SISSA  ISAS

Scuola Internazionale Superiore di Studi Avanzati
International School for Advanced Studies

# Statistical mechanics of spin systems on diluted random structures

Thesis submitted for the degree of
*Doctor Philosophiæ*

**Candidate:**
Michele Leone

**Supervisors:**
Prof. Amos Maritan
Prof. Riccardo Zecchina

September 2002

# Contents

# Introduction

## Random combinatorial problems and diluted spin systems

During the last two decades, in spite of many pioneering fundamental contributions ([1] and references therein), the main stream of analytical results in the field of statistical mechanics of spin-glasses and disordered systems focused mainly on mean-field models of large degree[1]([2, 3, 4, 5, 6] and references therein).

In the more recent years, a major effort has been devoted to the study of models that could retain, at least in a statistical way, some features of finite dimensionality, like finite degrees and presence of geometrical constraints influencing both the static and the dynamical properties of the systems. Spin glass models over diluted random graphs constitute by now the natural framework for the most advanced analytical studies concerning the glass transition in disordered systems.

The interest in diluted spin system is by far not limited to physics. As we shall discuss in great detail in this thesis, there exists a huge class of open root problems in theoretical computer science and in discrete mathematics which have a simple representation as diluted spin system.

From the point of view of pure physics, the study of diluted systems represents only a first step towards the treatment of finite dimensionality or geometrically structured models, and one could think for instance to even more complex or "semi-random" structures where some regularity reminiscent of a real lattice geometry is progressively introduced into the random adjacency matrix. But even if one limits the investigation to purely random diluted graphs and to classical spin models defined on them, the questions that arise are still of a deep kind both from a fundamental and from an application oriented point of view.

Why are this models interesting? The main reasons can be summarized in the following:

- From a fundamental point of view: they are still essentially mean field, however they retain finite interaction degrees that is reminiscent of finite dimensional cases. The presence of large scale structures like large loops has to be taken into consideration as a first step in the understanding the role of topology and geometry for the collective behavior of complex systems.

- Moreover, they are widely accepted as prototype models in the study of fundamental phenomena in the theory of Computational Complexity.

- From an applicative (but not less important) point of view: they have a natural wide range of applications to a class of systems that span over the following fields

[1] In the following we will call degree what usually physicists call connectivity, i.e. the number of neighbors of a vertex of the lattice or graph the model is defined on. We chose The first term in order to be consistent with mathematical and graph theory literature.

- Statistical analysis of the behavior of realistic neural networks ([2, 6, 27, 28] and references therein)
- Combinatorial optimization problems ([27, 29, 30, 31, 32, 34, 35, 36, 37, 117] and references therein)
- Error correcting codes and cryptography ([27, 38, 39] and references therein)
- Models of statistical information processing and image restoration ([27] and references therein)
- Statistical models of collective phenomena in biology (for instance. gene and protein regulatory networks, networks of cellular signalling pathways etc.) ([40, 41] and references therein)
- Statistical analysis and optimal design in complex artificial networks such as the Internet or the World Wide Web ([43, 44, 45, 46] and references therein)

In what follows we are going to deal both with basic theoretical aspects and with some specific applications belonging to computer science (combinatorial optimization, error correcting codes and cryptography). We are going to study the low temperature equilibrium and out-of-equilibrium phases of diluted spin-glasses with the aim of elucidating the geometrical structure of ground states underlying static and dynamic transitions. The computational counterpart of such a study arises from the elementary observation that (hard) combinatorial optimization problems can be easily reformulated as problems of finding ground states in spin-glass-like Hamiltonians. In this sense the idea of studying their topological structure is quite a natural one [2]. The recent efforts in developing a mathematical and physical understanding of such systems over diluted structures have opened new perspectives and new roads to solutions to those problems, tackling them in their natural *milieu*. The models reviewed and studied in this thesis are all of random nature. While this is usually the most natural thing to do in physics, the study of random combinatorial problems has been revealing itself useful also in computer science where it allows to broaden to the typical-case the classical worst-case notions of computational complexity [34].

This thesis is devoted to the analytical study of the dynamic and static transitions numerically observed in this whole class of models, with specific focus on combinatorial optimization problems and error correcting codes, once mapped on specific diluted spin systems. Stress is posed on the connection between the slowing down processes in algorithms behavior and statistical phase transitions due to some intrinsic property on the spin model, that can usually be tracked down to the emergence of non trivial frustrated topological structures in the underlying graph. The recent achievements [29, 30, 56] of a promising new class of algorithms that seems to outperform the other state-of-the-art search procedures for typically hard combinatorial problems are based on theoretical understanding rooted in the concepts reviewed in this work. This result, among others, seems to show how statistical physics of disordered systems has still a lot to teach us when applied to the field of computational complexity.

The thesis will be organized in the following way: in the **first chapter** some general guiding concepts of random graphs and modern statistical physics of disordered systems will be presented, and the connection with relevant problems in theoretical computer science will be stressed. In **chapter two** we will introduce in detail the mathematical techniques used to deal with the analytic computation of relevant physical quantities for a wide class of spin models defined over diluted random structures, such as random graphs or random graphs with arbitrary degree distribution (results for Erdös-Renyi graphs will follow as a special case). The

complete calculations will be shown in the case of a generalization of the $p$-spin model over such structures. Their validity can be seen to hold for a much wider family of random combinatorial optimization problem belonging to the NP class in the worst case, such as $K$-SAT, $Q$-coloring[57, 58] and many others. Some applications to specific *prototype* examples will be shown in the **third chapter**, while **chapter four** will deal with specific examples of two combinatorial optimization problems, namely the 3-SAT and the bicoloring problem of graphs of uniform rank 3[2]. **Chapter five** will be devoted to two relevant examples of the relation between the algorithmic computational complexity of a problem and the presence (and nature) of dynamic and static phase transitions in the associated spin model. In the first example the mapping will essentially be between the search for solutions of large random sparse linear system over finite fields[3] and the search of the zero temperature ground states of some *ad hoc* defined multiple rank interaction diluted ferromagnet. In the second part essentially the same mapping will be used to study the dynamic slowing down of parity check algorithms for error correcting codes - with the consequent onset of computational complexity - and the correspondent dynamic phase transition in spin glasses.

The mathematical language used throughout this work will be that of replica theory: we are well aware that this is a very controversial field, due to the lankness of clear and rigorous foundations that makes its mathematical interpretation obscure and its results "unreasonably successful"[42]. And this even after more than 20 years after the original formulation of the theory [59]. In the necessary attempt to overcome this problem a calculation in **chapter six** is presented with the aim of showing how replica theory can be at least interpreted as a systematic variational method also in the case on diluted models. The treatment will be a generalization of the method recently proposed by Guerra [60] for fully connected models. Moreover, very recent work [23, 24, 30] has clarified the equivalence between the cavity method and the replica results also in the diluted systems case. Since the first one deals with usual probabilistic objects, it has a clearer and more direct interpretation that could lend itself to further rigorous studies. Some directions for future work are summarized in the conclusions.

The calculations and the results presented in this thesis are the output of a three years collaboration with the I.C.T.P. condensed matter and statistical physics group in the names of Riccardo Zecchina, Silvio Franz, Alfredo Braunstein and Federico Ricci-Tersenghi (now in Rome). Great part of the work was also the output of a collaboration with Andrea Montanari (École Normale, Paris). This work would not have been possible without them, and I wish to thank them deeply.

[2]the definition of graph and of rank will be given at the beginning of chapter 1.

[3]See the definition in the chapter.

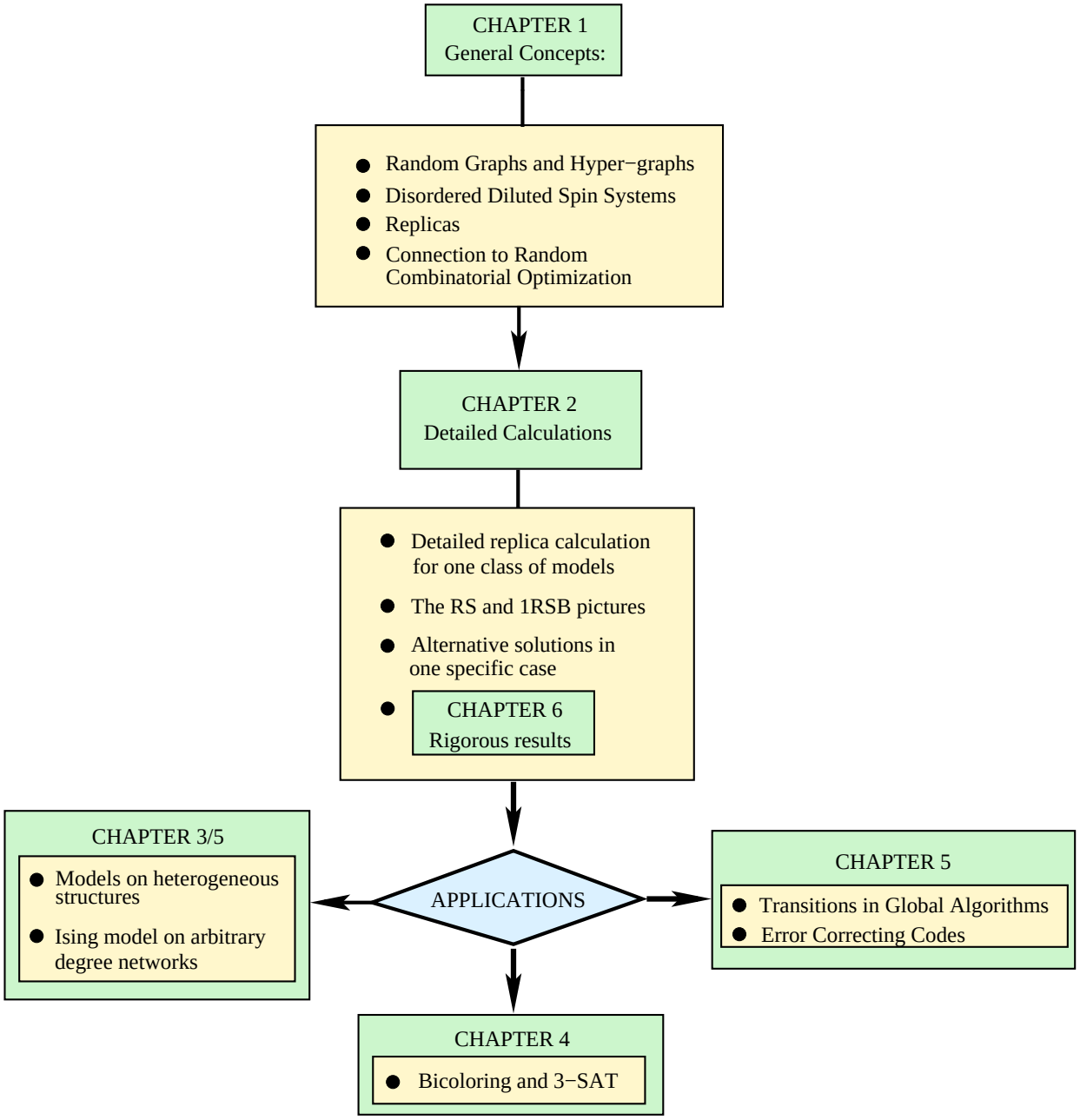



Figure 1: Skeleton of the chapters content.

# Chapter 1

# General techniques for diluted random models

## 1.1 Graphs and Hyper-graphs: preliminary definitions

During the whole length of this thesis we are going to deal with spin models defined on diluted random structures such as simple random graphs or hyper-graphs [61, 62, 63]. A graph $\mathcal{G}$ is commonly defined as a non-empty finite set $V(\mathcal{G})$ of elementary units called **vertices** or **nodes** or **sites** in our common notation, and a finite set $E(\mathcal{G})$ of distinct unordered pairs of distinct nodes called **edges** or **links** . We call $V(\mathcal{G})$ the vertex set and $E(\mathcal{G})$ the edge set of $\mathcal{G}$. In our notation the $i^{th}$ site will be denoted by its Latin index $i$ and an edge between sites $i$ and $j$ will be denoted as the couple $ij$. We will work with undirected edges (graphs). We will define the size or order of the graph as the cardinality of the vertex set or the number $N$ of sites, we will call $M$ the the cardinality of the edge set. A complete graph is a graph whose edge set is made of all possible links between nodes. In that case one has $M = N(N-1)/2 \sim \mathcal{O}(N^2)$. Many interesting models can be defined on a generalization of graph structures that go under the name of hyper-graphs. Let $X = \{x_1, ...., x_N\}$ be a finite set., and let $\mathcal{E} = \{E_i | i \in I\}$ be a family of subsets of $X$. $\mathcal{E}$ is said to be a hyper-graph on $X$ if $E_i \neq \emptyset \ \forall \ i \in I$ and $\bigcup_{i \in I} E_i = X$. The structure $\mathcal{H} = (X, \mathcal{E})$ is called hyper-graph. Again, $|X| = N$ is the order of the hyper-graph. It is easy ro see how a graph is simply a particular case of hyper-graph with $\mathcal{E}$ restricted to subsets of exactly two elements. $\mathcal{E}$ will be the generalized edge set (or hyper-edge set) of $\mathcal{H}$. Is it possible to draw a hyper-graph in many equivalent ways. One possibility is shown in figure (1.1), where edges are shown as multiple vertices plaquettes. This may not be the orthodox way to represent a general hyper-graph, but is reminiscent of the usual way to represent multi-spin or plaquette interaction in lattice field theory or statistical mechanics, so we will adopt it in the following. In the future chapters we will occasionally need the concept of *incidence matrix* as the matrix $\hat{A} = ((a_i^j))$ with $M$ rows that represent the edges of $\mathcal{H}$ and $N$ columns representing its vertices, such that:

$$\begin{aligned} a_i^j &= 1 \quad if \quad x_j \in E_i \\ a_i^j &= 0 \quad if \quad x_j \notin E_i \end{aligned}$$

In a hyper-graph $\mathcal{H}$, the *rank* $r(S)$ of a set $S \subset X$ is defined as

$$r(S) = max_i |S \cap E_i| \tag{1.1}$$

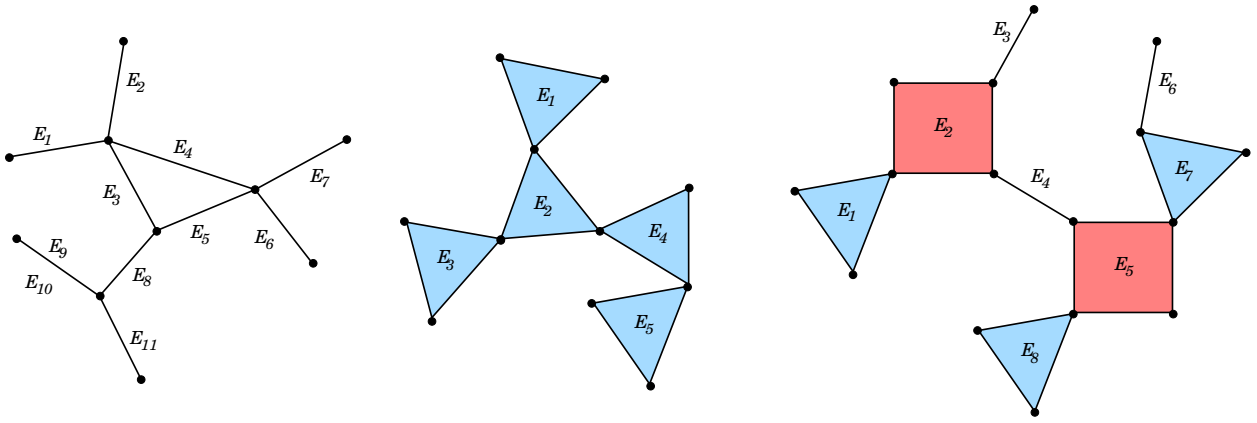



Figure 1.1: Trivial examples of a simple graph, two hyper-graphs of fixed rank 3 and an hyper-graph of rank 4 and minimal rank 2. also rank 2 edges are expressed in hyper-graph notation. All these example have $N$ very small compared with the structures we will be interested in, so they are only to be intended, along with others in the text, as a pictorial guide.

The rank of the hype-graph is therefore

$$r(X) = max_i |X \cap E_i| \tag{1.2}$$

If $r(X) = E_i \ \forall \ i$, then the hyper-graph is said to be of uniform rank. A simple graph will then be a hype-graph of uniform rank 2.

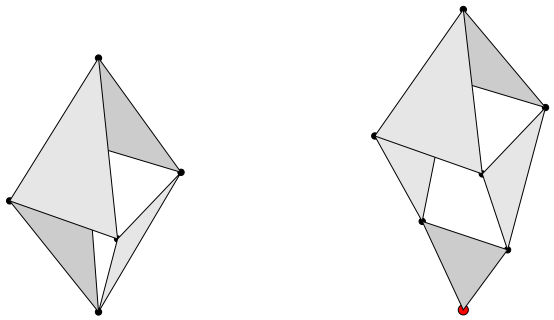
To each hyper-graph $\mathcal{H} = (X, E_1, ..., E_M)$ there corresponds a *dual* hyper-graph $\mathcal{H}^* = (E, X_1, ..., X_N)$ whose vertices are points $e_1, ..., e_M$ representing $E_1, ..., E_M$ and whose edges are sets $X_1, ..., X_N$ representing $x_1, ..., x_N$ where $\forall j$,

$$X_j = \{e_i | i \leq M \ \ , \ \ E_i \ni x_j\} \tag{1.3}$$

When dealing with the graphical interpretation of error correcting codes, we will switch to a representation of hyper-graphs in terms of *factor graphs* [64, 65, 66] (see also the appendix for a graphical example), more familiar to computer scientists, and where duality is made evident and explicitly exploited. Any hyper-graph can be read as a bipartite graph where one subset is $X$ and the other $E$, and where there is a edge pointing from $x_i$ to $e_l$ if the correspondent element of the incidence matrix of the original hyper-graph is non-zero. Such particular bipartite graph is called factor graph. Given a hyper-graph $\mathcal{H}$, a *chain of length* $q$ is defined [63] as a sequence $(x_1, E_1, x_2, E_2, ...., E_q, x_{q+1})$ s.t.

- $x_1, ...., x_q$ are distinct vertices
- $E_1, ...., E_q$ are distinct edges
- $x_k, x_{k+1} \in E_k \ \forall \ k = 1, ..., q$

In the physics jargon, chains are nothing but **connected components** of the hyper-graph $\mathcal{H}$. If $q > 1$ and $x_{q+1} = x_1$, then the chain is called a *cycle of length* $q$. A cycle in a graph of uniform



rank 2 is nothing but a **loop**. In the physics of disordered and frustrated systems a particular role turn out to play those cycles where every vertex belongs to an even number of edges. We will call those cycles "*compact cycles*" , "*hyper-cycles*" or "*hyper-loops*", for the similarity with the graphs case where loops always have this property. Two examples of very particular cycles (the first is also a compact cycle) are shown in fig. (1.1) for the case of a hyper-graph of uniform rank 3 (see also [19] for the first application to hyper-loops concepts to spin glasses, to my knowledge). A hyper-graph is the said to be **random** [62, 69, 68] whenever the presence or absence of each of its edges is given with a defined arbitrary probability. Traditionally, random graphs were introduced as those where the probability of having an edge between two given vertices is a constant $r$[1]:

$$\forall\ i,j\ Prob(ij \in E(\mathcal{G})) = r \tag{1.4}$$

If $r \propto \mathcal{O}(1)$ then the graph is said to be **dense** as well as its incidence matrix. If $r \propto \mathcal{O}(1/N)$ then the graph will be **thin** or **diluted** and its incidence matrix will be a sparse one. In this last case $M \propto N$. This will be the case we'll considered it the rest of the thesis. Complete hyper-graphs of finite rank $l$ have $C_l^N \propto N^{l-1}$ edges [2]. Therefore, in order to have a number of edges proportional to $N$ every plaquette containing $l$, vertices must have a probability to be present proportional to $1/N^{(l-1)}$. If each edge is present with the same fixed probability, properly rescaled with $N$, the hyper-graph will be diluted and each vertex $i$ will have a finite degree $k_i$ drawn from a poissonian probability degree distribution

$$c_k = e^{-\gamma}\frac{\gamma^k}{k!} \tag{1.5}$$

where $\gamma$ is a free parameter determining mean value and variance of the distribution. A particular "self similar" form is peculiar of the poissonian distribution: In this case the probability $c_k$ of finding a vertex of degree $k$ is equal to the probability $q_k$ of finding a nearest neighbor vertex with degree $k+1$, as can be seen applying eq. (1.5) to the definition [69]

$$q_k \equiv \frac{(k+1)c_{k+1}}{\sum_k kc_k} = \frac{(k+1)c_{k+1}}{< k >}. \tag{1.6}$$

This note is very important in practical calculations and is the origin of major simplifications in the replica and the cavity equations [23, 24] we will see later on. This is reflected by the fact

[1] A very rich phenomenology of structures appearing in the graph as a function of the degree and a complete study of graphs behavior as $r$ increases with $N$ has been performed on a rigorous mathematica basis staring from the seminal paper of Ërdos and Rényi [61]. For a systematic introduction see for instance [62] and [67] and references therein. To my knowledge no comparable systematic study has been undertaken in the case of rank $> 2$ hyper-graphs yet. For a clear introduction to hyper-graphs see [68].

[2] $C_l^N \equiv N!/((N-l)!l!)$ in the following.

that in the poissonian case the mean value uniquely determines the variance and vice-versa. As a consequence, a lot of simplifications and particular behaviors of poissonian hyper-graphs cannot be applied in wider families of random structures. However, it is possible to constrain the probability of the value of the number of edges incident on a fixed vertex in order to draw diluted hyper-graphs from ensembles with arbitrary degree distributions (arbitrary $c_k$). The constraints will be of global nature and will not introduce vertex-vertex correlations, as it will be seen in the following. Since the replica as well as the cavity equation for spin models defined over diluted hyper-graphs will be concerned in the computation of the local effective fields acting on each spin variable *in absence* of a particular edge incident to the vertex under consideration, The natural ensemble we are going to work with will indeed be that of the $q_k$ and not that of the $c_k$. We stress again that this change is immaterial in the poissonian case, where one falls back into the same ensemble, but not in the general one. Moreover, one could of course think to more complex or "semi-random" structures where some regularity reminiscent of a real lattice geometry is progressively introduced into the random matrix through the presence of correlations of various kind (see [41] for *one* among possible examples) or through the presence of regular sub-hyper-graphs merged in the whole one in a random way. But even if one limits the investigation to purely random diluted hyper-graphs and to simple classical spin models defined on them, the questions that arise are still of a deep kind both from a fundamental and from an application oriented point of view. Nevertheless, the immediate future directions for investigations will necessarily have to deal with the presence of such correlations [72, 46, 70, 71, 73], as well as with models where the interaction constraints are non local in nature [74] or non purely classical.

## 1.2 Spin models on diluted structures

In all cases, we are going to work with models that can be described, under appropriate mapping, via some spin Hamiltonian $H(\mathbf{J}, \mathbf{s})$, where $\{\mathbf{J}\}$ represents an ensemble of disordered interaction energy variables taking non zero values on the edges of the hyper-graph or defined as combinations of more elementary interaction terms as in the case of the $K$-SAT. $\mathbf{s}$) are $N$ $\pm 1$ spin variables (0 or 1 Boolean variables in the usual combinatorial problems encoding) living on the vertices of the hyper-graph. We will deal in the following with cases where the Hamiltonian can be written as a sum of *local energetic contributions* $\epsilon_\mu$ as

$$H(\mathbf{J}, \mathbf{s}) = \sum_\mu \epsilon_\mu(\{\mathbf{J}_\mu\}, \{\mathbf{s}^\mu\}) \ , \tag{1.7}$$

where $\mu$ indicates each subset (usually an edge of the underlying hyper-graph or a *clause* in SAT -like formulation) that contains a *small number* of both constraints and spin variables, relative to the total number $N$ of variables[3] . As a title of example, the simplest possible Hamiltonian is the Viana-Bray (see the original article by Viana and Bray in [1]):

$$H(\mathbf{J}, \mathbf{s}) = -\sum_{i<j} J_{ij} s_i s_j \ \ . \tag{1.8}$$

The diluted hyper-graphs that define the underlying topological structure will be drawn from the appropriate chosen statistical ensemble, fully determining the probability distribution $P(k)$

[3] $\mu$ is usually calle "clause index" in SAT-like formulations, but it can be extended in general to other spin systems.

of edge degrees and the probability distribution $Q(l)$ of ranks. The rank on each single hyper-graph edge is equal in the cases under consideration to the number of spin variables in the local energetic term $\epsilon_\mu$. Therefore the distribution $Q(l)$ is going to be strictly related to the fraction of $l$-variables interaction terms Hamiltonians summing up to the total $H(\mathbf{J},\mathbf{s})$[4].

### 1.2.1 Disorder

Once the set $\{\mathbf{J}\}$ of non zero couplings (equivalent to the set of present edges) is set, its elements can take values according to an a priori arbitrary distribution $\mu(\mathbf{J})$. For disordered pure ferromagnetic-type models $\mu(\mathbf{J})$ will read

$$\mu(\mathbf{J}) = \delta(\mathbf{J} - \hat{\mathbf{1}}) \; . \tag{1.9}$$

For disordered pure anti-ferromagnets

$$\mu(\mathbf{J}) = \delta(\mathbf{J} + \hat{\mathbf{1}}) \; . \tag{1.10}$$

Finally, for the pure generalized $\pm 1$ spin-glass case[5]:

$$\mu(\mathbf{J}) = \frac{1}{2}\Big(\delta(\mathbf{J} - \hat{\mathbf{1}}) + \delta(\mathbf{J} + \hat{\mathbf{1}})\Big) \tag{1.11}$$

More in general, the same models can be studied for other forms of the coupling distribution $\mu(\mathbf{J})$: continuous, mixtures of a continuous and a delta peaked part, mixtures of pure ferromagnetic and spin-glass terms, and so on. In chapter 5 we will work with models that are originally defined as a mixture of the previous ferromagnetic and spin-glass one

$$\mu(\mathbf{J}) = \frac{1}{2}\Big(p\delta(\mathbf{J} - \hat{\mathbf{1}}) + (1-p)\delta(\mathbf{J} + \hat{\mathbf{1}})\Big) \tag{1.12}$$

where $p$ is a parameter tuning the amount of "average frustration" or "average glassiness" present into the system. Finally, the rigorous results presented in chapter 6 will be derived for general forms of symmetric $\mu(\mathbf{J})$.

### 1.2.2 Frustration

It was observed right at the beginning of spin-glass theory by Toulouse [2, 75] that a mixture of ferromagnetic and anti-ferromagnetic couplings can give rise to conflicting constraints, such that it is in general impossible to minimize locally all the energy terms $\epsilon_\mu$. This property is widely known as *frustration*. In spin glass-models on diluted structures (Viana-Bray), this typically happens when the density of the graph allows particular compact structures such as loops to percolate in the system. In the case of higher rank hyper-graphs, loops percolation turns out not to be a sufficient condition for the existence of an extensive fraction of frustrated constraints, essentially because the extra degrees of freedom due to the possibility of adjusting the spin variables belonging to the edges but not to the loop. In fact, even more compact structures such as hyper-loops must percolate in the underlying matrix. The phenomenon is exemplified in fig. (1.2). The common presence of disorder and frustration allows for a phase

[4] In fact the two fractions will coincide in the generalized $p$-spin model.

[5] Historically the spin-glass models have been defined only in the case of two body interactions, as a physically sensible model for real magnetic materials. However, a generalized multi-spin interaction family of spin-glass type models can be justified not only for their use in random combinatorial optimization, but as an effective model for many bodies systems of local (often conflicting) constraints, where collective phenomena naturally emerge.

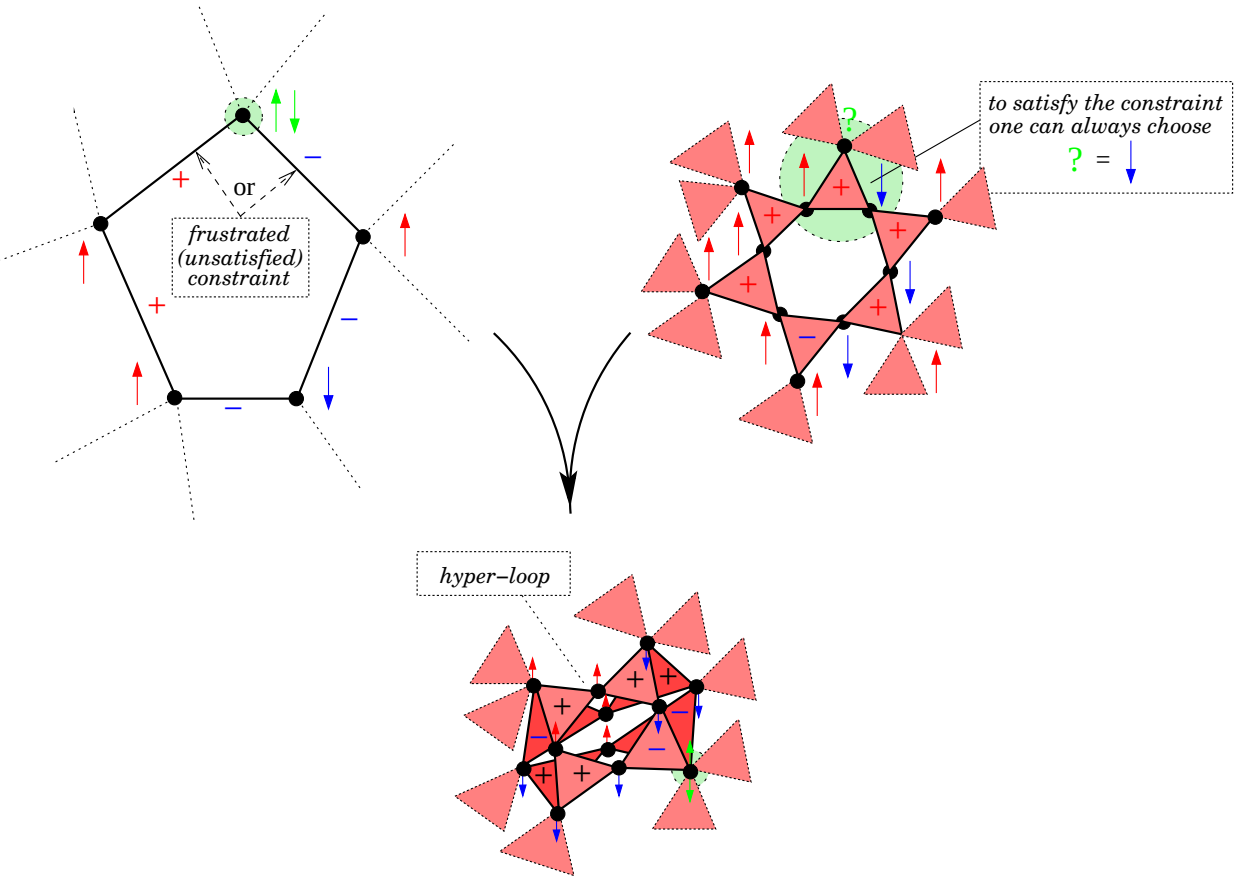



Figure 1.2: Frustration in graphs and hyper-graphs. This Picture is very similar to the one we will draw in chapter 2 for the core resolution under the action of the Leaf Removal algorithm (see section 2.7 for details). It is important to keep in mind this similarity, because it will be the main cause of the effectiveness of the algorithm in locating the spin-glass transition in the $p$-spin model.

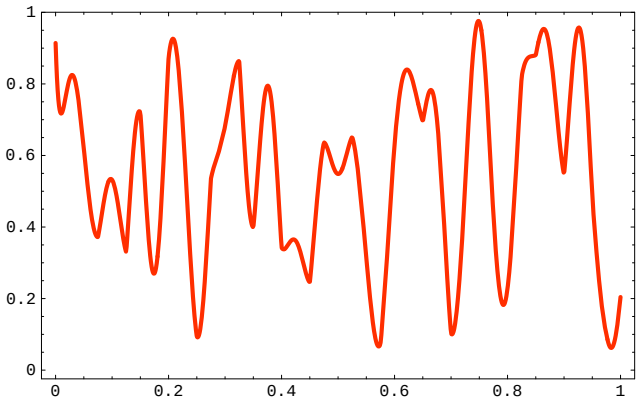



Figure 1.3: Pictorial one dimensional projection of rough energy landscape.

space structure with a large - typically exponential - number of degenerate global ground states as well as definite energy metastable states. Pictorially, one could think that these systems show an energy landscape of the kind exemplified in fig. (1.3). This picture is however often very misleading because the $x$-axis in the picture is in fact a projection of the high dimensional phase space, where all the topological structure is hidden. The degree and nature of the inner structure of the phase space can vary in principle from problem to problem. A better understanding of this topology in the case of some models interesting in random combinatorial optimization, coding theory and more in general disordered systems physics, is the main aim of the present work.

