17

XORSAT

Solving a system of linear equations over a finite field $\mathbb{F}$ is arguably one of the most fundamental operations in mathematics. Several algorithms have been devised to accomplich such a task in polynomial time. The best known is Gauss elimination, that has $O(N^3)$ complexity (here N is number of variabls in the linear system, and we assume the number of equations to be $M = \Theta(N)$). As a matter of fact, one can improve over Gaussian elimination, and the best existing algorithm for general systems has complexity $O(N^{2.376\ldots})$. Faster methods do also exist for special classes of instances.

The set of solutions of a linear system is an affine subspace of $\mathbb{F}^N$: an observation that allows to characterize it in a very compact way. Despite such an apparent simplicity, the geometry of affine or linear subspaces of $\mathbb{F}^N$ can be surprisingly rich. This observation is systematically exploited in coding theory. Linear codes are just linear spaces over finite fields and are nevertheless known to achieve Shannon capacity on memoryless symmetric channels. Further, random linear codes have with high probability minimum distance $\Theta(N)$. In Chapter 11 we showed that the structure of random linear codes defined through sparse matrices is far from trivial.

From a different point of view linear systems are a particular example of constraint satisfaction problems. We can associate with a linear system a decision problem (estabilishing whether it has a solution), a counting problem (counting the number of solutions), optimization problem (minimize the number of violated equations). While the first two are polynomial, the latter is known to be NP-hard.

In this chapter we consider a specific ensemble of random linear systems over $\mathbb{Z}_2$, and discuss the structure of its set of solutions. The ensemble definition is mainly motivated by its analogy with other random constraint satisfaction problems, which also explains the name XOR-satisfiability (XORSAT). Sum modulo 2 is in fact equivalent to exclusive OR operation.

In the next section we provide the precise definition of the XORSAT ensemble and recall a few elementary properties of linear algebra. We also introduce one of the main objects of study of this Chapter: the SAT-UNSAT threshold. Section **??** takes a detour into the properties of belief propagation for XORSAT. These are shown to be related to the correlation structure of the uniform measure over solution and **??** to the appearence of a 2-core in the associated factor graph. Sections **??** and **??** builds on these results to compute the SAT-UNSAT threshold and characterize the structure of the solution space. While many results can be derived rigorously, XORSAT offers an ideal playground for understanding the non-rigorous cavity method that will be further developed in the next Chapters.

This is the object of Section **??**. Finally, several extensions of the basic model are discussed in Section 17.6.1.

17.1 Definition and some general remarks

Let $\mathbb{H}$ be an $M \times N$ matrix with entries $H_{ai} \in \{0,1\}$, $a \in \{1,\dots,M\}$, $i \in \{1,\dots,N\}$ and $\underline{b} = (b_1,\dots,b_M) \in \{0,1\}^M$ a binary vector. An instance **k-XORSAT** is given by a couple $(\mathbb{H},\underline{b})$ such that $\mathbb{H}$ has row weigth k (i.e. each row has k non-vanishing entries). In the decision version, solving it requires to solve the linear system $\mathbb{H}\underline{x} = \underline{b} \mod 2$, or to show that it has no solutions.

We shall further be interested in the set of solutions, to be denoted by $\mathcal{S}$, and in its size $Z = |\mathcal{S}|$. An alternative description of this set is provided by the uniform measure over $\mathcal{S}$

$$\mu(\underline{x}) = \frac{1}{Z}\,\mathbb{I}(\,\mathbb{H}\underline{x} = \underline{b} \mod 2\,) = \frac{1}{Z}\prod_{a=1}^{M}\psi_a(\underline{x}_{\partial a})\,, \tag{17.1}$$

where $\partial a = (i_a(1),\dots,i_a(k))$ is the set of non-vanishing entries in the a-th row of $\mathbb{H}$, and $\psi_a(\underline{x}_{\partial a})$ is the characteristic function for the a-th equation in the linear system (explicitely $\psi_a(\underline{x}_{\partial a}) = \mathbb{I}(x_{i_1(a)} \oplus \cdots \oplus x_{i_k(a)} = b_a)$). In the following we shall omit to specify that operations are carried mod 2 when clear from the context.

It is convenient to recall a few well known facts of linear algebra that will be useful in what follows:

(*i*) If $\mathbb{H}$ has rank M (all of its lines are independent), then the linear system $\mathbb{H}\underline{x} = \underline{b}$ has a solution for any choice of $\underline{b}$.

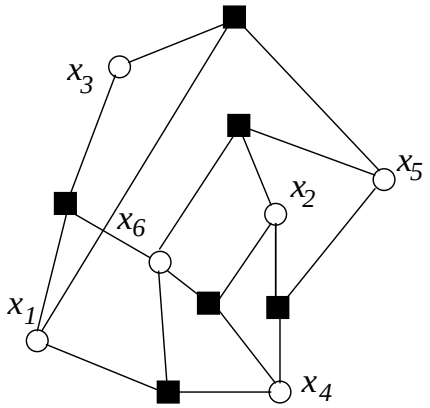
(*ii*) Conversely, if $\mathrm{rank}(\mathbb{H}) < M$, the linear system has solution if and only if $\underline{b}$ is in the image of $\mathbb{H}$ (which is a vector space of dimension $\mathrm{rank}(\mathbb{H})$).

If the system has at least one solution, then the set of solutions $\mathcal{S}$ is affine space of dimension $M - \mathrm{rank}(\mathbb{H})$. In particular $Z = 2^{N-\mathrm{rank}(\mathbb{H})}$. Further, given a solution $\underline{x}_*$, we have $\mathcal{S} = \underline{x}_* + \mathcal{S}_0$, where $\mathcal{S}_0$ is the linear space of solutions of the homogeneous system $\mathbb{H}\underline{x} = \underline{0}$. The last observation can be rephrased as follows.

(*iii*) If the number of solutions of the homogeneous system is $Z_0 = 2^{N-M}$, then the inhomogeneous system is satisfiable (SAT) for any $\underline{b}$ and has the same number of solutions.

(*iv*) Viceversa, if the number of solutions of the homogeneous system is $Z_0 > 2^{N-M}$, then the inhomogeneous one is SAT only for a fraction $2^{N-M}/Z_0$ of the $\underline{b}$'s.

The distribution μ admits a natural factor graph representation: variable nodes are associated to variables and factor node to linear equations, cf. Fig. **??**. Given a XORSAT formula F, we let $G(F)$ denote the associated factor graph. It is remarkable that one can identify subgraphs of $G(F)$ that serve as witnesses of satisfiability or unsatisfiability of F. By this we mean that the existence of such subgraphs imply satisfiability/unsatisfiability of F. Their construction is the



{fig:SimpleXORInstance} FIG. 17.1. Factor graph for a 3-XORSAT instance with $N = 6$, $M = 6$.

object of the exercise below. The existence of a simple witness for unsatisfiability is intimately related to the polynomial nature of XORSAT.

Exercise 17.1 Consider a 3-XORSAT instance defined through the 6×6 matrix

$$\mathbb{H} = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \tag{17.2}$$

(*a*) Compute the rank of $\mathbb{H}$. For which values of the right hand side $\underline{b}$ does the linear system $\mathbb{H}\underline{b} = \underline{0}$ have a solution? How many solution does it have in this case?

(*b*) Consider the factor graph associated to this linear system, cf. Fig. **??**. Show that each solution of the homogeneus system must correspond to a subset U of variable nodes with the following property. The subgraph induced by U and including all of the adjacent function nodes, has even degree at the function nodes. Find one subgraph with this property.

(*c*) Is there a graphical structure witnessing the fact that the rank of $\mathbb{H}$ is not maximal? Find such a structure in Fig. **??**.

(*d*) Assume to be given the factor graph representing $\mathbb{H}$ and the vector $\underline{b}$. Is there a subgraph witnessing unsatisfiability?

The **random** k**-XORSAT** ensemble is defined by taking $\underline{b}$ uniformly ar random in $\{0,1\}^M$, and $\mathbb{H}$ uniformly at random among the $N \times M$ $0-1$ matrices with k non-vanishing elements per row. More explicitely, each entry b_i is an

independent unbiased Bernoulli random variable, and each equation involves k distinct variables chosen uniformly among the $\binom{N}{k}$ k-uples. The resulting factor graph is distributed according to the $\mathbb{G}_N(k, M)$ ensemble. A slightly different ensembles might be defined by including each of the $\binom{N}{k}$ k-uples as a line of $\mathbb{H}$ indipendently with probability $p = N\alpha/\binom{N}{k}$: the corresponding factor graph is distributed according to the $\mathbb{G}_N(k, \alpha)$ ensemble

Given the relation between homogeneous and inhomogeneous systems described above, it is quite natural to introduce an ensemble of homogeneous linear systems. This is defined by taking $\mathbb{H}$ distributed as above, and $\underline{b} = \underline{0}$ deterministically. Since an homogeneous linear system has alwas at least one solution, this ensemble is sometimes referred to as **SAT k-XORSAT**. Given a k-XORSAT formula F, we shall denote by F_0 the corresponding SAT k-XORSAT formula. Further, if $\mu(\,\cdot\,)$ is the uniform measure over solutions F, $\mu_0(\,\cdot\,)$ will be the uniform measure over solutions of F_0.

⋆ The linear algebra observations (*iii*), (*iv*) above are easily shownto imply the following relation

$$\mathbb{P}\{F \text{ is SAT}\} = 2^{N-M}\mathbb{E}\{1/Z_{F_0}\}\,. \tag{17.3}$$

We are interested in the limit of large systems N, $M \to \infty$ with $\alpha = M/N$ fixed. By applying Friedgut Theorem it is possible to show that, for $k \geq 3$, the probability for a random formula F to be SAT has a sharp threshold. More precisely, there exists $\alpha_c(k; N)$ such that for $\alpha > (1 + \delta)\alpha_c(k; N)$ (respectively $\alpha < (1 - \delta)\alpha_c(k; N)$), $\mathbb{P}\{F \text{ is SAT}\} \to 0$ (respectively $\mathbb{P}\{F \text{ is SAT}\} \to 1$) as $N \to \infty$.

A moment of thought reveals that $\alpha_c(k; N) = \Theta(1)$. In fact, from Eq. (**??**) and recalling that $Z_0 \geq 1$, we get $\mathbb{P}\{F \text{ is SAT}\} \leq 2^{-N(\alpha-1)}$. As a consequence $\alpha_c(k; N) \leq 1$. On the other hand, for $\alpha < 1/k(k-1)$ the factor graph asssociated to F is formed, with high probability, by finite trees and unicyclic components. This corresponds to the matrix $\mathbb{H}$ being decomposable into blocks each one cor-
⋆ responding to a connected component. It is easy to show that,for $k \geq 3$ both a tree formula and an unicyclic component corresponds to a linear system of full rank. Since each block has full rank, $\mathbb{H}$ has full rank as well. As a consequence $\alpha_c(k; N) \geq 1/k(k-1)$.

Exercise 17.2 What happens for $k = 2$?

(*a*) Let $c(G)$ be the cyclic number of the factor graph G (number of edges minus vertices, plus 1). Show that $\mathbb{P}\{F \text{ is SAT}\} = \mathbb{E}\, 2^{-c(G)}$.

(*b*) Argue that this implies that $\mathbb{P}\{F \text{ is SAT}\}$ is bounded away from 1 for any $\alpha > 0$.

(*c*) Show that $\mathbb{P}\{F \text{ is SAT}\}$ is bounded away from 0 for any $\alpha < 1/2$.

