\mathcal{G}_h$ over normalized histograms can be done within the Lagrange multiplier formalism. The procedure consists in considering the modified function

$$\mathcal{G}_h^{LM}\big(\{\rho\},\lambda,\alpha\big) = \mathcal{G}_h\big(\{\rho\},\alpha\big) + \lambda\left(1-\sum_{\vec{x}}\rho\big(\vec{x}\big)\right) \quad , \tag{2.22}$$

and first maximise $\mathcal{G}_h^{LM}$ with respect to histograms ρ without caring about the normalisation constraint, and then optimise the result with respect to λ. We follow this procedure with $\mathcal{G}_h$ given by (2.21). Requiring that $\mathcal{G}_h^{LM}$ be maximal provides us with a set of 2^q coupled equations for ρ^*,

$$\ln\rho^*(\vec{x}) + 1 + \lambda - 3\,\alpha\,\frac{\displaystyle\sum_{\vec{x}'}\rho^*\big(\vec{x}'\big)\,\rho^*\big(\vec{x}+\vec{x}'\big)}{\displaystyle\sum_{\vec{x}',\vec{x}''}\rho^*\big(\vec{x}'\big)\,\rho^*\big(\vec{x}''\big)\,\rho^*\big(\vec{x}'+\vec{x}''\big)} = 0 \ , \tag{2.23}$$

one for each assignment vector $\vec{x}$. The optimisation equation over λ implies that λ in (2.23) is such that ρ^* is normalised. At this point of the above and rather abstract calculation it may help to understand the interpretation of the optimal histogram ρ^*.

2.3.3 *The order parameter*

Consider q' solutions labelled by $a = 1, 2, \ldots, q'$ of the same random and homogeneous instance and a variable, say, x_i. What is the probability, over instances and solutions, that this variable takes, for instance, value 0 in the first and fourth solutions, and 1 in all other solutions? In other words, what is the probability that the assignment vector $\vec{x}_i = (x_i^1, x_i^2, \ldots, x_i^{q'})$ is equal to $\vec{x}' = (0,1,1,0,1,1,\ldots,1)$? The answer is

$$p(\vec{x}') = \left\langle \frac{1}{(\mathcal{N}_h)^{q'}} \sum_{X^1, X^2, \ldots, X^{q'}} \delta_{\vec{x}_i - \vec{x}} \prod_{l=1}^{M} \prod_{a=1}^{q} e_\ell(X^a) \right\rangle \tag{2.24}$$

where the dependence on i is wiped out by the average over the instance. The above probability is an interesting quantity; it provides us information about the 'microscopic' nature of solutions. Setting $q' = 1$ gives us the probabilities $p(0), p(1)$ that a variable is false or true respectively, that is, takes the same value as in the null assignment or not. For generic q' we may think of two extreme situations:

- a flat p over assignment vectors, $p(\vec{x}') = 1/2^{q'}$, corresponds to essentially orthogonal solutions;
- on the opposite, a concentrated probability e.g. $p(\vec{x}') = \delta_{\vec{x}'}$ implies that variables are extremely constrained, and that the (almost) unique solution is the null assignment.

The careful reader will have already guessed that our calculation of the q^{th} moment gives access to a weighted counterpart of p. The order parameter

$$\rho^*(\vec{x}) = \frac{1}{\langle (\mathcal{N}_h)^q \rangle} \sum_{X^1, X^2, \ldots, X^q} \delta_{\vec{x}_i - \vec{x}} \left\langle \prod_{l=1}^{M} \prod_{a=1}^{q} e_\ell(X^a) \right\rangle \quad , \tag{2.25}$$

is not equal to p even when $q = q'$. However, at the price of mathematical rigor, the exact probability p over vector assignments of integer length q' can be reconstructed from the optimal histogram ρ^* associated to moments of order q when q is real-valued and sent to 0. The underlying idea is the following. Consider (2.25) and an integer $q' < q$. From any assignment vector $\vec{x}$ of length q, we define two assignment vectors $\vec{x}', \vec{x}''$ of respective lengths $q', q - q'$ corresponding to the first q' and the last $q - q'$ components of $\vec{x}$ respectively. Summing (2.25) over the $2^{q-q'}$ assignment vectors $\vec{x}''$ gives,

$$\sum_{\vec{x}''} \rho^*(\vec{x}', \vec{x}'') = \frac{1}{\langle (\mathcal{N}_h)^q \rangle} \sum_{\{X^a\}} \delta_{\vec{x}'_i - \vec{x}'} \left\langle \left(\mathcal{N}_h\right)^{q-q'} \prod_{l,a} e_\ell(X^a) \right\rangle \ . \tag{2.26}$$

As q now appears in the powers of $\mathcal{N}_h$ in the numerator and denominator only, it can be formally send to zero at fixed q', yielding

$$\lim_{q \to 0} \sum_{\vec{x}''} \rho^*(\vec{x}', \vec{x}'') = p(\vec{x}') \tag{2.27}$$

from (2.24). This identity justifies the denomination order parameter given to ρ^*.