We would like to mention that the families of models studied in the following chapters is *by no means* exhaustive. For instance, a natural generalization of the techniques explained is currently been applied to Potts-like models [76] and could be adapted in principle to Classical Heisenberg models and so on. However, in these last cases, the technical calculations are more involved [57, 58] because, as it turns out, one is forced to work with *functional order parameters* which can be written as distributions of effective local fields of vectorial instead of scalar nature, as it is the case of the examples treated in the present work. This leads to self consistent equations for the order parameters that are inter-wined in the various field components [58][6]. The body of the chapter will deal with the analytical replica techniques devised to compute thermodynamical quantities of physical systems on diluted hyper-graphs in absence of correlations and in presence of quenched disorder. Let us now explicit the connection between this class of models and combinatorial optimization theory.

[6]The coloring degree static threshold obviously depend on the number of colors available for the coloring, at fixed graph. The currently best rigorous upper bound for the 3-COL/UNCOL transition (three colors) in poissonian degree distributed random graphs is 5.06[77]. It was obtained using a refined first moment method, equivalent to an improved annealed approximation in statistical physics. The RS 5.1 threshold obtained in [57] exceeds the rigorous bound, while at the 1RSB level the authors of [58] were able to find a dynamical threshold for an average degree equal to 4.42, followed by the 3-COL/UNCOL transition at 4.69. The values are conjectured to be exact by the authors, and are indeed in very good agreement with numerical simulations [78]. The general discussion on the meaning of the dynamical threshold is done in chapter 2. Notice also that the calculations of chapter 6 will be in principle extendible to the coloring problem, so we could claim 4.69 to be at least the best upper bound to date.

### 1.2.3 Combinatorial optimization problems as spin models

Classical complexity theory [34], as arising from Cook's theorem of 1971 [47], deals with the issue of classifying combinatorial optimization problems according to the computational cost required for their solution. The hard problems are grouped in a class named NP, where NP stands for 'non-deterministic polynomial time'. These problems are such that a potential solution can be checked rapidly whereas finding one solution may require an exponential time in the worst case. In turn, the hardest problems in NP belong to a sub-class called NP-complete which is at the root of computational complexity. The completeness property refers to the fact that if an efficient algorithm for solving just one of these problems could be found, then one would have an efficient algorithm for solving all problems in NP. By now, a huge number of NP-complete problems have been identified [34], and the lack of an efficient algorithm corroborates the widespread conjecture that NP$\neq$P, i.e. that no such algorithm exists.

Complexity theory is based on a worst-case analysis and therefore does not depend on the properties of the particular instances of the problems under consideration. In practice algorithms display a huge variability of running times, ranging from linear to exponential, and therefore a theory for their most probable behavior represents the natural complement to the worst-case scenario.

The most common problems encountered in computer science and issue of theoretical analysis studies within computational complexity theory are of a type. A decision-making problem is often formulated as that of the maximization or minimization of a multi-variable function, an optimization problem[7]. The function to be minimized (maximized) is called *objective function* or *cost function*, and basically counts the number of violated constraints , given a particular configurational assignments to the variables on the problem. An example of combinatorial optimization problem familiar to physicists is that of finding the ground state of an Ising model. More in general, any search of ground states in any spin model on a given geometrical or topological structure can be seen as particular optimization problem. On the other hand, a large class of purely combinatorial optimization problems in principle not related to physics can be seen equivalent to the search for zero temperature ground states of *ad hoc* constructed spin models (often spin-glasses) on particular topological structures. Among others we can count the number partitioning problem, the graph partitioning, the graph and hyper-graph coloring, the knapsack problem, the scheduling problem and the satisfiability (SAT) one. A clear overview of some of these examples can be seen in [27] and an introduction to the study statistical mechanics study of random combinatorial optimization problems seen as spin systems can be found in [35]. In particular, SAT has been extensively studied due to its NP-completeness and general nature. Its mapping on a particular spin-glass model has been elucidated in [9]. As well as in many of its variations, the SAT cost function can be read as the collection of $M$ logical constraints that have to be satisfied by $N$ boolean variables. It turns out [9] that any SAT formula cost function can be written as the Hamiltonian of a spin model where $0-1$ variables are replaced by $\pm 1$ spins, and the constraints are well determined collections of edges or plaquettes of various rank of a given hyper-graph that completely characterizes the formula under study. If $M \sim \mathcal{O}(N)$, which is the case the most interesting formulas belongs to - i.e. those close to the satisfiability threshold - then the underlying hyper-graph is a diluted one. In order to study the SAT problem in its spin-glass formulation it is therefore necessary to develop a general formalism to be able to deal with topological structures such as diluted hyper-graphs.

[7] We will not here review in detail the complexity theory of optimization problems, that can be found for example in [34], together with the definition of $P$ and $NP$ complexity classes as well as more general ones

In the following this will be explicitly done for the case of the general diluted $p$-spin like models, but it will be then further generalized in order to tackle problems like the $K$-SAT one. Whenever the constraints forming the formula to be satisfied are drawn randomly from a previously defined ensemble, then the optimization problem will have a random nature. Instead of working on a particular hyper-graph, this will amount to averaging over the chosen ensemble of "quenched" structures. It will be then interesting to discern which properties (one for all the inner complexity of the problem) survive in shifting the search for solution from a particular to a random case. The following chapters will almost all be devoted to the application of the general analytical techniques developed here to various optimization problems, some of them used as toy models, as in chapter 3, some others of more complex analysis, as in the remaining chapters.

### 1.2.4 Quenched disorder averages and general computational strategies

Evaluation of a physical quantity using a spin Hamiltonian of the type (1.8) or any more complicated case considered in this work starts from the trace over the spin variables for a given fixed (*quenched*) set of couplings. For us, this corresponds to randomly choosing a diluted hyper-graph from a desired ensemble and a fixed form of the $\mu(\mathbf{J})$. The free-energy of the system

$$F[\mathbf{J}] = -\frac{1}{\beta}\log Tr_{\mathbf{s}}\left(e^{-\beta H(\mathbf{J},\mathbf{s})}\right) \tag{1.13}$$

can be harmlessly averaged over the quenched disorder in the thermodynamic limit, if the self-averaging condition over extensive thermodynamical quantities (like indeed the free-energy) is satisfied as we assume to be true throughout the whose treatment. This averaging procedure goes under the name of *configurational average* :

$$\langle F\rangle \equiv \int \mathcal{D}\mu(\mathbf{J})F[\mathbf{J}] \tag{1.14}$$

However, the dependence of the partition function on $\mathbf{J}$ is in general very complicated and it is not easy to calculate expression (1.14) directly. Moreover, in the case of real world optimization problems, the thermodynamic limit condition does not always hold, and more subtle single sample analysis also in the typical case have to be taken into consideration [30].

### 1.2.5 Replicas

The calculations are carried out via a "subtle trick": it much easier to compute

$$\langle \log Z\rangle = \lim_{n\to 0}\frac{Z^n-1}{n} \tag{1.15}$$

The last equation is an identity for continuous $n$, but the trick consists in calculating first $Z^n$ for integer $n$, taking the 0 limit is a second time. The replicated partition function, after averaging over *the same disorder realization* becomes a partition function of $n$ systems, *without disorder*, but with an *effective* attractive interaction between the various replicas. The reason for this attraction is intuitively quite simple [79]: because they share the same Hamiltonian and the same disorder, the various replicas will be attracted towards the same favorable regions of the phase space and repelled from the unfavorable ones. If one has a simple phase space,

with basically a single large deepest valley, then the replicas will all fall in that, and the order parameter will be a number $q$ which will measure the average distance between replicas within this single valley. But in a systems with several metastable states, the situation can be more complicated, with some replicas trapped in a valley and some in another. This effect is called replica symmetry breaking (RSB). Technically it appears as a standard spontaneous breaking of a symmetry, the permutation symmetry $S_n$ of the $n$ replicas. The problem is that this symmetry is broken only when one considers some number of replicas which is non-integer and in fact smaller than one. Even though this point has been elegantly solved by Parisi [2], the validity of taking the $n \to 0$ limit still lacks a general rigorous justification ([60], [59] and references therein). The last chapter will try to deal with this problem in an indirect way. We will not show (unfortunately) that the physical quantities defined on the $n \to 0$ vector spaces are well defined mathematical objects, but at least that, on the class of systems we are interested in, the effective replica Hamiltonian can lead to rigorous variational results. In the case of fully connected models, the replica mean field theory can be stated in terms of a single scalar $n \times n$ matrix, whose elements are the overlaps chosen via a determinate scheme and that play the role of order parameters. In the case of diluted systems, however, it emerges the need for the determination of a full distribution of multi-spin overlaps [1, 9] that can be completely characterized via the introduction of a class of functional order parameters [8, 9, 12]

$$\rho(\vec{\sigma})$$

that essentially enumerate the fraction of replicated spins in a particular replica state, as it will become clear in the course of the calculations[8]. These functional order parameters have still a mean field nature and will be expressed in terms of series of multi-spin overlap functions averaged over the mean local fields distributions seen by an average vertex in a particular state.

The free-energy of the system can be written as a function of $\rho(\vec{\sigma})$, and will therefore be a functional of the local fields probability distributions, averaged over all possible states of the system. In the $N \to \infty$ limit[9], the dominant contribution to the partition function is found extremizing the free energy with respect to the functional order parameter

One is left with a set of self consistent integral equations for the effective fields probability distributions, that can be solved analytically or numerically (depending on the cases). In some special cases, namely on the $T = 0$ line for some classes of models, these equations further simplify due to the collapsing of the functional form of the probability distributions into series of weighted delta functions. When this happens, one is left with a set of algebraic equations in the weights that often admit analytic solutions in a closed form. This is particularly interesting in the field of combinatorial optimization, thanks to the existing general mapping procedure between the solutions of the random combinatorial problem and the zero temperature ground states of the associated spin model. Moreover, the assignments of the problem variables with a given (typically low) number of violated constraints correspond to metastable local ground states with positive energy. The logarithm of the number $\mathcal{N}(e)$ of such metastable states is a function of the their energy density $e = E/N$ and is known as *Configurational Entropy* or *Complexity*[7] $\Sigma$:

$$\Sigma(e) = \frac{1}{N} \log[\mathcal{N}(e)] \tag{1.16}$$

[8] There are at least two ways to define the order parameter, depending on whether one focuses on the whole graphs or on some part of it. See appendices C, C.1 and C.2 for some details.

[9] $N$ is the number of variables in the system.

Therefore, the measure of the extensivity of the Complexity will be an important indirect way to study the hardness of the random combinatorial problem depending on the position in the phase space of the associated pin model, and will stress the deep connection between the theory of the glassy transitions in disordered systems and the concepts of computational complexity in theoretical computer science.

As we just said, the ingredients of frustration and/or disorder typically induce the onset of transitions from a uniform *paramagnetic* to one or more kind of *glassy* phases in the control parameters[10] space of the model.

### 1.2.6 Cavity

The same solutions and the same physical insights can be reached via the cavity method. Cavity was invented in 1986 for the solution of the SK model [2], but was recently reformulated in the diluted systems framework [23] and related to an algorithmic understanding of the process in the case of its direct zero temperature formulation in [24, 30, 29]. The basic idea of the method applied to spin models on diluted hyper-graphs is the following:

- Assume that, like in the replica method, due to the local tree-like structure of the hyper-graph and the mean field nature of the model, spin variables become uncorrelated at large distances if the system is in a single state. The influence of the graph on a single spin can be therefore easily written in terms of uncorrelated local effective fields acting on it.

- Starting with a system of $N$ variables, add now a variable $S_0$ of degree $k$ (on average one will add a fraction of spins $c_k$) and connect it to the rest of the hyper-graph in order to complete $k$ clauses of function nodes of the $N$ vertices graphs with variables $\{S_a^1, ..., S_a^k\}_a$, where $a$ is the *rank* index, i.e. it indexes all the variables other than $S_0$ belonging to a given clause (or energy constraint, as equivalently indicated throughout this thesis).

- Assume that $\{S_a^1, ..., S_a^k\}_a$ where previously disconnected with probability one in the thermodynamic limit (no short loops) and therefore uncorrelated:

$$P^{(N)}(\{S_a^1, ..., S_a^k\}_a) \simeq P_1^{(N)}(\{S_a^1\}_a)...P_k^{(N)}(\{S_a^k\}_a) \simeq \prod_a P_{1,a}^{(N)}(S_a^1)...P_{k,a}^{(N)}(S_a^k) \qquad (1.17)$$

  Then it is possible to compute the new $P^{(N+1)}(S_0; \{S_1^a, ..., S_k^a\}_a)$ via Bayes theorem as:

$$P^{(N+1)}(S_0; \{S_a^1, ..., S_a^k\}_a) \simeq \prod_{\mu=1}^{k} P_\mu^{(N)}(\{S_a^\mu\}_a) e^{-\beta\epsilon_\mu^{(0)}(S_0, \{S_a^\mu\}_a)} \simeq \prod_{\mu=1}^{k} \prod_a P_{\mu,a}^{(N)}(S_a^\mu) e^{-\beta\epsilon_\mu^{(0)}(S_0, \{S_a^\mu\}_a)} \qquad (1.18)$$

  where $\epsilon_\mu^{(0)}(S_0, \{S_a^\mu\}_a)$ is the local energy constraint $\epsilon_\mu$ of eq. (1.7) where the dependence on the $\mu$-th clause spin variables has been made explicit, as well as the reference spin index 0. Integrating over the variables $\{S_a^1, ..., S_a^k\}_a$ one finally obtains:

$$P^{(N+1)}(S_0) \simeq \prod_{\mu=1}^{k} \prod_a \sum_{S_a^\mu = \pm 1} P_{\mu,a}^{(N)}(S_a^\mu) e^{-\beta\epsilon_\mu^{(0)}(S_0, \{S_a^\mu\}_a)} \; . \qquad (1.19)$$

[10] We recall that the relevant control parameters are in these models the temperature $T$, the graph dilution $\gamma$ or $\alpha$ (depending on the notation in the literature) and in some cases some form of external magnetic field, as it will be the case in the section dedicated to error correcting codes.

This last equation defines an iterative method to calculate $P_0^{(N+1)}(S_0)$ from $\{P_{\mu,a}^{(N)}(S_a^\mu)\}_{\mu,a}$. Thanks to the first assumption, the equations for $P_j^{(N)}(S_j)$ and $P^{(N+1)}(S_0)$ can be easily written as

$$\begin{aligned} P_j^{(N)}(S_j) &= \frac{e^{\beta h_j S_j}}{2\cosh(\beta h_j)} \\ P_0^{(N+1)}(S_0) &= \frac{e^{\beta h_0 S_0}}{2\cosh(\beta h_0)} \end{aligned} \tag{1.20}$$

Writing self consistent equations for the cavity fields is then possible inserting (1.20) in (1.19) and iterating. In the typical case, one can then average over all spins, getting an expression for the distribution $P(h)$ weighted over the degree and rank distribution of the typical hyper-graphs.

In fact, this assumption is globally valid only if the system is in a single pure state. In many states $\alpha = 1, ..., \mathcal{N}_{states}$ are present, the previous equations are valid within a given state $\alpha$, i.e. a cluster of solution separated by other clusters. Equations (1.20) will then be state dependent and the self consistent condition (1.19) will have to be averaged both over the sites $i$ *and* over the states $\alpha$. This picture corresponds to the one step replica symmetry breaking one and is frequent in disordered spin systems. The cavity method formulated in this way works essentially by induction and assumes no non trivial correlations within clusters or inside the same cluster that could origin from the geometry of the graph, even though trivial correlations of a hierarchical nature can be taken into account[11]. The disregarding of correlations is common with the replica approach, as it should be if we claim the two to be equivalent, and it is a limitation of the theory that will have to be overcome in the near future if one wants to be able to systematically attack problems with more complex geometrical structure.

During the cavity iteration process, one is bound to make a small error of order $1/N$, since the ensemble of random graphs one is working with changes slightly under the $N \to N+1$ cavity iterations. This error can be healed via a clever balancing of vertices and edges additions and erasures. More in detail:

- A hyper-graph $\mathcal{H}_{N,M}$ with $N$ vertices and $M$ edges is drawn from the desired ensemble.
- A *cavity* is carved in it, where $q$ vertices are left with degree equal to minus one their initial one, through a proper erasure of surrounding vertices and edges. $q$ is chosen as a function of the degree of the erased vertices and the rank of the erased edges[12].
- Local cavity magnetic fields $h_i^\alpha$ acting on the cavity spins $S_i$ are supposed to follow an initially unknown probability distribution $P_i(h_i^\alpha)$, in principle different from site to site and with field values dependent on the state $\alpha$ of the system.
- Under the addition of a new cavity spin $S_j$ of degree $k_j$ connected with some of the previous cavity sites through given number of hyper-edges of suitably chosen ranks, the probability distributions of the new cavity fields are calculated in a self consistent iterative way. The

[11] Trivial correlations are taken in principle into account via further clusterization steps the same "clusters within clusters" hierarchy implied by the RSB Parisi's construction.

[12] For example for a hyper-graph of fixed rank $l$ and fixed degree $k$, $q$ will have value $l(l-1)k$ or integer multiples.

iteration is built in order to self consistently stabilize the cavity fields distributions once the original hyper-graph is retrieved[13].

- The procedure is repeated adding and deleting edges and vertices in a balanced way, in order to retrieve the hyper-graph belonging to the desired starting ensemble.
- Energy shifts are calculated under the iteration, allowing to calculate the free energy, the energy density and other physical quantities (for example the complexity) in the thermodynamic limit.
- Averages over the hyper-graphs ensemble and the model couplings are performed.

If applied to single spins, the cavity method is mean field in nature. In order to possibly effectively extend it to finite dimensional models or with lattices with some non trivial geometry one would need to consider the influence on the iteration of more complex groups of variables. This has been partially done with the cluster variation method (CVM) for ferromagnetic models, but the extension in presence of frustration is still an open issue.

### 1.2.7 Phase space structure

two possible scenarios have been encountered in the models studied:

- A **Replica Symmetric phase (RS)**: generically, the distance on the lattice between two spins is large, at least of the order of random loops forming in the topology, i.e. of the order $\mathcal{O}(\log N)$. It is therefore reasonable to assume that the spins remain uncorrelated. In the cavity language this means that the *Global Ground State* (GGS) energy of a graph with a reference cavity of $q$ spins carved in it can be written as an additive function of the values of the cavity spins $S_{i=1,\dots,q}$, weighted by the local fields $h_{i=1,\dots,q}$ acting on them. When considering the ensemble of random cavity graphs, the local fields turn out to be i.i.d. random variables, and their distribution is denoted with $P(h)$. The local field will therefore not fluctuate from state to state because of the presence on only one GGS $a$, and the distribution $P(h)$ will be an average over all sites. In the replica formalism, the same $P(h)$ will be the one determining the multi-spin overlaps contained in the functional order parameter $\rho(\vec{\sigma})$.
- A **One Step Replica Symmetry Broken phase (1RSB)**: The phase space splits in an exponential number of metastable *Local Ground States* (LGS), defined as states in which the energy cannot be lowered by flipping a finite number of spins. In presence of several ground states, the assumption is that there is a one-to-one correspondence among the LGS before and after the addition of spins or edges (at least for the LGS with low energies). Equivalently we assume that the perturbation due to the change of the value of a cavity spin propagates (in the limit $N$ going to infinity) only to an infinitesimal fraction of the lattice. Therefore it is possible to write an iteration procedure for the whole population of LGS with given energy. However it may well be that the order of the LGS energies change during the graph operations, and the GGS after iteration is not the same LGS as the one before. The problem is to take into account these *level crossings*, which is not done in the RS solution and turns out to be automatically done in the RSB

[13]Notice that an essentially equivalent procedure will be followed in chapter 5 to prove the variational nature of the replica method.

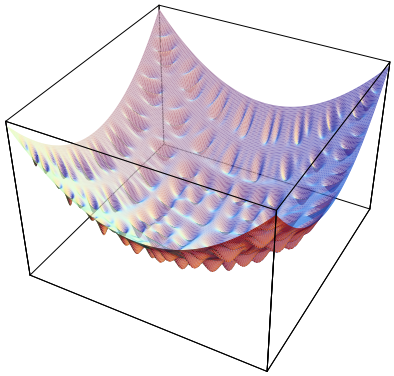


Figure 1.4: Pictorial view of the energy landscape in the phase space of a system in the 1RSB phase. The energy is on the vertical axis. cutting the picture at definite values of the energy one finds clusters of solutions increasing in number and dimension.

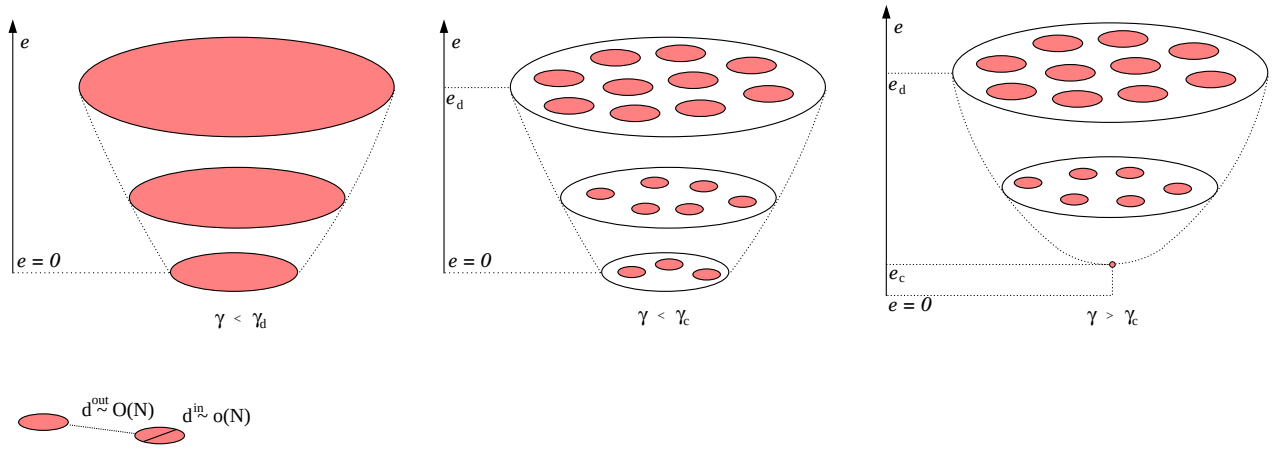



Figure 1.5: 1RSB clustering in phase space.

solutions via the replica formalism. One is then forced to follow a large population of the LGS of lowest energy, large enough so that one can be sure to obtain the GGS when iterating.

In fig. (1.4) we show a pictorial view of the energy clusters in the 1RSB phase. Typical fixed energy slices of this picture show how, increasing the energy, different clusters are selected. This is shown is fig. (1.5). This qualitative picture as been extensively studied for $p > 2$-spin and $K > 2$-SAT models in recent years [11, 21, 53], mainly with variational techniques. This is the intuitive idea we'll have in mind in the rest of this work. In some lucky cases - and indeed the $p$-spin model will be one of them - this picture will turn out to have an exact interpretation. In some others, as for instance the random 3-SAT, no rigorous proof is present. However this picture is highly probable to be correct and what is more important it turned out to be extremely useful in the development of a new class of algorithm of potential vast use. Indeed very recently [30, 29] exact solutions of the $p$-spin model and the $K$-SAT at zero temperature in a certain range of the phase space parameters have been achieved under this assumption on the form of the energy levels distribution.

There are of course models for which this picture is not complete: non trivial correlations arise among LGS, leading to further steps of replica symmetry breaking. This is for example

the case of the Viana-Bray model on diluted graphs [23, 24]. In this models typically slow decaying long range correlations are present. However, from a computational point of view the Viana-Bray models turns out to be easy in the phase space regions of interest. Indeed, it is also due to the presence of this long range correlations that Viana-Bray like models turn out to be computationally simple, because the solution space will in general be connected by paths allowing the reaching of any phase space point with a clever but sub-extensive sequence of local adjustments.

The main calculation steps reviewed in the last paragraphs are then the ones indicated in schema (1.6), where the connection to the field of combinatorial optimization is made evident.

Finally, some differences between the replica and the cavity methods are listed in the following:

- While replicas force the introduction of an order parameter that has already undergone average over the quenched disorder, the cavity equations can also be written on a single sample (hyper-graph). This makes the cavity approach more apt to be applied to specific real world problems.

- The cavity approach deals with well defined mathematical quantities and is manifestly variational, while the well definiteness of the replica method (namely in the RSB case) is still unclear.

- On the other hand, the replica method is much more elegant and compact (especially at finite temperature), it does not require further postulates and assumptions on the energy level distribution, that in principle depend on the model considered, and its equations can be handled in full generality.

We will develop the replica method, occasionally taking advantage of physical insights coming from the cavity picture. A throughout treatment on the state of the art of the cavity approach to diluted models and combinatorial optimization problems can be found in [23, 24, 30].

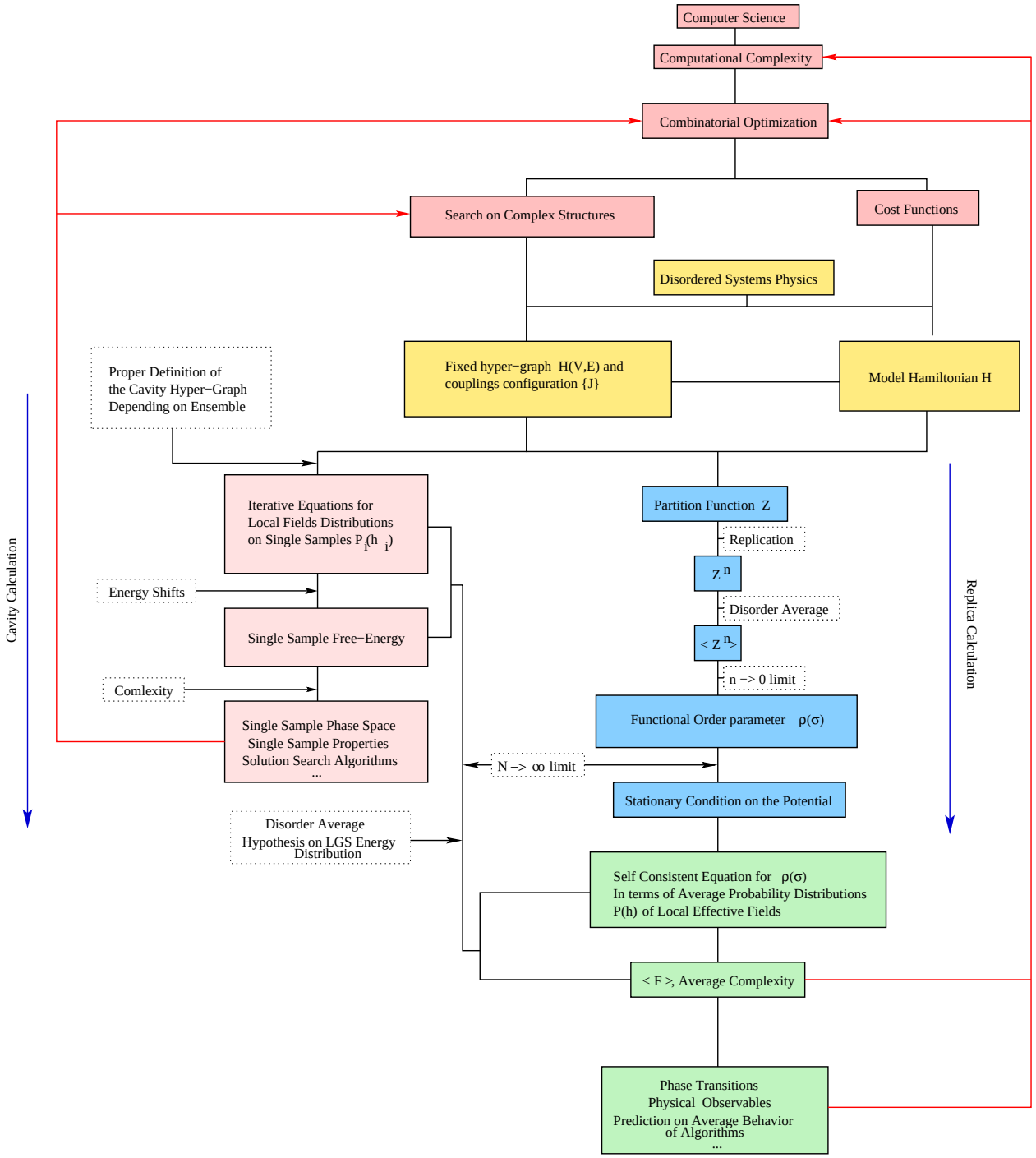



Figure 1.6: General calculation strategy via replica and cavity methods and connection to optimization theory.

# Chapter 2

# The generalized diluted $p$-spin model

We are now going to develop in details the analytical replica techniques previously described. In doing so we will choose a specific class of models of general importance, namely a generalization of the $p$-spin model on uncorrelated random hyper-graphs with arbitrary degree and rank distribution.

If we define $c_k$ as the fraction of spin variables with degree $k$ and $v_l$ the fraction of interactions of rank $l$, the resulting mixed hyper-graph structure will be characterized by the following distributions:

$$Q(\hat{l}) = \sum_l v_l \delta(\hat{l} - l) \tag{2.1}$$

$$P(\hat{k}) = \sum_k c_k \delta(\hat{k} - k) \tag{2.2}$$

$$< l > = \sum_l l v_l \tag{2.3}$$

$$< k > = \sum_l k c_k \tag{2.4}$$

We notice that we could introduce two generating functions

$$v(x) = \sum_l v_l x^l \tag{2.5}$$

$$c(x) = \sum_k c_k x^k \tag{2.6}$$

$$\tag{2.7}$$

where (2.6) is the same of [69], but the (2.5) generalizes it to more complex structures such as the mixed rank hyper-graphs we work with. The generating function formalism is not strictly necessary, but can be very helpful when one is interested in computing more complex topological properties of the hyper-graph and indeed will be explicitly used in some cases. In the generalized $p$-spin model the Hamiltonian therefore reads

$$H = M - \sum_l H_l \tag{2.8}$$

$$H_l = \sum_{i_1 < ... < i_l} J_{i_1,...,i_l} s_{i_1}, ..., s_{i_l} \tag{2.9}$$

with

$$M = \frac{< k >}{< l >} N \tag{2.10}$$

and

$$P(\{J_{i_1,\ldots,i_l}\}_l) = \prod_l \prod_{i_1<\ldots<i_l} ((1-\frac{l!\gamma_l}{N^{l-1}})\delta(J_{i_1,\ldots,i_l}) + \frac{l!\gamma_l}{N^{l-1}}\delta(J_{i_1,\ldots,i_l}-1)) \quad (2.11)$$

$$P(\{J_{i_1,\ldots,i_l}\}_l) = \prod_l \prod_{i_1<\ldots<i_l} ((1-\frac{l!\gamma_l}{N^{l-1}})\delta(J_{i_1,\ldots,i_l}) + \frac{l!\gamma_l}{2N^{l-1}}(\delta(J_{i_1,\ldots,i_l}-1)+\delta(J_{i_1,\ldots,i_l}+1)) \quad (2.12)$$

respectively for the ferromagnetic and for the frustrated case, and $\gamma_l = (< k > / < l >)v_l$.