The reader will surely be disppointed by the sloppines of the above bounds. She can improve over them by solving the Exercises below. Our best excuse is

however that one can prove that $\alpha_{\rm c}(k)$ does not depend on N and provide an explicit expression for its value. This will be the object of the next Sections.

Exercise 17.3 In order to obtain a better upper bound on $\alpha_{\rm c}(k;N)$ proceed as follows:

(*a*) Assume that, for any given α, $Z_{F_0} \ge 2^{nf_k(\alpha)}$ with probability at least 1/100. Show that Eq. (**??**) implies $\alpha_{\rm c}(k;N) \le \alpha^*(k)$, where $\alpha^*(k)$ is the smallest value of α such that $1-\alpha-f_k(\alpha) \le 0$.

(*b*) Show that the above assumption holds with $f_k(\alpha) = e^{-k\alpha}$. What is the asymptotic behavior of $\alpha^*(k)$ for large k? How can you improve the exponent $f_k(\alpha)$?

{ex:FirstMomentXOR}

Exercise 17.4 A better lower bound on $\alpha_{\rm c}(k;N)$ can be obtained through a first moment calculation. In order to simplify the calculations we consider here a modified ensemble in which the variables entering in equation a are chosen indipendently and uniformly at random (they do not need to be distinct). The scrupolous reader can check at the end that little changes when returning to the original ensemble.

(*a*) Show that Eq. (**??**) implies $\mathbb{P}\{F \text{ is SAT}\} \ge 2^{N-M}/\mathbb{E}\, Z_{F_0}$.

(*b*) Prove that

$$\mathbb{E}\, Z_{F_0} = \sum_{w=0}^{N} \binom{N}{w} \left[\left(\frac{N+w}{2N}\right)^k + \left(\frac{N-w}{2N}\right)^k \right]^M . \qquad (17.4)$$

(*c*) Let $g_k(x) = \mathcal{H}(x) + \alpha \log\left[\left(\frac{1+x}{2}\right)^k + \left(\frac{1-x}{2}\right)^k\right]$ and define $\alpha_*(k)$ to be the the largest value of α such that the maximum of $g_k(x)$ is achieved at $x = 1/2$. Show that $\alpha_{\rm c}(k;N) \ge \alpha_*(k)$.

17.2 Belief propagation and correlation decay

{sec:XORBP}

Equation (17.29) provides a representation of the uniform measure over solutions of a XORSAT instance as a graphical model. This naturally suggests to apply message passing techniques. We will in particular describe belief propagation and analyze its behavior. While this may seem at first sight a detour from the objective of computing $\alpha_{\rm c}(k;N)$, it will instead provide some important insight.

In order for the model (17.29) to be well defined, the linear system $\mathbb{H}\underline{x} = \underline{b}$ must admit at least one solution. If this is the case, we can, without loss of generality[57], set $\underline{b} = \underline{0}$. Applying the general definitions in Chapter 14, the BP update equations read

[57] Infact, if $\underline{b} \neq \underline{0}$, $\underline{x}^{(0)}$ is a fixed solution of the inhomogeneous linear system, and $\underline{x}$ is a uniformly random solution, then $\underline{x} = \underline{x}^{(0)} \oplus \underline{x}'$, where $\underline{x}'$ is a uniformly random solution of the inhomogeneous system.

$$m_{i\to a}^{(t+1)}(x_i) \cong \prod_{b\in\partial i\setminus a} \widehat{m}_{b\to i}^{(t)}(x_i)\,, \qquad \widehat{m}_{a\to i}^{(t)}(x_i) \cong \sum_{\underline{x}_{\partial a\setminus i}} \prod_{j\in\partial a\setminus i} m_{j\to a}^{(t)}(x_j)\psi_a(\underline{x}_{\partial a})\,, \tag{17.5}$$

where $\psi_a(\underline{x}_{\partial a})$ is the indicator function on $\sum_{j\in\partial a} x_j = \mathtt{0}$ (mod 2).

These equations can be considerably simplified using the linear structure. For the sake of clarity, we start from a more general viewpoint. Let $f : \{\mathtt{0},\mathtt{1}\}^N \to \{\mathtt{0},\mathtt{1}\}$ be a linear function mod 2. Explicitely, $f(\underline{x})$ is the mod 2 sum of a subset $x_{i(1)},\dots,x_{i(n)}$ of the bits. If $\underline{x}$ is drawn from the distribution $\mu_0(\,\cdot\,)$, $f(\underline{x})$
⋆ become a random variable taking values in $\{\mathtt{0},\mathtt{1}\}$. We leave to the reader the exercise of showing that the distribution of f can be of two possible forms. Either $f(\underline{x}) = \mathtt{0}$ with probability 1, or $f(\underline{x})$ is uniformly random in $\{\mathtt{0},\mathtt{1}\}$.

In particular, the same is true for the marginal distribution of a single bit x_i (i.e. $f(\underline{x}) = x_i$). In other words, given the formula F, one can distinguish between 'frozen' bits (i.e. bits that are forced to be $\mathtt{0}$) and 'floppy' ones (those that are equally likely to be $\mathtt{0}$ or $\mathtt{1}$). BP aims at determining whether any single bit belongs to one class or the other.

Consider now BP messages: they are also distributions over $\{\mathtt{0},\mathtt{1}\}$. If at any given time t all the messages coincide with one of the two distributions above (uniform over $\{\mathtt{0},\mathtt{1}\}$ or concentrated on $\mathtt{0}$), then this will be true at all subsequent times. Let us cosider an initial condition such that this is the case at time 0. At any time, messages take one of two possible values that we denote as $*$ (corresponding to the uniform distribution) and $\mathtt{0}$ (distribution entirely supported on $\mathtt{0}$). The update equations (**??**) correspond to the following rules. At a variable node the outgoing message is $\mathtt{0}$ unless all the incoming are $*$. At a function node the outgoing is $*$ unless all of the incoming are $\mathtt{0}$. In other words we reduced ourselves to the erasure decoder of Section 15.3.

These rules preserves a natural partial ordering. Given two sets of messages $m^{(t)} = \{m_{i\to a}^{(t)}\}$, $\widetilde{m}^{(t)} = \{\widetilde{m}_{i\to a}^{(t)}\}$, let us say that $m^{(t)} \succeq \widetilde{m}^{(t)}$ if for each directed edge $i \to a$ such that $\widetilde{m}_{i\to a}^{(t)} = \mathtt{0}$, $m_{i\to a}^{(t)} = \mathtt{0}$ as well. It follows immediately from the update rules that, if for some t $m^{(t)} \succeq \widetilde{m}^{(t)}$, then $m^{(s)} \succeq \widetilde{m}^{(s)}$ for all $s > t$.

Because of such a partial ordering, it is useful to begin the analysis with the two 'extremal' initial conditions, namely $m_{i\to a}^{(0)} = *$ for all directed edges $i \to a$, or $m_{i\to a}^{(0)} = \mathtt{0}$ for all $i \to a$. Since such initializations consists in both cases of iid messages (with degenerate distributions), we can apply density evolution. Denoting by Q_t the fraction of edges carrying a message $*$, we deduce that in the $N \to \infty$ limit, Q_t is a deterministic quantity satisfying the recursion

$$Q_{t+1} = 1 - \exp\{-k\alpha Q_t^{k-1}\}\,. \tag{17.6}$$

This has to be supplemented with $Q_0 = 1$ (respectively $Q_0 = 0$) for the $\mathtt{0}$ initial condition (respectively, the $*$ initial condition). The density evolution recursion is represented pictorially in Fig. **??**.

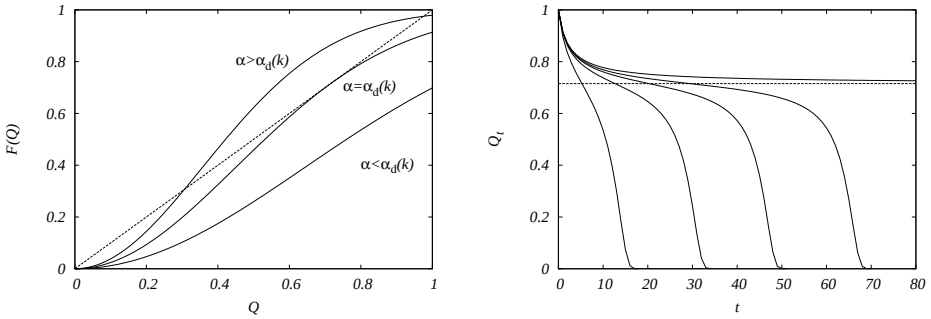


FIG. 17.2. Graphical representation of the density evolution recursion $Q_{t+1} = F(Q_t)$ for 3-XORSAT. On the left: the mapping $F(Q) = 1 - \exp(-k\alpha Q^{k-1})$ below, at and above the critical point. On the right: evolution of Q_t for (from bottom to top) $\alpha = 0.75$, 0.8, 0.81, 0.814, $\alpha_{\rm d}(3) \approx 0.818468$.

:DensityEvolutionXORSAT}

Under the $*$ initial condition, we have $Q_t = 0$ at all times t. This is indeed consistent with the observation that $m^{(*)} \equiv \{m_{i\to a} = * \text{ for all } i \to a\}$ is a fixed point of the message passing recursion. On the other hand, under the 0 initial condition (i.e., if we set $Q_0 = 1$), it is easy to show that that $Q_t \to 0$ for $\alpha < \alpha_{\rm d}(k)$, while $Q_t \to Q$ for $\alpha > \alpha_{\rm d}(k)$. Here $Q > 0$ the largest positive solution of $Q = 1 - \exp\{-k\alpha\, Q^{k-1}\}$. The critical value is defined as

$$\alpha_{\rm d}(k) = \sup\{\, \alpha \;:\; x < 1 - e^{-k\alpha\, x^{k-1}} \;\forall x \in (0,1]\,\}\,. \tag{17.7}$$

We get for instance $\alpha_{\rm d}(k) \approx 0.818469, 0.772280, 0.701780$ for, respectively, $k = 3$, 4, 5 and $\alpha_{\rm d}(k) = \log k/k[1 + o(1)]$ as $k \to \infty$.

We conclude that, for $\alpha < \alpha_{\rm d}(k)$ BP converges to the all $*$ fixed point[58] irrespective of the initial condition. The BP estimates for the local marginals are given in terms of the messages by

$$m_i^{(t)}(x_i) \cong \prod_{a\in\partial i} \widehat{m}_{a\to i}^{(t)}(x_i)\,. \tag{17.8}$$

Because of the argument above $m_i^{(t)}(x_i)$ is the uniform distribution over $\{0, 1\}$ for large enough t with high probability.

Is marginal distribution of bit x_i under the measure $\mu_0(\,\cdot\,)$ correctly computed by BP? The fact that BP estimates do not depend on the initial condition hints at a positive answer. This can indeed be proven starting from an alternative interpretation of Q_t. Let $i \in \{1, \dots, N\}$ be a uniformly rarndom variable index and consider the ball of radius t around i in the factor graph G: $\mathsf{B}_{i,t}(G)$. Imagine

[58] A vanishing fraction of messages $m_{i\to a} = 0$ is not excluded by this argument. See below for further inforation on this point.