Having understood the significance of ρ^* helps us to find appropriate solutions to (2.23). Intuitively and from the discussion of the first moment case $q = 1$, p is expected to reflect both the special role of the null assignment (which is

a solution to all homogeneous systems) and the ability of other solutions of a random system to be essentially orthogonal to this special assignment. A possible guess is thus

$$p(\vec{x}') = \frac{1-b}{2^{q'}} + b\ \delta_{\vec{x}'} \quad , \tag{2.28}$$

where b expresses some degree of 'correlation' of solutions with the null one. Hypothesis (2.28) interpolates between the fully concentrated ($b = 1$) and flat ($b = 0$) probabilities. b measures the fraction of variables (among the N ones) that take the 0 values in all q' solution, and coincides with the notion of backbone introduced in Section 2.1.2. Hypothesis (2.28) is equivalent, from the connection (2.27) between p and the annealed histogram ρ^* to the following guess for the solution of the maximisation condition (2.23),

$$\rho^*(\vec{x}) = \frac{1-b}{2^q} + b\ \delta_{\vec{x}}\ . \tag{2.29}$$

Insertion of Ansatz (2.29) in (2.23) shows that it is indeed a solution provided b is shrewdly chosen as a function of q and α, $b = b^*(q, \alpha)$. Its value can be either found from direct resolution of (2.23), or from insertion of histogram (2.29) in $\mathcal{G}_h$ (2.21) and maximisation over b, with the result,

$$g_h(q, \alpha) = \max_{0 \le b \le 1} A_h(b, q, \alpha) \tag{2.30}$$

where

$$\begin{aligned} A_h(b, q, \alpha) = &-\left(1 - \frac{1}{2^q}\right)\ (1-b)\ \ln\left(\frac{1-b}{2^q}\right) \\ &-\left(b + \frac{1-b}{2^q}\right)\ \ln\left(b + \frac{1-b}{2^q}\right) + \alpha\ \ln\left(b^3 + \frac{1-b^3}{2^q}\right)\ , \end{aligned} \tag{2.31}$$

where the maximum is precisely reached in b^*. Notice that, since ρ^* in (2.29) is entirely known from the value of b^*, we shall indifferently call order parameter ρ^*, or b^* itself.

2.3.4 *Results*

Numerical investigation of A_h (2.31) shows that: for $\alpha < \alpha_M(q)$ the only local maximum of A_h is located in $b^* = 0$, and $A_h(q, \alpha) = q(1-\alpha)\ln 2$; when $\alpha_M(q) < \alpha < \alpha^*(q)$, there exists another local maximum in $b > 0$ but the global maximum is still reached in $b^* = 0$; when $\alpha > \alpha^*(q)$, the global maximum is located in $b^* > 0$. The α_M and α^* lines divide the q, α plane as shown in Figure 2.6. Notice that, while the black dots in Figure 2.6 correspond to integer-valued q, the continuous lines are the output of the implicit analytic continuation to real q done by the replica calculation.

Taking the derivative of (2.30) with respect to q and sending $q \to 0$ we obtain the typical entropy of a homogeneous 3-XORSAT system at ratio α,

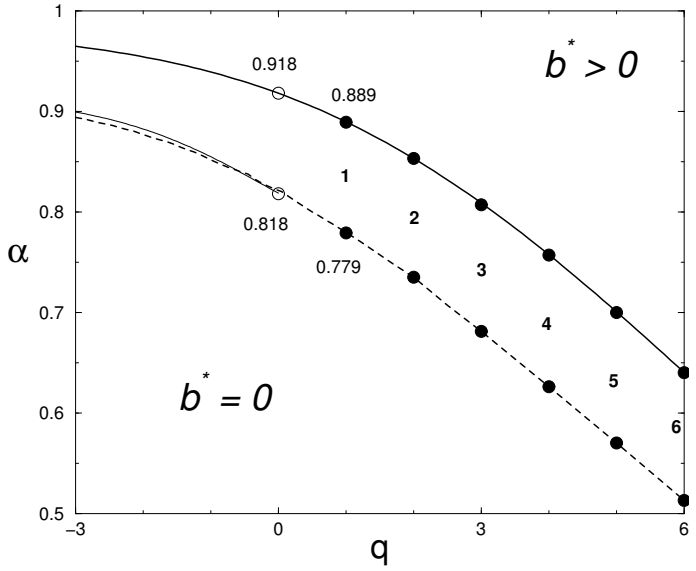

FIG. 2.6. The q, α plane and the critical lines $\alpha_M(q)$ (dashed), $\alpha^*(q)$ (full tick), and $\alpha_s(q)$ (full thin) appearing in the calculation of the q^{th} moment for homogeneous 3-XORSAT systems. Full dots correspond to integer q values, while continuous curves result from the analytic continuation to real q. The fraction of variables in the backbone, b^*, vanishes below the line $\alpha_M(q)$; the global maximum of A_h in (2.31) is located in $b^* > 0$ for ratios $\alpha > \alpha^*(q)$. Ansatz (2.29) is locally unstable in the hardly visible domain $q < 0, \alpha_M(q) < \alpha < \alpha_s(q)$.