## 2.1 Combinatorial optimization interpretation of $p$-spin models: the XOR-SAT

We notice that these Hamiltonians can be also seen as the cost function of a class a combinatorial optimization problems known under the name of XOR-SAT ([19, 21, 82], also extended in [25]). The XOR-SAT problem is not $NP$, but it is nevertheless a very useful prototype treatable optimization problem in order to test the power of statistical physics tools. Beside this, its diluted $p$-spin version bears many interesting properties from the point of view of structural glasses and granular physics [79, 20, 15, 80, 81], so its study is interesting for a transversal number of disciplines. We show the case of the $K$-XOR-SAT model with $K$ variables per constraint, which can be viewed as a perfectly balanced version of the random $K$-SAT problem[1]. Given a set of $N$ Boolean variables $\{x_i = 0, 1\}_{i=1,\ldots,N}$, we construct an instance of $K$-XOR-SAT as follows: given original $K$-SAT clauses $(\bar{x}_{i_1} \vee \bar{x}_{i_2} \vee \bar{x}_{i_k})$ or $(x_{i_1} \vee x_{i_2} \vee x_{i_k})$, every sub-clause contained in one of them must appear directed *and* negated in the corresponding $K$-XOR-SAT constraint an even number of times. In the $K = 2$ case we'll therefore define the following elementary constraints (2-clauses sets with 50% satisfying assignments)

$$\begin{aligned} C(ij|+1) &= (x_i \vee \bar{x}_j) \wedge (\bar{x}_i \vee x_j) \\ C(ij|-1) &= (x_i \vee x_j) \wedge (\bar{x}_i \vee \bar{x}_j) \ , \end{aligned} \quad (2.13)$$

In the $K = 3$ case we'll have constraints (4-clauses sets with 50% satisfying assignments)

$$\begin{aligned} C(ijk|+1) &= (x_i \vee x_j \vee x_k) \wedge (x_i \vee \bar{x}_j \vee \bar{x}_k) \\ &\wedge (\bar{x}_i \vee x_j \vee \bar{x}_k) \wedge (\bar{x}_i \vee \bar{x}_j \vee x_k) \\ C(ijk|-1) &= (\bar{x}_i \vee \bar{x}_j \vee \bar{x}_k) \wedge (\bar{x}_i \vee x_j \vee x_k) \\ &\wedge (x_i \vee \bar{x}_j \vee x_k) \wedge (x_i \vee x_j \vee \bar{x}_k) \ , \end{aligned} \quad (2.14)$$

in the $K = 4$ case we'll have 8-clauses of type

$$\begin{aligned} C(ijkl|+1) &= (\bar{x}_i \vee \bar{x}_j \vee \bar{x}_k \vee x_l) \wedge (\bar{x}_i \vee \bar{x}_j \vee x_k \vee \bar{x}_l) \\ &\wedge (\bar{x}_i \vee x_j \vee \bar{x}_k \vee \bar{x}_l) \wedge (\bar{x}_i \vee x_j \vee x_k \vee x_l) \\ &\wedge (x_i \vee x_j \vee x_k \vee \bar{x}_l) \wedge (x_i \vee x_j \vee \bar{x}_k \vee x_l) \\ &\wedge (x_i \vee \bar{x}_j \vee x_k \vee x_l) \wedge (\bar{x}_i \vee x_j \vee x_k \vee x_l) \end{aligned}$$

[1]The case $K = 2$ (Viana-Bray model) does not present any interesting computational features as far as hardness is concerned because it can be solved efficiently both by local and global methods.

$$\begin{aligned} C(ijkl|-1) &= (x_i \vee x_j \vee x_k \vee x_l) \wedge (\bar{x}_i \vee \bar{x}_j \vee \bar{x}_k \vee \bar{x}_l) \\ &\wedge \ (\bar{x}_i \vee \bar{x}_j \vee x_k \vee x_l) \wedge (\bar{x}_i \vee x_j \vee \bar{x}_k \vee x_l) \\ &\wedge \ (x_i \vee x_j \vee \bar{x}_k \vee \bar{x}_l) \wedge (x_i \vee \bar{x}_j \vee x_k \vee \bar{x}_l) \\ &\wedge \ (x_i \vee \bar{x}_j \vee \bar{x}_k \vee x_l) \wedge (\bar{x}_i \vee x_j \vee x_k \vee \bar{x}_l) \end{aligned} \tag{2.15}$$

and so on. Here $\wedge$ and $\vee$ stand for the logical AND and OR operations respectively and the over-bar is the logical negation. Let's concentrate on the $K = 3$ case, that contains all general elements. In the next chapter we will study a mixed version of this model in the case of a mixture of 2 and 4 clauses, which we will call 2+p-XOR-SAT as it shares many common features to the 2+p-SAT model studied in [11]. By randomly choosing[2] a set $E$ of $M$ triples $\{i, j, k\}$ among the $N$ possible indices and $M$ associated unbiased and independent random variables $J_{ijk} = \pm 1$, we construct a Boolean expression in Conjunctive Normal Form (CNF) as

$$F = \bigwedge_{\{i,j,k\} \in E} C(ijk|J_{ijk}) \ . \tag{2.16}$$

A logical assignment of the $\{x_i\}$'s satisfying all clauses, that is evaluating $F$ to true, is called a solution of the XOR-SAT problem. If no such assignment exists, $F$ is said to be unsatisfiable. A slightly different choice of $J_{ijk}$ allows to construct XOR-SAT formulæ which are random but guaranteed to be satisfiable. This will lead to the ferromagnetic spin case: to every Boolean variable we associate independently drawn random variables $\varepsilon_i = \pm 1$, and define $J_{ijk} = \varepsilon_i \varepsilon_j \varepsilon_k$ for all $\{i, j, k\} \in E$. For this choice, CNF formula in eq.(2.16) is satisfied by $\{x_i \mid x_i = +1 \text{ if } \varepsilon = +1, \ x_i = 0 \text{ if } \varepsilon = -1\}$. As we shall discuss in great detail, these formulæ provide a uniform ensemble of hard satisfiable instances for local search methods. We refer to this version of the model as the *satisfiable hSAT*. Indeed, the random signs of $J_{ijk}$ can be removed in this satisfiable case by negating all Boolean variables $x_i$ associated to negative $\varepsilon_i$. The resulting model has $J_{ijk} = +1$ for all $\{i, j, k\} \in E$, and the forced satisfying solution is $x_i = 1, \ \forall i = 1, ..., N$. The use of the $\{\varepsilon_i\}$ is a way of hiding the latter solution by a *random gauge transformation* without changing the properties of the model. The impossibility of inverting efficiently the gauge transformation by local methods is a consequence of the branching process arising form the presence of $K = 3$ variables in each constraint. For any $K > 3$ the same result would hold whereas for $K = 2$ the problem trivializes. The XOR-SAT model can be easily described as a minimization problem of a cost-energy function over a random hyper-graph. Given a random hyper-graph $\mathcal{G}_{N,M} = (V, E)$, where $V$ is the set of $N$ vertices and $E$ is the set of $M$ hyper-edges joining triples of vertices, the energy function to be minimized reads

$$H_J[\mathbf{S}] = M - \sum_{\{i,j,k\} \in E} J_{ijk} \, S_i S_j S_k \ , \tag{2.17}$$

where each vertex $i$ bears a binary "spin" variable $S_i = \pm 1$, and the weights $J_{ijk}$ associated to the random bonds can be either $\pm 1$ at random, in the so called *frustrated* case, or simply equal to 1 in the *unfrustrated* model. We see that this is indeed the particular case of the 3-spin of eq.(2.9). Once the mapping $S_i = 1$ if $x_i = 1$ and $S_i = -1$ if $x_i = 0$ is established, one can easily notice that the energy function in eq.(2.17) simply counts the number of violated clauses in the previously defined CNF formulæ with the same set of $J$'s. The frustrated and the unfrustrated cases correspond to the XOR-SAT and to the satisfiable XOR-SAT formulæ respectively.

[2] In the original random XOR-SAT version, $v(x)$ will therefore be the generating function of a Poissonian distribution.

## 2.2 From the partition function to the average free-energy

The constraints on the degree distribution will have to be introduced along the computation of the logarithm of the partition function.

$$Z = e^{-\beta M} \sum_{s_i} e^{\beta \sum_k H_k} \tag{2.18}$$

Following the approach of ref. [19], we compute the free energy of the model with the replica method, exploiting the identity $\log < Z^n >= 1 + n < \log Z > +O(n^2)$. The $n^{th}$ moment of the partition function is obtained by replicating $n$ times the sum over the spin configurations and then averaging over the quenched disorder The averaged n-th moment of the partition function takes therefore the following form, a part from a normalization factor:

$$< Z^n >= e^{-n\beta M} \sum_{\vec{s_i}} < e^{\beta \sum_{a=1}^{n} \sum_l \sum_{i_1,\dots,i_l} J_{i_1,\dots,i_l} s^a_{i_1} \dots s^a_{i_l}} > \tag{2.19}$$

where the average value of an observable is given by:

$$< \cdot > = \xi[P(k)] \int \prod_{i_1<\dots<i_l} P(J_{i_1,\dots,i_l})(\cdot) \prod_{i=1}^{N} \delta(\sum_l \sum_{i_1<\dots<i_l} |sign(J_{i_1,\dots,i_l})| - k_i) \cdot \tag{2.20}$$

$$\prod_l \delta(M v_l - \sum_{i_1<\dots<i_l} |sign(J_{i_1,\dots,i_l})|) \tag{2.21}$$

$\xi[P(k)]$ is a normalization factor necessary to rescale to one the sum over the constrained probability distribution of the couplings:

$$\xi[P(k)] \equiv \int \prod_{i_1<\dots<i_l} P(J_{i_1,\dots,i_l}) \prod_{i=1}^{N} \delta(\sum_l \sum_{i_1<\dots<i_l} |sign(J_{i_1,\dots,i_l})| - k_i) \prod_l \delta(M v_l - \sum_{i_1<\dots<i_l} |sign(J_{i_1,\dots,i_l})|) \tag{2.22}$$

The two inserted delta functions are there to ensure the constraints on degree and interaction terms distribution. In fact, the constraint over the fraction of fixed rank plaquettes is already taken into account in the particular form of the distribution, therefore the normalization can be limited to the term

$$\xi[P(k)] \equiv \int \prod_{i_1<\dots<i_l} P(J_{i_1,\dots,i_l}) \prod_{i=1}^{N} \delta(\sum_l \sum_{i_1<\dots<i_l} |sign(J_{i_1,\dots,i_l})| - k_i) \tag{2.23}$$

Its value is calculated in the appendix in this case. The final value in the large N limit is:

$$\xi[P(k)] \sim e^{-N\left(<k> - \sum_k c_k \log\left(\frac{<k>^k}{k!}\right)\right)} \tag{2.24}$$

Even more in generality, $H_l$ could be in the form

$$H_l = \sum_{i_1<\dots<i_l} J_{i_1,\dots,i_l} G^{(l)}[\vec{s}] \tag{2.25}$$

where the functions $G^{(l)}$ depend on the particular model under consideration. In this work, for instance, we consider other relevant examples such as the Bicoloring problem of a random rank 3 hyper-graph, where only $G^{(3)} = -(s_{i_1} s_{i_2} + s_{i_1} s_{i_3} + s_{i_2} s_{i_3} + 2)$ is present, and the random 3-SAT

model, where $G^{(3)} = \prod_{l=1}^{3} \delta(s_{i_l}; -1)$ and the coupling variables follow a different probability distribution too. Going back to our generalized $p$-spin model we can write the delta functions in their integral form

$$\prod_l \delta(Mc_l - \sum_{i_1<\ldots<i_l} J_{i_1,\ldots,i_l}) =$$
$$\int \prod_l (\frac{d\phi_l}{2\pi}) \exp(-iM \sum_l \phi_l v_l) \exp(i \sum_l \phi_l \sum_{i_1<\ldots<i_l} |sign(J_{i_1,\ldots,i_l})|) \tag{2.26}$$
$$\prod_i \delta(\sum_l \sum_{<i_2,\ldots,i_l>_i} |sign(J_{i_1,\ldots,i_l})| - k_i) =$$
$$\int \prod_i (\frac{d\psi_i}{2\pi}) \exp(-i \sum_i \psi_i k_i) \exp(i \sum_{i_1<\ldots<i_l} (\sum_{j=1}^{k} \psi_{i_j}) |sign(J_{i_1,\ldots,i_l})|) \tag{2.27}$$

In fact, as we said, the choice we have made on the probability distribution of the couplings (and the consequent value of the quantities $\gamma_k$) already implies the first constraint to be satisfied in the large N limit. Indeed, if we explicitly insert the first delta function (also the normalization factor will accordingly change), we are left with one supplementary series of saddle point equations in the variables $\phi_l$. Inserting the solutions for the latter variables into the common saddle point equations, we retrieve equivalent expressions. The averaged n-th power of the partition function becomes, in the case of the diluted ferromagnet,

$$< Z^n > \sim \exp(-\beta n M) \sum_{\vec{s}_i} \int \prod_i (\frac{d\psi_i}{2\pi}) \exp\left(-i \sum_{i=1}^{N} \psi_i k_i\right)$$
$$\exp\left(-\frac{< k >}{< l >} N + \sum_l \frac{v_l}{N^{l-1}} \exp\left(\beta \sum_{i_1,\ldots,i_l} \sum_a s^a_{i_1} \ldots s^a_{i_l} + i \sum_{j=1}^{l} \psi_{i_j}\right)\right) \tag{2.28}$$

We could now go on in the calculation treading a path similar to the one followed for the fully connected models, tracing out the replicated spin variables through the introduction of a whole series of overlap and multi-overlap quantities. Due to the distribution of ranks and degrees, however, the number of overlap function that we would need to take into consideration is infinite, and we are better off if we exploit a more compact mathematical notation via a generating function formalism of the overlap series [3]. The correct generating function for this kind of problems turns out to be writable as a functional order parameter in the form [19, 9, 12]

$$\rho(\vec{\sigma}) = \frac{1}{N} \sum_i \delta(\vec{\sigma} - \vec{s}_i) e^{i\psi_i} \ . \tag{2.29}$$

In the case of Poissonian hyper-graphs, due to the *self similarity* property of eq. (1.5) that substituted int eq. (1.6) leads to $q_k^{poiss} = c_k^{poiss}$, the fields $\psi_i$ are redundant and re-absorbed in the degree distribution (Poissonian degree hyper-graphs are the ones obtained in the thermodynamic limit when using the "free"couplings probability distributions (2.11) and (2.12)). In this case the quantity (2.29) directly represents the fraction of replicated spins $s_i^a$ in the replica state $\sigma^a$ in the *whole* graph as well as in the cavity one. However, in the general case it is necessary to add a field $\psi_i$ that can be physically interpreted in the following way: $e^{i\psi_i}$ is an

[3] However, a full series expansion in terms of multi-overlaps will be treated formally in the discussion of chapter 6

operator that acts "erasing" from the spin fraction the contribution of the neighboring variables disconnected from the $i$-th one, during the removal of the coupling $J_{i_1 \dots i_l}$. This means that the replica automatically takes into account the fact that we are working on the cavity graph. This sets the connection between the replica and the cavity method, where in the course of the self consistent computation edges and vertices of the hyper-graph are opportunely erased [24]. This forces us to work with the cavity hyper-graph, shifting the degree probability ensemble and asking for a rescaling of the value of the order parameter, that might not be normalized any more. In particular the condition

$$\sum_{\vec{\sigma}} \rho(\vec{\sigma}) = 1 \tag{2.30}$$

is not automatically verified anymore and we will have to pay attention to this fact in the following calculations. One can see that $\rho(\vec{\sigma})$ indeed is a multi-overlap generating functional observing that

$$\begin{aligned}
&\rho(\vec{\sigma}) = \frac{1}{N}\sum_{i=1}^{N}\left[\prod_{a=1}^{n}\left(\frac{1+s_i^a\sigma^a}{2}\right)e^{i\psi_i}\right] = \\
&\frac{1}{2^n N}\sum_{i=1}^{N}\left[e^{i\psi_i} + \sum_a s_i^a\sigma^a e^{i\psi_i} + \sum_{a<b} s_i^a s_i^b \sigma^a\sigma^b e^{i\psi_i} + \sum_{a<b<c} s_i^a s_i^b s_i^c \sigma^a\sigma^b\sigma^c e^{i\psi_i} + \ ...\right] \\
&\frac{1}{2^n}\left[\rho + Q_{cav}^a\sigma^a + \sum_{a<b} Q_{cav}^{ab}\sigma^a\sigma^b + \sum_{a<b<c} Q_{cav}^{abc}\sigma^a\sigma^b\sigma^c + \ ...\right]
\end{aligned} \tag{2.31}$$

where the scalar $\rho \equiv 1/N\sum_{i=1}^{N} e^{i\psi_i}$ is defined in the appendix and will cancel out with the normalization factor in the final expression for the free energy, and the overlaps $Q_{cav}$ are the usual multi-replica overlaps

$$Q_{cav}^{abc\dots} \equiv \frac{1}{N}\sum_{i=1}^{N} s_i^a s_i^b s_i^c \dots e^{i\psi_i} \tag{2.32}$$

computed *in the cavity hyper-graph*. This has an intuitive interpretation if we realize that these quantities correctly describe the mean field nature of the models only when the *direct* connection between two vertices is zero with probability 1 in the large N limit. This observation will be of crucial importance in the determination of rigorous bounds in the last chapter. We can introduce the functional order parameter via the delta function

$$\delta\left(\rho(\vec{\sigma}) - \frac{1}{N}\sum_i \delta(\vec{\sigma}-\vec{s}_i)e^{i\psi_i}\right) = \int \frac{d\rho(\vec{\sigma})d\hat{\rho}(\vec{\sigma})}{2\pi N^{-1}} \exp\left(-N\sum_{\vec{\sigma}}\rho(\vec{\sigma})\hat{\rho}(\vec{\sigma}) + \hat{\rho}(\vec{\sigma})\sum_i \delta(\vec{\sigma}-\vec{s}_i)e^{i\psi_i}\right) \tag{2.33}$$

where $\hat{\rho}(\vec{\sigma})$ is a conjugated functional that we'll see to own an important physical meaning. Plugging (2.33) into (2.28) via integrals over the replica spin values we obtain

$$\begin{aligned}
< Z^n > \ \sim\ & \exp\left(-\beta n N\frac{< k >}{< l >}\right)\sum_{\vec{S}_i}\int\prod_i\left(\frac{d\psi_i}{2\pi}\right)\exp\left(-i\sum_{i=1}^{N}\psi_i k_i\right)\exp\left(-N\frac{< k >}{< l >}\right)\cdot \\
& \int\prod_{\vec{\sigma}}\frac{N d\rho(\vec{\sigma})d\hat{\rho}(\vec{\sigma})}{2\pi}\exp\left(-N\sum_{\vec{\sigma}}\rho(\vec{\sigma})\hat{\rho(\vec{\sigma})}\right)\cdot \\
& \exp\left(N\frac{< k >}{< l >}\sum_l v_l \sum_{\vec{\sigma}_1,\dots,\vec{\sigma}_l}\rho(\vec{\sigma}_1)\dots\rho(\vec{\sigma}_l)\exp(\beta\sum_a \sigma_1^a\dots\sigma_l^a)\right)\cdot
\end{aligned}$$

$$\sum_{\vec{s_i}} \exp\left(\sum_{\vec{\sigma}} \hat{\rho}(\vec{\sigma}) \sum_i \delta(\vec{\sigma} - \vec{s}_i) e^{i\psi_i}\right) \tag{2.34}$$

Where

$$\begin{aligned}
&\sum_{\vec{\sigma}_1,...,\vec{\sigma}_l} \rho(\vec{\sigma}_1)...\rho(\vec{\sigma}_l) \exp\left(\beta \sum_a \sigma_1^a ... \sigma_l^a\right) = \\
&\frac{1}{N^l} \sum_{i_1,...,i_l} \sum_{\vec{\sigma}_1,...,\vec{\sigma}_l} \prod_{a=1}^{n} \delta(s_{i_1}^a; \sigma_1^a)...\delta(s_{i_l}^a; \sigma_l^a) e^{i\psi_{i_1}} ... e^{i\psi_{i_l}} \exp\left(\beta \sum_a \sigma_1^a ... \sigma_l^a\right) = \\
&\frac{1}{N^l} \sum_{i_1,...,i_l} \exp\left(i\left(\psi_{i_1} + ... + \psi_{i_l}\right)\right) \exp\left(\beta \sum_a s_{i_1}^a ... s_{i_l}^a\right)
\end{aligned} \tag{2.35}$$

Tracing over the replicated spins and later integrating out the $\psi_i$ variables one obtains, for the last term,

$$\int \prod_i \left(\frac{d\psi_i}{2\pi}\right) \exp\left(-i \sum_{i=1}^{N} \psi_i k_i\right) \sum_{\vec{s}_i} \exp\left(i \sum_{\vec{\sigma}} \hat{\rho}(\vec{\sigma}) \sum_i \delta(\vec{\sigma} - \vec{s}_i) e^{i\psi_i}\right) \quad = \tag{2.36}$$

$$\exp\left(\sum_i \log\left(\sum_{\vec{\sigma}} \frac{(\hat{\rho}(\vec{\sigma}))^{k_i}}{(k_i)!}\right)\right) \tag{2.37}$$

Averaging over the $P(\hat{k})$ this last term becomes

$$\exp\left(\sum_k c_k \log\left(\sum_{\vec{\sigma}} \frac{(\hat{\rho}(\vec{\sigma}))^k}{k!}\right)\right) \tag{2.38}$$

For normalization convenience we can rescale the conjugate order parameter $\hat{\rho(\vec{\sigma})} \longrightarrow < k > \hat{\rho(\vec{\sigma})}$. Adding then in the exponential in $N$ the contribution due to the quenched disorder probability distribution normalization factor (see appendix), the potential eventually reads:

$$\begin{aligned}
-n\beta F[\rho(\vec{\sigma}), \hat{\rho}(\vec{\sigma})] \quad = \quad & - < k > \sum_{\vec{\sigma}} \rho(\vec{\sigma})\hat{\rho}(\vec{\sigma}) + < k > - \frac{< k >}{< l >} - n\beta \frac{< k >}{< l >} + \\
& \frac{< k >}{< l >} \sum_l v_l \sum_{\vec{\sigma}_1,...,\vec{\sigma}_l} \rho(\vec{\sigma}_1)...\rho(\vec{\sigma}_l) \exp\left(\beta \sum_a \sigma_1^a ... \sigma_l^a\right) + \\
& \sum_k c_k \log\left(\sum_{\vec{\sigma}} \hat{\rho}(\vec{\sigma})^k\right)
\end{aligned} \tag{2.39}$$

The dominant contribution $F[\rho_{saddle}(\vec{\sigma}), \hat{\rho}_{saddle}(\vec{\sigma})]$ to the potential in the thermodynamic limit is evaluated via the following functional saddle point equations in the order parameters:

$$\frac{\delta F[\rho(\vec{\sigma}), \hat{\rho}(\vec{\sigma})]}{\delta \rho(\vec{\sigma})} = 0 \Longleftrightarrow \rho(\vec{\sigma}) = \frac{1}{< k >} \sum_k k c_k \frac{(\hat{\rho}(\vec{\sigma}))^{k-1}}{\sum_{\vec{\sigma}} (\hat{\rho}(\vec{\sigma}))^k} \tag{2.40}$$

$$\frac{\delta F[\rho(\vec{\sigma}), \hat{\rho}(\vec{\sigma})]}{\delta \hat{\rho}(\vec{\sigma})} = 0 \Longleftrightarrow \hat{\rho}(\vec{\sigma}) = \frac{1}{< l >} \sum_l l v_l \sum_{\vec{\sigma}_2,...,\vec{\sigma}_l} \rho(\vec{\sigma}_2)...\rho(\vec{\sigma}_l) \exp(\beta \sum_a \sigma^a \sigma_2^a ... \sigma_l^a) \tag{2.41}$$

The ground state solution gives, in the ferromagnetic case, the value of the entropy of the model both into the paramagnetic and into the magnetized states. For the case of spin-glasses,

typically there will exist a range of $< k > / < l >$[4] where the ground state energy vanishes approaching to zero temperature and again the free energy will coincide with the full entropy of the spin-glass states. Increasing the average degree distribution leads to a critical point beyond which the ground states energy becomes higher than zero also at zero temperature. In this case the main contribution to the potential gives us the internal energy of the model, while the entropy is sub-leading in temperature and has to be computed from eq.(2.39) via the usual relation

$$S = \beta^2 \frac{\partial F}{\partial \beta} \tag{2.42}$$

Before taking the $\beta \to \infty$ limit. The thermodynamic transition turns out to be of second order in the Viana-Bray case[5], as we will see in the next chapter. In other and more interesting cases, as well as in many relevant combinatorial optimization problems like $K$-SAT, the transition between the paramagnetic to the spin-glass (or magnetized in the case of the ferromagnet) state is first order and preceded (in the SG case) by a dynamic transition where the total entropy can be split in two contribution: A *complexity* term [7, 19, 22, 26, 24] due to the exponential multiplicity of the metastable states, and a residual entropy contribution (see last section for details). In the pure $p > 2$ spin glass model [19, 26] the two terms are completely separated due to a property of orthogonality for the stable states.

**Paramagnetic and $\beta = 0$ cases**

Equations (2.40) and (2.41) admit the completely paramagnetic solution $\rho(\vec{\sigma}) = \rho(\hat{\vec{\sigma}}) = 1/2^n$. Inserting it in (2.39) and retaining order $\mathcal{O}(n)$ terms, one easily obtains:

$$\begin{aligned} -n\beta F_{para} &= -< k > + n < k > \log 2 + < k > - \frac{< k >}{< l >} - n\beta \frac{< k >}{< l >} + \\ &\quad \frac{< k >}{< l >} + n \frac{< k >}{< l >} \log\left(\cosh(\beta)\right) + (< k > -1) n \log 2 \qquad (2.43) \\ &= n \left[ \left( 1 - \frac{< k >}{< l >} \right) \log 2 + \frac{< k >}{< l >} \left( \log(2\cosh(\beta)) - \beta \right) \right] \qquad (2.44) \end{aligned}$$

$\forall\ \beta$, so that

$$\begin{aligned} S_{para, T=0} &= \left( 1 - \frac{< k >}{< l >} \right) \log 2 \qquad (2.45) \\ S_{\beta=0} &= \log 2\ . \qquad (2.46) \end{aligned}$$

### 2.2.1 Some considerations on normalization

The omission of the explicit delta function on the hyper-graph rank distribution constraint leads to apparently slightly different expressions for the free energy and for the saddle point equation. Normally the equations would have been

$$-n\beta F = -< k > \sum_{\vec{\sigma}} \rho(\vec{\sigma}) \hat{\rho}(\vec{\sigma}) + < k > - n\beta \frac{< k >}{< l >} +$$

[4] in the case of Poissonian graphs, for example, $< k > / < l >= \gamma$ is a continuous parameter that can be freely adjusted

[5] and, more generally, whenever the fraction $v_2$ of 2-spins interactions is hight enough compared to the rest, as will be shown in chapter four

$$\frac{< k >}{< l >} \sum_l v_l \log \left( \sum_{\vec{\sigma}_1,\ldots,\vec{\sigma}_l} \rho(\vec{\sigma}_1)...\rho(\vec{\sigma}_l) \exp\left(\beta \sum_a \sigma_1^a ... \sigma_l^a\right)\right) + \sum_k c_k \log\left(\sum_{\vec{\sigma}} \hat{\rho}(\vec{\sigma})^k\right) \tag{2.47}$$

and

$$\rho(\vec{\sigma}) = \frac{1}{< k >} \sum_k k c_k \frac{(\hat{\rho}(\vec{\sigma}))^{k-1}}{\sum_{\vec{\sigma}} (\hat{\rho}(\vec{\sigma}))^k} \tag{2.48}$$

$$\hat{\rho}(\vec{\sigma}) = \frac{1}{< l >} \sum_l l v_l \frac{\sum_{\vec{\sigma}_2,\ldots,\vec{\sigma}_l} \rho(\vec{\sigma}_2)...\rho(\vec{\sigma}_l) \exp(\beta \sum_a \sigma^a \sigma_2^a ... \sigma_l^a)}{\sum_{\vec{\sigma}_1,\ldots,\vec{\sigma}_l} \rho(\vec{\sigma}_1)...\rho(\vec{\sigma}_l) \exp(\beta \sum_a \sigma_1^a ... \sigma_l^a)} \tag{2.49}$$

respectively. It is easy to see, however, that the expressions are numerically equivalent both into the RS and the 1RSB cases. One can easily check this equivalence exploiting the fact that given a term $A$ that in the second case appears inside the new logarithm, the quantity is always in the form $A^n$, so we can exploit the "replica trick" in the $n \to 0$ limit to show the equivalence of the two expressions[6]. Moreover, in the saddle point equations, we have introduced no Lagrangian parameter ensuring the normalization of the order parameters. Indeed, the two order parameters written in the form of (2.29) and its conjugate are not in principle properly normalized. There is an equivalent but somehow more cumbersome way of introducing a normalized order parameter via the use of a Lagrange multiplier, as we will show for completeness in the particular case of the 3-spin in a next paragraph, but it is easy to show that, in the present case, the normalization lets the equations unchanged, leaving us with the possibility of working on $\rho(\vec{\sigma})$ and $\hat{\rho}(\vec{\sigma})$ as if they were the normalized ones $\rho_n(\vec{\sigma})$ and $\hat{\rho_n}(\vec{\sigma})$. Indeed, we can define

$$\rho_n(\vec{\sigma}) = \frac{\rho(\vec{\sigma})}{\lambda} \tag{2.50}$$

$$\hat{\rho_n}(\vec{\sigma}) = \frac{\hat{\rho}(\vec{\sigma})}{\hat{\lambda}} \tag{2.51}$$

$$\tag{2.52}$$

with

$$\lambda = \sum_{\vec{\sigma}} \rho(\vec{\sigma}) \tag{2.53}$$

$$\hat{\lambda} = \sum_{\vec{\sigma}} \hat{\rho}(\vec{\sigma}) \tag{2.54}$$

Moreover, as can be easily seen from (2.40)-(2.41)or (2.49),

$$\sum_{\vec{\sigma}} \rho(\vec{\sigma}) \hat{\rho}(\vec{\sigma}) = 1 \tag{2.55}$$

and

$$\lambda\hat{\lambda} = \frac{1}{< k >} \sum_k k c_k \frac{\sum_{\vec{\sigma}} \hat{\rho_n}(\vec{\sigma})^{k-1}}{\sum_{\vec{\sigma}} (\hat{\rho_n}\vec{\sigma})^k} \ . \tag{2.56}$$

[6]In fact we must compute that limit in order to retrieve the physical expressions

As we will see in the following section, a general term $\sum_{\vec{\sigma}} \hat{\rho_n}(\vec{\sigma})^t$ and $\rho_n(\vec{\sigma})^t$ can be written respectively as $A_t^n \sim 1 + n \log A_t$ and $B_t^n \sim 1 + n \log B_t$ where $A_t$ and $B_t$ do not depend on $n$ any more. Consequently eq.(2.56) becomes

$$\begin{aligned} \lambda\hat{\lambda} &\sim \frac{1}{< k >} \sum_k k c_k \frac{(1 + n \log A_{k-1})}{(1 + n \log A_k)} \sim \\ & 1 + \frac{n}{< k >} \sum_k k c_k \log\left(\frac{A_{k-1}}{A_k}\right) \end{aligned} \tag{2.57}$$

This result tells us that the functional order parameter are already normalized in the $n \to 0$ limit. Moreover, the term $\sum_{\vec{\sigma}} \rho_n(\vec{\sigma})\hat{\rho_n}(\vec{\sigma})$ can be written as $1 + n\Omega$ where again $\Omega$ does not depend of $n$. If we plug eq.(2.57) and this last expression into eq.(2.47), calling $\frac{1}{<k>} \sum_k k c_k \log\left(\frac{A_{k-1}}{A_k}\right) \equiv C$ we get

$$\begin{aligned} -n\beta F[\rho(\vec{\sigma}), \hat{\rho}(\vec{\sigma})] &= - < k > (1 + n\Omega)(1 + nC) + < k > -n\beta \frac{< k >}{< l >} + \\ & \frac{< k >}{< l >} \sum_l v_l \log\left( \sum_{\vec{\sigma_1},\ldots,\vec{\sigma_l}} \rho_n(\vec{\sigma_1}) \ldots \rho_n(\vec{\sigma_l}) \exp\left( \sum_a \sigma_1^a \ldots . \sigma_l^a \right) \right) \\ & + < k > \log(1 + nC) + \sum_k c_k \log\left( \sum_{\vec{\sigma}} \hat{\rho}(\vec{\sigma})^k \right) \\ &= -n\beta F[\rho_n(\vec{\sigma}), \hat{\rho_n}(\vec{\sigma})] \end{aligned} \tag{2.58}$$

As we will see later, this is not true anymore in the 1RSB case, where the normalization factors will be proportional to a power of the replica parameter $m$ which in general does not tend to zero. Nevertheless, in that case the normalization parameters explicitly disappear from the expression of the RSB potential for any value of $m$, leaving it formally unchanged. We drop the subindex "n = norm" in the following. In the frustrated spin glass version of the model, all previous calculations are still valid, provided one uses (2.12) instead of (2.11). As a consequence, all previous equations are left unchanged but for the substitution of the following internal factors:

$$\begin{aligned} \exp(\beta \sum_a \sigma_1^a \ldots \sigma_k^a) &\implies \cosh(\beta \sum_a \sigma_1^a \ldots \sigma_k^a) \\ \exp(\beta \sum_a \sigma^a \sigma_2^a \ldots \sigma_k^a) &\implies \cosh(\beta \sum_a \sigma^a \sigma_2^a \ldots \sigma_k^a) \end{aligned} \tag{2.59}$$

For a more general choice of $\mu(\mathbf{J})$, we will have to change:

$$\begin{aligned} \exp\left(\beta \sum_a \sigma_1^a \ldots \sigma_k^a\right) &\implies \int d\mu(J) \exp\left(\beta J \sum_a \sigma_1^a \ldots \sigma_k^a\right) \\ \exp\left(\beta \sum_a \sigma^a \sigma_2^a \ldots \sigma_k^a\right) &\implies \int d\mu(J) \exp\left(\beta J \sum_a \sigma^a \sigma_2^a \ldots \sigma_k^a\right) \end{aligned} \tag{2.60}$$

The expression in presence of a magnetic field will be shown when treating error correcting codes. If $\mu\mathbf{J}$ is symmetric in any component of $\mathbf{J}$ the system will be a pure spin-glass. The resulting effect is that the potential will be explicitly symmetric under the exchange of the positive and the negative support values of the functional order parameters. However, the value of the pure ferromagnetic and pure $J = \pm 1$ spin-glass potentials will coincide at the

saddle point since the particular choice of symmetric order parameters is supported also in the ferromagnetic case. While in the spin glass the symmetric $\rho(\sigma)$ will describe also the minimal energy states, the ferromagnetic ground state will be asymmetric. and will be described by an order parameter with no negative support in the zero temperature limit[7]. Therefore, if we force to write a solution to the ferromagnetic saddle point equations that is to be symmetric under the spin inversion, we'll find positive energy saddle point metastable states that coincide in energy with the glassy ground states due to the coincidence of the potential at the saddle point. No other metastable solutions are found other than the symmetric ones in the pure spin-glass. We must keep this in mind when we'll write apparently different expressions for the two models, nevertheless using some saddle point results of the ferromagnetic case into the spin glass one.