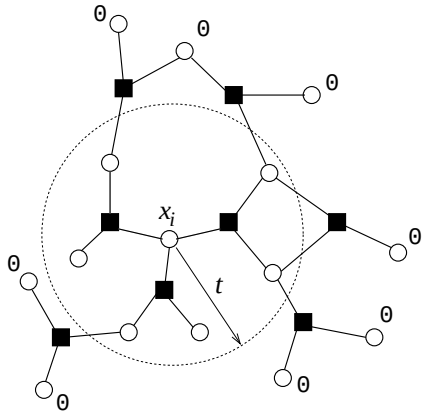


FIG. 17.3. Factor graph for a 3-XORSAT instance with the depth $t = 1$ neighborhood of vertex i, $\mathsf{B}_{i,t}(G)$ indicated. Fixing to 0 all the variables outside $\mathsf{B}_{i,t}(G)$ does not imply that x_i must be 0 in order to satisfy the homogeneous linear system. {fig:BallXOR}

to set $x_j = 0$ all the variables x_j with $j \in G \backslash \mathsf{B}_{i,t}(G)$. Let $Q_t^{(N)}$ be the probability that, under this condition, all the solutions of the linear system $\mathbb{H}\underline{x} = \underline{0}$ have $x_i = \underline{0}$. Equivalently

$$Q_t^{(N)} = \mathbb{P}\left\{\mu_0(x_i = 0 | \underline{x}_{\sim i,t} = \underline{0}) = 1\right\} . \tag{17.9}$$

Then the convergence of $\mathsf{B}_{i,t}(G)$ to the tree model $\mathbb{T}(k, \alpha)$ discussed in Section 9.5 implies that, for any given t, $\lim_N Q_t^{(N)} = Q_t$, where the initial condition $Q_0 = 1$ is understood.

Consider now the marginal distribution $\mu_0(x_i)$. If $x_i = 0$ in all the solutions of $\mathbb{H}\underline{x} = \underline{0}$, then, a fortiori $x_i = 0$ in all the solutions that fulfill the additional condition $x_j = 0$ for $j \notin \mathsf{B}_{i,t}(G)$. Therefore we have $\mathbb{P}\{\mu_0(x_i = 0) = 1\} \le Q_t^{(N)}$. By taking the $N \to \infty$ limit we get

$$\lim_{N\to\infty} \mathbb{P}\{\mu_0(x_i = 0) = 1\} \le \lim_{N\to\infty} Q_t^{(N)} = Q_t \, . \tag{17.10}$$

Letting $t \to \infty$ and noticing that the left hand side does not depend on t we get $\mathbb{P}\{\mu_0(x_i = 0) = 1\} \to 0$ as $N \to \infty$. In other words most of the bits have marginal distribution $\mu_0(x_i = 0) = \mu_0(x_i = 0) = 1/2$ for $\alpha < \alpha_{\rm d}(k)$ (are floppy).

Building on this result one can show that, for $\alpha < \alpha_{\rm d}(k)$ the rank of $\mathbb{H}$ is maximal with high probability. In other words, both the linear systems $\mathbb{H}\underline{x} = \underline{0}$ and $\mathbb{H}\underline{x} = \underline{b}$ have $Z = 2^{N-M}$ solutions with high probability. Since (as we will see below) $\alpha_{\rm d}(k) < \alpha_{\rm c}(k)$ strictly, we will not provide the full argument here. A possible route is provided by the exercise below (proving a slightly weaker statement).

Exercise 17.5 In the following G denotes the factor graph of a random SAT k-XORSAT formula, and $a \in \{1,\dots,M\}$ a uniformly random factor node (an equation) in G. Let $G\backslash a$ be the (factor graph of) formula with $M-1$ equations over the same N variables obtaibed by eliminating a from G. Finally let $i_1,\dots i_k$ the indices of variables involved in equation a and $\mathcal{S}_a$ the subset of assignments to $\underline{x}_{\partial a} = (x_{i_1(a)},\dots,x_{i_k(a)})$ that can be extended to solutions of $G\backslash a$.

The objective is to show, for $\alpha < \alpha_{\rm d}(k)$, $\mathrm{rank}(\mathbb{H}) > M - \Theta(\log N)$ with high probability by justifying the following steps.

(*a*) A first linear algebra reminder: $\mathcal{S}_a$ is a linear subspace of $\{0,1\}^k$. There exists $\mathbb{H}_a$ the the k columns $0-1$ matrix such that $\mathcal{S}_a = \{\underline{x}_{\partial a} :\ \mathbb{H}_a\underline{x}_{\partial a} = \underline{0}\}$.

(*b*) A second linear algebra reminder: $\mathrm{rank}(\mathbb{H})$ is at least the number of equation indices $a \in \{1,\dots,M\}$, such that the length–k vector $(1,\dots,1)$ is linearly independent from the rows of $\mathbb{H}_a$ (we will denote this number as $M - J(G)$).

(*c*) Linear independence holds if $\mu_0(\underline{x}_{\partial a}|\underline{x}_{\sim a,t} = \underline{0}) = 1/2^k$ for some $t > 0$, where $\underline{x}_{\sim a,t} = \{x_j :\ j \notin \mathsf{B}_{a,t}(G)\}$ and $\mathsf{B}_{a,t}(G)$ is the neighborhood of radius t around a.

(*d*) If $\widetilde{Q}_t^{(N)}$ is the probability that $\mu_0(\underline{x}_{\partial a}|\underline{x}_{\sim a,t} = \underline{0}) \neq 1/2^k$, then $\widetilde{Q}_t^{(N)} \to \widetilde{Q}_t$ as $N \to \infty$, where $\widetilde{Q}_t \le A\exp\{-b^t\}$ for some $A, b > 1$.

(*e*) Refining the results in Section 9.5 it is possible to show that $|\widetilde{Q}_t^{(N)} - \widetilde{Q}_t| \le Be^{\gamma t}/N$, for some $B, \gamma > 0$. Show that this implies the thesis by taking $t = C\log\log N$, and applyng Markov inequality to $J(G)$.

We conclude by providing a last interpretation of the result $Q_t \to 0$ that holds for $\alpha < \alpha_{\rm d}(k)$. First consider the following modification. Choose a solution $\underline{x}^{(*)}$ of the homogeneous linear system and, instead of fixing $x_j = 0$ for all $j \notin \mathsf{B}_{i,t}(G)$, let $x_j = x_j^{(*)}$. Then Eq. (**??**) immediately implies

$$Q_t^{(N)} = \mathbb{P}\left\{\mu_0(x_i = x_i^{(*)}|\underline{x}_{\sim i,t} = \underline{x}^{(*)}_{\sim i,t}) = 1\right\}\,. \tag{17.11}$$

Next notice that the same conclusion is literally true if we consider $\underline{b} \neq 0$, the measure $\mu_0(\,\cdot\,)$ (uniform over solutions of $\mathbb{H}\underline{x} = \underline{0}$), is replaced by $\mu(\,\cdot\,)$ (uniform over solutions of $\mathbb{H}\underline{x} = \underline{b}$) and $\underline{x}^{(*)}$ is an arbitrary solution of $\mathbb{H}\underline{x} = \underline{b}$.

Finally, there is still one unpleasant feature about the above formulation. It relies too much to a dichotomy that is very specific to XORSAT. Either the 'far away' variables completely determine x_i (and therefore $\mu(x_i = x_i^{(*)}|\underline{x}_{\sim i,t} = \underline{x}^{(*)}_{\sim i,t}) = 1$), or they have no influence on it ($\mu(x_i = x_i^{(*)}|\underline{x}_{\sim i,t} = \underline{x}^{(*)}_{\sim i,t}) = 1/2$). A possible route to obtain a more generic formulation consists in comparing two different choices $\underline{x}^{(1)}$, $\underline{x}^{(2)}$ of the reference solution. Our final statement is that, for $\alpha < \alpha_{\rm d}(k)$

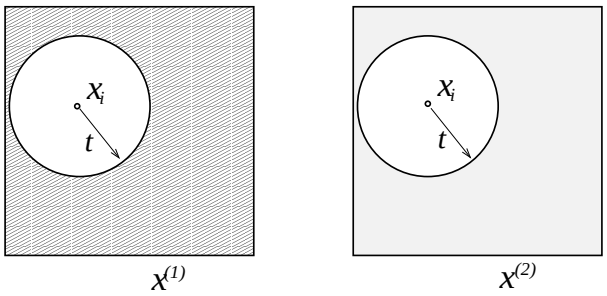


FIG. 17.4. A thought experiment: fix variables 'far' from i to two different assignments and check the influence on x_i. {fig:TwoBC_XOR}

$$\lim_{N\to\infty} \mathbb{E}\left\{ \sup_{\underline{x}^{(1)},\underline{x}^{(2)}} |\mu(x_i|\underline{x}^{(1)}_{\sim i,t}) - \mu(x_i|\underline{x}^{(2)}_{\sim i,t})| \right\} = Q_t \to 0\,, \qquad (17.12)$$

as $t \to \infty$. This expresses a 'worst case' correlation decay property: the marginal distribution of x_i is independent of the assignment of far away variables, whatever this is, cf. Fig. **??**. As we will see in the next chapters, this property has some chances to hold in more general settings.

17.3 2-core percolation

{sec:XORCore}

What happens for $\alpha > \alpha_{\rm d}(k)$? A first hint is provided by the instance in Fig. **??**. In this case, the configuration of messages $m^{(t)}_{i\to a} = \mathtt{0}$ on all directed edges $i \to a$ is a fixed point of the BP update. A moment of reflection shows that this happens because G has the property that each variable node at degree at least 2.

We already encounterd similar structures in Section 15.3, where we identified them as responsible for error events in iterative decoding of LDPC codes over the erasure channel. Let us recall the relevant points[59]. Given a factor graph G, its l-core $K_l(G)$ is the maximal subset of the function nodes such that no variable has degree between 1 and $l-1$ in the induced subgraph. Equivalently each variable that appears in the subgraph has degree at least l. Following the coding litterature, we shall call any subset of function nodes sharing the same property but not necessarily maximal, a 'stopping set'.

Consider now the factor graph G associated to a SAT k-XORSAT formula and let $m^{(\infty)}_{i\to a}$, $\widehat{m}^{(\infty)}_{a\to i}$ be the fixed point reached by belief propagation under
⋆ initialization $m^{(0)}_{i\to a} = \mathtt{0}$ for all $i \to a$ (we invite the reader to show that such a fixed point is indeed reached after a number of iterations at most equal to the number of messages). The following properties can be proved by induction over t: (i) $m^{(\infty)}_{i\to a} = \widehat{m}^{(\infty)}_{a\to i} = \mathtt{0}$ for each edge (i,a) in $K_2(G)$. (ii) Vice-versa, if a variable node $i \in \{1,\dots,N\}$ has $\widehat{m}^{(\infty)}_{a\to i} = \mathtt{0}$ for at least 2 of the neighborhing function

[59] Notice that the relevant structures for the decoding problem was the 2-core of the *dual* factor graph that is obtained by exchanging variable and function nodes.