$$s_h^*(\alpha) = \ln 2 \times \max_{0 \le b \le 1} \left[(1-b)\big(1 - \ln(1-b)\big) - \alpha\,(1-b^3) \right] . \tag{2.32}$$

The optimal value for b coincides with the solution of (2.3). The typical entropy is plotted in Figure 2.7, and is equal to:

- $(1-\alpha)\ln 2$ when $\alpha < \alpha_c \simeq 0.918$ (Figure 2.6); in this range of ratios, homogeneous and full (with random second members) systems have essentially the same properties, with the same cluster organisation of solutions, and identical entropies of solutions.
- a positive but rapidly decreasing function given by (2.32) when $\alpha > \alpha_c$; above the critical ratio, a full system has no solution any more, while a homogeneous instance still enjoys a positive entropy. The expression for $s_h^*(\alpha)$ coincides with the continuation to $\alpha > \alpha_c$ of the entropy $s_{in}(\alpha)$ (2.5) of solutions in a single cluster for a full system. In other words, a single cluster of solutions, the one with the null solution, survive for ratios $\alpha > \alpha_S$ in homogeneous systems.

Atypical instances can be studied and the large deviation rate function for the entropy can be derived from (2.30) for homogeneous systems, and using equivalence (2.14), for full systems. Minimizing over the entropy we obtain the rate function $\omega_3(\alpha)$ associated to the probability that a random 3-XORSAT system is satisfiable, with the result shown in Figure 2.7. As expected we find $\omega_3 = 0$ for $\alpha < \alpha_c$ and $\omega_3 > 0$ for $\alpha > \alpha_c$, allowing us to locate the Sat/Unsat threshold.

Notice that the emergence of clustering can be guessed from Figure 2.6. It coincides with the appearance of a local maximum of A_h (2.31) with a non vanishing backbone b. While in the intermediate phase $\alpha_d < \alpha < \alpha_c$, the height of the global maximum equals the total entropy s^*, the height of the local maximum coincides with the entropy of clusters $s_{cluster}$ (2.2).

2.3.5 *Stability of the replica Ansatz*

The above results rely on Ansatz (2.29). A necessary criterion for its validity is that ρ^* locates a true local maximum of $\mathcal{G}_h$, and not merely a saddle-point. Hence we have to calculate the Hessian matrix of $\mathcal{G}_h$ in ρ^*, and check that the eigenvalues are all negative [**?**]. Differentiating (2.21) with respect to $\rho(\vec{x})$ and $\rho(\vec{x}')$ we obtain the Hessian matrix

$$H(\vec{x},\vec{x}') = -\frac{\delta_{\vec{x}+\vec{x}'}}{\rho^*(\vec{x})} + 6\alpha\,\frac{\rho^*(\vec{x}+\vec{x}')}{D} - 9\alpha\,\frac{N(\vec{x})}{D}\,\frac{N(\vec{x}')}{D}\ , \tag{2.33}$$

where $D = \frac{1-b^3}{2^q} + b^3$, $N(\vec{x}) = \frac{1-b^2}{2^q} + b^2\,\delta_{\vec{x}}$. We use b instead of b^* to ligthen the notations, but it is intended that b is the backbone value which maximizes A_h (2.31) at fixed q, α. To take into account the global constraint over the histogram (2.18) one can express one fraction, say, $\rho(\vec{0})$, as a function of the other fractions $\rho(\vec{x})$, $\vec{x} \neq \vec{0}$. $\mathcal{G}_H$ is now a fonction of $2^q - 1$ independent variables, with a Hessian matrix $\tilde{H}$ simply related to H,

$$\tilde{H}(\vec{x},\vec{x}') = H(\vec{x},\vec{x}') - H(\vec{x},\vec{0}) - H(\vec{0},\vec{x}') + H(\vec{0},\vec{0})\ . \tag{2.34}$$

Plugging expression (2.33) into (2.34) we obtain

$$\begin{aligned}
\tilde{H}(\vec{x},\vec{x}') &= \lambda_R\,\delta_{\vec{x}+\vec{x}'} + \frac{1}{2^q-1}\big(\lambda_L - \lambda_R\big) \qquad \text{where} \\
\lambda_R &= 6\alpha\,\frac{b}{D} - \frac{2^q}{1-b} \\
\lambda_L &= 2^q\left(6\alpha\,\frac{b}{D} - \frac{2^q}{(1-b)(1-b+2^q b)} - 9\alpha(1-2^{-q})\frac{b^4}{D^2}\right)\ .
\end{aligned} \tag{2.35}$$

Diagonalization of $\tilde{H}$ is immediate, and we find two eigenvalues:

- λ_L (non degenerate). The eigenmode corresponds to a uniform infinitesimal variation of $\rho(\vec{x})$ for all $\vec{x} \neq \vec{0}$, that is, a change of b in (2.29). It is an easy check that

$$\lambda_L = \frac{2^q}{1-2^{-q}} \frac{\partial^2 A_h}{\partial b^2}(b,q,\alpha) \ , \tag{2.36}$$

where A_h is defined in (2.31). As we have chosen b to maximize A_h this mode, called longitudinal in replica literature, is stable[15].