## 2.3 The Replica Symmetric Results

In the replica symmetric (RS) case we can unravel the structure of the order parameter in terms of the effective fields acting onto the $\sigma$ spins. Indeed, if we assume $\rho(\vec{\sigma})$[8] to be symmetric under the permutation $S_n$ of the replica variables $\sigma_1, ..., \sigma_n$, we can write it in terms of the distribution function of the local magnetization $P(m)$:

$$P(m) \equiv \frac{1}{N} \sum_i \prod_a \delta\left(s_i^a - m\right) \tag{2.61}$$

such that

$$\begin{aligned} \rho(\vec{\sigma}) \equiv & \int dm P(m) \prod_a \frac{1 + m\sigma^a}{2} = \\ & \int dm P(m) \left(\frac{1+m}{2}\right)^{n_+} \left(\frac{1-m}{2}\right)^{n_-} \\ & \int dm P(m) \left(\frac{1-m^2}{4}\right)^{\frac{n}{2}} \left(\frac{1+m}{1-m}\right)^{\frac{1}{2}\sum_a \sigma^a} = \\ & \int dm P(m) \left(\frac{1-m^2}{4}\right)^{\frac{n}{2}} \exp\left(\frac{1}{2}\tanh^{-1}(m) \sum_a \sigma^a\right) \end{aligned} \tag{2.62}$$

If we then define an effective field $h$ at any temperature as

$$h = \frac{1}{\beta}\tanh^{-1}(m) \tag{2.63}$$

we can eventually write an expression of the functional order parameters in terms of the fields acting on the direct as well as the dual hyper-graph:

$$\rho(\vec{\sigma}) = \int dh P(h) \frac{e^{\beta h \sum_{a=1}^n \sigma_a}}{(2\cosh(\beta h))^n} \tag{2.64}$$

$$\hat{\rho}(\vec{\sigma}) = \int du Q(u) \frac{e^{\beta u \sum_{a=1}^n \sigma_a}}{(2\cosh(\beta u))^n} \tag{2.65}$$

[7] for cases of hyper-graphs of only even rank there will be of course the usual twofold degeneracy

[8] and consequently its conjugated parameter

Since the replica saddle point equations in the $n \to 0$ are equivalent to the cavity iteration equations, the effective field $h$ turns out to be the local cavity field acting on a vertex of given degree. The index on the vertex has been dropped in the RS case where only one state is present and therefore the field distribution does not depend on the particular spin one is working with, but only on the average degree distribution. Substituting definitions (2.64) and (2.65) into the saddle point equations, and noticing that we can fully characterize the distributions in the $n \to 0$ limit, the saddel point equations read

$$\begin{aligned}
\int dh P(h) e^{\beta h f} &= \frac{1}{< l >} \sum_k k c_k \int \prod_{t=k}^{k-1} du_t Q(u_t) e^{\beta f \sum_t u_t} \\
&= \frac{1}{< k >} \sum_k k c_k \int dh e^{\beta h f} \int \prod_{t=1}^{k-1} du_t Q(u_t) \delta \left( h - \sum_t u_t \right) \qquad (2.66) \\
\int du Q(u) e^{\beta u f} &= \frac{1}{< l >} \sum_k k c_k \int \prod_{t=1}^{l-1} dh_t P(h_t) e^{f \tanh^{-1}(\tanh(\beta) \prod_t \tanh(\beta h_t))} \\
&= \frac{1}{< l >} \sum_l l v_l \int du e^{\beta u f} \int \prod_{t=1}^{l-1} dh_t P(h_t) \delta \left( u - u(\beta, \{h_t\}_t) \right) \qquad (2.67)
\end{aligned}$$

with $f \equiv \sum_{a=1}^{n} \sigma_a$ and

$$u(\beta, \{h_t\}_t) \equiv \frac{1}{\beta} \tanh^{-1} \left( \tanh(\beta) \prod_t \tanh(\beta h_t) \right) \qquad (2.68)$$

We thus obtain self consistent equations for the fields probability distributions in a form ready for further analytical manipulation or for numerical solution:

$$\begin{aligned}
P(h) &= \frac{1}{< k >} \sum_k k c_k \int \prod_{t=1}^{k-1} du_t Q(u_t) \delta \left( h - \sum_t u_t \right) \qquad (2.69) \\
Q(u) &= \frac{1}{< l >} \sum_l l v_l \int \prod_{t=1}^{l-1} dh_t P(h_t) \delta \left( u - \frac{1}{\beta} \tanh^{-1} \left( \tanh(\beta) \prod_t \tanh(\beta h_t) \right) \right) \qquad (2.70)
\end{aligned}$$

for the diluted ferromagnet, and

$$\begin{aligned}
P(h) &= \frac{1}{< k >} \sum_k k c_k \int \prod_{t=1}^{k-1} du_t Q(u_t) \delta \left( h - \sum_t u_t \right) \qquad (2.71) \\
Q(u) &= \frac{1}{< l >} \sum_l l v_l \int \prod_{t=1}^{l-1} dh_t P(h_t) \left[ \delta \left( u - \frac{1}{\beta} \tanh^{-1} \left( \tanh(\beta) \prod_t \tanh(\beta h_t) \right) \right) + \right. \\
&\quad \left. \delta \left( u + \frac{1}{\beta} \tanh^{-1} \left( \tanh(\beta) \prod_t \tanh(\beta h_t) \right) \right) \right] \qquad (2.72)
\end{aligned}$$

for the spin glass.

Notice that these equations could have also been easily obtained via the cavity method under the hypothesis of only one state and substituting the local energetic terms of the generalized $p$-spin Hamiltonian into (1.20), and following the cavity procedure introduced in chapter 1.

The number of multiple integrals involved and the structure of the equation is not well suited for a direct numerical integration, but an iterative method like an ad hoc devised population

dynamics [23] works very well this case. Substituting into the expression for the potential one derives:

$$\begin{aligned}
-\beta F &= -<k>\int\int dhduP(h)Q(u)\log\left(1+\tanh(\beta h)\tanh(\beta u)\right)+ \\
&\frac{<k>}{<l>}\sum_l v_l\int\prod_{t=1}^{l}dh_tP(h_t)\log\left(1+\tanh(\beta)\prod_{t=1}^{l}\tanh(\beta h_t)\right)+\frac{<k>}{<l>}\left(\log(\cosh(\beta))-\beta\right) \\
&+\sum_k c_k\int\prod_{t=1}^{k}du_tQ(u_t)\log\left(\prod_{t=1}^{k}(1+\tanh(\beta u_t))+\prod_{t=1}^{k}(1-\tanh(\beta u_t))\right) \qquad (2.73)
\end{aligned}$$

for the ferromagnet, and

$$\begin{aligned}
-\beta F &= -<k>\int\int dhduP(h)Q(u)\log\left(1+\tanh(\beta h)\tanh(\beta u)\right)+\frac{<k>}{<l>}\left(\log(\cosh(\beta))-\beta\right) \\
&\frac{<k>}{<l>}\sum_l v_l\int\prod_{t=1}^{l}dh_tP(h_t)\left[\log\left(1+\tanh(\beta)\prod_{t=1}^{l}\tanh(\beta h_t)\right)+\right. \\
&\left.\log\left(1-\tanh(\beta)\prod_{t=1}^{l}\tanh(\beta h_t)\right)\right] \\
&+\sum_k c_k\int\prod_{t=1}^{k}du_tQ(u_t)\log\left(\prod_{t=1}^{k}(1+\tanh(\beta u_t))+\prod_{t=1}^{k}(1-\tanh(\beta u_t))\right) \qquad (2.74)
\end{aligned}$$

for the spin glass. The calculations are the same as the manipulations of the saddle point equations. The only difference lying in the fact that one is led to retain $\mathcal{O}(n)$ terms. The average values $< l >$ and $< k >$ can be varied smoothly and they play the role of tuning parameters within a fixed choice of probability distribution types. This has been in particular investigated in spin models on Poissonian distributed graphs, but can be extended to any other geometrical structure. varying $< l >$ and $< k >$ at $T = 0$ one typically enters two different regimes. A paramagnetic phase of vanishing fields (at low values of $< l > / < k >$ and a phase of frozen fields which dominate and collapse at zero temperature to integer values.

### 2.3.1 Vanishing fields

In this phase, where present, the equations take the same form as before, but for a rescaling $\beta u \longrightarrow u$ and $\beta h \longrightarrow h$.

$$\begin{aligned}
P(h) &= \frac{1}{<k>}\sum_k kc_k\int\prod_{t=1}^{k-1}du_tQ(u_t)\delta\left(h-\sum_t u_t\right) \qquad (2.75)\\
Q(u) &= \frac{1}{<l>}\sum_l lv_l\int\prod_{t=1}^{l-1}dh_tP(h_t)\delta\left(u-\frac{1}{\beta}\tanh^{-1}(\tanh(\beta)\prod_t\tanh(h_t))\right)\ , \qquad (2.76)
\end{aligned}$$

with

$$\begin{aligned}
-\beta F &= -<k>\int\int dhduP(h)Q(u)\log\left(1+\tanh(h)\tanh(u)\right)+ \\
&\frac{<k>}{<l>}\sum_l v_l\int\prod_{t=1}^{l}dh_tP(h_t)\log\left(1+\tanh(\beta)\prod_{t=1}^{l}\tanh(h_t)\right)+\frac{<k>}{<l>}\left(\log(\cosh(\beta))-\beta\right) \\
&+\sum_k c_k\int\prod_{t=1}^{k}du_tQ(u_t)\log\left(\prod_{t=1}^{k}(1+\tanh(u_t))+\prod_{t=1}^{k}(1-\tanh(u_t))\right) \qquad (2.77)
\end{aligned}$$

for the ferromagnet, and

$$\begin{aligned}
-\beta F &= -<k>\int\int dhduP(h)Q(u)\log\left(1+\tanh(h)\tanh(u)\right)+\frac{<k>}{<l>}\left(\log(\cosh(\beta))-\beta\right) \\
&\quad \frac{<k>}{<l>}\sum_l v_l\int\prod_{t=1}^{l}dh_tP(h_t)\left[\log\left(1+\tanh(\beta)\prod_{t=1}^{l}\tanh(h_t)\right)+\right. \\
&\quad \left.\log\left(1-\tanh(\beta)\prod_{t=1}^{l}\tanh(\beta h_t)\right)\right] \\
&\quad +\sum_k c_k\int\prod_{t=1}^{k}du_tQ(u_t)\log\left(\prod_{t=1}^{k}(1+\tanh(u_t))+\prod_{t=1}^{k}(1-\tanh(u_t))\right) \qquad (2.78)
\end{aligned}$$

for the spin glass. However, it is easy to see that the trivial solution $P(h)=\delta(h)$ is the only one in the $T=0$ limit. This result is confirmed in numerical evaluation of (2.76) and in numerical simulations. This is NOT the case of other models like for instance random $K$-SAT, where a non trivial structure of the $P(h)$ appears as soon as the degree $\gamma$, which plays the same role as $<k>/<l>$, departs from the zero value, as it was seen in [9, 83] via a Taylor functional expansion of the $P(h)$ in series of Dirac delta function around $<k>=0$. The role of the vanishing field is not completely clear yet. In particular, their influence could extend down to $T=0$ in the RSB phase, where their value is technically zero, but their presence could contribute in inducing non trivial correlations between local ground states. As we will say in chapter 3, this seems not to be the case for $K$-SAT in the satisfiable region, even though evidence of $\infty$-RSB is retrieved for very high values of $\gamma$.

### 2.3.2 Analytical Ansatz for $T=0$ solutions with non vanishing fields

Solutions of the saddle point equations and the free energy, as well as other thermodynamic quantities that can be similarly defined and computed, can be found via an iterative population dynamics procedure described in [23]. However, we are here mainly interested in the behavior of diluted systems at zero temperature, keeping in mind the connection between the search for $T=0$ ground states of the Hamiltonians and that for the solutions of corresponding random combinatorial optimization models [9, 19, 35]. This connections will be further exploited in the following chapters. If we look for $T=0$ solutions with non vanishing fields, we can hope to find analytical results using an Ansatz that supports fields only on integer values. Indeed, the saddle point equation at zero temperature read, after properly taking the $\beta\to\infty$ limit,

$$P(h) = \frac{1}{<k>}\sum_k kc_k\int\prod_{t=1}^{k-1}du_tQ(u_t)\delta\left(h-\sum_t u_t\right) \qquad (2.79)$$

$$Q(u) = \frac{1}{<l>}\sum_l lv_l\int\prod_{t=1}^{l-1}dh_tP(h_t)\delta\left(u-min(1,|h_1|,...,|h_{l-1}|)\prod_t sign(h_t)\right) \qquad (2.80)$$

and it is evident the self consistency of an integer field Ansatz. Moreover, it is clear from the parallel cavity approach[26, 29, 30] that the fields $u$ (also called "cavity biases"), are the information felt by a spin upon the magnetization bias coming from a definite hyper-edge the considered spin belongs to. This bias can be 0 or $\pm1$ at zero temperature. The cavity fields $h$ are then the sum of all biases acting on the spin, after deleting (cavity) one hyper-edge incident on the considered vertex. The situation is exemplified in fig. (2.3.2), a pictorial view of the

effective fields acting on a given hyper-edge $a$ and on a given spin $S$ in a hyper-graph of uniform rank 3: $h_1$ and $h_2$ are the sums of the cavity "biases" $\{u_i^1\}_i$ and $\{u_j^2\}_j$ coming from the blue hyper-edges, and in turn generate a new bias $u_a$ attached to the red hyper-edge. The bias $u_a$ merges following the cavity/replica iterative prescription (also called sum/product rule in computer science) with bias $u_b$ coming from hyper-edge $b$. Together they form field $h$ acting on spin $S$. The fields are then further propagated in the rest of the hyper-graph (white in the picture) and updated through eqs. (2.79) and (2.80). The general rank case is analogous. The integer fields Ansätze read

$$\begin{aligned} P(h) &= \sum_{t=-\infty}^{+\infty} p_t \delta(h-t) && (2.81)\\ Q(u) &= q_+\delta(u-1) + q_-\delta(u+1) + q_0\delta(u) && (2.82) \end{aligned}$$

with $\sum_t p_t = 1$, $\sum_{t>0} p_t = p_+$, $\sum_{l<0} p_l = p_-$ and $q_+ + q_- + q_0 = 1$. The functional saddle point equations turn into a set of self consistency equations for the distribution weights:

$$\begin{aligned} p_t &= \frac{1}{<k>}\sum_k k c_k \sum_{n_+,n_-,n_0\geq 0} \frac{(k-1)!}{n_+!n_-!n_0!} q_+^{n_+} q_-^{n_-} q_0^{n_0} \delta_{n_++n_-+n_0,k-1}\delta_{n_+-n_-,t} && (2.83)\\ p_+ &= \frac{1}{<k>}\sum_k k c_k \sum_{n_+,n_-,n_0\geq 0;n_+>n_-} \frac{(k-1)!}{n_+!n_-!n_0!} q_+^{n_+} q_-^{n_-} q_0^{n_0} \delta_{n_++n_-+n_0,k-1} && (2.84)\\ p_- &= \frac{1}{<k>}\sum_k k c_k \sum_{n_+,n_-,n_0\geq 0;n_->n_+} \frac{(k-1)!}{n_+!n_-!n_0!} q_+^{n_+} q_-^{n_-} q_0^{n_0} \delta_{n_++n_-+n_0,k-1} && (2.85)\\ q_+ &= \frac{1}{2<l>}\sum_l l v_l((p_+ + p_-)^{l-1} + (p_+ - p_-)^{l-1}) && (2.86)\\ q_- &= \frac{1}{2<l>}\sum_l l v_l((p_+ + p_-)^{l-1} - (p_+ - p_-)^{l-1}) && (2.87) \end{aligned}$$

In the spin glass case the last two equations are explicitly symmetric in the exchange $p_+ \leftrightarrow p_-$:

$$q_+ = q_- = \frac{1}{2<l>}\sum_l l v_l (p_+ + p_-)^{l-1} \qquad (2.88)$$

### 2.3.3 The ferromagnetic solution

The saddle point equations of the ferromagnetic case admit a zero energy solution with $p_- = q_- = 0$ other than the trivial paramagnetic one:

$$\begin{aligned} p_0 &= \frac{1}{<k>}\sum_k k c_k (1 - \frac{1}{<l>}\sum_l l v_l (1-p_0)^{l-1})^{k-1}\\ q_+ &= 1 - q_0 = \frac{1}{<l>}\sum_l l v_l (1-p_0)^{l-1}\\ p_+ &= 1 - p_0 && (2.89) \end{aligned}$$

The energy of the ferromagnetic solution is always equal to zero, so the value of the potential returns the zero temperature entropy of the ground states (GS). With a little algebra we get:

$$S_{GS} = \log(2)[-<k>(1-p_0)(1-q_0) + \frac{<k>}{<l>}\sum_l v_l (1-p_0) +$$

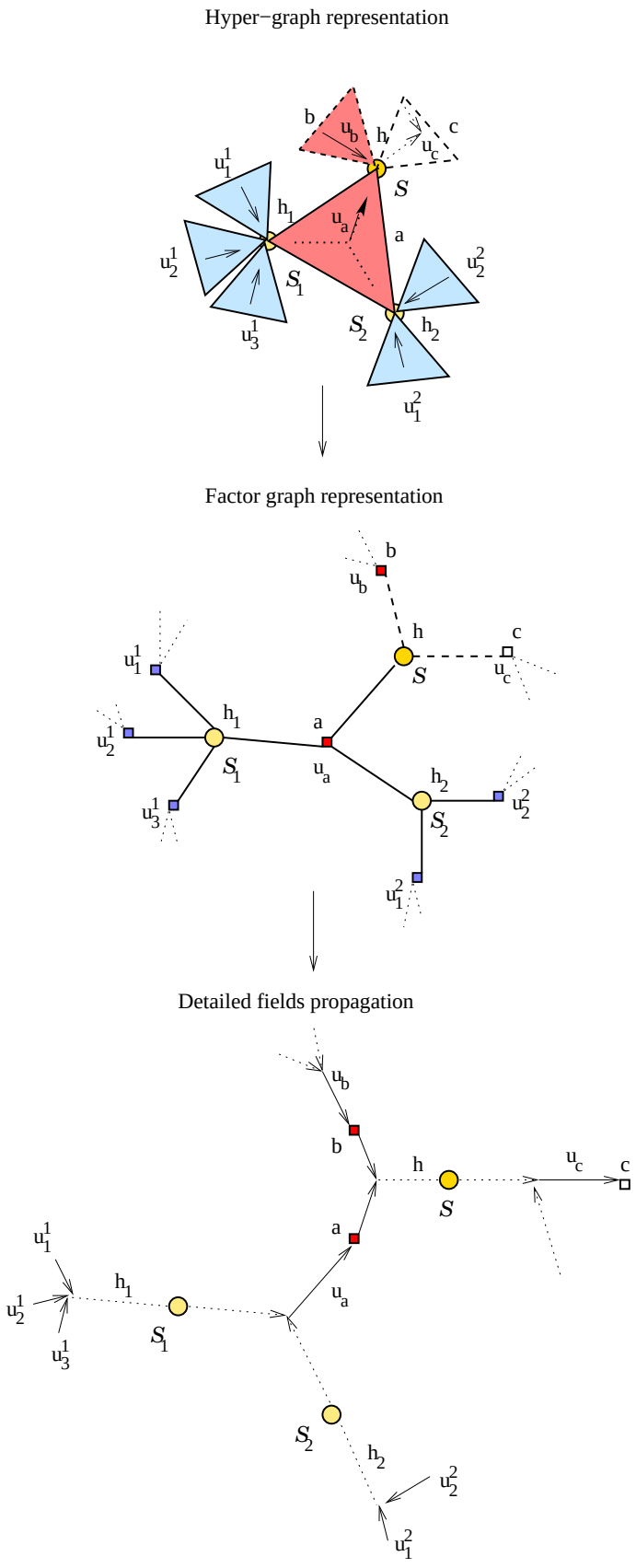



Figure 2.1: Pictorial view of the effective fields acting on a given hyper-edge $a$ and on a given spin $S$ in a hyper-graph of uniform rank 3. The rank 3 was taken as the simplest example of a general-like case.

| $p$ | $\gamma_d$ | $\gamma_c$ |
|---|---|---|
| 2 | 1/2 | 1/2 |
| 3 | 0.818469 | 0.917935 |
| 4 | 0.772278 | 0.976770 |
| 5 | 0.701780 | 0.992438 |
| 6 | 0.637080 | 0.997380 |

Table 2.1: Static and Dynamic Thresholds for the $p$-spin on Poissonian distributed hyper-graphs.

$$\begin{aligned} & < k > (1-q_0) + \sum_k c_k q_0^k - \frac{< k >}{< l >}] \\ = & -\frac{< k >}{< l >} \log 2(1 + \sum_l v_l (l(1-p_0)^l - (1-p_0)^l - l(1-p_0)^{l-1})) + \\ & \log 2 \sum_k c_k (1 - \frac{1}{< l >} \sum_l l v_l (1-p_0)^{l-1})^k \end{aligned} \tag{2.90}$$

The appearance of a solution of (2.89) as a function of a particular values of $< k > / < l > \equiv \gamma_d$ signals the birth of a metastable ferromagnetic state, that becomes thermodynamically favored when $S_{para} = S_{GS}$. Typically, the two entropy lines will cross at a critical value of $< k > / < l > \equiv \gamma_c$. After that value the GS entropy will gradually tend to zero. In the dense hyper-graph limit one retrieves the usual infinite dimensional mean field ferromagnet with zero ferromagnetic GS entropy and a finite number (2) of ground states. An example of this curves can be seen in fig.(2.21) for the Poissonian 3-spin case. In the pure 2-spin case the transition if always of second order, regardless of the graph degree distribution:

$$\gamma_d = \gamma_c = 1/2 \ , \tag{2.91}$$

which is the percolation point. Indeed, the system progressively magnetizes as soon as it percolates, i.e. as soon as a magnetic perturbation can propagate along a finite fraction of the graph.

**A special case: Poissonian random hyper-graphs of average degree $< k >=< l > \gamma$**

This simpler special case can be retrieved putting

$$c_k = \frac{e^{-<l>\gamma} (< l > \gamma)^k}{k!} \tag{2.92}$$

and consequently obtaining

$$p_0 = e^{-\gamma \sum_l l v_l (1-p_0)^{l-1}} \tag{2.93}$$

$$S_{GS} = \log 2 [p_0 (1 - \log(p_0)) - \gamma \sum_l v_l (1 - (1-p_0)^l)] \tag{2.94}$$

In the table 2.1 the values of gamma at the appearance of the ferromagnetic solution and at the ferromagnetic transition are shown for some models of increasing fixed rank $l$.

We called the ferromagnetic thresholds with the same name of the spin-glass ones, because we will see further in the text how the values coincide in the two classes of models. The 3-spin (3-XOR-SAT) [19] and the 2+$p$-spin [21] special cases are contained in these equations. No sign of replica symmetry breaking is present in the pure ferromagnetic models. As we will see in the next section, the physical interpretation of the RSB phenomenon can be explained in the generalized $p$-spin case (but also in a more general framework, for instance in the $K$-SAT case) as a clustezization process in the space of solutions (ground states) of the model. The number of such clusters is in general exponential in $N$ as well as the number of solution within each cluster. Solutions in different clusters are separated by $\mathcal{O}(N)$ spin flips. In the ferromagnetic case, however, there are only ferromagnetic solutions, forming a single clusters. After the transition from the paramagnetic to the ferromagnetic state, there cannot be a further phase transition. We will also see that in the 2-spin-glass case also the SG transition is second order in nature. Clusterization is therefore not possible because the whole system progressively falls in the same GS attraction basin. If the hyergraph is made of a fraction of rank 2 and another of higher rank, the two phenomena can be seen to compete as it is shown in an applied example in chapter 5.

### 2.3.4 The spin-glass states and the RS energy lines

The glass saddle point equations can be further simplified explicitly exploiting the symmetry of the effective fields and biases distributions $P(h)$ and of the $Q(u)$. Everything can be written as a function of the single parameter $p_0$, that counts the fraction of free spins:

$$p_0 = \frac{1}{<k>}\sum_k k c_k \sum_n^{[\frac{k-1}{2}]} (1-\frac{1}{<l>}\sum_l l v_l (1-p_0)^{l-1})^{2n} (\frac{1}{2<l>}\sum_l l v_l (1-p_0)^{l-1})^{k-1-2n} \quad (2.95)$$

$$q_+ = q_- = \frac{1-q_0}{2} = \frac{1}{2<l>}\sum_l l v_l (1-p_0)^{l-1} \quad (2.96)$$

$$p_+ = p_- = \frac{1-p_0}{2} \quad (2.97)$$

For Poissonian hyper-graphs the general replica symmetric result will read, after some algebraic manipulation of the series defining $p_0$ and the general $p_t$[9],

$$p_0 = \exp\left(-\gamma\sum_l l v_l (1-p_0)^{l-1}\right) I_0\left(\gamma\sum_l l v_l (1-p_0)^{l-1}\right) \quad (2.98)$$

$$p_k = p_{-k} = \exp\left(-\gamma\sum_l l v_l (1-p_0)^{l-1}\right) I_k\left(\gamma\sum_l l v_l (1-p_0)^{l-1}\right) \quad (2.99)$$

$$(2.100)$$

The GS energy of the glassy states will be:

$$E_0 = -<k>\frac{(1-p_0)(1-q_0)}{2} + \frac{<k>}{<l>}\sum_l v_l (1-p_0)^l + 2\sum_k c_k \sum_{n_+,n_-,n_0\geq 0} \frac{k!}{n_+!n_-!n_0!}(\frac{1-q_0}{2})^{n_++n_-} q_0^{n_0} min(n_+,n_-)\delta_{n_++n_-+n_0;k} \quad (2.101)$$

[9]Notice that the next expressions are normalized thanks to the property $\sum_{t=-\infty}^{+\infty} I_t(x) = e^x$.

This expression further simplifies in the case of fixed rank models. In particular for the 3-spin the GS energy reads[10]:

$$E_0 = \frac{\gamma(1-p_0)^3}{2} - \frac{3\gamma(1-p_0)^2}{2} p_1 \ . \tag{2.102}$$

However, the above equation leads to wrong predictions: a solution different from the trivial paramagnetic one, $Q_j(u) = \delta(u)\ \forall$ spins $j$, appears at $\gamma_d^{RS} = 1.16682$ with a negative energy. At $\gamma_c^{RS} = 1.29531$ the energy becomes positive, giving a lower bound for the true energy of the system. The *backbone* ($1 - p_0$, fraction of fixed spins) values are respectively $1 - p_d) = 0.52042$ and $1 - p_c = 0.656153$. The values of $\gamma_d^{RS}$ and $\gamma_c^{RS}$ can be variationally refined via the introduction of a fractional valued fields Ansatz as in [9], that can be seen to close on the saddle point equations. In particular, the best "RS" static threshold was ground down to 1.216. This Ansatz has however no physical meaning.

On the other hand, the numerical zero temperature Monte-Carlo simulations indicate that there exits a non-trivial solution from the point $\gamma \sim 0.82$. A careful look at the numerics of the population dynamics solution of the more general 1RSB equations we'll write in the next section shows that the probability distributions of cavity fields $u$ on a given site $i$ indeed take the form

$$Q_i(u) = \eta_i\ \delta(u) + \frac{1-\eta_i}{2}\left[\delta(u-1) + \delta(u+1)\right] \quad , \tag{2.103}$$

with fields distribution scalar weights labeled by the site indices and fluctuating from site to site, and with a fraction $t$ always being trivial, i.e. $\eta_i = 1$ and $Q_i(u) = \delta(u)$. This is the signature of replica symmetry breaking. The positive energy GS corresponds, in the optimization problem interpretation, to the fact that increasing the number of constraints over that of variables there is usually a thershold beyond which some constraints are violated even by the globally best variable assignments. The RS $T = 0$ energy curve for the poissonian 3-spin is shown in fig. (2.2), while in fig. (2.3) the function $G(p_0, \gamma) \equiv p_0 - e^{-3\gamma(1-p_0)^2} I_0(3\gamma(1-p_0)^2)$ in the paramagnetic phase and at $\gamma_d^{RS}$ and $\gamma_c^{RS}$ is shown as a title of example.

## 2.4 The 1RSB calculations

In this section we will focus on the 1RSB solution. When working at $T = 0$ we will disregard the contribution of vanishing fields. As we anticipated in the previous section, the replica symmetric results are correct for the ferromagnetic disordered models, but give wrong quantitative results for the transition thresholds and for the energy in the spin-glass case. To go one further step towards the exact solution of this class of models, we observed good numerical evidence that the replica symmetry does in fact spontaneously break down in a region sufficiently close to the satisfiability threshold. Therefore, the quantitatively wrong results of the RS picture underlie a very different qualitative structure of the phase space.

The 1RSB hypotesis assumes that on a given site $i$, the local cavity fields in the various states, $h_i^a$, are i.i.d. variables taken from the same distribution $P_i(h)$ ([14, 12] and De Dominicis-P. Mottishaw and Wong-Sherrington in [1]). However, the distribution $P_i(h)$ fluctuates from site to site, so that the correct order parameter is a functional $\mathcal{P}[P(h)]$ giving the probability, when one picks up a site at random to find on this site a cavity field distribution $P_i(h) = P(h)$. Moreover the cavity fields and the LGS energies are not correlated (There will however be correlation between the local fields and the energy shifts computed in the cavity approach).

[10] Notice that it will be possible to reproduce the RS results as a limiting case of the 1RSB calculation.