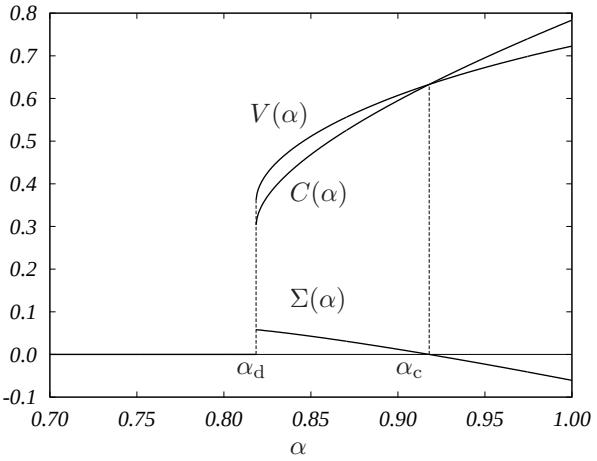


FIG. 17.5. Normalized number of variables $V(\alpha)$ and of equations $C(\alpha)$ in the core of random 3-XORSAT formulae. The number of solutions turns out to be $\Sigma(\alpha) = V(\alpha) - C(\alpha)$. {fig:XORcore}

nodes $a \in \partial i$, then $i \in K_2(G)$. (*iii*) Finally, if a function node $a \in \{1, \dots, M\}$ has $m^{(\infty)}_{i\to a} = 0$ for all the neighborhing variable nodes $i \in \partial a$, then $a \in K_2(G)$.

It follows from the density evolution analysis that, after any bounded number of iterations t, messages $\widehat{m}^{(t)}_{a\to i}$ entering a variable node are asymptotically iid with $\mathbb{P}\{\widehat{m}^{(t)}_{a\to i} = 0\} = \widehat{Q}_t \equiv Q_t^{k-1}$. Let us for a moment assume that the limits $t \to \infty$ and $N \to \infty$ can be exchanged without much harm. This means that the fixed point messages $\widehat{m}^{(\infty)}_{a\to i}$ entering a variable node i are asymptotically iid with $\mathbb{P}\{\widehat{m}^{(\infty)}_{a\to i} = 0\} = \widehat{Q} \equiv Q^{k-1}$. The number of incoming messages with $\widehat{m}^{(\infty)}_{a\to i} = 0$ converges therefore to a Poisson random variable with mean $k\alpha\widehat{Q}$. The expected number of variable nodes in the core will be $\mathbb{E}|K_2(G)| = NV(\alpha, k) + o(N)$, where $V(\alpha, k)$ is the probability that such a Poisson random variable is larger than one, that is

$$V(\alpha, k) = 1 - e^{-k\alpha\widehat{Q}} - k\alpha\widehat{Q}\, e^{-k\alpha\widehat{Q}}\,. \tag{17.13}$$

In Fig. **??** we plot the normalized expected size as a function of α. It is obviously 0 for $\alpha < \alpha_{\rm d}(k)$, then it jumps to some finite value at $\alpha_{\rm d}(k)$ and smoothly approaches 1 as $\alpha \to \infty$.

Is $K_2(G)$ a random factor graph or does it kave any particular structure? By construction it does not include either variable nodes of degree zero or one. Under the hypotheses made above, its expected degree profile (explected number of nodes of any given degree) will be asymptotically $\widehat{\Lambda} \equiv \{\widehat{\Lambda}_l\}$, where $\widehat{\Lambda}_l$ is the probability that a Poisson random variable of parameter $k\alpha\widehat{Q}$, coditioned to be larger than 1, is equal to l. Explicitely $\widehat{\Lambda}_0 = \widehat{\Lambda}_1 = 0$, and

$$\widehat{\Lambda}_l = \frac{1}{e^{k\alpha\widehat{Q}} - 1 - k\alpha\widehat{Q}} \frac{1}{l!} (k\alpha\widehat{Q})^l \qquad \text{for } l \geq 2. \tag{17.14}$$

Somewhat surprisingly (and in a sense to be precised below) $K_2(G)$ does not have any more structure than this.

The above result allows us to compute the expected number of equations in the core. This is given by the number of vertices times their average degree, divided by k, which yields $NC(\alpha, k) + o(N)$ where

$$C(\alpha, k) = \alpha\widehat{Q}(1 - e^{-k\alpha\widehat{Q}}) \,. \tag{17.15}$$

{thm:XORCore}

Although this was an informal calculation, the result is correct as spelled out by the following

Theorem 17.1 *Consider a factor graph G from the $\mathbb{G}_N(k, N\alpha)$ ensemble with $k \geq 3$. Then*

(*i*) *$K_2(G) = \emptyset$ with high probability for $\alpha < \alpha_{\rm d}(k)$.*

(*ii*) *For $\alpha > \alpha_{\rm d}(k)$, $|K_2(G)| = nV(\alpha, k) + o(n)$ with high probability.*

(*iii*) *The fraction of vertices of degree l in $K_2(G)$ is between $\widehat{\Lambda}_l - \varepsilon$ and $\widehat{\Lambda}_l + \varepsilon$ with probability greater than $1 - e^{-\Theta(N)}$.*

(*iv*) *Conditionally on the number of variable nodes $n = |K_2(G)|$ the degree profile being Λ, $K_2(G)$ is distributed according to the $\mathbb{D}_n(\Lambda, x^k)$ ensemble.*

Proof: We only sketch some of the basic ideas involved in traducing the above calculation in a proof. We also limit ourselves to points (*i*) and (*ii*). The reader is invited to consult the Notes section for pointers to the literature.

(*i*) The first step is to show that, for any $\varepsilon > 0$ and $\alpha < \alpha_{\rm d}(k)$ the core size is with high probability smaller than $N\varepsilon$.

Consider any edge $i \to a$ or $a \to i$ in the core and assume the BP messages have been initialized to $\mathtt{0}$. It is easy to show inductively that $m^{(t)}_{i\to a} = \widehat{m}^{(t)}_{a\to i} = \mathtt{0}$ at any time t. Fix now a finite t (say 100 or 10^6). The number of variable nodes in the core $|K_2(G)|$ can be upper bounded as the number of variable nodes such that at least two of the incoming messages have value $\mathtt{0}$ *at time t*.

For large enough N, the messages entering node i at time t are approximately independent with $\mathbb{P}\{\widehat{m}^{(t)}_{a\to i} = \mathtt{0}\} = \widehat{Q}_t$. It follows that

$$|K_2(G)| \leq N\{1 - e^{-k\alpha\widehat{Q}_t} - k\alpha\widehat{Q}_t e^{-k\alpha\widehat{Q}_t}\} + o(N) \tag{17.16}$$

with high probability[60]. But now, since $\widehat{Q}_t \to 0$ as $t \to \infty$, we can chose $t = t(\varepsilon)$ such that the first term is smaller than $N\varepsilon/2$ thus obtaining $|K_2(G)| \leq N\varepsilon$ with high probability.

The proof is completed by showing that, with high probability, G does not contain stopping sets of size smaller than $N\varepsilon_*$ for some $\varepsilon_* > 0$. This is in turn

[60]The 'with high probability' requires some more work. The basic idea is that, after a finite number of iterations, far apart messages are independent.

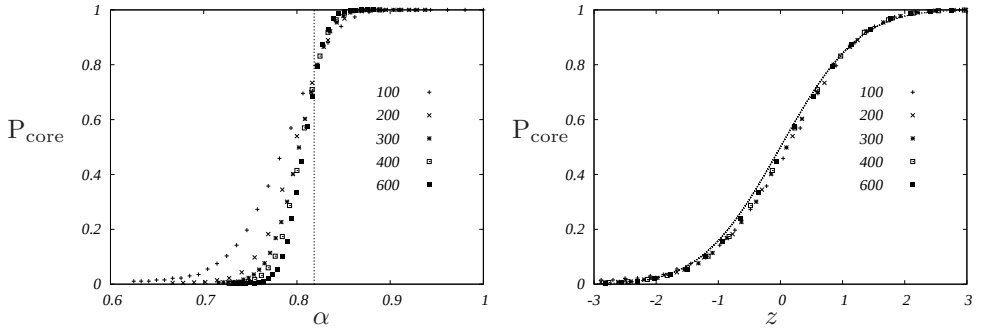


FIG. 17.6. Probability that a random graph form the $\mathbb{G}_N(k,\alpha)$ ensemble with $k=3$ (equivalently, the factor graph of a random 3-XORSAT formula) contains a 2 core. On the left, the outcome of numerical simulations is compared with the asymptotic threshold $\alpha_{\rm d}(k)$. On the right, scaling plot (see text). {fig:CoreCritical}

done by computing the expected number of such stopping sets and showing that it vanishes as $N\to\infty$. The calculation is very similar to the one in Section 11.2 and we omit it here.

(*ii*) The argument above also implies that $|K_2(G)|\le NV(\alpha,k)+o(N)$ with high probability for $\alpha\ge\alpha_{\rm d}(k)$.

Imagine to have run BP for a large number of iterations t. Let $K_2^{(t)}(G)$ be the current set of variable nodes i such that for at least 2 neighboring check nodes a, $\widehat{m}_{a\to i}^{(t)}=0$. Since $K_2(G)\subseteq K_2^{(t)}(G)$, it is enough to prove that $|K_2^{(t)}(G)\backslash K_2(G)|\le N\varepsilon(t)$ for any N, where $\varepsilon(t)\to 0$ as $t\to\infty$.

In order to prove the last fact one can construct $K_2(G)$ from $K_2(G)$ through the sequential, 'peeling' procedure already described in Section **??**. At each steps one picks a variable node of degree one uniformly at random and peel it together with the adjacent function node. The procedure halts when no variable node is left: our objective is to show that it halts with high probability after $N\varepsilon(t)$ steps.

Let us do the back-of-the-envelope calculation. At each steps the number of degree one variable nodes decreases at least by one because the selected node is removed and increases by the number of variable nodes of degree 2 in the function node removed. The expected change is about $\Delta=-1+(k-1)k\alpha\widehat{Q}_*/(e^{k\alpha\widehat{Q}_*}-1)$. Here we used the fact that the degree distribution is close to the fixed point one. It is easy to check that $\Delta<0$.

Since $K_2^{(t)}(G)$ has at most $N\varepsilon(t)$ nodes of degree one for some $\varepsilon(t)\to 0$ with t, standard probabilistic arguments allow to show that the procedure stops with high probability after $2N\varepsilon(t)/\Delta$ steps (the factor 2 is inserted to get the whp statement). □

In Fig. **??** we compare the statement in this Theorem with numerical simulations. The probability that G contains a 2 core $\mathrm{P}_{\rm core}(\alpha)$ increases from 0 to 1 as α ranges from 0 to ∞, with a threshold becoming sharper and sharper as the size N increases. The threshold behavior can be accurately described using

finite size scaling. Setting $\alpha = \alpha_{\rm d}(k) + \beta(k)\, z\, N^{-1/2} + \delta(k)\, N^{-2/3}$ one can show that $\mathrm{P}_{\rm core}(\alpha)$ approaches a finite limit smooth in z.

{sec:XORThreshold}

17.4 The SAT-UNSAT threshold

Why did we devote the last Section to a long detour through properties of the 2-core of G? A first indication is provided by the following simple remark. Let $\mathbb{H}_*$ denote the $\mathtt{0}-\mathtt{1}$ matrix associated with the core, i.e. the matrix including those rows/columns such that the associated function/variable nodes belong to $K_2(G)$. Notice that if a given row is included in $\mathbb{H}_*$ then all the columns corresponding to non-zero entries of that row are also in $\mathbb{H}_*$. As a consequence, a necessary condition for the rows of $\mathbb{H}$ to be independent is that the rows of $\mathbb{H}_*$ are independent. This is in turn impossible if the number of columns in
⋆ $\mathbb{H}_*$ is smaller than its number of rows. More quantitatively, one can show that $M - \mathrm{rank}(\mathbb{H}) \geq \mathrm{rows}(\mathbb{H}_*) - \mathrm{cols}(\mathbb{H}_*)$ (with the obvious meanings of $\mathrm{rows}(\,\cdot\,)$ and $\mathrm{cols}(\,\cdot\,)$).