- λ_R ($2^q - 2$-fold degenerate): the eigenmodes correspond to fluctuations of the order parameter ρ transverse to the replica subspace described by (2.29), and are called replicon in spin-glass theory. Inspection of λ_R as a function of α, q shows that it is always negative when $q > 0$. For $q < 0$ the replicon mode is stable if

$$\alpha > \alpha_s(q) = \frac{1 - b^3 + 2^q\, b^3}{6\, b(1-b)} \ . \tag{2.37}$$

which is a function of q only once we have chosen $b = b^*(q, \alpha_s)$.

The unstable region $q < 0, \alpha_M(q) < \alpha < \alpha_s(q)$ is shown in Figure 2.6 and is hardly visible when $q > -3$. In this region a continuous symmetry breaking is expected. In particular α_s stay below the α^* line for small (in absolute value) and negative q. We conclude that our Ansatz (2.29) defines a maximum of $\mathcal{G}_h$.

Is it the global maximum of $\mathcal{G}_h$? There is no simple way to answer this question. Local stability does not rule out the possibility for a discontinuous transition to another maximum in the replica order parameter space not described by (2.29). A final remark is that a similar calculation can be done for any value of K. The outcome for $K = 2$ is the rate function ω_2 plotted in Figure 1.5, in good agreement with numerics close to the threshold.

2.4 Exercise

Let us consider the following heuristic algorithm to solve 3-XORSAT formulae, called Unit-Clause (UC) procedure. Initially all variables are unassigned. At time t=0, if there is no clause (equation) with a single variable, a variable is randomly picked up and set to 1 or 0 with probability $\frac{1}{2}$. If there is one equation with a single variable, e.g. $x_1 = 1$, then its variable is assigned to satisfy the clause; in case of more than one equation with a single variable one such equation is picked up uniformly at random. The algorithm stops when all equations have disappeared (are satisfied), or when a contradiction is found (two opposite equations $x_i = 0$ and $x_i = 1$ are found). Calculate the probability that this algorithm solves successfully a random 3-XORSAT formula as a function of the ratio α in the infinite N limit.

[15] Actually b^* is chosen to *minimize* A_h when $q < 0$, thus λ_L has always the right negative sign.

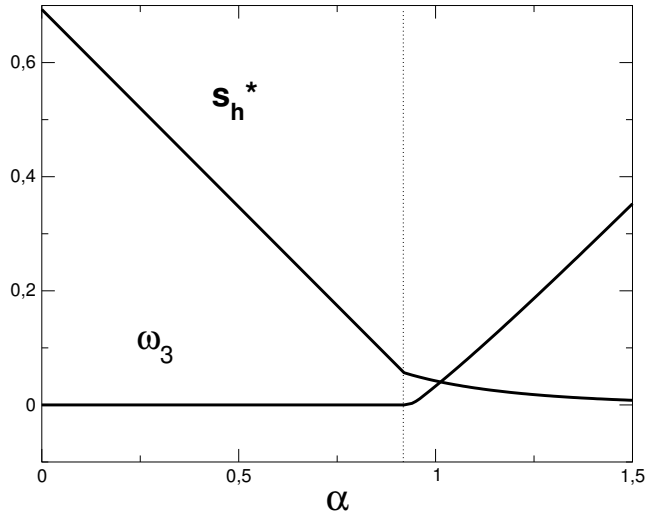

FIG. 2.7. Rate function ω_3 for the probability of satisfaction of full (bottom curve) and entropy s_h^* of solutions for homogeneous (top curve) 3-XORSAT systems vs. α. The vertical dotted lines indicate the critical Sat/Unsat threshold, $\alpha_c \simeq 0.918$. For $\alpha < \alpha_c$ $\omega_3 = 0$, and $s_h^* = (1-\alpha)\ln 2$ is the same as for full systems. Above the threshold $\omega^* < 0$. Homogeneous systems are, of course, always satisfiable: the entropy s_h^* is a positive but quickly decreasing function of α.

3

SOLUTIONS TO EXERCISES

3.1 Exercise 1: Detailed study of 1-XORSAT

Figure 3.1(top) shows the probability P_{SAT} that a randomly extracted 1-XORSAT formula is satisfiable as a function of the ratio α, and for sizes N ranging from 100 to 1000. We see that P_{SAT} is a decreasing function of α and N.