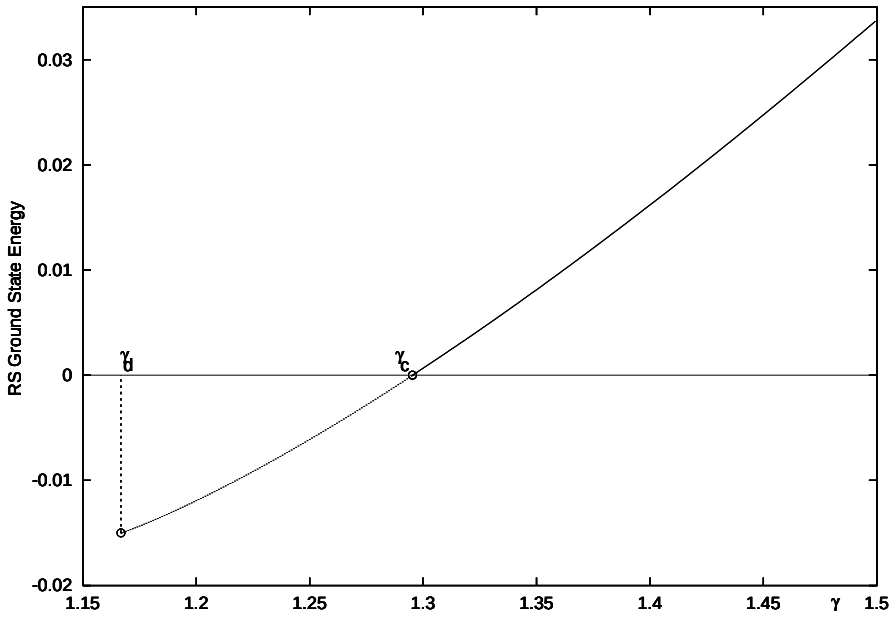



Figure 2.2: Integer fields RS spin-glass energy in the Poissonian 3-spin case. It is negative below $\gamma_c$.

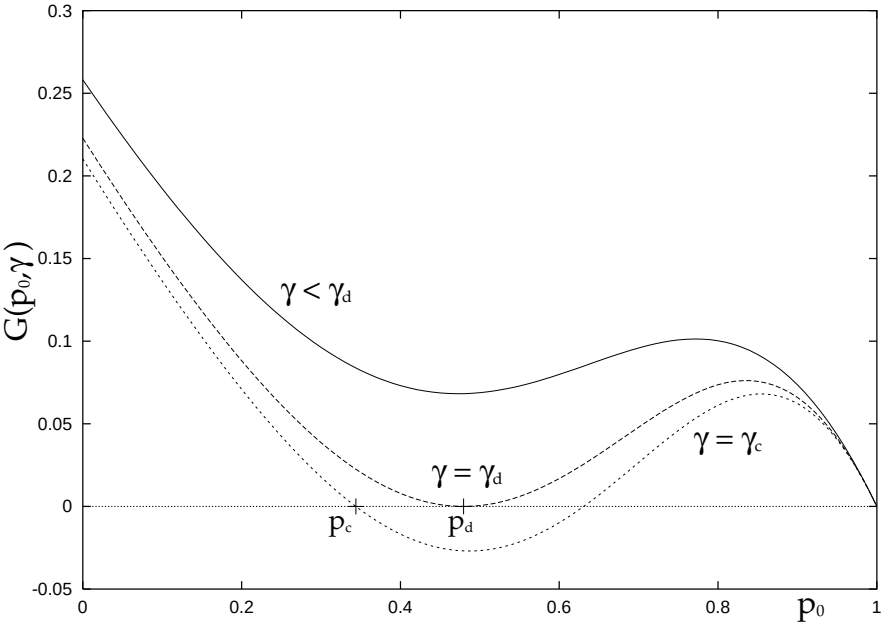



Figure 2.3: RS Self consistent function $G(p_0, \gamma)$ for the fraction $p_0$ of free spins.

The same hypothesis must hold in for the $u$-fields acting on the nodes of the dual hypergraph (check nodes in the factor graph notation, see appendix). Averaging over the sites and assuming the validity of the Parisi breaking scheme [2], the functional orders paramenets can now be written as

$$\rho(\vec{\sigma}) = \int dP\mathcal{P}[P] \int \prod_{g=1}^{n/m} dh^g P_g(h^g) \prod_{g=1}^{n/m} \left( \frac{e^{\beta h^g \sum_{a=1}^{m} \sigma_g^a}}{(2\cosh(\beta h^g))^m} \right) \tag{2.104}$$

$$\hat{\rho}(\vec{\sigma}) = \int dQ\mathcal{Q}[Q] \int \prod_{g=1}^{n/m} du^g Q_g(u^g) \prod_{g=1}^{n/m} \left( \frac{e^{\beta u^g \sum_{a=1}^{m} \sigma_g^a}}{(2\cosh(\beta u^g))^m} \right) \tag{2.105}$$

where the $n$ replicas have been each divided into $n/m$ groups of $m$ replicated spins, and $\sigma_g^a$ represents the $a$-th replica spin belonging to group $g$. $P_g$ and $Q_g$ are local fields probabilities distributions within group $g$. In the RS case there is only one state $\alpha$. The effective fields cannot therefore fluctuate from LGS to LGS and the unique global ground state can be obtained in this framework by fixing the local distribution to be $P_i(h) = \delta(h - \tilde{h}_i)$, so that all the LGS are automatically equal. On a given *site* $i$, this distribution is fixed by the single number $\tilde{h}_i$. The various $\tilde{h}_i$'s are i.i.d., taken from a distribution $P_{RS}(\tilde{h})$ such that

$$\mathcal{P}_{RS}[P(\cdot)] = \int d\tilde{h} P_{RS}(\tilde{h}) \delta\left(P(\cdot) - \delta((\cdot) - \tilde{h})\right) \tag{2.106}$$

Substituted into (2.104) gives back definition (2.64) with

$$\begin{aligned} \tilde{h} &\rightarrow h \\ P_{RS}(\tilde{h}) &\rightarrow P(h) \end{aligned}$$

and therefore satisfies exactly the RS recursion relation. The same considerations as usual apply to the $u$-fields.

Finding a close analytical solution to the self consistent equations (2.40) and (2.41) in the 1RSB case is in general not easy. In order to proceed we first propose a simpler variational approximation of the free-energy (2.39) and of the functional order parameters space. In the general case this Ansatz is NOT exact because neglects correlations between LGS induced by different degree fluctuations from site to site and assumes an extra symmetry that is usually not contained in the model. Nevertheless, it is pointed out in [22] and we will see later in the chapter that it gives very good variational estimates on the transition thresholds and correctly predicts for the models studied the presence of a dynamical region characterized by a non zero value of the complexity. Moreover, for the $p$-spin there exists a class hyper-graphs (namely the fixed degree ones) where the Ansatz self consistently closes under the original complete form (2.39) of the potential, and it gives nearly exact results in the low temperature region in remarkable agreement with the numerics. Overall this simpler variational calculation is important because it introduces some key features of the full solution:

### 2.4.1 The variational factorized Ansatz

In the following propose the use of a simple Ansatz which was first studied in (Wong and Sherrington in [1]), and developed for the Bethe lattice spin glass by Goldschmidt and Lai (in [1]), is named the *Factorized Ansatz*. The underlying idea is to assume that the distributions

$P_i(h)$ are $i$ independent, i.e. that the $\mathcal{P}[P]$ is a functional $\delta$ function

$$\mathcal{P}[P_g] = \delta\left(P_g - P\right) \tag{2.107}$$
$$\mathcal{Q}[Q_g] = \delta\left(Q_g - Q\right) \tag{2.108}$$

The assumption is simple because the order parameter is a single function $P(h)$ and the RS equation are only slightly modified. However one should note that, in general, one may expect a $P_i(h)$ which fluctuates: as anticipated,this is obviously the case whenever the degree fluctuates, but also in the case of the fixed degree, the factorized Ansatz is not necessarily exact. Some special models where the factorized Ansatz gives an exact solution have been studied recently in the context of error correcting codes [154]. Using (2.107) and (2.107) into (2.104) and (2.105) one immediately finds:

$$\begin{aligned} \rho(\vec{\sigma}) &= \prod_{g=1}^{n/m} \rho_g(\vec{\sigma_g}) \\ \rho_g(\vec{\sigma_g}) &= \int dh^g P(h^g) \frac{e^{\beta h^g \sum_{a=1}^{m} \sigma_g^a}}{(2\cosh(\beta h^g))^m} \end{aligned} \tag{2.109}$$

$$\begin{aligned} \hat{\rho}(\vec{\sigma}) &= \prod_{g=1}^{n/m} \hat{\rho}_g(\vec{\sigma_g}) \\ \hat{\rho}_g(\vec{\sigma_g}) &= \int du^g Q(u^g) \frac{e^{\beta u^g \sum_{a=1}^{m} \sigma_g^a}}{(2\cosh(\beta u^g))^m} \end{aligned} \tag{2.110}$$

Notice that eqs. (2.109) and (2.110) give back the RS solution for $m = n \to 0$.

In the replica $n \to 0$ limit we can write:

$$\begin{aligned} \sum_{\vec{\sigma}} \rho(\vec{\sigma})\hat{\rho}(\vec{\sigma}) = \prod_{g=1}^{n/m} (\sum_{\vec{\sigma_g}} \rho_g(\vec{\sigma_g})\hat{\rho}_g(\vec{\sigma_g}) &\sim 1 + \frac{n}{m} \log(\sum_{\vec{\sigma_g}} \rho_g(\vec{\sigma_g})\hat{\rho}_g(\vec{\sigma_g})) \\ \sum_k c_k \log(\sum_{\vec{\sigma}} (\hat{\rho(\vec{\sigma})})^k) &= \frac{n}{m} \sum_k c_k \log(\sum_{\vec{\sigma_g}} (\hat{\rho_g(\vec{\sigma_g})})^k) \\ \sum_{\vec{\sigma}_1,\ldots,\vec{\sigma}_l} \rho(\vec{\sigma}_1)\ldots\rho(\vec{\sigma}_l) \exp(\beta \sum_a \sigma_1^a \ldots \sigma_l^a) &= \frac{n}{m} \sum_{\vec{\sigma_{g,1}},\ldots,\vec{\sigma_{g,l}}} \rho_g(\vec{\sigma_{g,1}})\ldots\rho_g(\vec{\sigma_{g,l}}) \exp(\beta \sum_a {\sigma_{g,1}}^a \ldots {\sigma_{g,l}}^a) \end{aligned} \tag{2.111}$$

where the new $\sigma_g$ vectors are m-dimensional quantities (the replica index runs now from 1 to m) inside each single cluster. Due to cluster equivalence the index $g$ will be dropped in the following. We are left with the following expression for the potential:

$$\begin{aligned} -\beta m F[\beta, m] = & - < k > \log(\sum_{\vec{\sigma}} \rho(\vec{\sigma})\hat{\rho}(\vec{\sigma})) - \beta \frac{< k >}{< l >} + \\ & \frac{< k >}{< l >} \sum_l v_l \log(\sum_{\vec{\sigma}_1,\ldots,\vec{\sigma}_l} \rho(\vec{\sigma}_1)\ldots\rho(\vec{\sigma}_l) \exp(\beta \sum_a \sigma_1^a \ldots \sigma_l^a)) + \\ & \sum_k c_k \log(\sum_{\vec{\sigma}} (\hat{\rho(\vec{\sigma})})^k) \end{aligned} \tag{2.112}$$

at the saddle point, the previous quantity will represent the free energy of a single generic cluster. The stationary condition on (2.112) leads to saddle point equations:

$$\rho(\vec{\sigma}) = \sum_{\vec{\sigma}} \rho(\vec{\sigma})\hat{\rho}(\vec{\sigma}) \frac{1}{< k >} \sum_k k c_k \frac{(\hat{\rho}(\vec{\sigma}))^{k-1}}{\sum_{\vec{\sigma}} (\hat{\rho}(\vec{\sigma}))^k} \tag{2.113}$$

$$\hat{\rho}(\vec{\sigma}) = \sum_{\vec{\sigma}} \rho(\vec{\sigma})\hat{\rho}(\vec{\sigma}) \frac{1}{<l>} \sum_l l v_l \frac{\sum_{\vec{\sigma}_1,...,\vec{\sigma}_{l-1}} \rho(\vec{\sigma}_1)...\rho(\vec{\sigma}_{l-1}) \exp(\beta \sum_a \sigma^a \sigma_1^a ... \sigma_{l-1}^a)}{\sum_{\vec{\sigma}_1,...,\vec{\sigma}_l} \rho(\vec{\sigma}_1)...\rho(\vec{\sigma}_l) \exp(\beta \sum_a \sigma_1^a ... \sigma_l^a)} \quad (2.114)$$

Equations (2.112), (2.113) and (2.114) are homogeneous in the order parameters $\rho(\vec{\sigma})$ and $\hat{\rho}(\vec{\sigma})$ that can be considered as automatically normalized. We recall that now $P(h)$ and $Q(u)$ are single inner cluster distributions. Substituting into the saddle point equations, after a calculation analogous to the RS case we obtain[11]:

$$\begin{aligned} P(h) &= \frac{(2\cosh(\beta h))^m}{<k>} \left\langle \frac{(2\cosh(\beta(u'+h')))^m}{(2\cosh(\beta h')2\cosh(\beta u'))^m} \right\rangle_{u',h'} \cdot \\ &\sum_k k c_k \frac{\left\langle \frac{\delta(h - \sum_{t=1}^{k-1} u_t)}{(\prod_{t=1}^{k-1} 2\cosh(\beta u_t))^m} \right\rangle_{\{u_t\}}}{\left\langle \frac{(2\cosh(\sum_{t=1}^{k} u_t))^m}{(\prod_{t=1}^{k} 2\cosh(\beta u_t))^m} \right\rangle_{\{u_t\}}} \end{aligned} \quad (2.115)$$

$$\begin{aligned} Q(u) &= \frac{2^m}{<l>} \left\langle \frac{(2\cosh(\beta(u'+h')))^m}{(2\cosh(\beta h')2\cosh(\beta u'))^m} \right\rangle_{u',h'} \cdot \\ &\sum_l l v_l \frac{\left\langle \delta(u - \frac{1}{\beta}\tanh^{-1}(\tanh(\beta)\prod_{t=1}^{l-1}\tanh(\beta h_t))) \right\rangle_{\{h_t\}}}{\left\langle (1+\tanh(\beta)\prod_{t=1}^{l}\tanh(\beta h_t))^m \right\rangle_{\{h_t\}}} \end{aligned} \quad (2.116)$$

for the diluted ferromagnet. The spin glass solutions coincide with the previous ones at the symmetric saddle point in the same way as in the RS case. As a function of the effective fields, the potential now reads

$$\begin{aligned} -m\beta F &= -<k> \log \langle A(\beta,h,u)^m \rangle_{h,u} + \sum_k c_k \log \langle B(\beta,u_1,...,u_k)^m \rangle_{u1,...,u_k} + \\ &\frac{<k>}{<l>} \sum_l v_l \log \left( (\cosh\beta)^m \left\langle C^+(\beta,h_1,...,h_l)^m \right\rangle_{h_1,...,h_l} \right) - \beta m \frac{<k>}{<l>} \end{aligned} \quad (2.117)$$

for the ferromagnet and

$$\begin{aligned} -m\beta F &= -<k> \log \langle A(\beta,h,u)^m \rangle_{h,u}) + \sum_k c_k \log \langle B(\beta,u_1,...,u_k)^m \rangle_{u1,...,u_k} + \\ &\frac{<k>}{2<l>} \sum_l v_l \left[ \log \left( (\cosh\beta)^m \left\langle C^+(\beta,h_1,...,h_l)^m \right\rangle_{h_1,...,h_l} \right) + \right. \\ &\left. \log \left( (\cosh\beta)^m \left\langle C^-(\beta,h_1,...,h_l)^m \right\rangle_{h_1,...,h_l} \right) \right] - \beta m \frac{<k>}{<l>} \end{aligned} \quad (2.118)$$

for the spin glass, with:

$$\begin{aligned} A(\beta,h,u) &= \frac{1+\tanh(\beta h)\tanh(\beta u)}{2} \\ B(\beta,u_1,...,u_k) &= \frac{2\cosh(\beta\sum_{t=1}^k u_t)}{\prod_{t=1}^k 2\cosh(\beta u_t)} \\ C^{\pm}(\beta,h_1,...,h_l) &= 1 \pm \tanh(\beta)\prod_{t=1}^{l}\tanh(\beta h_t) \end{aligned} \quad (2.119)$$

[11] From now on we will often use the notation $\int dx P(x)(\cdot) \equiv \langle(\cdot)\rangle_x$.

### Ferromagnetic metastable states and spin-glass LGS symmetry

It could seem useless to write the 1RSB expressions also for the ferromagnetic model, since we know that in this case the RS solution is correct for the GS. Forcing the 1RSB factorized Ansatz on the ferromagnet physically means that we look at the structure of the positive energy metastable states. We did it to stress the fact that the saddle point equations of the two models admit a *common symmetric solution* also in the non paramagnetic phase. The expression for the free-energy of the two models coincide at this saddle point. However, the symmetric one is NOT the lowest energy GS solution of the ferromagnetic model, which always have zero reference energy, but it describes positive energy metastable states. On the other hand, these metastable states coincide with the LGS of the spin-glass in the disordered phase. This property is a peculiar symmetry of the $p$-spin model and will give us an alternative way to compute the exact complexity without resorting to the complete 1RSB solution.

### The zero temperature phase

If we adopt zero temperature Ansätze (2.81), (2.82) and keep

$$m\beta = y \tag{2.120}$$

finite, we get the following saddle point equations:

$$q_0 = 1 - \frac{1}{\sum_l l v_l \frac{1}{\Omega_l}} \sum_l l v_l \frac{1}{\Omega_l} (1-p_0)^{l-1} \tag{2.121}$$

$$p_0 = 1 - \frac{2\sum_k k c_k \frac{1}{\Xi_k} \sum_{n_+>n_-,n_0\geq 0} \frac{(k-1)!}{n_+!n_-!n_0!} q_+^{n_+} q_-^{n_-} q_0^{n_0} e^{-2yn_-} \delta_{n_++n_-+n_0,k-1}}{\sum_k k c_k \frac{1}{\Xi_k} \sum_{n_+,n_-,n_0\geq 0} \frac{(k-1)!}{n_+!n_-!n_0!} q_+^{n_+} q_-^{n_-} q_0^{n_0} e^{-2ymin(n_+,n_-)} \delta_{n_++n_-+n_0,k-1}} \tag{2.122}$$

$$p_\pm = \frac{1-p_0}{2} \tag{2.123}$$

$$q_\pm = \frac{1-q_0}{2} \tag{2.124}$$

with

$$\Omega_l = 1 + \frac{e^{-2y}-1}{2}(1-p_0)^l \tag{2.125}$$

$$\Xi_k = \sum_{n_+,n_-,n_0\geq 0} \frac{k!}{n_+!n_-!n_0!} q_+^{n_+} q_-^{n_-} q_0^{n_0} e^{-2ymin(n_+,n_-)} \delta_{n_++n_-+n_0,k} \tag{2.126}$$

and the expression for the potential can be written in terms of $y$ as:

$$F(y) = \frac{1}{y}\left[ < k > \log(1 + \frac{e^{-2y}-1}{2}(1-q_0)(1-p_0)) - \frac{< k >}{< l >} \sum_l v_l \log \Omega_l - \sum_k c_k \log(\Xi_k) \right] \tag{2.127}$$

The choice (2.120) is necessary to find a solution that is self consistent and in best possible agreement with numerical simulations. In fact, the scaling parameter $y$ has a much deeper physical meaning that will be elucidated in the following.

The stationary conditions also admit a completely paramagnetic $p_0 = 1$, $q_0 = 1$, $F = 0$ solution that puts us back into the paramagnetic phase. In the limit $y \to 0$[12] one retrieves

[12] This limit can indeed be read as $m \to n$.

the RS results. In order to find the physical value of the free-energy, expression (2.127) for the potential has to be further maximized with respect to the parameter $y$. The study of the potential $F(y)$ allows us to reach a qualitative understanding of the typical phase diagrams, even though the exact nature of the symmetry phenomena is not properly caught by the factorized Ansatz. The following picture will therefore retain its validity in the complete 1RSB solution.

### 2.4.2 The construction of the phase diagram

In order to build the zero temperature phase diagram of this class of models we have to make case by case a sensible choice of the control parameters[13]. A priori the control parameters space is very large, including the values of all the fractions $\{c_k\}$ and $\{v_l\}$. However, typically only a small number of this quantities plays a relevant role: the dilution parameter $\gamma =< k > / < l >$[14], the fraction of 2-edges $v_2$, the quotient $v_2/v_3$[15] and few other collective combinations on the rank and degree distributions weights.

If the fraction $v_2$ is bigger than a certain critical value depending on the remaining order parameters, the model is found to be Viana-Bray like. In the ferromagnetic case, the transition is a continuous one from the trivial paramagnetic to the magnetized phase. In the spin-glass, the glassy phase most probably is reached through a continuous $\infty$-RSB cascade. The onset of the continuous transition is set by the 2-loops percolation condition of the fraction of rank 2 graph merged in the whole topological structure. There are no precursor phenomena in neither of the transitions, which means no formation of finite energy metastable states in the ferromagnet and no LGS complexity in the spin-glass. From the physical point of view, the 1RSB picture - even in the general treatment - is therefore only an approximation of the Viana-Bray spin-glass behavior. From the computational complexity side, however, the GS search is simpler because of the absence of metastable states of Hamming distance $\mathcal{O}(N)$. The zero temperature related 2-XOR-SAT like problems are Polynomial also in the UNSAT phase and they present no hard region before the SAT/UNSAT transition.

Whenever a tricritical point [11, 21] condition can be met[16], the models undergo a crossover into a phase diagram where the transition are discontinuous: paramagnetic/1RSB or paramagnetic/first order ferromagnetic respectively. In these cases overwhelming evidence for a precursors/dynamical region has been observed. From the computational complexity point of view, the presence of a dynamical region coincides with typical (exponential or polynomial, depending on the problem class) slowing down in the solution times of the search algorithms. From the physics point of view, precursors are LGS that appear with a higher energy but exponential in number, so that the system freezes without reaching the still present $E = 0$ true GS essentially for entropic reasons. In the optimization problem these states correspond to quasi optimal solutions with deep enough basins of attraction to trap the searching procedure. For some particular choices of the rank and degree distributions the condition for the existence of the tricritical point cannot be fulfilled. In those cases intermediate models can be explored, that show both a dynamical region and a continuous phase transition, followed by a further discontinuous jump. Examples of these somehow pathological cases are shown in the first section of chapter 5. The dynamical region is denoted by the hyper-graph diluteness interval $[\gamma_d, \gamma_c]$.

[13] This is true in general and has to be done also in the RS and in the complete 1RS case.

[14] often denoted with $\alpha$ in the literature, for instance in the $K$-SAT case.

[15] The importance of this quotient will be stressed in two examples in chapter 3 and 5.

[16] We anticipate the condition to be $v_2 = 3v_3 = 1/(2\gamma_{tricritical})$ in the generalized $p$-spin case.

**The complexity**

The complexity $\Sigma(e,\gamma)$ was defined as the logarithm of the number of the LGS of a given energy density $e$ at a value of the diluteness $\gamma$, divided by the number of the variables $N$. It is a crucial thermodynamical quantity[17] whose presence tell us we are in a symmetry broken phase. The explicit computation of $\Sigma(e,\gamma)$ at $T=0$ has been carried out in [24, 30] for the Viana-Bray and the 3-SAT model. The case of the generalized $p$-spin is completely analogous and we refer to those papers for details. It turns out that the zero temperature complexity can be calculated as the Legendre transform of the potential $F(y)$. Indeed, the $T\to 0$ limit of the discussion in [7] gives

$$e^{-yF(y)} = \int de\mathcal{N}(e,\gamma)e^{ye} \ , \tag{2.128}$$

where we have already defined the number of metastable states at a given energy density $e$ and tuning parameter $\gamma$ in terms of the complexity $\Sigma(e,\gamma)$ via

$$\mathcal{N}(e,\gamma) \equiv e^{-N\Sigma(e,\gamma)} \ . \tag{2.129}$$

therefore we obtain, retaining only dominant contributions at the saddle point in $y$ in the large $N$ limit,

$$\Sigma(e,\gamma) = ye - yF(y) \tag{2.130}$$

$$e = \frac{\partial yF(y)}{\partial y} \tag{2.131}$$

$$y = \frac{d\Sigma(e,\gamma)}{de} \tag{2.132}$$

at fixed $\gamma$. From the previous equations we can also write

$$\Sigma(y,\gamma) = y^2\frac{\partial F(y)}{\partial y} \ , \tag{2.133}$$

that is the $T=0$ correct limit of the construction of [7]. We see eventually the physical meaning of the scaling parameter $y$ as the derivative of the complexity with respect to a variation of the energy of the local ground states. This quantity therefore regulates the quantity of metastable states one is bound to meet varying the energy. The distribution density of these states turn out to determine a level crossing phenomenon under the 1RSB cavity equations iteration. Indeed, one of the *postulates* [24] of the cavity method that was not clearly yet stated is that the energies $E_0^\alpha$ of the $\alpha$-LGS of low energy (near to that of the GGS) are assumed to be i.i.d. variables with a distribution given by a Poisson process of density

$$\rho(E_0) = \exp(y(E_0 - E_{ref})) \tag{2.134}$$

where $E_{ref}$ is a reference energy, which is near to the GGS energy, and $y$ must be equal to our replica scaling parameter in order for the two methods to give the same results in the 1RSB case. During the iteration of the cavity equations, the local energy shifts can therefore induce a level crossing, and the fields distributions have to be re-weighted accordingly. Since the level crossing dynamics will be driven by the geometry of the phase space which in turn is determined by (2.134), we see how the scaling parameter $y$ is so important. Its role is automatically taken

[17] of not trivial definition, since the notion of LGS in disordered systems is still not completely clear.

in the correct account by Parisi's RSB prescription in replica method, where the parameter $m$ adds an extra variational dimension in the variational space and maximizing the potential with respect to $m$ essentially corresponds to choosing the best replica symmetry broken states distribution picture. Lowering the temperature the replica states landscape changes and $m$ must follow accordingly. Since the equations for the potential can be written in terms of $m\beta$ in the low temperature limit, is is natural to explore the possibility of $m$ scaling as $1/\beta$. In the cavity picture there is no initial notion of RSB, that has to be introduced via an *ad hoc* postulate. However, as we have seen, this allows to clarify the physical meaning of this $1/\beta$ scaling.

How can one practically draw the phase diagram from the knowledge of the potential (2.127)?

- In general, for regions of high hyper-graph diluteness (very low $\gamma$), $F(y)$ is equal to zero: the system is paramagnetic and the only possible non trivial contribution to the entropy are given by the presence of vanishing fields. As it was already mentioned in the RS section, this is however not the case of the $p$-spin model, where it is possible to prove [18] that the paramagnetic phase is always trivial. This result is in perfect agreement with numerics.

- Entering the dynamical region, $F(y)$ is negative for any value of $y$ and monotonically increasing, with typical shape shown in fig. (2.4). Its maximum tends back to zero in the limit $y \to \infty$. In this limit, eqs. (2.121)-(2.124) reduce to a non trivial symmetric glassy solution with $p_0$ , $q_0 > 0$ that we will explicitly write for the case of the Poissonian 3-spin in the following. This solution is in fact not exact, because it disregards site to site fluctuations that lead to a non zero fraction of spins $i$ with free fields (i.e. with $p_0^i = q_0^i = 1$) that are numerically observed solving the full equations via a population dynamics introduced in [23, 24]. Indeed, numerically is well observed an adiabatic like separation in the degrees of freedom of some spins compared to others, as it was documented in [18]. This is reflected in the fact that not all spins have the same fields distributions, but the same distribution of fields distributions. This concept is at the basis of the complete 1RSB picture and will be made clear in the next section. Nevertheless, we can here compute a variational bound complexity at energy density $e = 0$, even if its nature is not completely clear in the variational Ansatz context.

  - $\Sigma(e = 0)$ is found to be non zero in $[\gamma_d, \gamma_c]$, monotonically decreasing with $\gamma$. However, the spin-glass has already an exponential number of LGS, even if in this phase $e = 0$ and therefore they are also GGS.
  - At $\gamma = \gamma_d$ the complexity is non zero *only* for $e = 0$, which means that LGS appear initially as GGS, and the search algorithms, even if trapped in one of them, still can solve the problem.
  - If $\gamma_d < \gamma < \gamma_c$, a non zero energy density complexity interval forms, s.t. $\Sigma(e) > 0$ for $e \in [0, e_d]$. The dynamical region is therefore not only characterized by a sudden clustering of ground states: at the same point an exponential number of metastable states appear. Such states are expected to act as a trap around $e_d > 0$ sub-optimal solutions for local search algorithms, causing an exponential slowing down of the

[18] Calculations have been done but are not shown in this thesis.

search process. This picture applies for instance to simulated annealing or greedy procedures based on local information.

- At $\gamma = \gamma_c$ the zero energy density complexity goes to zero. This means that the number of GGS is not exponential any more and the associated combinatorial problem has no zero cost solutions in the typical case. There could be of course *rare satisfiable instances events*, such that the probability of finding non zero energy goes exponentially to zero with $N$, but is strictly zero only in the thermodynamic limit. These rare events can play a relevant role in practical design of search solution procedures in [85, 86, 87, 88], but they will not be studied here. The $\gamma = \gamma_c$ point corresponds to the ferromagnetic first order transition in the unfrustrated model the crossing points of the $S_{ferro}$ and the $S_{para}$ analytical lines of fig (2.21).

- For $\gamma > \gamma_c$ the maximum of $F(y)$ is positive and it is reached for a finite value $y^*$ of the scaling parameter. This corresponds to a positive value of the lowest energy: it is no longer possible to satisfy simultaneously all the hyper-edges constraints.

As will have said, it is possible to calculate the complexity $\Sigma(e)$ of states with $e > 0$ by the Legendre transform of the potential $F(y)$. $\Sigma(e)$ is found to be typically non negative inside an energy density interval $[e_c, e_d]$[19]. This corresponds to the *dashed* regions of the curves for the potential $F(y)$ in fig. (2.4)-**A**, where $dF(y)/dy < 0$. An energy therefore gap opens up, s.t. $e_c > 0$ and increases with $\gamma$.

**Explanation of fig. (2.4):**

fig.**A**: Qualitative typical scheme of the potential $F(y)$ and behavior. The picture reproduces the RS limit along the line $y = 0$. The 1RSB potential curves tend to the RS result in this limit, and correspond to the maximum of the potential only on the lower dimensional $y = 0$ line. Enlarging the variational space introducing $y$, and therefore taking into account the complexity, gives the blue point better results. We will argue in the next section that in the complete 1RSB picture this variational space is indeed large enough to find the exact solution for the $p$-spin model. Recently it has been shown [30] that this could be the case also for more complicated models. In order to obtain the results for non negative complexity one only needs the function $F(y)$ in the left region where $dF(y)/dy \geq 0$. fig.**B**: $\Sigma(e)$ at increasing values of $\gamma$. The meaning of $e_d$, $e_c$ and $\hat{\gamma}$ is explained in the text. Regions of negative complexity are not shown. The complexity shows a somewhat unusual two branched form: the lower branch is concave and goes from $e = e_c$, the ground state (GGS) energy where the complexity vanishes, to $e = e_d$, the maximal energy beyond which one does not find any local ground state, which corresponds to a value $y = y^M$. It corresponds to the black continuous regions of the $F(y)$ curves in **A** The upper branch is convex, and interpolates between the RS solution (obtained at $y = 0$) and the maximal complexity point (obtained at $y = y_M$). This second branch does not seem to have a direct physical interpretation and in this context can be simply ignored. On the other hand, it must be present insofar as the $y \to 0$ limit of our RSB solution gives back the RS solution (the green arrow in **A** represent the branch of the potential curves that tend to the red RS subspace, where each point is picked by a particular value of $\gamma$). Clearly a better understanding of this second branch would be welcome. fig.**C-D**: $e_d$, $e_c$,$\Sigma(e_d)$, $\Sigma(e_c)$ as a function of $\gamma$. This

[19] in the interval $[0, e_c)$ $\Sigma(e) < 0$. This means that the probability of finding a state of energy density within that interval is exponentially small in $N$. $\Sigma(e_c) = 0$.