Let us consider random formulae. In view of Theorem **??**, $\mathrm{rows}(\mathbb{H}_*) - \mathrm{cols}(\mathbb{H}_*) = N\Sigma(k,\alpha) + o(N)$, where

$$\Sigma(k,\alpha) = V(k,\alpha) - C(k,\alpha)\,. \tag{17.17}$$

If $\Sigma(k,\alpha) < 0$ then $\mathbb{H}_*$ has more rows than columns and, by the argument above, $\mathrm{rank}(\mathbb{H}) < M$ with high probability. The function $\Sigma(k,\alpha)$ is plotted in Fig. **??** for $k = 3$. This argument implies an upper bound $\alpha_{\rm c}(k,N)$. Remarkably this bound is tight as stated below.

Theorem 17.2 *For $k \geq 3$, let $\Sigma(k,\alpha)$ be defined as above and $\alpha_{\rm c}(k) = \inf\{\alpha : \Sigma(k,\alpha) < 0\}$. Then, a random k-XORSAT formula with N variables and $N\alpha$ equations is satisfiable with high probability if $\alpha < \alpha_{\rm c}(k)$ and unsatisfiable with high probability if $\alpha > \alpha_{\rm c}(k)$.*

Further, for $\alpha < \alpha_{\rm c}(k)$ the number of solutions is, with high probability, 2^{N-M}.

Proof: Once again we shall try to convey the basic ideas and refer to the literature for technical details.

Let F be a random k-XORSAT formula with N variables and $N\alpha$ equations. The paragraphs above already contain a proof that F is with high probability unsatisfiable if $\alpha > \alpha_{\rm c}(k)$. In order to prove that it is satisfiable if $\alpha < \alpha_{\rm c}(k)$ we will show the following facts: (A) if the core matrix $\mathbb{H}_*$ has maximum rank, then $\mathbb{H}$ has maximum rank as well; (B) if $\alpha < \alpha_{\rm c}(k)$, then $\mathbb{H}_*$ has maximum rank with high probability. As a byproduct, the number of soutions is $2^{N-\mathrm{rank}(\mathbb{H})} = 2^{N-M}$ with high probability.

(A) The first step follows from the observation that $K_2(G)$ can be constructed from G through a peeling procedure. At each step one function node is removed having at least one adjacent variable node of degree one. Inverting this procedure, G can be constructed from $K_2(G)$ by adding at each step a function node involving a degree one variable. Obviously the newly added equation is linearly

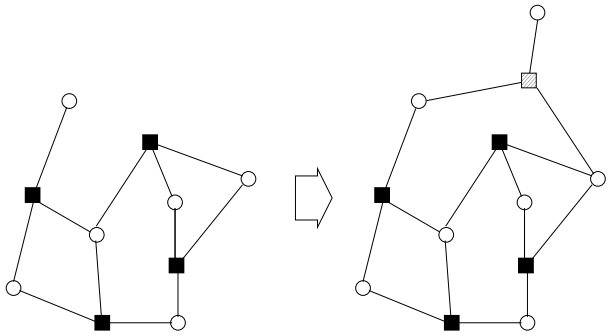


FIG. 17.7. Adding a function nodes involving a variable node of degree one. The corresponding linear equation is independent from the other ones.

{fig:AddLeaf}

independent of the previous ones, implying the thesis. We refer to Fig. **??** for an illustration.

(B) Let n the number of variable nodes and m the number of function nodes in $K_2(G)$ (equivalently, $n = \mathrm{cols}(\mathbb{H}_*)$ and $m = \mathrm{rows}(\mathbb{H}_*)$. The idea is to show that the number of solutions of $\mathbb{H}_*\underline{x} = \underline{0}$ (call it Z_*) is, with high probability 2^{n-m} (i.e. the dimension of the kernel of $\mathbb{H}_*$ is $n-m$). This implies our claim.

According to Theorem **??**, the core is a uniformly random factor graph conditional on its size n and degree profile Λ. The simplest way to prove that $Z_* = 2^{n-m}$ with high probability is to show that

$$\mathbb{E}\{Z_* \mid n, \Lambda\} = 2^{n-m}[1 + o_N(1)]\,. \tag{17.18}$$

In fact, we know that Z_* is *at least* 2^{n-m} and by Markov inequality $\mathbb{P}\{Z_* > 2^{n-m} \mid n, \Lambda\} \le 2^{-n+m}\mathbb{E}\{Z_* \mid n, \Lambda\} - 1$.

The surprise is that such a simple estimate works. In other words, Eq. (**??**) holds true when we take $n = NV(k,\alpha) + o(N)$ and $\Lambda = \widehat{\Lambda} + o(1)$ and any $\alpha < \alpha_{\rm c}(k)$. This should be contrasted with the first moment approach applied directly to the original linar system $\mathbb{H}\underline{x} = \underline{0}$ (instead of $\mathbb{H}_*\underline{x} = \underline{0}$), that fails above some $\alpha_*(k)$ strictly smaller than $\alpha_{\rm c}(k)$, cf. Exercise **??**. Reducing the original graph to its two-core drastically reduced the fluctuations, thus allowing for a sucessful application of the first moment method.

Rather than engaging in a full–blown proof of Eq. (**??**), we shall limit ourselves to compute $\mathbb{E}\{Z_* \mid n, \Lambda\}$ to the leading exponential order, when the core size and degree profile take their typical values $n = NV(k,\alpha)$ and $\Lambda = \widehat{\Lambda}$. We already considered similar computations in Section 11.2. The result takes the typical form

$$\mathbb{E}\{Z_* \mid n, \Lambda\} \doteq \exp\Big\{N \sup_{\omega\in[0,V(k,\alpha)]} \phi(\omega)\Big\}\,. \tag{17.19}$$

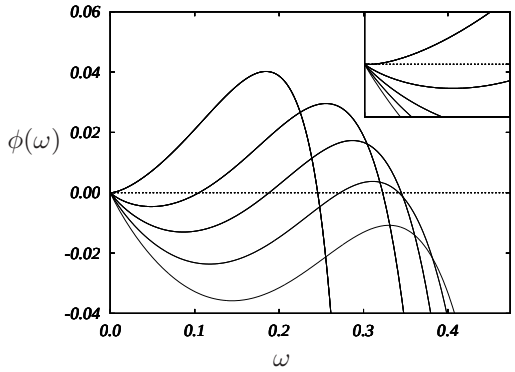


FIG. 17.8. The exponential rate $\phi(\omega)$ of the weight enumerator of the core of a random 3-XORSAT formula. From top to bottom $\alpha = \alpha_{\rm d}(3) \approx 0.818469$, 0.85, 0.88, 0.91, and 0.94 (recall that $\alpha_{\rm c}(3) \approx 0.917935$). In the inset: blow up of the small ω region. {fig:WeCore}

Here $\phi(\omega)$ is the exponential rate for the number of solutions with weight $N\omega$. Adapting Eq. (11.18) to the present case (and using Eqs. (**??**) and (**??**), with the shorthand $\eta = k\alpha\widehat{Q}_*$) we obtain the parametric expression

$$\phi(\omega) = -\omega \log x - \eta(1-e^{-\eta})\log(1+yz) + \qquad (17.20)$$
$$+ \sum_{l\geq 2} e^{-\eta}\frac{\eta^l}{l!}\,\log(1+xy^l) + \frac{\eta}{k}(1-e^{-\eta})\log q_k(z)\,,$$

$$\omega = \sum_{l\geq 2} e^{-\eta}\,\frac{\eta^l}{l!}\,\frac{xy^l}{1+xy^l}\,. \qquad (17.21)$$

where $q_k(z) = [(1+z)^k + (1-z)^k]/2$ and $y = y(x)$, $z = z(x)$ are the solution of

$$z = \frac{\sum_{l\geq 1}\eta^l e^{-\eta}/l!\; xy^{l-1}/(1+xy^l)}{\sum_{l\geq 1}\eta^l e^{-\eta}/l!\; 1/(1+xy^l)}\,, \qquad y = \frac{(1+z)^{k-1}-(1-z)^{k-1}}{(1+z)^{k-1}+(1-z)^{k-1}}\,. \qquad (17.22)$$

If we let $\omega_* = V(k,\alpha)/2$, a straightforward calculation shows that $\phi(\omega_*) = \Sigma(k,\alpha)\log 2$ (hint: in the above notations $V(k,\alpha) = 1-e^{-\eta}-\eta\,e^{-\eta}$ and $C(k,\alpha) = \eta(1-e^{-\eta})/k$). Further ω_* is a local maximum of $\phi(\omega)$. As long as ω_* is a global maximum as well $\mathbb{E}\{Z_*|n,\Lambda\} \doteq \exp\{N\phi(\omega_*)\} \doteq 2^{n-m}$. It turns out, cf. Fig. **??**, that the only other local maximum is at $\omega = 0$ corresponding to $\phi(0) = 0$. As a consequence $\mathbb{E}\{Z_*|n,\Lambda\} \doteq 2^{n-m}$ as long as $\phi(\omega_*) = \Sigma(k,\alpha) > 0$, i.e. for any $\alpha < \alpha_{\rm c}(k)$, thus proving our claim. □

The prediction of the above theorem is compared with numerical simulations in Fig. **??**.

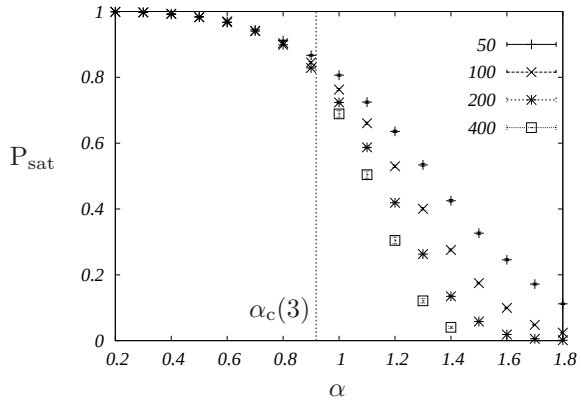


FIG. 17.9. Probability that a random 3-XORSAT formula with N variables and $N\alpha$ equations is SAT, estimated numerically by generating $10^3 \div 10^4$ random instances.

{fig:Xorsat}

17.5 Clusters: geometry of the solution space

{sec:XORClusters}

In the SAT phase $\alpha < \alpha_c(k)$ the number of solution is, with high probability $Z \doteq 2^{N\phi}$, with entropy per variable

$$\phi(\alpha) = 1 - \alpha\,. \tag{17.23}$$

This result does not carry any trace of the sudden appearence of a non-empty two core at $\alpha_d(k)$. Surprisingly this phenomenon translates into a phase transition in the structure of the solution space.

Given an assignment $\underline{x}$, denote by $\pi_*(\underline{x})$ its projection onto the core, i.e. the vector of those entries in $\underline{x}$ that corresponds to vertices in the core. If the graph does not contain a core $\pi_*(\underline{x}) = \emptyset$ for any $\underline{x}$. In the opposite case, if $\underline{x}$ is a solution, then $\underline{x}_* = \pi_*(\underline{x})$ is a solution of the core linear system $\mathbb{H}_*\underline{x}_* = \underline{0}$. The set of solution $\mathcal{S}$ is then naturally partitioned into classes according to their core projection. We shall refer to such classes as **clusters** (the reader interested in a general definition of 'clusters' in constraint satisfaction problems is referred to Chapter **???**). Two solutions $\underline{x}^{(1)}$ and $\underline{x}^{(2)}$ belong to the same cluster if and only if $\pi_*(\underline{x}^{(1)}) = \pi_*(\underline{x}^{(2)})$. If the core of G is empty, we shall adopt the convention that the entire set of solutions forms a unique cluster.