Consider the subformula made of the n_i equations with first member equal to x_i. This formula is always satisfiable if $n_i = 0$ or $n_i = 1$. If $n_i \geq 2$ the formula is satisfiable if and only if all second members are equal (to 0, or to 1), an event with probability $(\frac{1}{2})^{n_i-1}$ decreasing exponentially with the number of equations. Hence we have to consider the following variant of the celebrated Birthday problem[16]. Consider a year with a number N of days, how should scale the number M of students in a class to be sure that no two students have the same birthday date?

$$\bar{p} = \prod_{i=0}^{M-1} \left(1 - \frac{i}{N}\right) = \exp\left(-\frac{M(M-1)}{2N} + O(M^3/N^2)\right) . \qquad (3.1)$$

Hence we expect a cross-over from large to small $\bar{p}$ when M crosses the scaling regime $\sqrt{N}$. Going back to the 1-XORSAT model we expect P_{SAT} to have a non zero limit value when the number of equations and variables are both sent to infinity at a fixed ratio $y = M/\sqrt{N}$. In other words, random 1-XORSAT formulas with N variables, M equations or with, say, $100 \times N$ variables, $10 \times M$ equations should have roughly the same probabilities of being satisfiable. To check this hypothesis we replot the data in Figure 3.1 after multiplication of the abscissa of each point by $\sqrt{N}$ (to keep y fixed instead of α). The outcome is shown in the bottom panel of Figure 3.1. Data obtained for various sizes nicely collapse on a single limit curve function of y.

The calculation of this limit function, usually called scaling function, is done hereafter in the fixed-probability 1-XORSAT model where the number of equations is a Poisson variable of mean value $\bar{M} = y\sqrt{N}$. We will discuss the equivalence between the fixed-probability and the fixed-size ensembles later. In the fixed-probability ensemble the numbers n_i of occurence of each variable x_i are

[16]The Birthday problem is a classical elementary probability problem: given a class with M students, what is the probability that at least two of them have the same birthday date? The answer for $M = 25$ is $p \simeq 57\%$, while a much lower value is expected on intuitive grounds when M is much smaller than the number $N = 365$ of days in a year.

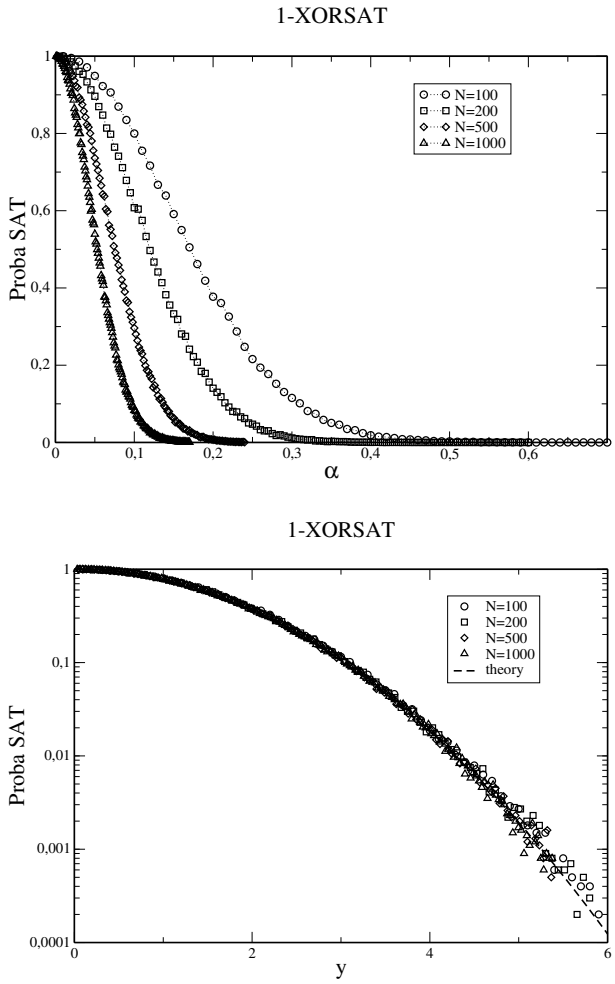

FIG. 3.1. Top: Probability that a random 1-XORSAT formula is satisfiable as a function of the ratio α of equations per variable, and for various sizes N. Bottom: same data as in the left panel after the horizontal rescaling $\alpha \to \alpha \times \sqrt{N} = y$; note the use of a log scale for the vertical axis. The dashed line shows the scaling function $\Phi_1(y)$ (3.3).

independent Poisson variables with average value $\bar{M}/N = y/\sqrt{N}$. Therefore the probability of satisfaction is

$$P^p_{SAT}(N, \alpha = \frac{y}{\sqrt{N}}) = \left[e^{-y/\sqrt{N}} \left(1 + \sum_{n \geq 1} \frac{(y/\sqrt{N})^n}{n!} \left(\frac{1}{2} \right)^{n-1} \right) \right]^N$$

$$= \left[2e^{-y/(2\sqrt{N})} - e^{-y/\sqrt{N}}\right]^N \ , \tag{3.2}$$

where the p subscript denotes the use of the fixed-probability ensemble. We obtain the desired scaling function

$$\Phi_1(y) \equiv \lim_{N\to\infty} \ln P^p_{SAT}(N, \alpha = \frac{y}{\sqrt{N}}) = -\frac{y^2}{4} \ , \tag{3.3}$$

in excellent agreement with the rescaled data of Figure 3.1 (bottom) [**?**].

For finite but large N there is a tiny probability that a randomly extracted formula is actually satisifiable even when $\alpha > 0$. A natural question is to characterize the 'rate' at which P_{SAT} tends to zero as N increases (at fixed α). Answering to such questions is the very scope of large deviation theory. Looking for events with very small probabilities is not only interesting from an academic point of view, but can also be crucial in practical applications.