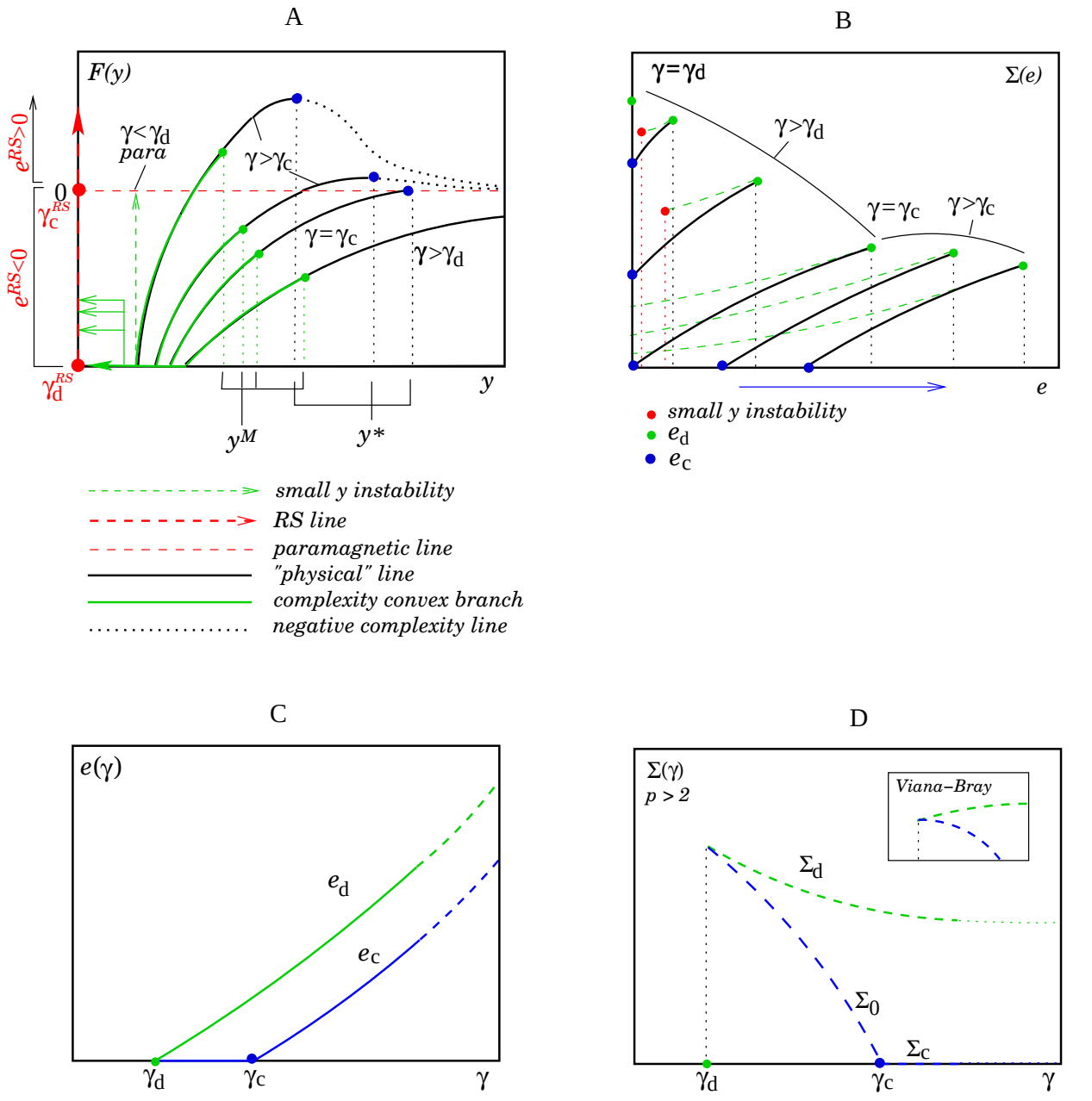



Figure 2.4: Typical behavior of the Potential $F(y)$ and derived thermodynamical quantities in the 1RSB picture. We refer to the text for an exhaustive explanation.

is the typical picture given by the factorized Ansatz in the fixed degree $p$-spin. In the case of fluctuating degree, $\Sigma(e_d)$ is found to increase with $\gamma$ also for $p > 2$, as in the case of the fixed degree Viana-Bray model. It has not been checked yet whether this is an artifact of the factorized approximation. Let's compare the two models at the same fixed $l$ and such that the average degree $l\gamma$ of the Poissonian case is equal to $k$ of the fixed degree one: for low $\gamma$ the high fraction of "free" spins in the fluctuating degree case has a large weight and therefore contributes a lot to lowering the configurational entropy. This effect is more pronounced for large $l$. Increasing $\gamma$, the fluctuating model tends to the fixed degree one, and both of them to the fully connected $l$-spin in the $\gamma \to \infty$ limit. Therefore, the lowering effect on the complexity of the free spins diminishes and the total value of the threshold energy complexity increases to saturate the fixed degree upper bound. The picture is qualitatively shown in fig .(2.6).

It is important to notice that in the dynamical region the $y \to \infty$ limit means that the energy/complexity curves have infinite derivative in $e = 0$. This means not only that the number of metastable states is exponential, but that its relative variation with energy is infinite when they appear. This property follows directly from the definition of complexity and from the constraint of having a finite value of it already at zero energy density. This enormous explosion of states is however surprising. It indicates a critical transition in complexity characterized by an infinite *"suscettivity"* of the number of GS to an infinitesimal change in energy. Therefore $e = 0$ is an critical instability point of the system. In the dynamical region, this instability point is not separated from the higher energy metastable states. The number of GGS is large, but nevertheless the number of LGS at energy density just above zero is exponentially larger. This pictures recalls qualitatively the formation of scale-free domains at any size at the critical point in continuous phase transitions. Above $\gamma_c$, on the other hand, even if the fluctuations in the *relative* number of metastable states are large, they loosely speaking *explore* an almost empty space because the total number of states is $o(1)$. Because of this disconnectedness property of the configurational space at energy below $e_c$, In the thermodynamic limit (and for all practical purposes for very large single instances in combinatorial optimization problems), the system does not feel the presence of the instability because it is in a region that can be explored only by means of *rare events*. At $\gamma_c$, the typical number of GGS is $\mathcal{O}(1)$, so it is clear that the jump must be infinite at $e = 0$, since we have

$$y^*(\gamma_c) \sim \frac{1}{\mathcal{O}(N^2)} \frac{d\mathcal{N}(e)}{de}_{|e=0} \tag{2.135}$$

and the variation of states must be exponential in order to have finite complexity at $e > 0$. The situation is shown in the blow up in fig. (2.5)and in figs. (2.8) and (2.9), where the exponential explosion in the number of metastable states is underlined. In those "pathological" cases where a continuous transition appears inside the dynamical region, the zero energy complexity drops suddenly to zero as shown in fig (5.9). Some examples of energy/complexity curves have been computed in fig. (2.7) for particular values of $\gamma$ in the Poissonian 3-spin. Analogous curves in the context or error correcting codes are shown in chapter 5. In regions of very high $\gamma$, it might occur that $e_c \to e_d \to 0$ and the number of LGS *might* cease to be exponential for all energies. Clusters of sub-optimal solutions could be no more separated by a Hamming distance of order $N$ In fact, in that region the validity of the 1RSB picture for $\gamma >> \gamma_c$ is still uncertain. This in particularly could be true in more complicated models as the $K$-SAT, as it has been noted in [89, 90]. The 1RSB picture, however, gives a bound on the asymptotic values of the complexity, in case no further symmetry breaking was present increasing graph density.

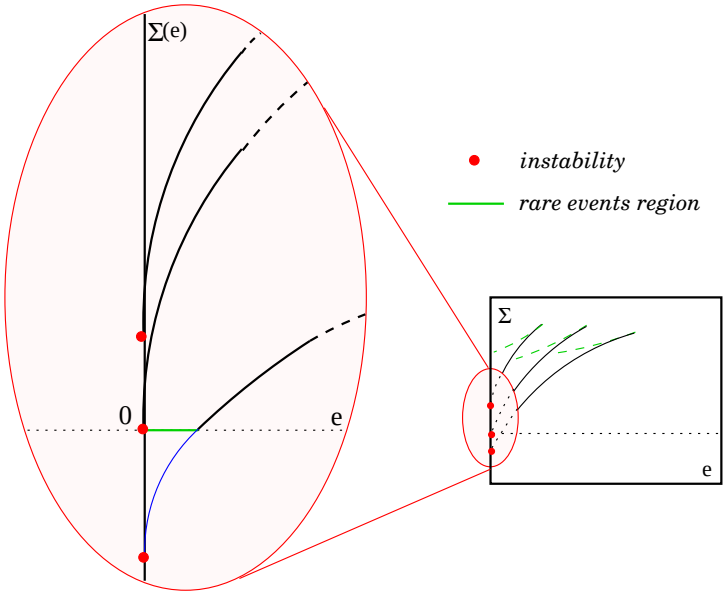



Figure 2.5: $\Sigma(e)$ close to $e_c = 0$ in the dynamical region.

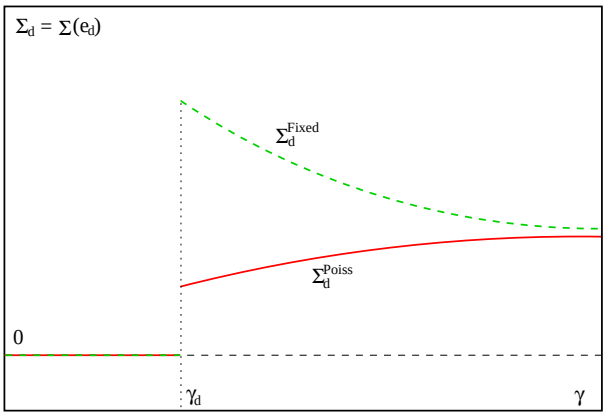



Figure 2.6: $\Sigma(e_d)$ as a function of $\gamma$ for the Poissonian fluctuating and the fixed degree at equal $l > 2$ in the factorized Ansatz picture.

**3-spin with Poissonian degree distribution**

In the case of Poissonian degree distributions, the summations into the saddle point equations and the free energy can be explicitly done, leading to more compact expressions. This can be done in general for any degree $k$, but we will here only give the expressions for the 3-spin ($< k >= 3\gamma$), without loosing generality. After some algebra one finds

$$p_0 = \frac{I_0(z_1)}{I_0(z_1) + 2\sum_{k>0} I_k(z_1)e^{y\cdot k}} \tag{2.136}$$

$$p_l = = p_{-l} = \frac{I_l(z_1)e^{y\cdot l}}{I_0(z_1) + 2\sum_{k>0} I_k(z_1)e^{y\cdot k}} \tag{2.137}$$

$$z_1 = \frac{3\gamma}{\Omega}(1-p_0)^2 \tag{2.138}$$

$$\Omega = e^y - (1-p_0)^3\sinh(y) \tag{2.139}$$

for the saddle point equations and

$$F(y) = -\frac{1}{y}(\gamma\log\Omega - \log\Lambda - z_1\cosh(y) - z_1\sinh(y)p_0) + \gamma \tag{2.140}$$

$$\Lambda = \frac{1}{I_0(z_1) + 2\sum_{k>0} I_k(z_1)e^{y\cdot k}} \tag{2.141}$$

for the potential. $I_l(x)$ is the modified Bessel function of $l$-th order. Following the previous prescription on the potential, in the $y^* = \infty$ limit eq. (2.136) reduces to

$$p_0 = \frac{1}{2e^{\frac{3\gamma(1-p_0)^2}{2-(1-p_0)^3}-1}}\ , \tag{2.142}$$

with $\lim_{y\to\infty} F(y) = 0$. Besides the trivial paramagnetic one, equation (2.142) admits a symmetric zero energy non trivial solution in the dynamical region $[\gamma_d, \gamma_c] = [0.851428, 0.939083]$. One can explicitly check that no other non trivial $y^* < \infty$ solutions are stable in this region. At $\gamma_d = 0.851428$, the transition is discontinuous and a finite back-bone suddenly appears with weight $1 - p_0 = 0.798335$. At $\gamma_c$, the predicted value for the backbone is $1 - p_0 = 0.9309$. This means that in the factorized Ansatz approximation more than 93% of the spins are fixed with probability 1 at the transition, for the 3-spin model. These values are upper bounds for the true values, that will be retrieved via the complete 1RSB calculation. In picture (2.7) the behavior of the $\Sigma(e,\gamma)$ and $F(y)$ for some examples around the static transition is shown. One could argue that the natural scaling to correctly focus on the critical behavior of the potential curve around the transition is given by the change of variable $t \equiv e^{-y}$. The plot of $F(t)$ is also shown as a title of example. From that plot the singularity in the $y \to \infty \Longleftrightarrow t \to 0$ is made evident. In the plots of the potential, the occurrence of the static transition point is better seen rescaling the $y$ axis as $t \equiv e^{-y} \in (0,1)$. Notice how for values of $y$ too small the solution is unstable with respect to the paramagnetic one. In particular this implies the instability of the RS solution ($y \to 0$).

### 2.4.3 On the physical *ir*-relevance of fractional fields

The zero temperature saddle point equations for the potential admit a closed solution also if the effective fields $h$ have rational support. This solutions can be seen as an improvable RS scheme

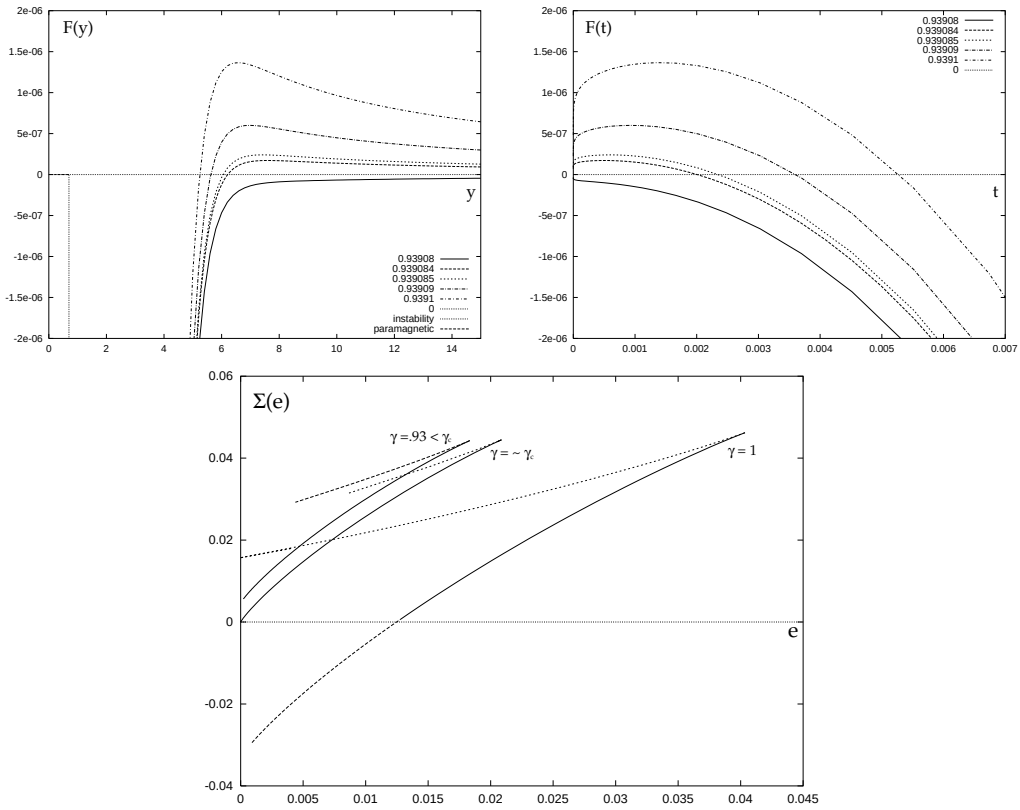



Figure 2.7: $\Sigma(e,\gamma)$, $F(y)$ and $F(t)$ for the 3-spin model around the variational static threshold.

and can be proved to give variational results with the technique of chapter 6. Solutions of such a kind have been explored in the past for the random 3-SAT model [9], and very recently in a RS approach[20] to the graph coloring problem in [57]. However, it is clear from the physical nature of the $u$ and $h$ fields that their non vanishing part should be integer at zero temperature. Nevertheless, since we are working in a variational context, the attempt to refine the threshold values via rational fields is legitimate. Let us again specialize to the Poissonian 3-spin case. If we introduce a fractional field Ansatz as in [9, 11]

$$P_r(h) = \sum_{l=-\infty}^{+\infty} p_{\frac{l}{r}} \delta\left(h - \frac{l}{r}\right) = P_r(-h) \tag{2.143}$$

bypassing the introduction of local $u$-fields saddle point equations read

$$p_{\frac{l}{r}<1} = \Xi e^{g_0(y)} \eta_l \tag{2.144}$$

$$\Xi = \frac{e^{-g_0(y)}}{\eta_0 + 2\sum_{l>0}\eta_l} \tag{2.145}$$

$$\eta_l = e^{\frac{yl}{r}} \int_0^{2\pi} \frac{d\theta}{2\pi} \cos(l\theta) e^{\sum_{j=1}^{r} g_{\frac{j}{r}}(y) cos(\theta j)} \tag{2.146}$$

$$g_0(y) = \frac{3\gamma}{\Omega}(1-(1-p_0)^2) \tag{2.147}$$

[20]At the beginning of this thesis the RS analysis with fractional fields has been extensively carried out with pedagogical purpose also for the 3-spin and the 3-hyper-graph bicoloring problem, with results analogous to the ones in [9] and that are not reported here.

$$g_{\frac{l}{r}<1}(y) = \frac{12\gamma}{\Omega}(p_{\frac{l}{r}} + 1 - p_0 - 2\sum_{l'=1}^{l} p_{\frac{l'}{r}})p_{\frac{l}{r}}e^{-\frac{yl}{r}} \quad (2.148)$$

$$g_1(y) = \frac{12\gamma}{\Omega}(\frac{1-p_0}{2} - \sum_{l=1}^{r-1} p_{\frac{l}{r}})^2 e^{-y} \quad (2.149)$$

$$\Omega = 1 - \frac{(1-p_0)^3}{2} + \frac{1}{2}\sum_{l=1}^{r}((1-p_0-2\sum_{j=1}^{l-1} p_{\frac{j}{r}})^3 - (1-p_0-2\sum_{j=1}^{l} p_{\frac{j}{r}})^3)e^{-\frac{2ly}{r}} \quad (2.150)$$

where $r$ is a *filter* parameter that can be arbitrarily increased to thicken the fields sieve. As it turns out in the calculation (analogously to the RS case), only the first $r$ weights are needed to write the potential

$$F(y) = -\frac{1}{y}(\gamma\log(\Omega) - 3\gamma + \Xi) + \gamma \quad (2.151)$$

Analogous equations can be written in the general $l$-spin case, the bicoloring and the random 3-SAT models and - in a much less compact form - for generic choices of the generating functions (2.5) and (2.6). However, we won't further write down the equations because fractional fields do not show to improve the optimal saddle point value of (2.127). Numerically, no solutions seem to be stable at zero temperature other than the integer fields one. This is also the case for the other studied models: Bicoloring over 3-hyper-graphs and random 3-SAT. This result is different from the RS case, where in fact the fractional Ansatz gave better empirical threshold values. This is a hint for the fractional Ansatz to be a sign of RSB phenomena. Since we are already working here in a RSB framework, it is therefore plausible for this spurious solution not to be stable any more.

### 2.4.4 A particular exact case: hyper-graphs with fixed degree distribution

The case of fixed rank and degree hyper-graphs[21] is a peculiar one, because all spins are topologically equivalent on the hyper-graph, leading to a factorized closed form of the complete saddle point equations. This is not peculiar of $p$-spin like models, but can be extended, as we will see for the bicolorig problem, to other systems of spins on a random graph with fixed rank and degree. Notice that strictly speaking the solution is still non exact, because it neglects site to site fluctuations that may depend on the state of the system and not on its topological properties. However, it gives results [22] in very good agreement with numerics. In this case the exact equations (2.40) and (2.41) can be written in a factorized and normalized closed form as

$$\rho(\vec{\sigma}) = \frac{(\hat{\rho}(\vec{\sigma}))^{k-1}}{\sum_{\vec{\sigma}}(\hat{\rho}(\vec{\sigma}))^{k-1}} \quad (2.152)$$

$$\hat{\rho}(\vec{\sigma}) = \sum_{\vec{\sigma}_1,\ldots,\vec{\sigma}_{l-1}} \rho(\vec{\sigma}_1)\ldots\rho(\vec{\sigma}_{l-1})\exp(\beta\sum_a \sigma^a\sigma_1^a\ldots\sigma_{l-1}^a - 1) \quad (2.153)$$

[21] or the slightly more general version of a degree distribution with constant sub-degrees, taking advantage of the alternative formalism of appendices C.

where $\hat{\rho}(\vec{\sigma})$ has to be normalized: $\hat{\rho}(\vec{\sigma}) \to (2\cosh(\beta)^{-m}\hat{\rho}_{norm}(\vec{\sigma})$ and $\hat{\rho}_{norm}(\vec{\sigma}) \to \hat{\rho}(\vec{\sigma})$. After some algebra one obtains:

$$-m\beta F(\beta, m) = (1 - \frac{k(l-1)}{l}) \log(\sum_{\vec{\sigma}} \hat{\rho}(\vec{\sigma})^k) + \frac{k(l-1)}{l} \log(\sum_{\vec{\sigma}} \hat{\rho}(\vec{\sigma})^{k-1}) \tag{2.154}$$

with:

$$P(h) = \frac{(2\cosh(\beta h))^m \left\langle \frac{\delta(h - \sum_{t=1}^{k-1} u_t)}{\prod_{t=1}^{k-1}(2\cosh(\beta u_t))^m} \right\rangle_{\{u_t\}}}{\left\langle \frac{(2\cosh(\beta \sum_{t=1}^{k} u_t))^m}{\prod_{t=1}^{k}(2\cosh(\beta u_t))^m} \right\rangle_{\{u_t\}}} \tag{2.155}$$

$$Q(u) = \left\langle \delta \left( u - \frac{1}{\beta} \tanh^{-1}(\tanh(\beta) \prod_{t=1}^{l-1} \tanh(\beta h_t)) \right) \right\rangle_{\{h_t\}} \tag{2.156}$$

For the $l$-spin with even degree the Ansatz closes on $q_0 = 0 = p_0$ and consequently $p_\pm = q_\pm = 1/2$, because on every spin the effective cavity field is given by the contribution of $k-1$ odd $\pm$ local fields. using this result a very simple expression in the scaling regime $m\beta = y$ is obtained[22]:

$$F(y) = -\frac{1}{y} \left( (1 - \frac{k(l-1)}{l}) \log(\frac{1}{2^k} \sum_{i=0}^{k} \frac{k!}{(k-i)!i!} e^{y|k-2i|}) + \frac{k(l-1)}{l} \log(\frac{1}{2^{k-1}} \sum_{i=0}^{k-1} \frac{(k-1)!}{(k-1-i)!i!} e^{y|k-1-2i|}) \right) \tag{2.157}$$

For odd degrees eq. (2.158) is more involved and has the form

$$F(y) = -\frac{1}{y} \left( (1 - \frac{k(l-1)}{l}) \log g(k, y) + \frac{k(l-1)}{l} \log(k-1, y) \right) \tag{2.158}$$

$$g(k, y) = e^{y \cdot k} \sum_{n_+, n_-, n_0 > 0} \frac{k!}{n_+! n_-! n_0!} (\frac{q_0}{2})^{n_0} (\frac{1 - q_0}{2})^{n_+ + n_-} e^{-2y min(n_+, n_-)} \delta_{k; n_0 + n_+ + n_-} \tag{2.159}$$

In table 2.4.4 the optimal value $y^*$ of the scaling parameter and the GS energy densities $e_{gs} = \partial_{y=y^*}(yF(y)) = F(y^*)$ are shown in the 3-spin for various values of the graph degree $k$. We also report numerical estimations of the GS energy ($e_{gs}^{num}$) obtained by extrapolating the results of exhaustive enumerations (sizes up to $N = 60$ averaged over $1000 - -10000$ samples). Moreover in [22] the $y^*$ value for the 3-spin model with $l = 4$ has been estimated to be 1.41(1), perfectly compatible with our analytic value. In figs (2.8)-(2.11), some examples of the behavior of $\Sigma(e)$, $F(y)$, $e(y)$ and $\Sigma(y)$ for fixed degree and rank hyper-graphs are shown. Notice the different behavior of $l = 2$ cases, corresponding to the Viana-Bray models. The meaning of the different curves branches has been previously explained and is the same as in fig (2.4). In fig (2.12) the dependence of $\Sigma(e_d)$ on $k$ at fixed rank $l$. In fig (2.13) the dependence of the $\Sigma(e)$ curve on $l$ for a fixed degree ($k = 10$ in the example) is shown.

[22] With the alternative formalism of appendix C.1 we can write an exact factorized Ansatz for structure with arbitrary degree distribution and fixed sub-degrees (one for each k-sub-hyper-graph). The final formulas are reported in appendix C.2.

| $k$ | $e_{gs}$ | $e_{gs}^{num}$ | $y^*$ |
|---|---|---|---|
| 1–3 | -$(k)/3$ | | $\infty$ |
| 4 | -1.21771 | -1.218(6) | 1.41155 |
| 5 | -1.39492 | -1.395(7) | 1.09572 |
| 6 | -1.54414 | -1.544(9) | 0.90163 |

Table 2.2: Optimal value $y^*$ of the scaling parameter and the GS energy densities for the 3-spin and for various values of the graph degree $k$.

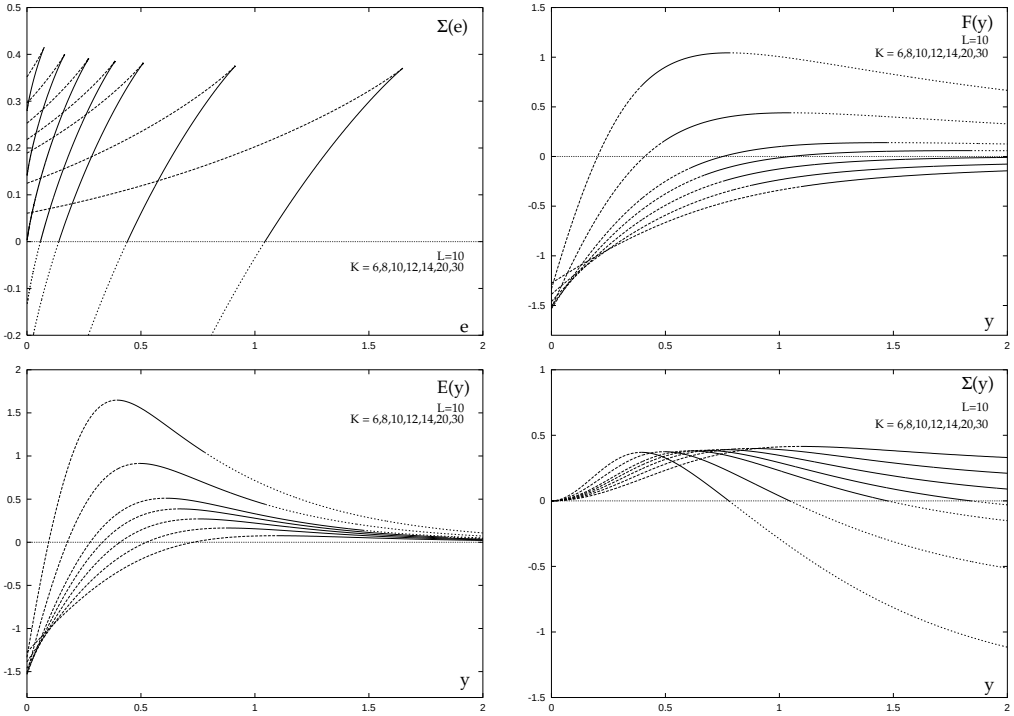



Figure 2.8: Potential, Energy and Complexity for $l = 10$-spin model on a hyper-graph of fixed degree $k = 10$.

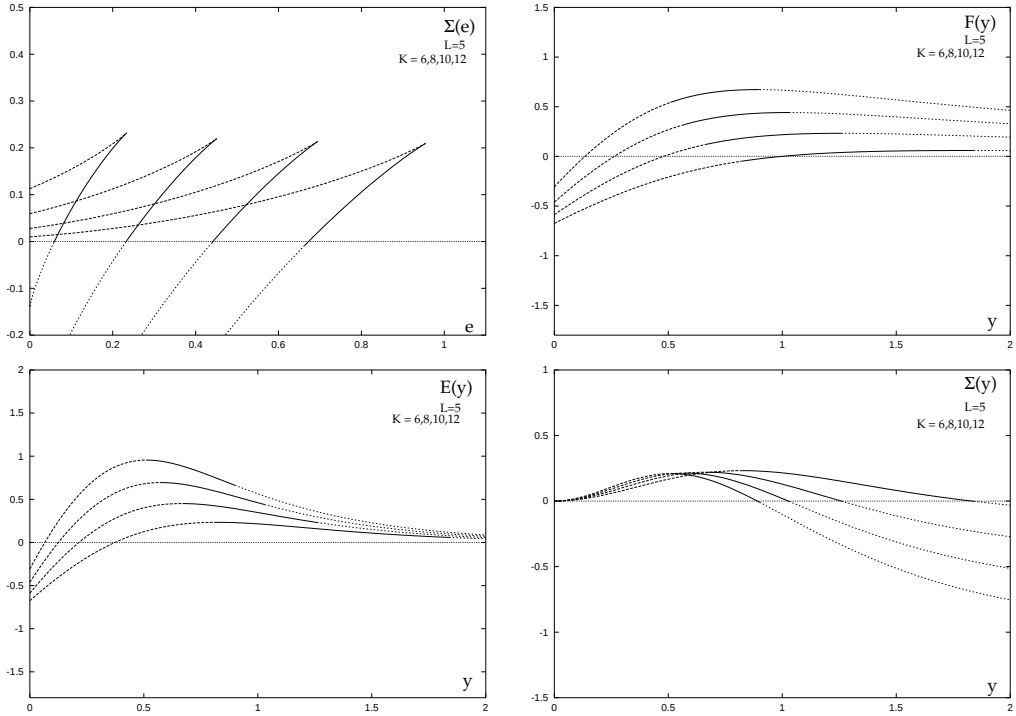



Figure 2.9: Potential, Energy and Complexity for $l = 5$-spin model on a hyper-graph of fixed degree $k = 10$.

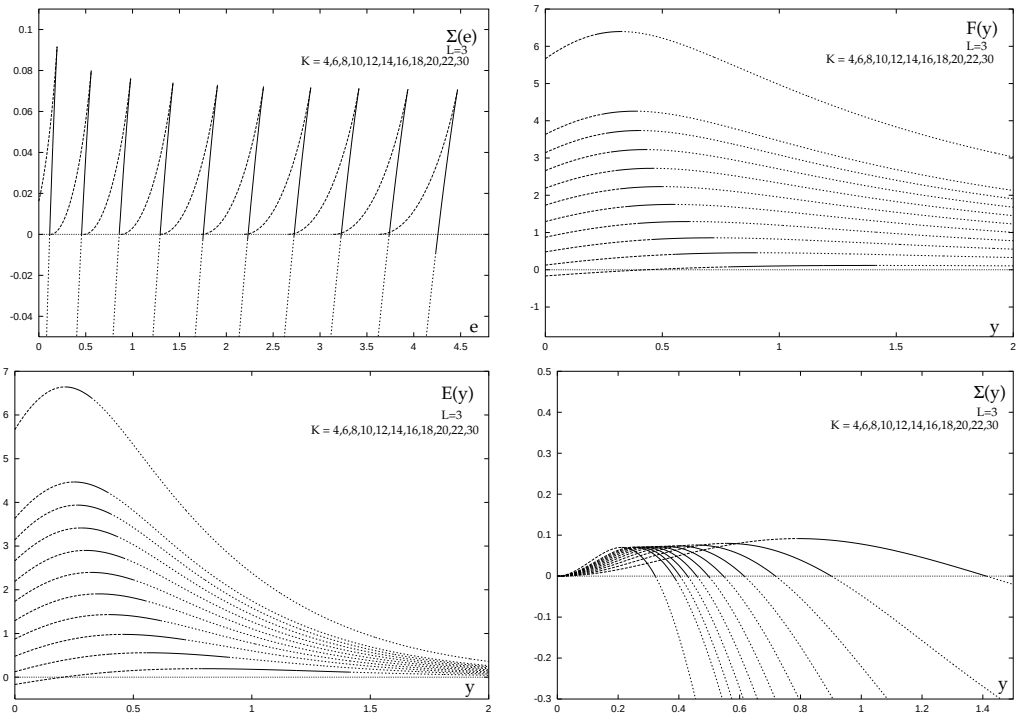



Figure 2.10: Potential, Energy and Complexity for $l = 3$-spin model on a hyper-graph of fixed degree $k = 10$.