Given a solution $\underline{x}_*$ of the core linear system, we shall denote the corresponding cluster as $\mathcal{S}(\underline{x}_*)$. Clusters have several remarkable properties, that justify their name. We shall start from some simple remarks:

(A) Given a XORSAT formula G, define its **backbone** $B(G)$ as the subgraph of G that is obtained augmenting $K_2(G)$ as follows. Set $B_0(G) = K_2(G)$. For any $t \geq 0$, pick a function node a that is not in $B_t(G)$ and such that at least $k-1$ of its neighborihing variable nodes are in $B_t(G)$, and set $B_{t+1}(G)$ to be the subgraph obtained by adding a (and the new neighborhing variable node) to $B_t(G)$. If no such a function node exists, set $B(G) = B_t(G)$ and halt the

procedure. It is simple to understad that the definition of $B(G)$ does not depend on the order in selecting function nodes.

(B) Any two solutions within the same cluster coincide on the backbone. This follows from the recursive construction above. In fact, if two solutions coincide on $B_t(G)$ they necessarily coincide on $B_{t+1}(G) = B_t(G) \cup \{a, i\}$ because the newly added variable x_i is uniquely determined by the new equation a.

(C) Each cluster $\mathcal{S}(\underline{x}_*)$ is an affine subspace of the Hamming cube $\{0,1\}^N$. More precisely, given $\underline{x} \in \mathcal{S}(\underline{x}_*)$, such a subspace can be written as $\mathcal{S}(\underline{x}_*) = \underline{x} \oplus \mathcal{S}(\underline{0})$. This follows immediately from the the remark that, for any other $\underline{x}' \in \mathcal{S}(\underline{x}_*)$, $\underline{x}' \oplus \underline{x}$ vanishes on the core $K_2(G)$, and therefore (by definition) belongs to the cluster $\mathcal{S}(\underline{0})$.

A precise picture of the clusters structure can be obtained in the case of random formulae. In particular we have the following.

Theorem 17.3 *Consider a random k-XORSAT formula with N variables and $N\alpha$ equations, with $\alpha < \alpha_{\rm c}(k)$ and assume it to be satisfiable. If $\alpha > \alpha_{\rm d}(k)$ then:*

(*i*) *The solution space decomposes into $2^{N\Sigma(k,\alpha)+o(N)}$ clusters with high probability.*

(*ii*) *There exists $\delta(k,\alpha)$ such that two solutions in distinct clusters have Hamming distance larger than $N\delta(k,\alpha)$ with high probability.*

Proof: The first statement is a consequence the definition of cluster and the calculation of the typical number of solutions of the core linear system described in the previous Section.

Statement (ii) follows from the computation of the weight enumerator exponent $\phi(\omega)$, cf. Eq. (11.17) and Fig. **??**. A little calculus shows that for any $\alpha > \alpha_{\rm d}(k)$, $\phi'(0) < 0$, and, as a consequence there exists $\delta(k,\alpha) > 0$ such that $\phi(\omega) < 0$ for $0 < \omega < \delta(k,\alpha)$. This implies that if $\underline{x}_*$, $\underline{x}'_*$ are two distinct solution of the core linear system, then either $d(\underline{x}_*, \underline{x}'_*) = o(N)$ or $d(\underline{x}, \underline{x}') > N\delta(k,\alpha)$. It turns out that the first case can be excluded along the lines of the minimal distance calculation of Section 11.2. Therefore, if $\underline{x}$, $\underline{x}'$ are two solutions belonging to distinct clusters $d(\underline{x}, \underline{x}') \geq d(\pi_*(\underline{x}), \pi_*(\underline{x}')) \geq N\delta(k,\alpha)$. □

This result suggest to regard clusters as 'lumps' of solutions well separated from each other. This picture would be complete if we could show that solutions in each sincle cluster are well connected to each other. For $\alpha < \alpha_{\rm d}(k)$, as we have seen in Sec. **??**, given a solution $\underline{x}$ and a variable index $i \in \{1, \dots, N\}$, with probability $1 - Q_t$ there exists at least one solution $\underline{x}'$ such that $x'_i \neq x_i$ and $\underline{x}'$ differ from $\underline{x}'$ only in a neighborhood of radius t around i. Since $Q_t \to 0$ as $t \to \infty$, this means that most of variables can be flipped by changing a bounded number of other coordinates.

For $\alpha > \alpha_{\rm d}(k)$ the same is true if the variable node i is not in the backbone of G. This suggests that clusters cannot be further splitted into smaller groups of solutions.

It has been suggested that clusters form indeed 'connected components' in the following sense. Given a subset $\mathcal{S} \subseteq \mathcal{S}$ of the set of solutions, a **path** in $\mathcal{S}$

with maximal step size s is a sequence of solutions $\{\underline{x}^{(0)}, \underline{x}^{(1)}, \dots, \underline{x}^{(n)}\}$ such that $\underline{x}^{(t)} \in \mathcal{S}$ for any $0 \le t \le n$, and $d(\underline{x}^{(t)}, \underline{x}^{(t+1)}) \le s$ for any $0 \le t \le n-1$. We say that the set $\mathcal{S}$ is **s-connected** if for any two solutions $\underline{x}$, $\underline{x}' \in \mathcal{S}$ there exists a path joining them (i.e. such that $\underline{x}^{(0)} = \underline{x}$, $\underline{x}^{(n)} = \underline{x}'$, with maximal step size s. The following conjectures have been put forward

(*i*) If $\alpha < \alpha_{\rm d}(k)$, then there exists $s(N) = \Theta(\log N)$ such that the space of solutions is $s(N)$-connected with high probability.

(*ii*) There exists $s(N) = \Theta(\log N)$ such that each cluster is $s(N)$-connected with high probability.

17.6 An alternative approach: the cavity method

{sec:XORCavity}

The analysis of random k-XORSAT in the previous Sections is somewhat unsatisfactory. Our derivation relied heavily on the linear structure of the problem, as well as on the very simple instance distribution. This Section describes an alternative approach that is potentially generalizable to more complex situations. The price to pay is that this second derivation relies on some assumptions on the structure of the solution space. The observation that our final results coincide with the ones obtained in the previous Section give some credibility to these assumptions.

The starting point is the remark that BP correctly computes the marginals of $\mu(\,\cdot\,)$ (the uniform measure over the solution space) for $\alpha < \alpha_{\rm d}(k)$, i.e. as long as the set of solutions forms a single cluster. We want to extend its domain of validity to $\alpha > \alpha_{\rm d}(k)$. If we index by $n \in \{1, \dots, \mathcal{N}\}$ the clusters, the uniform measure $\mu(\,\cdot\,)$ can be decomposed into the convex combination of uniform measures over each single cluster:

$$\mu(\,\cdot\,) = \sum_{n=1}^{\mathcal{N}} w_n \, \mu_n(\,\cdot\,)\,. \tag{17.24}$$

Notice that, in the case under consideration $w_n = 1/\mathcal{N}$ is independent of n and the measures $\mu_n(\,\cdot\,)$ are obtained from each other via a traslation. This will not be true in more general cases, but is not cruciual in the present derivation.

The first crucial assumption is that BP (or the Bethe approximation) provides an accurate 'local' description of each measure $\mu_n(\,\cdot\,)$. We shall express this as our

Assumption 1: For each n, $\mu_n(\,\cdot\,)$ is with high probability a **Bethe measure**.

For a general definition of Bethe measures, we refer to Section **???**. In the present context what we mean is that there exists a set of messages $m^{(n)}_{i\to a} \in \{0, 1, *\}$, depending on the cluster n such that the following is for any finite ℓ. Given a vertex i, denote by $\underline{x}_{i,\ell}$ the restriction of an assignment $\underline{x}$ to the neighborhood of radius ℓ around i, $\mathsf{B}_{i,\ell}$, and by $\mathbb{H}_{i,\ell}$ the restriction of $\mathbb{H}$ to this neighborhood. The matrix $\mathbb{H}_{i,\ell}$ includes all the columns (rows) of $\mathbb{H}$ such that the

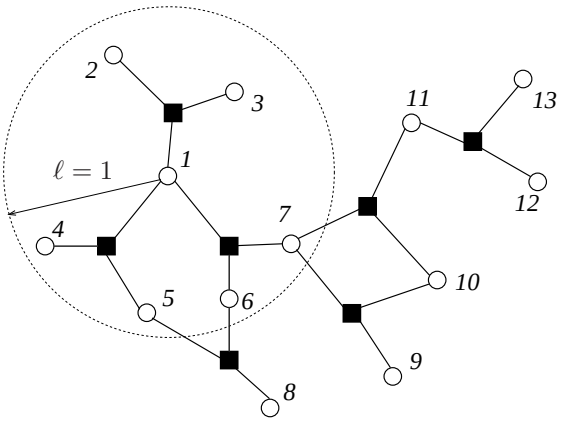


FIG. 17.10. Small 3-XORSAT formula, and the radius 1 neighborhood of node 1: $\mathsf{B}_{1,1}$. Assumption 1 of the cavity method concerns the joint distribution of variables within any such neighborhood. {fig:XorsatBall}

corresponding variable (function) nodes appear in $\mathsf{B}_{i,\ell}$. Notice that the marginal distribution of $\underline{x}_{i,\ell}$ when $\underline{x}$ is distributed according to $\mu_n(\,\cdot\,)$, is supported over the solutions of $\mathbb{H}_{i,\ell}\underline{x}_{i,\ell} = \underline{0}$. It must be true that its distribution is uniform over the solutions of this linear system conditional to $x_j = m_{j\to a}$ for j on the boundary of $\mathsf{B}_{i,\ell}$ (here a is the unique function node adjacent to j in $\mathsf{B}_{i,\ell}$, and $x_j = *$ is interpreted as x_j being free).

Example 17.4 Consider the 3-XORSAT formula whose factor graph is reproduced in Fig. **??**. For $i = 1$ and $\ell = 1$, we have

$$\mathbb{H}_{i,\ell} = \begin{bmatrix} 1\,1\,1\,0\,0\,0\,0 \\ 1\,0\,0\,1\,1\,0\,0 \\ 1\,0\,0\,0\,0\,1\,1 \end{bmatrix} \tag{17.25}$$

Describe the marginal distribution of $(x_1, x_2, \dots, x_7)$ when $\underline{x}$ is a uniformly random solution of this XORSAT formula.