Figure 3.2 shows minus the logarithm of P_{SAT}, divided by N, as a function of the ratio α and for various sizes N. Once again the data corresponding to different sizes collapse on a single curve, meaning that

$$P_{SAT}(N, \alpha) = e^{-N\ \omega_1(\alpha) + o(N)} \ . \tag{3.4}$$

Decay exponent ω_1 is called rate function in probability theory. We can derive its value in the fixed-probability ensemble from (3.2) with $y = \alpha \times \sqrt{N}$, with the immediate result

$$\omega_1^p(\alpha) = \alpha - \ln\left(2\ e^{\alpha/2} - 1\right) \ . \tag{3.5}$$

The agreement with numerics is very good for small ratios, but deteriorates as α increases. The reason is simple. In the fixed-probability ensemble the number M of equations is not fixed but may fluctuate around the average value $\bar{M} = \alpha N$. The ratio $\tilde{\alpha} = M/N$, is with high probability equal to α, but large deviations ($\tilde{\alpha} \neq \alpha$) are possible and described by the rate function[17],

$$\Omega(\tilde{\alpha}|\alpha) = \tilde{\alpha} - \alpha - \alpha\ \ln(\alpha/\tilde{\alpha}) \ . \tag{3.6}$$

However the probability that a random 1-XORSAT formula with M equations is satisfiable is also exponentially small in N, with a rate function $\omega_1(\alpha)$ increasing with α. Thus, in the fixed-probability ensemble, a trade-off is found between ratios $\tilde{\alpha}$ close to α (formulas likely to be generated) and close to 0 (formulas likely to be satisfiable). As a result the fixed-probability rate function is

[17] M obeys a Poisson law with parameter $\bar{M}$. Using Stirling formula,

$$e^{-\bar{M}}\frac{\bar{M}^M}{M!} \simeq e^{-\alpha N}(\tilde{\alpha}N)^{\alpha N}\sqrt{2\pi N}\left(\frac{e}{\alpha N}\right)^{\alpha N} = e^{-N\,\Omega(\tilde{\alpha}|\alpha)+o(N)} \ ,$$

where Ω is defined in (3.6).

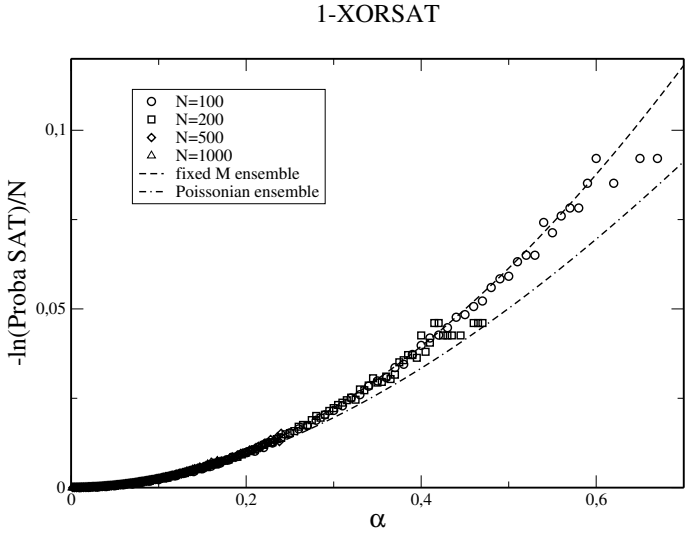

FIG. 3.2. Same data as Figure 3.1 with: logarithmic scale on the vertical axis, and rescaling by $-1/N$. The scaling functions ω_1 (3.7) and ω_1^p (3.5) for, respectively, the fixed-size and fixed-probability ensembles are shown.

$$\omega_1^p(\alpha) = \min_{\tilde{\alpha}} \left[\omega_1(\tilde{\alpha}) + \Omega(\tilde{\alpha}|\alpha)\right] , \tag{3.7}$$

and is smaller than $\omega_1(\alpha)$. It is an easy check that the optimal ratio $\tilde{\alpha}^* = \alpha/(2 - e^{-\alpha/2}) < \alpha$ as expected. Inverting (3.7) we deduce the rate function ω_1 in the fixed-size ensemble, in excellent agreement with numerics (Figure 3.2). This example underlines that thermodynamically equivalent ensembles have to be considered with care as far as rare events are concerned.

Remark that, when $\alpha \to 0$, $\tilde{\alpha} = \alpha + O(\alpha^2)$, and $\omega_1^p(\alpha) = \omega_1(\alpha) + O(\alpha^3)$. This common value coincides with the scaling function $-\Phi_1(\alpha)$ (3.3). This identity is expected on general basis, and justifies the agreement between the fixed-probability scaling function and the numerics based on the fixed-size ensemble (Figure 3.1, right).