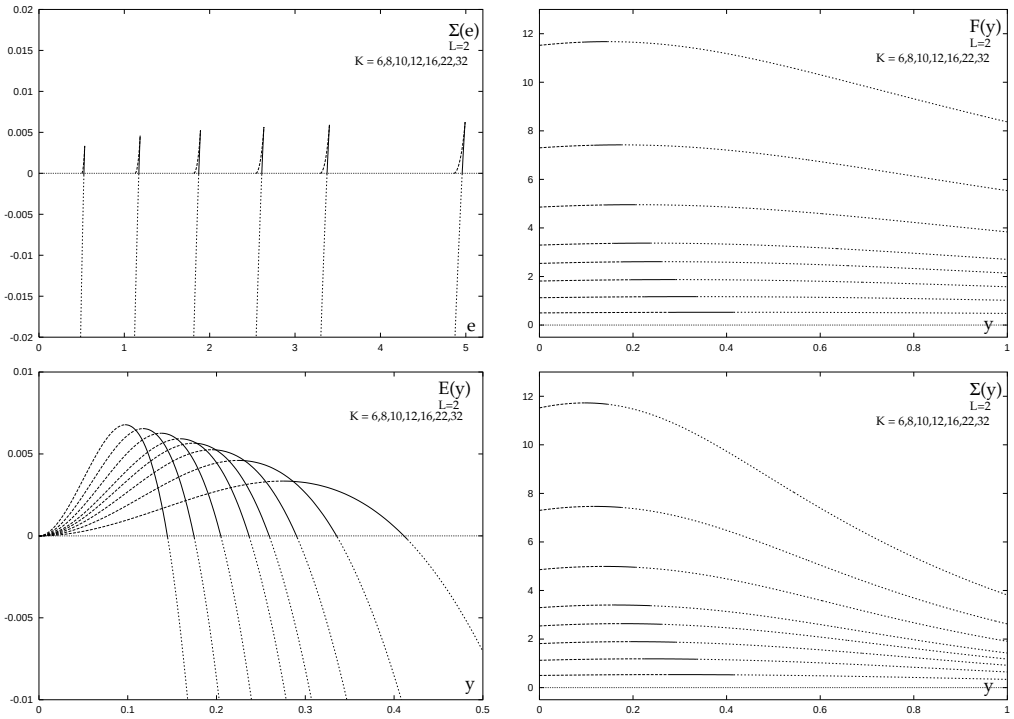



Figure 2.11: Potential, Energy and Complexity for $l = 2$-spin model on a hyper-graph of fixed degree $k = 10$.

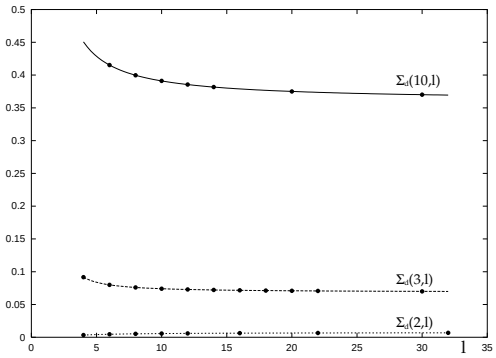



Figure 2.12: Complexity at the dynamical threshold $\Sigma_d^{(l)}(k)$ as a funtion of the fixed degree $k$

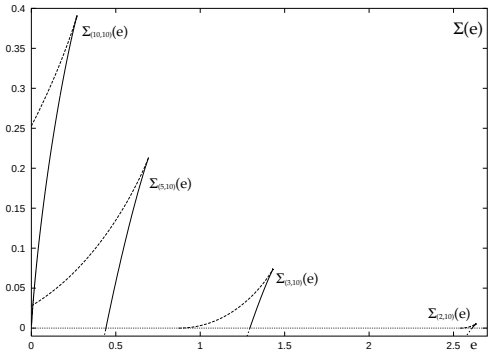



Figure 2.13: Examples of dependence of the $\Sigma(e)$ curve on $l$ for a fixed degree $k = 10$.

## 2.5 The general 1RSB equations

The picture that came out from the use of the facorized Ansatz was a big improvement compared to the RS approximation and it will qualitatively hold in many aspects in the following, but we pointed out some not satisfactory features of it, in particular the fact thet we are still essentially neglecting site dependence of the local fields distributions. If we stick to the more general (within Parisi's scheme) forms (2.104) and (2.104) of the functional order parameters and we plug it into the exact expression for the potential (2.39) we can write, after a calculation that is longer and a bit more involved but essentially equivalent to the RS case:

$$\begin{aligned} m\beta F_{1RSB}(m,\beta) &= \beta\frac{<k>}{<l>} - \frac{<k>}{<l>}\left\langle \log(\cosh(\beta J))\right\rangle_J + \\ &< k > \left\langle \log\left\langle \left(\frac{2\cosh(\beta(h+u))}{2\cosh(\beta h)2\cosh(\beta u)}\right)^m \right\rangle_{h,u}\right\rangle_{P,Q} - \\ &\sum_k c_k \left\langle \log\left\langle \left(\frac{2\cosh(\beta\sum_{t=1}^k u_t)}{\prod_{t=1}^k 2\cosh(\beta u_t)}\right)^m \right\rangle_{\{u_t\}}\right\rangle_{\{Q_t\}} - \\ &\frac{<k>}{<l>}\sum_l v_l \left\langle \log\left\langle \left(1+\tanh(\beta J)\prod_{t=1}^l \tanh(\beta h_t)\right)^m \right\rangle_{\{h_t\}}\right\rangle_{\{P_t\},J} \end{aligned} \tag{2.160}$$

One has to keep in mind that there are now two levels of distributions, and the cavity fields on one site are not fixed in one state anymore, but are only "biased" toward one set of values by a given site dependent distribution. In this sense the $u$-fields (that are the polarizations felt by one spin coming from neighboring variables) have been called cavity *biases*. In the same sense, an algorithm that exploits the RSB biases structure to propagate information along the vertices of the hyper-graph will have to work pass information on the whole probability distributions - the *survey* - of biases instead of a simple belief of the scalar value of the field. This is the reason why the new algorithm class presented in [29, 30] has been called *Survey Propagation*. The survey passing procedure acting on a single spin $S_0$ is shown in fig 2.14). The complete saddle point conditions are this time translated into integral equations on $\mathcal{P}[P]$ and $\mathcal{Q}[Q]$[23]:

$$\mathcal{P}(P) = \frac{1}{<k>}\sum_k k c_k \int \prod_{t=1}^{k-1} \mathcal{D}Q_t \mathcal{Q}(Q_t)\delta(P(\cdot) - P(\cdot|Q_1,...,Q_{k-1})) \tag{2.161}$$

$$\mathcal{Q}(Q) = \frac{1}{<l>}\sum_l l v_l \prod_{t=1}^{l-1} \mathcal{D}P_t \mathcal{P}(P_t)\left\langle \delta\left(Q(\cdot) - Q(\cdot|P_1,...,P_{l-1},J)\right)\right\rangle_J \tag{2.162}$$

$$Q(u|P_1,...,P_{l-1},J) = \mathcal{N}_P^{l-1}[P_1,...,P_{l-1},J]\int \prod_{t=1}^{l-1} dh_t P_t(h_t) B_{\mathbf{J}}^{l-1}(h_1,...,h_{l-1})^m \delta\left(u - u_{\mathbf{J}}(h_1,...,h_{l-1})\right) \tag{2.163}$$

$$P(h|Q_1,...,Q_{k-1}) = \mathcal{N}_Q^{k-1}[Q_1,...,Q_{k-1}](2\cosh(\beta h))^m \int \prod_{t=1}^{k-1} du_t \frac{Q_t(u_t)}{(2\cosh(\beta u_t))^m}\delta(h - \sum_{l=1}^k u_l) \tag{2.164}$$

where $\mathcal{N}_Q^{k-1}[Q_1,...,Q_{k-1},J]$ and $\mathcal{N}_P^{l-1}[P_1,...,P_{l-1}]$ insure normalization and $B_{\mathbf{J}}^{l-1}(h_1,...,h_{l-1})$ is a rescaling term that can be re-absorbed in the normalization in the case of the $p$-spin model[24].

[23] For the reader interested in reproducing this results we remind that in the following expression the limit for the number of replica groups $= n/m \to 0$ has been taken. In (2.160) the terms of order $\mathcal{O}(n/m)$ are retained.

[24] In that case it does not depend on the fields.

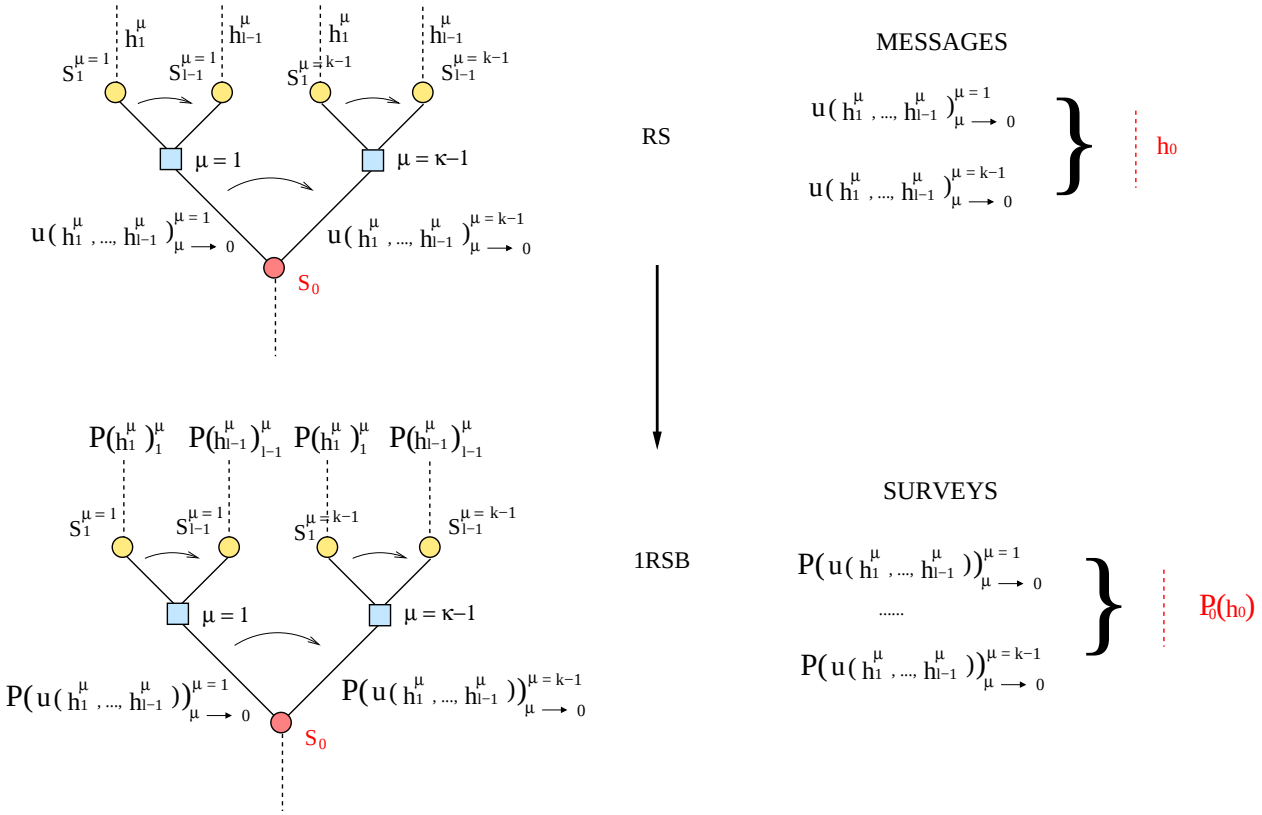



Figure 2.14: From messages (RS) to surveys (1RSB) passing.

Eqs (2.161)- (2.164) are very general and valid for models other that the $p$-spin. From model to model the nature of the functions $u_{\mathbf{J}}$ and $B_{\mathbf{J}}^{l-1}$ change. $\mathbf{J}$ represent the set of all couplings contained in an elementary energetic constraint, and it is a simple scalar for the $p$-spin. $m$ is a number in the interval $(0, 1]$, which selects families of solutions at different free-energy levels. The physical free-energy is estimated maximizing over $m$. For the $p$-spin $u_J$ has the usual form

$$u_J(h_1, ..., h_{l-1}) = \frac{1}{\beta} \tanh^{-1} \left( \tanh(\beta J) \prod_{t=1}^{l-1} \tanh(\beta h_t) \right) , \tag{2.165}$$

where $J$ is a scalar because only one coupling enters the local energetic term. Another example is the $K$-SAT case, where with calculations very similar to the $p$-spin model one finds

$$u_{\mathbf{J}}(h_1, ..., h_{p-1}) \equiv u_J(\{J_t\}, \{h_t\}) = \frac{J}{\beta} \tanh^{-1} \left[ \frac{\frac{\xi}{2} \prod_{t=1}^{p-1} \left( \frac{1+J_t \tanh(\beta h_t)}{2} \right)}{1 + \frac{\xi}{2} \prod_{t=1}^{p-1} \left( \frac{1+J_t \tanh(\beta h_t)}{2} \right)} \right] \tag{2.166}$$

$$B_{\mathbf{J}}(h_1, ..., h_{p-1}) \equiv B(\{J_t\}, \{h_t\}) = 1 + \frac{\xi}{2} \prod_{t=1}^{p-1} \left( \frac{1 + J_t \tanh(\beta h_t)}{2} \right) . \tag{2.167}$$

It is evident the *re-weighting* of the inner distributions with $m$ that becomes responsible for the $y$-regulated $T = 0$ level crossing[25] Depending on the choice of the quenched disorder distribution $\mu(\mathbf{J})$, we can specialize (2.160) the the ferromagnetic as well as the spin-glass cases. The expression for the free-energy for models other than the $p$-spin can be calculated along the same lines. For instance, the general 1RSB energy for the $K$-SAT model is given in chapter 6.

### 2.5.1 General Solution at $T = 0$

The previous equations can be iteratively solved via a population dynamics algorithm presented in [23] and valid in principle at all temperatures. The algorithm explicitly makes use of the re-weighting terms in (2.161)-(2.164). The zero temperature limit of (2.161)-(2.164) and (2.160) can be directly computed, or from the replica equations or exploiting the straightforward generalization of the $T = 0$ replica/cavity self consistent equations written in [24] for the Vian-Bray model. Equivalently, their limit can be directly calculated from the replica results (2.161)-(2.164), substituting (in the scaling regime $y \equiv m\beta$)

$$\left( \frac{2\cosh(\beta h)}{2\cosh(\beta u_t)} \right)^m \to e^{-y\left( \sum_{t=1}^{k-1} |u_t| - \left| \sum_{t=1}^{k-1} u_t \right| \right)} \tag{2.168}$$

in the general case,

$$u_J(h_1, ..., h_{l-1}) \to min(|J|, |h_1|, ..., |h_{l-1}|) \cdot sign \left( J \prod_{t=1}^{l-1} h_t \right) \tag{2.169}$$

for the $p$-spin,

$$u_J(\{J_t\}, \{h_t\}) \to -\frac{J}{2} \prod_{t=1}^{K-1} \Theta(J_t h_t) \tag{2.170}$$

$$B(\{J_t\}, \{h_t\})^m \to 1 \tag{2.171}$$

[25]The re-weighting is obviously present also at finite temperature, as well as the level crossing, and is even more complicated due to thermal effects. We focused on zero temperature because of the direct connection with optimization theory.

for the $K$-SAT[26] and rescaling the normalization factors accordingly. If the quenched disorder distribution $\mu(\mathbf{J})$ has support only on $\pm 1$ values, eq. (2.169) reduces to the usual

$$u_J(h_1, ..., h_{l-1}) \to J \cdot min(1, |h_1|, ..., |h_{l-1}|) \cdot sign\left(\prod_{t=1}^{l-1} h_t\right) \tag{2.172}$$

already seen in the $p$-spin spin-glass in the RS and factorized cases. We would like to stress here that all calculations could be redone for a more general choice of $\mu(\mathbf{J})$. The exponential term, when calculated directly via the cavity method, reads

$$e^{-y(e_{min}^{(N+1)} - e_{min}^{(N)})} = e^{-(\Sigma_{min}^{(N+1)} - \Sigma_{min}^{(N)})} \tag{2.173}$$

and plays the role of a re-weighting of states due to a population shifts in the number (complexity) of states (clusters) under the cavity equation iteration from an $N$ to an $N+1$ hyper-graph. This terms essentially favors terms with low minimal ($min$ in the equation) energy or complexity, helping the equations to converge towards the correct GS. Notice that inside the dynamical region the GS is found for $y \to \infty$.

In this case the re-weighting factor (2.173) will become in general an *Indicator function* $\chi(A(\{P(h)\}))$ (or $\chi(A(\{Q(u)\}))$, depending on which fields we decide to work with) over the set $A$ of effective fields distributions that do not lead to local constraints contradiction and therefore do not increase the value of the energy from the $e = 0$ GS one. Beyond $\gamma_c$ this in in the typical case no longer possible, because no all local contradictions can be satisfied due to frustration percolation. However, solutions with a minimal number of violated energy constraints will be favored.

Similarly to the RS or the factorized case, one can on physical grounds require the form of a given site field distribution function to close on an integer support[27]. Given $k_i$ the degree of spin $i$ belonging to an edge of rank $l_i$ we can write

$$P(h|k_i - 1)(\vec{p^{i,k_i}}) = \sum_{r=-k_i+1}^{k_i-1} p_r^{i,k_i} \delta(h - r) \tag{2.174}$$

$$P(u|l_i - 1)(\vec{q^{i,l_i-i}}) = \sum_{r=-1}^{1} q_r^{i,l_i} \delta(u - r) \tag{2.175}$$

It is parametrized by a vector of weights, $\vec{p^i} = (p^i_{-k_i}, ..., p^i_{k_i})$[28] which can fluctuate from one site $i$ to the next. Since at $T = 0$ the fields take integer values, the probability depends on a finite number $(2k)$ of parameters for all fractions of vertices of degree $k$, and the full order parameter is not a functional, but a function $R(\vec{p})$ of the vector of weights which is given in the limit of large $N$ by:

$$R_h(\vec{p}) = \frac{1}{N} \sum_j \left[ \prod_{r=-k_i+1}^{k_i-1} \delta\left(p_r^j - p_r\right) \right] = \frac{1}{< k >} \sum_k k c_k \left[ \prod_{r=-k_1}^{k-1} \delta\left(p_r^k - p_r\right) \right] , \tag{2.176}$$

[26] In [30], where for the 3-SAT case all details of the calculation via the cavity method are shown, the function $u_J$ appears rescaled by a factor 2 necessary to work with integer fields. Indeed, the factor can be simply re-absorbed from the beginning defining the $K$-SAT Hamiltonian has twice the value of the cost function of the combinatorial problem. The same holds for other models such has the hyper-graphs Bicoloring of chapter 4.

[27] In some cases, as for instance the $K$-SAT, this hypothesis is the only one possible.

[28] we have dropped the apex $k_i$.

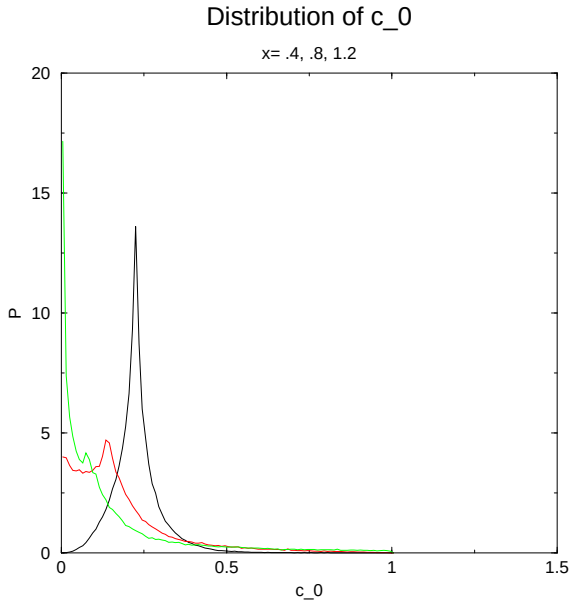



Figure 2.15: Probability distribution of the $p_0$ weights in the Viana-Bray model, obtained after evolving a population of $N = 10^5$ sites. Plotted are the cases $y = 0.4$ (black), $y = 0.8$ (red) and $y = 1.2$ (green). Notice the big effect of non-factorization. The best factorized solution, with $y = 0.4174$, would give a $\delta$ peak at $p_0 = .3353$. The RS solution would give a $\delta$ peak at $p_0 = 1/3$.

where $p_r^k$ is the weight of a filed $r$ of a spin of degree $k$ and the second equation holds on the typical sample, once averaged over the hyper-graph ensemble. Analogously for the $u$-biases:

$$R_u(\vec{q}) = \frac{1}{N}\sum_j \left[\prod_{r=-1}^{1} \delta\left(q_r^j - q_r\right)\right] = \frac{1}{< l >}\sum_l l v_l \left[\prod_{r=-l}^{l} \delta\left(q_r^l - q_r\right)\right] \ , \tag{2.177}$$

Therefore, two Ansätze have to be checked in order to find an analytical solution: the one on the weights of a single site distribution , attached to $P(h)$ or $Q(u)$, and the fractions of sites given a certain distribution of fields, attached to $R_h(\vec{p})$ and $R_q(\vec{u})$. Differently from the RS and the factorized Ansatz approach, the qualitative consequences of the general RSB equations are clearly visible on the fact that the probability distribution of cavity fields is site dependent, and this picture survive at zero temperature, as it is shown for instance for the case of the Viana-Bray model in fig. (2.15). There the probability distributions $P(p_0) = (1/N)\sum_i \delta\left(p_0^i - p_0\right)$ for the zero cavity fields weights $p_0$ ($c_0$ in the figure) are shown for different values of the scaling parameter $y$. The distributions are broad due different site-to-site. Both the RS *and* the factorized solution give a single $\delta$ peak in the same situation. taken from [24]. Moreover, the individual cavity field distributions $P_i(\vec{p})$ are not symmetric under field reversal (i.e. $P_i(p_r) \neq P_i(p_{-r})$), while only the full order parameter is statistically symmetric (i.e. the site to site fluctuations of $p_r$ are identical to those of $p_{-r}$).

If as a title of example one specializes to the Poissonian $p$-spin case, whose specific results have been already given in the last sections, equations (2.169) and (2.171) reduce to a single

closed form that can be written only in terms of the $u$-biases distributions:

$$Q_0(u) = C_0 \int \prod_{t=1}^{p-1} \prod_{\mu=1}^{k^t} du_t^\mu Q_t(u_t^\mu) \delta \left( u - u_J \left( \sum_{\mu=1}^{k^1} u_1^\mu, \dots \sum_{\mu=1}^{k^{p-1}} u_{p-1}^\mu \right) \right) \cdot \cdot \exp \left[ -y\, w_J \left( \sum_{\mu=1}^{k^1} u_1^\mu, \dots \sum_{\mu=1}^{k^{p-1}} u_{p-1}^\mu \right) \right] \quad , \tag{2.178}$$

where $C_0$ is a normalization factor, $\mu$ is the "clause" index,

$$w_J \left( \sum_{\mu=1}^{k^1} u_1^\mu, \dots \sum_{\mu=1}^{k^{p-1}} u_{p-1}^\mu \right) = 1 - \sum_{t=1}^{p-1} \left| \sum_{\mu=1}^{k^t} u_t^\mu \right| \tag{2.179}$$

is the re-weighting factor and numbers $\{k^t\}_{t=1}^{p-1}$ are i.i.d. random numbers taken from a Poisson distribution of mean $\gamma p$[29]. Since the cavity biases, as said, take values $\{0, \pm 1\}$, symmetric solutions of the form

$$Q_i(u) = \eta_i\, \delta(u) + \frac{1-\eta_i}{2} \left[ \delta(u-1) + \delta(u+1) \right] \quad , \tag{2.180}$$

can be sought in general[30]. Indeed, form (2.180) is very well observed numerically, with a fraction $r$ of trivial distributions with $\eta_i = 1$. Moreover, the weights $\eta_i$ can be computed analytically [26, 30]. As in the factorized Ansatz case, various phases are found, their stability depending on $\gamma$.

The histogram picture for the site fields distributions $Q_i(u_i)$ is pictorially shown in fig. (2.16) From eq. (2.178), in the limit $y \to 0$, the site fields distributions concentrate on one single delta function for each site $i$. There is no re-weighting factor and the average

$$\mathcal{Q}(Q(u)) \equiv \frac{1}{N} \sum_{i=1}^{N} Q_i(u_i) \tag{2.181}$$

can be seen as an average over the values of the single scalar fields $u_i$, giving back the average RS solution (calculations can be directly done via inspection).

In the factorized Ansatz case, due to the re-weighting, a normalization $C_i(y)$ is present ($C_0$ for the reference spin $S_0$ in (2.178)). However in this case $C_i(y) = C(y)\ \forall i \in \{1, ..., N\}$, because all sites share the same state to state fluctuations (see again fig. (2.16).

In the general 1RSB case, the normalization (and the re-weighting) factors are site dependent, all site distributions (or their numerical coefficients at $T = 0$) fluctuate from site to site and eq. (2.181) gives the general 1RSB replica solutions[31].

Looking at the iteration equation for general values of $y$ (2.178), the only way one can obtain a trivial distribution $Q_0(u) = \delta(u)$ on the l.h.s. is when $\exists\ t$ such that all the $k^t$ distributions are trivial Therefore, for one given iteration with given $\{k^t\}$, the probability that $Q_0(u) = \delta(u)$

[29] Notice that the sums here go up to $k$ instead of the $k-1$ of the cavity original formulation. This is a peculiarity of the Poissonian degree distribution "self similarity" as it has been already seen in the previous sections.

[30] $\eta_i \equiv q_0^i$ of eq.(2.177).

[31] Again calculations can be checked directly. In order to prove equivalence the reitroduction of $h$ fields distributions is then not necessary, but it simplifies a bit the notation.

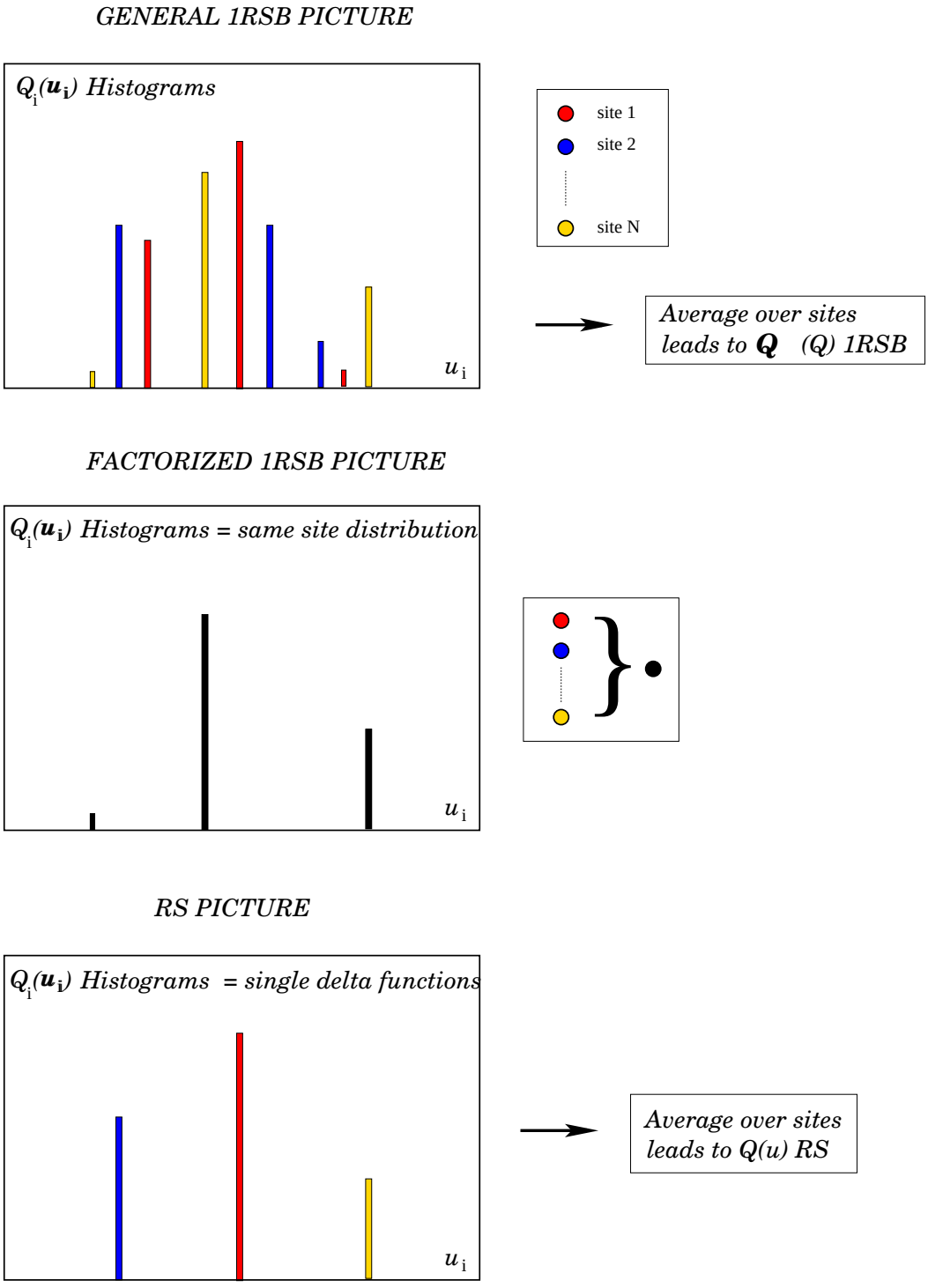



Figure 2.16: Pictorial description of the histograms of the distributions $Q_i(u_i)$ in the general 1RSB, RS and factorized cases.

is $1-\prod_{t=1}^{p-1}(1-r^{k^t})$. The average over iterations and over the random connectivities $\{k^t\}$lead to a simple equation for the fraction of trivial distributions:

$$r = e^{-2p\gamma} \sum_{k^1,\ldots,kp-1=0}^{\infty} \prod_{t=1}^{p-1} \frac{(p\gamma)^{k^t}}{k^t!} \Big(1 - \prod_{t=1}^{p-1}(1-r^{k^t})\Big) = 1 - \Big(1 - e^{-p\gamma(1-r)}\Big)^{p-1} \quad . \tag{2.182}$$

For $\gamma < \gamma_d$ the only solution is $r = 1$, while above $\gamma_d$ a non-trivial solution appears. Notice that equation (2.182) is identical to the magnetization condition of the ferromagnetic model, confirming our previous observations of thresholds coincidence.

For large $y$, numerical results show that the cavity biases spontaneously divide in two categories: cavity biases of type "a" with $Q_i(u) = \delta(u)$ and those of type "b" with $Q_i(u) = \frac{1}{2}[\delta(u-1) + \delta(u+1)]$ that are responsible for the propagation of the interactions. In fact, the following distribution of cavity biases

$$Q_i(u) = \begin{cases} \delta(u) & with\ \ prob. \quad r \quad (`type\ \ a') \\ \frac{1}{2}\left[\delta(u-1) + \delta(u+1)\right] & with\ \ prob. \quad 1-r \quad (`type\ \ b') \end{cases} \tag{2.183}$$

is a fixed point under the iteration process (2.178) for $y = \infty$, provided the fraction of trivial knowledges $t$ satisfies (2.182). Using the extension to the hyper-graphs case of the expressions in [24], one finds the complete 1RSB expression for the potential $F(y \to \infty) = 0$, which is indeed the expected result.

### Beyond $\gamma_d$: the location of the static phase transition

In order to study the complexity and the phase transition point one needs to take care of the leading corrections in the limit $y \gg 1$. For finite $y$, the distribution (2.183) is no longer stable; we need to study a more general distribution of biases which takes care of the appearance of a non-trivial contribution to the peak in $u = 0$, arising from frustrated interactions:

$$Q_i(u) = \begin{cases} \delta(u) & with\ \ prob. \quad r \quad (`type\ \ a') \\ \frac{1}{2}(1-\eta_i)\left[\delta(u-1) + \delta(u+1)\right] + \eta_i\,\delta(u) & with\ \ prob. \quad 1-r \quad (`type\ \ b') \end{cases} \tag{2.184}$$

where the fraction $r$ of trivial biases is always fixed by (2.182). For large $y$, substituting this distribution into the self-consistency equation (2.178) shows that the weight can be computed as a series expansion in powers of $e^{-y}$, rapidly decreasing for large $y$. If one proceeds in doing so the expression for the potential $F(y)$ can be calculated around the static transition and a value of $\gamma_c$ again coinciding with the ferromagnetic one in found.