The above definition of a Bethe measure must satisfy an obvious consistency condition. Consider the marginal distribution of $\underline{x}_{i,\ell}$. This can be obtained by marginalizing the distribution of $\underline{x}_{j,\ell+1}$ for any of the variable nodes j at distance
⋆ at most 1 from i. It is easy to show that this consistency condtition is satisfied if the corresponding messages are a fixed point of the BP equations. We recall that, in the present case BP equations read

$$m_{i\to a}^{(n)} = \begin{cases} * & \text{if } \widehat{m}_{b\to i}^{(n)} = * \text{ for all } b \in \partial i\backslash a, \\ \widehat{m}_{b\to i}^{(n)} & \text{otherwise.} \end{cases} \tag{17.26}$$

$$\widehat{m}_{a\to i}^{(n)} = \begin{cases} * & \text{if } \exists j \in \partial a\backslash i \text{ s.t. } \widehat{m}_{j\to a}^{(n)} = *, \\ m_{j_1\to a}^{(n)} \oplus \cdots \oplus m_{j_l\to a}^{(n)} & \text{otherwise.} \end{cases} \tag{17.27}$$

where we denoted $\partial a\backslash i = \{j_1, \dots, j_l\}$. Below we shall denote symbolically these equations as

$$m_{i\to a}^{(n)} = \varphi\{\widehat{m}_{b\to i}^{(n)}\}\,, \qquad \widehat{m}_{a\to i}^{(n)} = \psi\{m_{j\to a}^{(n)}\}\,. \tag{17.28}$$

In principle one would like to identify the set of messages $\{m_{i\to a}^{(n)}\}$ for each cluster. The next step is to give up this ambitious objective and try instead to compute the distribution of $m_{i\to a}^{(n)}$ for any fixed edge $i \to a$, when n is a cluster index drawn with distribution $\{w_n\}$. For instance, in the present case one may want to compute the quantities

$$Q_{i\to a}(m) = \mathbb{P}\left\{m_{i\to a}^{(n)} = m\right\}\,, \qquad \widehat{Q}_{a\to i}(\widehat{m}) = \mathbb{P}\left\{\widehat{m}_{a\to i}^{(n)} = \widehat{m}\right\}\,. \tag{17.29}$$

for $m, \widehat{m} \in \{\mathtt{0}, \mathtt{1}, *\}$. Computing these probabilities is an extremely challenging task. In order to proceed, we make some assumptions on the joint distribution of the messages $m_{i\to a}^{(n)}$ when n is a random cluster index. The simplest idea would be to assume that, for any finite collection of directed edges, the corresponding messages $\{m_{i\to a}^{(n)}, \widehat{m}_{b\to j}^{(n)}\}_{i\to a, b\to j\in\mathcal{C}}$ are asymptotically independent. Of course this is false because of Eqs. (**??**), (**??**). If for instance we take the collection of directed edges $\mathcal{C} = \{i \to a, b \to i, b \in \partial i\backslash a\}$, then Eq. (**??**) gives one of the corresponding messages in terms of the others.

However one may hope that the correlations induced by Eqs. (**??**), (**??**) decrease at large distances. In particular, if we consider the set of messages entering a given variable node i (or function node a) their only correlations are induced through BP equations along the loops to which i (respectively a) belongs. Since in random k-XORSAT formulae such loops have, with high probability, length of order $\log N$, one might think that messages incoming a given node are asymptotically independent.

Unhappily also this assumption is false. The reason is easily understood if we assume that $\widehat{Q}_{a\to i}(\mathtt{0}), \widehat{Q}_{a\to i}(\mathtt{1}) > 0$ for at least two of the function nodes a adjacent to a given variable node i. This implies that, with finite probability one sample a cluster such that $m_{a\to i}^{(n)} = \mathtt{0}$, and $m_{b\to i}^{(n)} = \mathtt{1}$. If however this is the case, there is no consistent prescription for the marginal distribution of x_i under $\mu^{(n)}(\,\cdot\,)$.

Our assumption will be that the next simplest thing happens: messages are indipendent conditional to the fact that they do not dontradict each other. In order to state such an hypothesis, we denote by $\vec{\mathsf{B}}_{i,\ell}$ the set of directed edges originating from vrariable nodes at distance ℓ from i and directed towards i.

Assumption 2: Let $\ell \geq 1$, $i \in G$ a uniformly random node and n be a random cluster index with distribution $\{w_n\}$. Then the messages $\{m^{(n)}_{j\to b}\}_{j\to b\in\vec{\mathsf{B}}_{i,\ell}}$ are asymptotically independent under the condition of being **compatible**.

Here 'compatible' means the following (we refer to Section ??? for a more general definition). Consider the linear system $\mathbb{H}_{i,\ell}\underline{x}_{i,\ell} = \underline{0}$ for the neighborhood of node i. If this admits a solution under the boundary condition $x_j = m_{j\to b}$ for all $j \to b \in \vec{\mathsf{B}}_{i,\ell}$ then the messages $\{m_{j\to b}\}$ are said to be compatible. As above we interpred $x_j = *$ as imposing no condition on x_j.

Given the messages at the boundary of a radius ℓ neighborhood, the BP equations (**??**) and (**??**) allow to determine the messages inside such a neighborhood. Consider in particular two nested neighborhoods $\mathsf{B}_{i,\ell}$ and $\mathsf{B}_{i,\ell+1}$. The inwards messages on the boundary $\vec{\mathsf{B}}_{i,\ell+1}$ of the largest neighborhood completely determines the ones on the boundary $\vec{\mathsf{B}}_{i,\ell}$ of the smallest one. A little thought shows
⋆ that, if the messages on $\vec{\mathsf{B}}_{i,\ell+1}$ are distributed according to Assumption 2, the distribution of the resulting messages on $\vec{\mathsf{B}}_{i,\ell}$ also satisfies the same assumption. Furthermore, the marginal distribution of messages on $\vec{\mathsf{B}}_{i,\ell}$ can be expressed in terms of those on $\vec{\mathsf{B}}_{i,\ell+1}$.

One therefore obtains, for each edge $(i,a) \in G$, the relations

$$Q_{i\to a}(m) = \frac{1}{Z_{i\to a}} \sum_{\{\widehat{m}_b\}} \prod_{b\in\partial i\setminus a} \widehat{Q}_{b\to i}(\widehat{m}_b)\ \mathbb{I}(m = \varphi\{\widehat{m}_b\})\, \mathbb{I}(\{\widehat{m}_b\} \in \mathsf{COMP}) \tag{17.30}$$

$$\widehat{Q}_{a\to i}(\widehat{m}) = \sum_{\{m_j\}} \prod_{j\in\partial a\setminus i} Q_{j\to a}(m_j)\ \mathbb{I}(\widehat{m} = \psi\{m_j\})\,. \tag{17.31}$$

Here $Z_{i\to a}$ is a normalization constant and $\{\widehat{m}_b\} \in \mathsf{COMP}$ only if the messages are compatible (i.e. they do not contain both a 0 and a 1). Since Assumptions 1, 2 above hold only with high probability and asymptotically in the system size, the equalities in (**??**), (**??**) must also be interpreted as approximate. More precisely, these equations are satisfied within some fixed precision ε, with high probability as $N \to \infty$.

Exercise 17.6 Show that Eqs. (**??**), (**??**) can be written explicitely as

$$Q_{i\to a}(0) = \frac{1}{Z_{i\to a}} \left\{ \prod_{b\in\partial i\setminus a} (\widehat{Q}_{b\to i}(0) + \widehat{Q}_{b\to i}(*)) - \prod_{b\in\partial i\setminus a} \widehat{Q}_{b\to i}(*) \right\}, \quad (17.32)$$

$$Q_{i\to a}(1) = \frac{1}{Z_{i\to a}} \left\{ \prod_{b\in\partial i\setminus a} (\widehat{Q}_{b\to i}(1) + \widehat{Q}_{b\to i}(*)) - \prod_{b\in\partial i\setminus a} \widehat{Q}_{b\to i}(*) \right\}, \quad (17.33)$$

$$Q_{i\to a}(*) = \frac{1}{Z_{i\to a}} \prod_{b\in\partial i\setminus a} \widehat{Q}_{b\to i}(*)\,, \quad (17.34)$$

and

$$\widehat{Q}_{a\to i}(0) = \frac{1}{2} \left\{ \prod_{j\in\partial a\setminus i} (Q_{j\to a}(0) + Q_{j\to a}(1)) + \prod_{j\in\partial a\setminus i} (Q_{j\to a}(0) - Q_{j\to a}(1)) \right\}, \quad (17.35)$$

$$\widehat{Q}_{a\to i}(1) = \frac{1}{2} \left\{ \prod_{j\in\partial a\setminus i} (Q_{j\to a}(0) + Q_{j\to a}(1)) - \prod_{j\in\partial a\setminus i} (Q_{j\to a}(0) - Q_{j\to a}(1)) \right\}, \quad (17.36)$$

$$\widehat{Q}_{a\to i}(*) = 1 - \prod_{j\in\partial a\setminus i} (Q_{j\to a}(0) + Q_{j\to a}(1))\,. \quad (17.37)$$

The final step consists in looking for a solution of Eqs. (**??**), (**??**). There are no rigorous results on the existence or number of such solutions. Further, since these equations are only approximate, approximate solutions should be considered as well. In the present case a very simple (and somewhat degenerate) solution can be found that yields the correct predictions for all the quantities of interest. In this solution message distributions take one of two possible forms: either $Q_{i\to a}(0) = Q_{i\to a}(1) = 1/2$ (we shall write $\eta_{i\to a} = 0$) or $Q_{i\to a}(*) = 1$ ($\eta_{i\to a} = *$). Analogous forms hold for $\widehat{Q}_{a\to i}$. A little algebra shows that this is a solution if the η's satisfy

$$\eta_{i\to a} = \begin{cases} * & \text{if } \widehat{\eta}^{(n)}_{b\to i} = * \text{ for all } b\in\partial i\setminus a, \\ 0 & \text{otherwise.} \end{cases} \quad (17.38)$$

$$\widehat{\eta}^{(n)}_{a\to i} = \begin{cases} * & \text{if } \exists j\in\partial a\setminus i \text{ s.t. } \widehat{\eta}^{(n)}_{j\to a} = *, \\ 0 & \text{otherwise.} \end{cases} \quad (17.39)$$

These equations are very similar to the original BP ones (**??**), (**??**) (they indeed coincide with the BP equations if 1 messages are not allowed). This is due to

the particularly simple nature of the problem and will not happen in more advanced applicaions of the method. However the interpretation is now completely different. For some of the edges the corresponding message $m^{(n)}_{i\to a}$ depend on the cluster n and $m^{(n)}_{i\to a} = \mathtt{0}$ (respectively $= \mathtt{1}$) in half of the clusters. For other edges, the message does not depend upon the cluster and $m^{(n)}_{i\to a} = *$ for all n's.

An even more concrete interpretation is obtained if we consider the one bit marginals $\mu^{(n)}(x_i)$ under the single cluster measure. According to Assumption 1 above, we have $\mu^{(n)}(x_i = \mathtt{0}) = \mu^{(n)}(x_i = \mathtt{1}) = 1/2$ if $\widehat{m}^{(n)}_{a\to i} = *$ for all $a \in \partial i$. If on the other hand $\widehat{m}^{(n)}_{a\to i} = \mathtt{0}$ (respectively $= \mathtt{1}$ for at least one $a \in \partial i$), then $\mu^{(n)}(x_i = \mathtt{0}) = 1$ (respectively $\mu^{(n)}(x_i = \mathtt{0}) = 0$).

According to the above solution for the messages distributions, for some of the variable nodes i (those such that $\widehat{\eta}_{a\to i} = *$ for all $a \in \partial i$) we have $\mu^{(n)}(x_i = \mathtt{0}) = \mu^{(n)}(x_i = \mathtt{1}) = 1/2$ for all the clusters n. In other words within each cluster x_i takes both values in the same number of solutions. For the rest of the variable nodes $\mu^{(n)}(x_i = \mathtt{0}) = 1$ in half of the clusters and $\mu^{(n)}(x_i = \mathtt{1}) = 1$ in the other half.