3.2 Exercise 2: dynamics of the UC heuristics

Let α_0 denote the equation per variable ratio of the 3-XORSAT instance to be solved. We call $E_j(T)$ the number of j–equations (including j variables) after T variables have been assigned by the solving procedure. T will be called hereafter 'time', not to be confused with the computational effort. At time $T = 0$ we have $E_3(0) = \alpha_0 N$, $E_2(0) = E_1(0) = 0$. Assume that the variable x assigned at time T is chosen from a single-variable clause, that is, independently of the j-equation content. Call $n_j(T)$ the number of occurrences of x in j-equations ($j = 2, 3$). The evolution equations for the populations of 2-,3-equations read

$$E_3(T+1) = E_3(T) - n_3(T) \ , \quad E_2(T+1) = E_2(T) - n_2(T) + n_3(T) \ . \quad (3.8)$$

Flows n_2, n_3 are of course random variables that depend on the instance under consideration at time T, and on the choice of variable done by UC. What are their distributions? At time T there remain $N-T$ untouched variables; x appears in any of the $E_j(T)$ j-equation with probability $p_j = \frac{j}{N-T}$, independently of the other equations. In the large N limit and at fixed fraction of assigned variables, $t = \frac{T}{N}$, the binomial distribution converges to a Poisson law with mean

$$\langle n_j \rangle_T = \frac{j\, e_j}{1-t} \qquad \text{where} \qquad e_j = \frac{E_j(T)}{N} \quad (3.9)$$

is the density of j-equations at time T. The key remark is that, when $N \to \infty$, e_j is a slowly varying and non stochastic quantity and is a function of the fraction $t = \frac{T}{N}$ rather than T itself. Let us iterate (3.8) between times $T_0 = t\,N$ and $T_0 + \Delta T$ where $1 \ll \Delta T \ll N$ e.g. $\Delta T = O(\sqrt{N})$. Then the change ΔE_3 in the number of 3-equations is (minus) the sum of the stochastic variables $n_j(T)$ for $T = T_0, T_0+1, \ldots, T_0+\Delta T$. As these variables are uncorrelated Poisson variables with $O(1)$ mean (3.9) ΔE_3 will be of the order of ΔT, and the change in the density e_3 will be of order of $\Delta T/N \to 0$. Applying central limit theorem $\Delta E_3/\Delta T$ will be almost surely equal to $-\langle n_3 \rangle_t$ given by (3.9) and with the equation density measured at reduced time t. The argument can be extended to 2-equations, and we conclude that e_2, e_3 are deterministic (self-averaging) quantities obeying the two coupled differential equations

$$\frac{de_3}{dt}(t) = -\frac{3\, e_3}{1-t} \quad , \qquad \frac{de_3}{dt}(t) = \frac{3\, e_3}{1-t} - \frac{2\, e_2}{1-t} \ . \quad (3.10)$$

Those equations, together with the initial condition $e_3(0) = \alpha_0$, $e_2(0) = 0$ can be easily solved,

$$e_3(t) = \alpha_0 (1-t)^3 \quad , \qquad e_2(t) = 3\,\alpha_0\, t\, (1-t)^2 \ . \quad (3.11)$$

To sum up, the dynamical evolution of the equation populations may be seen as a slow and deterministic evolution of the equation densities to which are superimposed fast, small fluctuations. The distribution of the fluctuations adiabatically follows the slow trajectory. This scenario is pictured in Figure 3.3.

The trajectories we have derived in the previous Section are correct provided no contradiction emerges. But contradictions may happen as soon as there are $E_1 = 2$ unit-equations, and are all the more likely than E_1 is large. Actually the set of 1-equations form a 1-XORSAT instance which is unsatisfiable with a finite probability as soon as E_1 is of the order of $\sqrt{N}$ from the results of Exercise 1. Assume now that $E_1(T) \ll N$ after T variables have been assigned, what is the probability ρ_T that no contradiction emerges when the T^{th} variable is assigned by UC? This probability is clearly one when $E_1 = 0$. When $E_1 \geq 1$ we pick up a 1-equation, say, $x_6 = 1$, and wonder whether the opposite 1-equation,

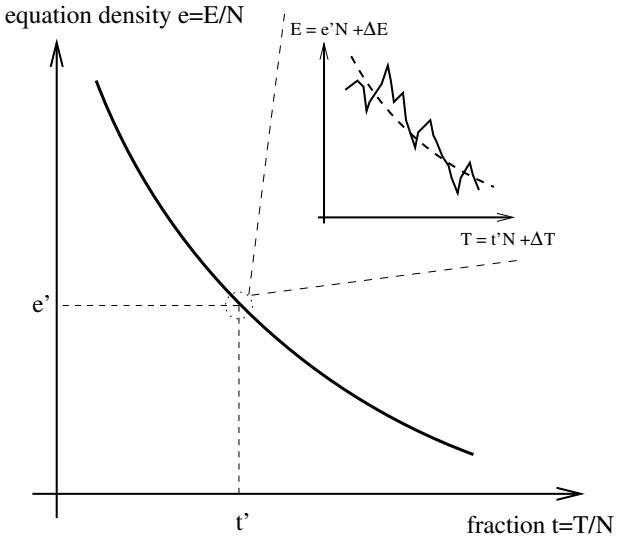

FIG. 3.3. Deterministic versus stochastic dynamics of the equation population E as a function of the number of steps T of the algorithm. On the slow time scale (fraction $t = T/N$) the density $e = E/N$ of (2- or 3-) equations varies smoothly according to a deterministic law. Blowing up of the dynamics around some point t', e' shows the existence of small and fast fluctuations around this trajectory. Fluctuations are stochastic but their probability distribution depends upon the slow variables t', e' only.

$x_6 = 0$, is present among the $(E_1 - 1)$ 1-equations left. As equations are uniformly distributed over the set of $N - T$ untouched variables

$$\rho_T = \left(1 - \frac{1}{2(N-T)}\right)^{\max(E_1(T)-1,0)} . \tag{3.12}$$

The presence of the max in the above equation ensures it remains correct even in the absence of unit-equations ($E_1 = 0$). $E_1(T)$ is a stochastic variable. However from the decoupling between fast and slow time scales sketched in Figure 3.3 the probability distribution of $E_1(T)$ depends only on the slow time scale t. Let us call $\mu(E_1; t)$ this probability. Multiplying (3.12) over the times $T = 0$ to $T = N - 1$ we deduce the probability that DPLL has successfully found a solution without ever backtracking,

$$\rho_{success} = \exp\left(-\int_0^1 \frac{dt}{2(1-t)} \sum_{E_1 \geq 1} \mu(E_1; t)\ (E_1 - 1)\right) \tag{3.13}$$

in the large N limit.

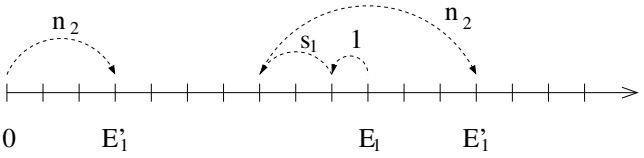

FIG. 3.4. Evolution of the number E_1 of 1-equations as one more variable is assigned. n_2 denotes the number of 2-equations reduced to 1-equations, s_1 the number of 1-equations satisfied. If $E_1 \geq 1$ a variable is fixed through unit-propagation: E_1 decreases by one plus s_1, and increases by n_2. In the absence of unit-equation ($E_1 = 0$) the number of 1-equations after the assignment is simply $E_1' = n_2$.

We are left with the calculation of μ. Figure 3.4 sketches the stochastic evolution of the number E_1 during one step. The number of 1-equations produced from 2-equations, n_2, is a Poisson variable with average value, from (3.11),

$$d(t) = \frac{2\,e_2(t)}{1-t} = 6\,\alpha_0\,t(1-t) \tag{3.14}$$

when $N \to \infty$. The number of satisfied 1-equations, s_1, is negligible as long as E_1 remains bounded. The probability that the number of 1-equations goes from E_1 to E_1' when $T \to T+1$ defines the entry of the transition matrix

$$M(E_1', E_1; t) = \sum_{n_2 \geq 0} e^{-d(t)} \frac{d(t)^{n_2}}{n_2!} \delta_{E_1' - (E_1 + n_2 - \delta_{E_1})} \ . \tag{3.15}$$

from which a master equation for the probability of E_1 at time T may be written. On time scales $1 \ll \Delta T \ll N$ this master equation converges to the equilibrium distribution μ, conveniently expressed in terms of the generating function

$$G(x;t) = \sum_{E_1 \geq 0} \mu(E_1;t)\ x^{E_1} = \frac{(1-d(t))(x-1)}{x\ e^{d(t)\ (1-x)} - 1} \quad . \tag{3.16}$$

The above is a sensible result for $d(t) \leq 1$ but does not make sense when $d(t) > 1$ since a probability cannot be negative! The reason is that we have derived (3.16) under the implicit condition that no contradiction was encountered. This assumption cannot hold when the average rate of 1-equation production, $d(t)$, is larger that one, the rate at which 1-equations are satisfed by unit-propagation. From (3.14) we see, when $\alpha > \alpha_E = \frac{2}{3}$, the trajectory would cross the

$$\alpha_D(p) = \frac{1}{2(1-p)} \tag{3.17}$$

on which $d = 1$ for some time $t_D < 1$. A contradiction is very likely to emerge before the crossing.

When $\alpha < \alpha_E$ d remains smaller than unity at any time. In this regime the probability of success reads, using (3.13) and (3.16),

$$\rho_{success} = \exp\left(\frac{3\alpha}{4} - \frac{1}{2}\sqrt{\frac{3\alpha}{2-3\alpha}}\ \tanh^{-1}\left[\sqrt{\frac{3\alpha}{2-3\alpha}}\right]\right) \ . \tag{3.18}$$

$\rho_{success}$ is a decreasing function of the ratio α, down from unity for $\alpha = 0$ to zero for $\alpha = \alpha_E$. In can be shown that, right at α_E, $\rho_{success} \sim \exp(-Cst \times N^{\frac{1}{6}})$ decreases as a stretched exponential of the size. The value of the exponent, and its robustness against the splitting heuristics are explained in Deroulers, Monasson, Critical behaviour of combinatorial search algorithm and the unit-clause universality class, Europhysics Letters 68, 153 (2004).