We already studied the solutions of Eqs. (**??**), (**??**) in Section ??. One particular solution amounts to $\eta_{i\to a} = \mathtt{0}$ the edges of the backbone and $\eta_{i\to a} = *$ elsewhere. This corresponds to the fraction of $\eta_{i\to a} = \mathtt{0}$ messages being Q_*, the largest solution of $Q_* = 1 - \exp\{-k\alpha Q_*^{k-1}\}$. Following the interpretation above, this solution reproduces indeed the cluster structure we derived in the previous Sections.

The cavity approach allow to compute the complexity $\Sigma(k,\alpha)$ as well as many other properties of the measure $\mu(\,\cdot\,)$. We refer for such developments to Section ???

{sec:XORTemperature}

17.7 Temperature, energy, and the dynamical transition

There are many extension of the XORSAT problem studied in the previous Sections. One of the most interesting is to consider the associated optimization problem. Given an $N \times M$ binary matrix $\mathbb{H}$ and a vector $\underline{b}$, this requires to maximize the number of satisfied equations in the linear system $\mathbb{H}\underline{x} = \underline{b}$.

We can define the cost (energy) $E(\underline{x})$ of an assignment $\underline{x}$ to be proportional to the number of equations that are not satisfied by $\underline{x}$. Denoting by $w(\underline{z})$ the weight (number of non-zero entries) of a binary vector $\underline{z}$ we have (the factor 2 is introduced for future convenience):

$$E(\underline{x}) = 2w(\mathbb{H}\underline{x} \oplus \underline{b})\,. \tag{17.40}$$

The MAX-XORSAT problem consists in computing $E_{\rm gs} \equiv \min_{\underline{x}} E(\underline{x})$. While deciding whether $E_{\rm gs} = 0$ or $E_{\rm gs} > 0$ amounts to solving the linear system $\mathbb{H}\underline{x} = \underline{b}$ and can therefore be done in polynomial time, the general optimization problem is extremely hard. In fact, unless P=NP, there exists no algorithm that is guarannteed to satisfy a fraction larger than 1/2 of the equations. Saisfying

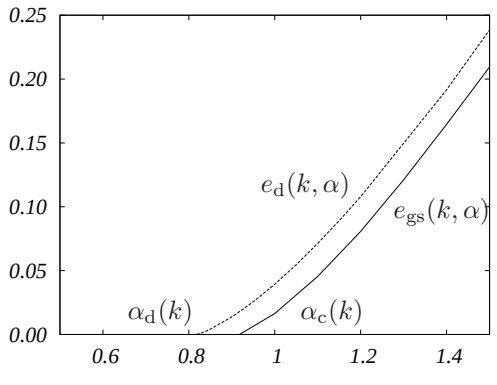


FIG. 17.11. Asymptotyc ground state energy per spin $e_{\rm c}(k,\alpha)$ for random k-XORSAT formulae: here $k = 3$. The dashed line $e_{\rm d}(k,\alpha)$ is the highest energy density e such that configurations with $E(\underline{x}) < Ne$ are clustered. {fig:XORGSFig}

half of the equations is trivial: either the all zeros or the all ones assignment do the job.

Notice that the above cost function can be written as the energy of an Ising spin model with muti-spin interactions. More precisely, if we let $\sigma_i = +1$ $(= -1)$ for $x_i = \mathtt{0}$ $(= \mathtt{1})$ and $J_a = +1$ $(= -1)$ for $b_a = \mathtt{0}$ $(= \mathtt{1})$, we have, with a slight abuse of notation

$$E(\underline{\sigma}) = \sum_{a=1}^{M} (1 - J_a \sigma_{i_a(1)} \cdots \sigma_{i_a(k)}) \,. \tag{17.41}$$

What is the minimal cost $E_{\rm gs}$ for random XORSAT formulae? Using standard concentration arguments, one can show that $E_{\rm gs}$ is closely concentrated around its expectation (more precisely, the probability of a $\Theta(N)$ deviation from the expectation is exponentially small in N). For $\alpha < \alpha_{\rm c}(k)$, the arguments in the previous pages show that $E_{\rm gs} = 0$ with high probability. For $\alpha > \alpha_{\rm c}(k)$ one can prove that $\mathbb{E}E_{\rm gs} = Ne_{\rm gs}(k,\alpha) + o(N)$, with $e_{\rm gs}(k,\alpha) > 0$ increasing with α.

The asymptotic cost per variable $e_{\rm gs}(k,\alpha)$ can be computed using the (non-rigorous) cavity method that has been briefly introduced in the previous Section and will be developed in the next Chapters. Close to the SAT-UNSAT phase transition one obtains

$$e_{\rm gs}(k, \alpha_{\rm c}(k) + \delta) = A(k)\, \delta + O(\delta^2) \,, \tag{17.42}$$

with $A(k) =$???. At large α on the other hand $e_{\rm gs}(k,\alpha) = \alpha - \sqrt{\alpha} e_*(k) + o(\sqrt{\alpha})$. The positive constant $e_*(k)$ is the absolute value of the ground state energy of the fully connected k-spin model studied in Chapter ???. This indicates that there is no interesting intermediate asymptotic regime between the $M = \Theta(N)$ (treated in the present Chapter) and $M = \Theta(N^{k-1})$ (treated in Chapter ???). A sketch of the function $e_{\rm gs}(k,\alpha)$ is shown in Fig. 17.4

The next interesting question concerns the structure of optimal or 'quasi-optimal' assignments $\underline{x}$. In the previous Sections we have seen that the set of zero energy assignments (i.e. solutions of $\mathbb{H}\underline{x} = \underline{b}$) may split into 'clusters', with the minimal Hamming distance between solutions in distinct clusters being $\Theta(N)$. In other words (clusters of) minima of the energy function $E(\underline{x})$ are well separated. A natural question is whether thy are shallow or deep and separated by high 'barriers'. It turns out that the second scenario holds for $\alpha_{\rm d}(k) < \alpha < \alpha_{\rm c}(k)$. To formalize this statement, one can define the **energy barrier** between two solutions $\underline{x}$, $\underline{x}'$ in two equivalent ways. In the first one, the barrier is the minimum over all paths[61] γ in the space of assignments joining $\underline{x}$ and $\underline{x}'$, of the maximum energy along γ. According to the second one has to take the maximum over all subsets of assignments $\Omega \subseteq \{0,1\}^N$ such that $\underline{x} \in \Omega$, $\underline{x}' \notin \Omega$ of the minimum energy over the boundary[62] $\partial\Omega$ of Ω. In formulae

$$\Delta(\underline{x},\underline{x}') = \min_{\gamma:\underline{x}\to\underline{x}'} \max_{\underline{z}\in\gamma} E(\underline{z}) \tag{17.43}$$

$$= \max_{\Omega} \min_{\underline{z}\in\partial\Omega} E(\underline{z})\,. \tag{17.44}$$

It can be proved that, if $\underline{x}$ and $\underline{x}'$ are two solutions belonging to distinct clusters, then $\Delta(\underline{x},\underline{x}') = \Theta(N)$ with high probability. On the other hand it is expected that for most solution pairs belonging to the same cluster $\Delta(\underline{x},\underline{x}') = O(1)$.

A similar picture is conjectured to hold for $\alpha > \alpha_{\rm c}(k)$. In this case with high probability there are no zero energy assignments. In order to construct clusters one has to define 'quasi optimal' assignments as follows. Fix a number $\varepsilon > 0$. An assignment $\underline{x}$ is ε quasi-optimal if $E(\underline{x}) < E_{\rm max} \equiv E_{\rm gs} + N\varepsilon$. One expects that, for any $\alpha > \alpha_{\rm c}(k)$, there exists $\varepsilon_* > 0$ such that for any $0 < \varepsilon < \varepsilon_*$ the set of ε quasi-optimal assignments is split in 'clusters'. In particular, for most of couples of assignments $\underline{x}$, $\underline{x}'$ in the same cluster $\Delta(\underline{x},\underline{x}') - E_{\rm max} \le O(1)$, while, for assignments in different clusters $\Delta(\underline{x},\underline{x}') - E_{\rm max} = \Theta(N)$

One last possible extension consists in introducing the Boltzmann distribution with energy function $E(\underline{x})$:

$$\mu_\beta(\underline{x}) = \frac{1}{Z(\beta)}\, e^{-\beta E(\underline{x})} = \frac{1}{Z(\beta)} \prod_{a=1}^{M} \psi_a(\underline{x}_{\partial a})\,. \tag{17.45}$$

As stressed here, this takes the form of a graphical model with the same factor graph G as the original XORSAT formula. The compatibility function $\psi_a(\underline{x}_{\partial a})$ takes value 1 if the a-th equation in the linear system $\mathbb{H}\underline{x} = \underline{0}$, and $e^{-2\beta}$ otherwise.

The 'clustering' and SAT-UNSAT critical points $\alpha_{\rm d}(k)$ and $\alpha_{\rm c}(k)$ get promoted to lines $\alpha_{\rm d}(\beta;k)$, $\alpha_{\rm c}(\beta;k)$, cf. Fig. **??** for an illustration. Thanks to the

[61] A path is a sequence of assignments $\underline{x}^{(0)}, \cdots, \underline{x}^{(n)}$ such that, for any $t \in \{0,\dots,n-1\}$, $\underline{x}^{(t)}$ and $\underline{x}^{(t+1)}$ differ in at most one position.

[62] The boundary of Ω is defined as the seto of assignments that are not in Ω, but differ from an assignment in Ω in one coordinate.

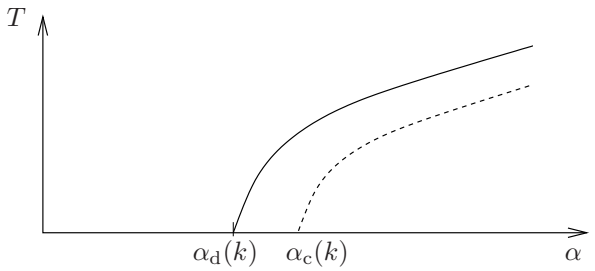


FIG. 17.12. Schematic phase diagram of the finite-temperature XORSAT model (**??**). Here $T = 1/\beta$ is the temperature and the continuous (dashed) lines correspond to the dynamical (static) phase transitions.

{fig:SketchTgamma}

introduction of a finite temperature, one can introduce a simple Markov dynamics that has $\mu_\beta(\,\cdot\,)$ as stationary (and reversible) measure. The simplest example is Glauber dynamics introduced in Section ???. For $\beta < \infty$, the simplest and more concrete characterization of the phase transition at $\alpha_{\rm d}(k;\beta)$ is in terms of such a dynamics: as α crosses $\alpha_{\rm d}(k;\beta)$ the relaxation slows down dramatically.

More precisely, one considers the stationary dynamics defined by drawing $\underline{x}(0)$ according to the equilibrium measure $\mu_\beta(\,\cdot\,)$ and monitor relaxation through correlation functions of local observables such as $C(t) = \mathbb{E}\langle x_i(0); x_i(t)\rangle$. A relaxation time scale can be defined as

$$\tau(\varepsilon) = \inf\{\, t :\ C(t) \le \varepsilon \,\} \tag{17.46}$$

where ε is a given small number. Then it is expected that $\tau(\varepsilon) = O(1)$ for $\alpha < \alpha_{\rm d}(\beta;k)$ while $\tau(\varepsilon) = \exp\{\Theta(N)\}$ for $\alpha > \alpha_{\rm d}(\beta;k)$.

Notes