Thanks to the Legendre transform already used in the factorized Ansatz approximation the complexity cam be calculated, leading to important corrections to the factorized results.

We would like to stress in conclusion that this is only an introductory review of the steps of complete 1RSB solution, that can be found in details in [26, 30], and that the 1RSB equations can be reformulated also in the single sample cavity analysis presented in [29, 30] for the 3-SAT model, where the re-weighting factor (2.173) lies at the hearth of the effectiveness of the proposed Survey Propagation algorithm. There, the indicator function $\chi(A)$ plays the role of a filter on the messages surveys that would lead to conflicting information coming from a function node (clause) to the variable to be fixed.

## 2.6 "Ferromagnetic complexity"

From the usual definition of the free energy $\beta F = \beta E - S_{tot}$ and from the fact that we are working with a clusterized system of m replicas, we can split the total entropy of our system in an $mS$ part counting the contribution within clusters and a complexity $\Sigma$ counting the clusters multiplicity. We can therefore write $-m\beta F(m,\beta) = \Sigma(\beta, m) + mS(\beta) - m\beta U(\beta, m)$, where $U$ is the total internal energy. The complexity of the original, $m = 1$ system will be therefore given by the stationary point condition [7]

$$\Sigma^*(\beta) = m^2 \frac{\partial \beta F(m,\beta)}{\partial m}_{|m=1} \tag{2.185}$$

at finite temperature. However, if we want to compute $\Sigma^*(\infty)$ we must solve the saddle point equations for $m = 1$, and then take the zero temperature limit, which is a case not contained in the $y \to \infty$ limit of the previous section. This limit in principle underestimates the number of LGS at $\beta = \infty$, and does not allow to compute the complexity at finite energy above the static transition, because in that case the states at $y = 0$ (and $m = 1$ counts part of them) turn out not to be locally stable, as we have seen on the general discussion on the complexity. In the general case therefore

$$\Sigma^*(\infty) \neq \Sigma(y^*) \tag{2.186}$$

and it is *not correct*. We will call $\Sigma^*(\infty)$ maybe with abuse of language the *zero temperature ferromagnetic complexity* of the diluted $p$-spin model for the following reasons: eq. (2.185) does compute the configurational entropy of the metastable states of the ferromagnetic $p$-spin diluted model, and indeed, explicitly solving the $T = 0$ 1RSB saddle point equations for $m = 1$ with a calculation similar to the RS case[32] one finds:

$$\Sigma^*(\gamma) = S_{para}(\gamma) - S^{RS}_{ferro}(\gamma) \tag{2.187}$$

where $S_{ferro}$ simply is the zero temperature entropy of the RS ferromagnetic solution and we have made explicit the dependence on $\gamma$. This result is valid for all degrees distributions in the ferromagnet[33].

The existence of a metastable states complexity for disordered ferromagnets is not in contrast with the fact that the GS is replica symmetric. After the magnetization transition, a ferromagnetic solution is always present in the model, but is the center of a single cluster. There cannot be more than one magnetized cluster, because the fixed spins are the ones belonging to a core subgraph that is univocally defined and shared by all other solutions, at Hamming distance $\mathcal{O}(1)$ and found by spin flipping in the paramagnetic fraction of variables. This properties will be discussed in the last section for the spin-glass case, but is valid also for the single ferromagnetic cluster. However, also in this cases a dynamical transition *in the metastable states* is present. Between $\gamma_d$ and $\gamma_c$ an exponential number of states appear between $e = 0$ and $e = e_d$. Even though all clusters at $e = 0$ are identically magnetized, the

[32]The reader interested in reproducing this calculation should nevertheless be careful to the fact that while in the RS limit the analytic continuation of $x \equiv \sum_{a=1}^{n} \sigma^a \in \Im$ is taken, in this case obviously $x \equiv \sum_{a=1}^{m} \sigma^a = sigma^1 = \pm 1$.

[33]Notice that when more that one possible value for $S^{RS}_{ferro}(\gamma)$ is present one has to take the largest one which is the thermodynamically favored entropy within the non paramagnetic choices. This means in case the system undergoes a continuous transition *before* the discontinuous one (see chapter 5 for examples), $\Sigma^*(\gamma)$ drops to zero at the transition point $\gamma = 1/(2v_2)$.

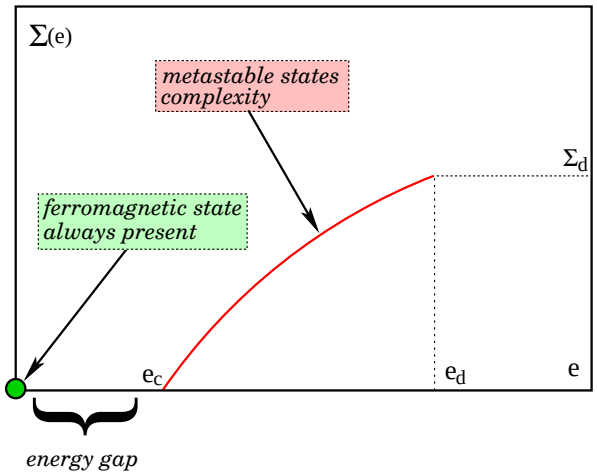



Figure 2.17: complexity versus energy density of metastable states above the ferromagnetic transition for models with dynamical 1RSB phase. The lower left dot at $e = 0$ is the ferromagnetic solution.

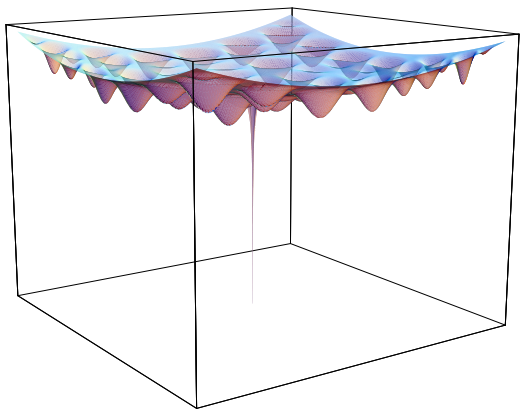


Figure 2.18: Energy landscape above the ferromagnetic transition. The narrow central dip represents the zero energy ferromagnetic solution.

presence of non zero energy metastable states is responsible for a slowing down of the dynamics analogous to the glassy case. A finite complexity therefore arises and indeed can be calculated via a 1RSB steps. The glassy behavior of $p > 2$-spin ferromagnets has been studied in [20] also at finite temperature as a model for structural glass transition or blocked configurations complexity in granular systems [80]. Also the models studied in chapter 5 in the error correcting codes application are ferromagnetic in nature. It is important to notice that also in this cases a dynamical transition *in the metastable states only* is present. After $\gamma_c$ an energetic gap in complexity opens up. However, differently from the spin-glass case, a single ferromagnetic cluster at zero energy is always present. This situation in pictorially shown in figs.(2.17) and (2.18), and is also the case of some *ad hoc* built ferromagnetic-like hard-satisfiable versions of the satisfiability model we studied in [55] and exploited to build a generator of very hard but satisfiable clauses. For this class of models we expect local search algorithms of any presently available kind not to be able to overcome the energy gap and find the global ferromagnetic solution for large system sizes. This was successfully verified with SAT solvers like walk-sat in

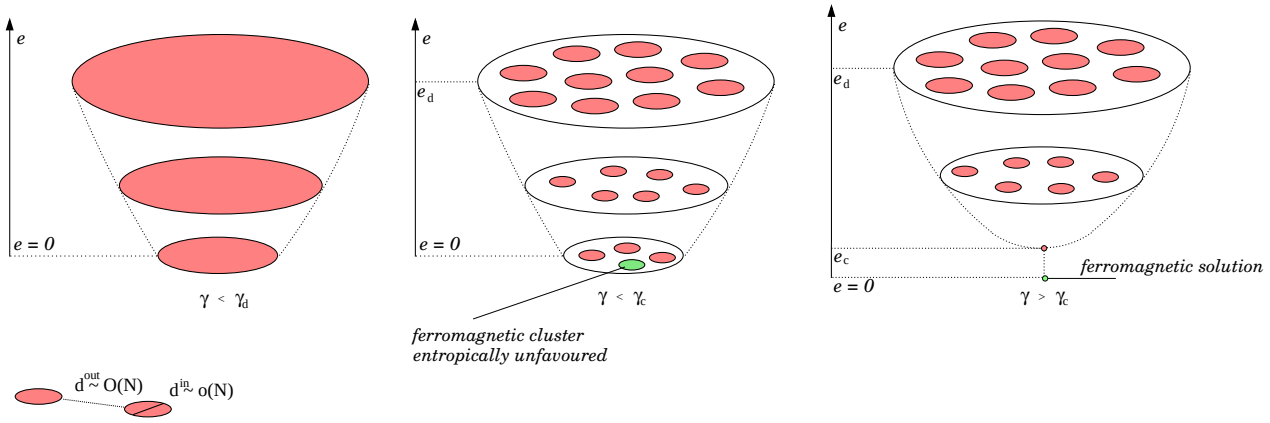



Figure 2.19: Scheme of solution clustering in ferromagnetic models with dynamical 1RSB phase.

[55] and for decoding sum-product algorithms in e.c.c. in chapter 5, as well as for simulating annealing. Moreover, this should be the case also for algorithms that are much less affected from the dynamical transition and perform very well throughout the $[\gamma_d, \gamma_c]$ region, like Survey Propagation [29, 30].

The cluster picture in energy and $\gamma$ is modified consequently in the way show in fig. (2.19) Some real complexity plots for the case of error correcting codes will be shown in Chapter 5. For Poissonian degrees distribution the ferromagnetic complexity reads

$$\Sigma^*(\gamma) = \log 2 \left( 1 - p_0(1 - \log p_0) - \gamma \sum_l v_l (1 - p_0)^l \right) \tag{2.188}$$

and

$$\Sigma^*(\gamma) = \log 2 \left( 1 - p_0(1 - \log p_0) - \gamma (1 - p_0)^3 \right) \tag{2.189}$$

for the 3-spin. Remarkably enough, $\Sigma^*(\gamma)$ is in *perfect agreement* with numerical simulations [19, 22] of the true $\Sigma(e = 0; \gamma)$ *and* with the general 1RSB analytical results of the previous section, with the Poissonian case and can in principle be seen for any $l$ and any degree distribution. In fig. (2.22) The analytic expression for $\Sigma^{3-spin\, poiss}(e = 0; \gamma)$ calculated via eq. (2.185) is compared with numerical simulations. The results of numerical clustering with an overlap cut-off of 0.7 (averaged over 1000, 1000, 500 and 50 samples) converge to the analytical prediction. Extensive numerical experiments on both versions (ferromagnetic and spin-glass) of $T = 0$ 3-spin (3-XOR-SAT) were performed in [19] in order to confirm analytical predictions. We remind that in a region where an extensive number of GGS is present, the combinatorial problem is Polynomial in the worst case as will be extensively review (and exploited) in chapter 3 and 5. We used a global polynomial method that reduces the problem of the GGS search to that of solving a large sparse linear system in Galois Field 2 (GF[2])[34]. The simulations whose output is shown in figs. (2.20),(2.21) and (2.22) used the polynomial procedure as well as local algorithms, namely the Davis-Putnam (DP) complete backtrack search [91] and the incomplete walk-SAT randomized heuristic search [92] , to check the hardness of the problem for local search[35]. The existence of at least one solution in the satisfiable 3-XOR-SAT allowed us to run

[34] This method will be reviewed in chapters 3 and 5 for the interested reader.

[35] mixed randomized and backtracking procedures have been also recently investigated. See for example [88], based on a systematic study reported in [93].

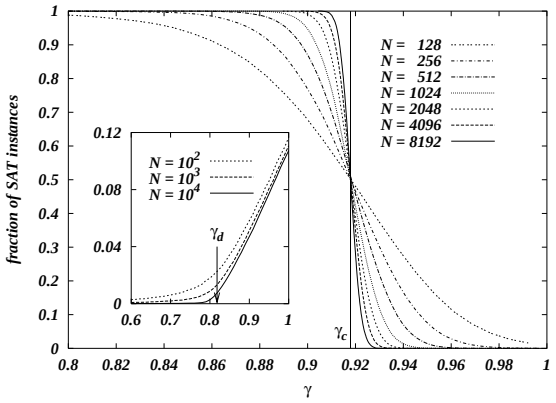



Figure 2.20: The probability that a formula is SAT as a function of the coupling density. Inset: The energy reached by a deterministic rule becomes different from zero at the dynamical critical point.

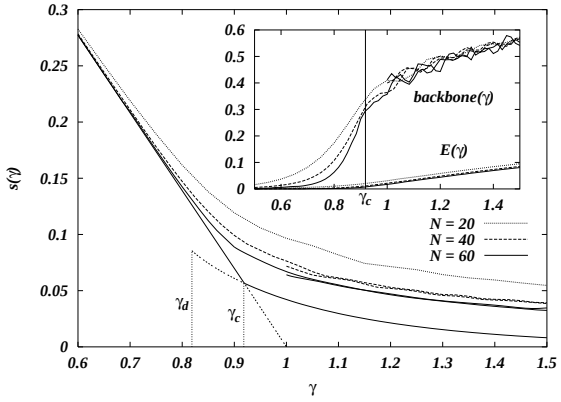



Figure 2.21: The lowest lines are the analytical expressions for the entropy of the ferromagnetic model. The numerical estimation (not reported) perfectly coincide. Dashed parts correspond to metastable states. The rest of the data (entropy in the main body and energy and backbone size in the inset) come from exhaustive enumeration of the ground states in the spin-glass model and of first excited states in the ferromagnetic one (only $N = 40, 60$) and they coincide.

walk-SAT in the whole range of $\gamma$, the halting criterion always being finding a SAT assignment. These results are quite surprising because tells us that the dynamic and static $p$-spin spin-glass thresholds *coincide* with the values of appearance of a metastable ferromagnetic solution and with the thermodynamic ferromagnetic transition (some values where given in the Poissonian and $l$ fixed case in table 2.4.4). We will see in the next section *why* it is so.

### 2.6.1 Hiding solutions in random satisfiability problems

We would like to make here a very brief digression to say, as we pointed out a few lines above, that the peculiar low and zero temperature solutions space structure of the ferromagnetic-like models described in this chapter is not restricted to the generalized $p$-spin model, but the same qualitative picture of figs. (2.17), (2.18) and (2.19) also applies to *ad hoc* constructed ferromagnetic versions of combinatorial optimization problems such as Hyper-graphs Bicoloring[36]

[36]See later chapter 3 for details.

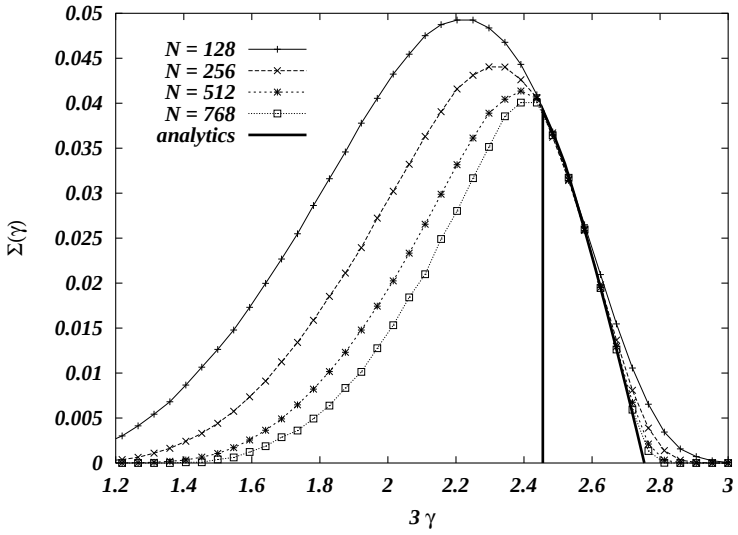



Figure 2.22: Ground states configurational entropy versus mean connectivity for the Poissonian 3-spin. With the analytic result we mean in this case $\Sigma^*(\gamma)$, which is also in perfect agreement with the complete 1RSB curve.

and random $K$-SAT. In this context, the extreme hardness of finding the narrow basin ferromagnetic solution hidden among a much larger exponential number of metastable states at higher energies, for $\gamma >> \gamma_d$, has revealed itself very useful in the design of hard and solvable combinatorial instances. Indeed, this is a very welcome in computer science, since a major problem in evaluating stochastic local search algorithms for NP-complete problems is the need for a systematic generation of hard test instances having previously known properties of the optimal solutions. On the basis of statistical mechanics results, we therefore proposed a class of random generators of hard and satisfiable instances for the 3-satisfiability problem based of a well suited ferromagnetic version of it. The design of the hardest problem instances is based on the existence of a first order ferromagnetic phase transition and the glassy nature of excited states. This subject would surely deserve a chapter on its own, but we decided not to include it here in order not to overload the thesis. However, at the end of this chapter we included the published article [55] - presenting our results - in its entireness. We would also like to mention that the generator described in the article was effectively implemented and submitted in the **SAT2002** Cincinnati Sat-Solvers competition, where it performed excellently. We believe these results to be e very clear example of the utility of statistical physics insight in the field of combinatorial optimization

Notice, on the opposite side, we will see in details in chapter 5 how error correcting codes algorithms explicitly try to avoid entering the dynamical region (and therefore to work in a regime of an effective $\gamma < \gamma_d$) in order to work efficiently, since a larger basin of for the ferromagnetic solution[37] is needed for the algorithms to rapidly converge.

[37]The ferromagnetic solution can be gauged to correspond to the complete retrieved original (before corruption) message parity check error correcting codes. See chapter 5 for details.

## 2.7 An exact alternative solution of the $p$-spin model at $T = 0$

We would like here to review a rigorous alternative solution for both the dynamical and static thresholds of the generalized $p$-spin. We stress that the following solution is exact. No need for either replica or cavity calculations is encountered. This does not invalidate the relevance of previous sections, because this last method is limited to the $p$-spin at zero temperature ($p$-XOR-SAT), whose configurational space symmetries do not in general occur in other models. Moreover, this derivation is a strong *psychological* argument in favor of the exactness of 1RSB calculations in more complicated cases. The method was presented in [26] for the special case of the 3-spin Poissonian hyper-graphs (as the prototype model of this whole line of research) and, with an almost equivalent formulation, in [94]. In this section we'll strictly follow [26], where all the results have been already established. Extending the calculations to arbitrary rank and degree distribution hyper-graphs was straightforward, so that this section will not contain any original result. It was only written for completeness, to show a clear example of the growing interplay between statistical physics methods and algorithms analysis. Indeed, a large amount of work is currently being performed in this direction with benefits for both fields. See [95, 93] and references for some examples. We will exploit concepts from graph theory and all the calculations will be simple annealed averages, which are rigorous. All the formulas will be written for the generic $p$-spin, and the particular case $p = 3$ on Poissonian hyper-graphs will be considered in order to make connection with the explicit results of the previous sections.

The physical idea behind the graph theoretical derivation is the following. In a random hyper-graphs there are many variables with connectivities 0 and 1, whose cavity/effective fields at zero temperature are null. A small fluctuation in the number of these variables, induce very large fluctuations in physical observables, as for example in the entropy. Thus, the idea is to remove all these *"floppy"* spins and to study the properties of the residual hyper-graph, the *"core"*, where conflicting constraints, if present, must lie. We find that, on the core, *sample-to-sample fluctuations are negligible* and this allows us to study its properties by mean of very simple annealed averages.

### 2.7.1 The onset of frustration: hyper-loops in the graph

Analogously to what happens with loops in usual graphs ($p = 2$), in a disordered model defined on a hyper-graph ($p > 2$) frustration is induced by the presence of hyper-loops [19, 21], which are also called hyper-cycles in the literature [68, 63] and where already introduced in chapter 1 and fig. (1.1). We recall here that a hyper-loop is a sub-hyper-graph $\mathcal{C} \subset \mathcal{H}$, such that every vertex in $\mathcal{C}$ has even degree in $\mathcal{C}$. In terms of the *incidence matrix* $\hat{A}$, the hyper-loop corresponds to a set of rows $\mathcal{R}$ such that, for every column, the sum modulo 2 of the elements is zero, i.e. $\sum_{i\in\mathcal{R}} a_i^j \ mod[2] = 0 \ \forall j$. The presence of hyper-loops is directly related to the presence of frustration in the system: If the product of the signs of hyperloop interactions is negative, $\prod_{m\in\mathcal{C}} J_m = -1$, then not all such interactions can be satisfied at the same time. The critical point $\gamma_c$, where hyperloops percolate, is a $T = 0$ phase boundary for the $p$-spin glass models defined by Hamiltonian (2.9): For $\gamma < \gamma_c$ all the interactions can be satisfied and the GS energy is zero, while for $\gamma > \gamma_c$ the system is in a frustrated spin glass phase and GGS of zero energy no longer exist. The critical point $\gamma_c$ corresponds to the SAT/UNSAT threshold for the random $p$-XORSAT problem. In terms of the random linear system $\hat{A}\,\vec{x} = \vec{y}\ mod[2]$, as long as $\gamma < \gamma_c$, solutions to the system will exist with probability 1 in the large $N$ limit *for any*

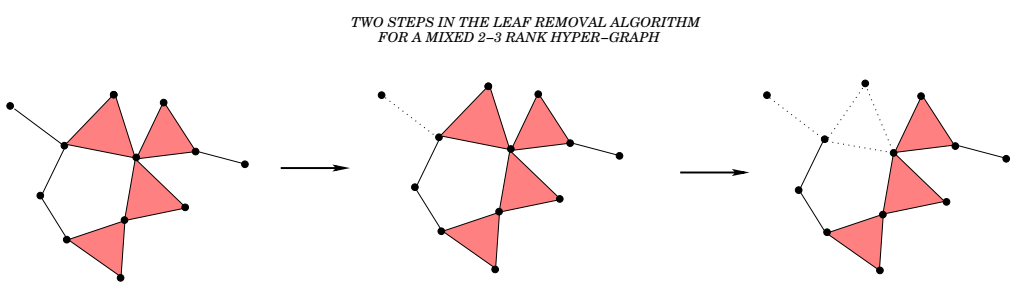



Figure 2.23: Two generic steps of the leaf removal algorithm on a portion of $2+3$-hyper-graph.

$y$. We would like to recall again the existence of somehow anomalous models. If the fraction $v_2$ of rank 2 edges is larger than a certain critical threshold, a giant component made of a purely 2-sub-hyper-graph (plus fractions of other edges of order $\bar{l}O(1)$), forms. Within this extensive connected sub-graph, 2-loops percolate at $\gamma = 1/2$ and give rise to frustration. More general hyper-loops, formed by a finite fraction of all ranks edges, percolate at the static threshold (2.187), giving rise to a discontinuous ferromagnetic transition in ferromagnetic models[38] , or spin-glass in the frustrated cases. But at that point the continuous transition at $\gamma = 1/2$ has already taken place. In fact, these models do not radically differ from the other cases, because the topological emergent structures that lead to propagation of frustration in the hyper-graph are the same. The only difference being a "time"[39] scale separation in the fixed rank hyper-graphs An axample of general phase diagram that include these cases will be drawn in the first section of chapter 5.

### 2.7.2 Leaf removal algorithm

Given a hypergraph the leaf removal algorithm proceeds as follows [96]: As long as there is a vertex of degree 1 remove its unique hyper-edge. Two subsequent steps of the algorithm are illustrated in fig. 2.23 for a $2+3$-hyper-graph. Very similar algorithms have been recently studied in [97, 95]. During the whole process the remaining hyper-graph is still a random one, since no correlation can arise among the hyper-edges if it was not present at the beginning. When there are no more vertices of degree 1 in the hypergraph the process stops and we call *core* the resulting hypergraph, cleared of all isolated vertices. However, while in poissonian cases we can infer the degree distribution of $k \geq 2$ vertices to remain poissonian during the whole precess [95, 26], when working in a more general case the leaf removal in principle allows for a trajectory in the random graphs ensemble space. The evolution equations at each step can still be written, but one is not guaranteed eny more that the solutions will refer to the starting graph of to some different structure. Since the equations we will retrieve coincide to the ones givin the ferromagnetic thresholds also in the general case, we believe the method to

[38]Rigorously speaking, hyper-loops are not responsible for the ferromagnetic transition, but only for the spi-glass one. The extensive ferromagnetic cluster appears when similar structures that have been called hyper-constraints percolate. A pictorial example of such a structure, which is strictly speaking also a cycle, is given in the right drawing of fig. (1.1). However, in the random hyper-graph these structures are both of typical size $\mathcal{O}(\log N)$ and they differ one from the other by a small stattistical variation of the graph. We therefore infer that tey appear at the same time. This is the physical reason for the coincidence of critical lines at $T = 0$ in the ferromagnetic and in the spin-glass model.

[39]I.e. the growing hyper-graph mean density $\gamma$, if we imagine to randomly grow the hyper-graph from an initial set of disconnected vertices.

work also away from the poissonian case.

The leaf removal algorithm is not able to break up any hyper-loop, since each vertex in the hyperloop has at least degree 2. The $\gamma$ value where the core size becomes different from zero, let us call it $\gamma_d$, is therefore certainly smaller than the percolation point of hyperloops $\gamma_c$ (for $p = 2$ these two values coincide).

The evolution of a hypergraph in extensive time $T \in [0, M]$ under the application of the leaf removal algorithm can be described in terms of the probability, $c_k(t)$, of finding a vertex of degree $k$ after having removed $T = tN$ hyperedges where the rescaled 'time' $t$ ranges from 0 to $\gamma$. let us call $N_k(T)$ the number of surviving vertices of degree $k$ at extensive time $T$, and $M_l(T)$ the number of $l$-edges at time $T$. At time $T+1$ (one leaf removal iteration) we randomly choose vertex of degree one and remove the edge among the vertex belongs to. Therefore the number of zero degree vertices will increase by one, plus the probability $N_1(T)/sum_{k'}k'N_{k'}(T)$ that the other $l-1$ vertices of the erased edge have degree one (in that case also those vertices will have degree zero after the iteration), weighted over the probability $lM_l(T)/\sum_{l'} l'M_{l'}(T)$ of having found a rank $l$ edge. Putting all together one can write:

$$N_0(T+1) = N_0(T) + 1 + \frac{N_1(T)\sum_l (l-1) l M_l(T)}{\sum_{k'} k' N_{k'}(T) \sum_{l'} l' M_{l'}(T)} \tag{2.190}$$

In the same way we can write the evolution equations for $N_k(T)$ as:

$$N_1(T+1) = N_1(T) - 1 + \frac{(2N_2(T) - N_1(T))\sum_l (l-1) l M_l(T)}{\sum_{k'} k' N_{k'}(T) \sum_{l'} l' M_{l'}(T)} \tag{2.191}$$

$$N_{k>1}(T+1) = N_k(T) - 1 + \frac{((k+1)N_{k+1}(T) - kN_k(T))\sum_l (l-1) l M_l(T)}{\sum_{k'} k' N_{k'}(T) \sum_{l'} l' M_{l'}(T)} \ . \tag{2.192}$$

Defining a rescaled time $t = T/N \in [0, \gamma]$ and

$$c_k(t) \equiv \frac{N_k(T)}{N} = \frac{N_k(tN)}{N} \tag{2.193}$$

($c_k(t)$ and $v_l(t)$ are well behaved quantities in the $N$ large limit, with of course $c_k(0) = c_k$ and $v_l(0) = v_l$ of the initial hyper-graph), to the leading order in $N$ we can write the evolution equations (see Ref. [95] for a detailed derivation of similar equations) for the fractions $c_k(t)$ as

$$\begin{aligned}
\frac{\partial c_0(t)}{\partial t} &= \frac{\sum_l l(l-1) v_l(t) c_1(t)}{< l >_t < k >_t} + 1 \quad , \\
\frac{\partial c_1(t)}{\partial t} &= \frac{\sum_l l(l-1) v_l(t)(2c_2(t) - c_1(t))}{< l >_t < k >_t} - 1 \quad , \\
\frac{\partial c_k(t)}{\partial t} &= \frac{\sum_l l(l-1) v_l(t)((k+1)c_{k+1}(t) - k c_k(t)}{< l >_t < k >_t} \qquad \forall k \geq 2 \quad ,
\end{aligned} \tag{2.194}$$

where $< k >_t = \sum_k k c_k(t) =< k > (\gamma - t)$, since the mean degree linearly decreases with time (we remove one interaction per step) and vanishes at $t = \gamma$; while $< l >_t = \sum_l l v_l(t)$. These equations are the generalization of eqs.(22) in [26], since one has to take into account the probability $\propto l v_l$ that the edge removed has rank $l$. It is more convenient in the general case to resort to the generating functional formalism of eqs. (2.5) and (2.6): summing up all power-weighted terms of (2.194) one obtains the general evolution equation

$$\dot{c}(x,t) = (1-x)\left[1 + \frac{v''(1,t)}{v'(1,t)} \frac{c'(x,t)}{c'(1,t)}\right] \tag{2.195}$$

where $\dot{f}(x,t) \equiv \partial f(x,t)/\partial t$ and $f'(x,t) \equiv \partial f(x,t)/\partial x$. On the other hand, we must follow in parallel the evolution equation for the rank fraction $v_l(t)$: we can write

$$M_l(T+1) = M_l(T) - \frac{l M_l(T)}{\sum_{l'} l' M_{l'}(T)} \ , \tag{2.196}$$

Rescaling as the time as before in $t \to tN$ as in the degrees equation and noticing that $M_l(tN) = N v_l(t)$, we are left with:

$$\dot{v}(x,t) = \frac{1}{\gamma - t}\left[v(x,t) - \frac{x v'(x,t)}{v'(1,t)}\right] \tag{2.197}$$

The particular boundary conditions under which we are interested in solving eqs. (2.195) and (2.197) are

$$\begin{aligned} v(x,0) &= v(x) \\ c(x,0) &= c(x) \\ v'(1,0) &= v'(1) = \gamma c'(1) = \gamma c'(1,0) \ . \end{aligned}$$

Eqs (2.195) and (2.197) are standard partial linear differential equations. Exploiting (2.198), after some analytics we can write:

$$v(x,t) = \frac{1}{1-\frac{t}{\gamma}} v\left(x v^{-1}\left(1-\frac{t}{\gamma}\right)\right) \tag{2.198}$$

$$\begin{aligned} c(x,t) &= c\left(1 + \frac{c'\left(c^{-1}\left(1-\frac{t}{\gamma}\right)\right)}{c'(1)}(x-1)\right) + \\ &\quad \gamma(1-x)\left(1 - c^{-1}\left(1-\frac{t}{\gamma}\right)\right) c'\left(c^{-1}\left(1-\frac{t}{\gamma}\right)\right) \end{aligned} \tag{2.199}$$

It is convenient to work in the variable $z \equiv v^{-1}(1 - t/\gamma)$, s.t. the fraction of degree 1 variables can be written as

$$\dot{c}(0,t) = c'\left(1 + \frac{v'(z)}{v'(1)}\right)\frac{c'(z)}{c'(1)} - \gamma(1-z)v'(z) \ . \tag{2.200}$$

A part from the always present $\dot{c}(0,\gamma) = 0$ solution, more non trivial solutions $z^*$ of the equation

$$1 - z^* = \frac{c'\left(1 + \frac{v'(z^*)}{v'(1)}\right)}{c'(1)} \tag{2.201}$$

can be found in certain regions of values of $\gamma$. This equation turns out to be equivalent to the self-consistent condition for the magnetization in the unfrustrated model, found via the replica or the cavity calculation, through the mapping

$$1 - z \implies p_0 \ , \tag{2.202}$$

where we recall $p_0$ to be the fraction of vertices whose spins feel effective field equal to zero. Writing (2.201) in terms of the *link* probability distributions (1.6), we can rescale the generating functions as

$$c^{link}(x) = \frac{c'(x)}{c'(1)}$$

$$v^{link}(x) = \frac{v'(x)}{v'(1)}$$

so that to obtain:

$$1 - z^* = c^{link}\left[1 - v^{link}(z^*)\right] \ . \tag{2.203}$$

Armed with the results of the previous sections, we'll call $\gamma_d$ the graph density at the particular $z_d^*$ the point where (2.201) is satisfied together with its $z$-derivative

$$\frac{\partial c^{link}\left[1 - v^{link}(z)\right]}{\partial z}_{|_{z^*}} + 1 = 0 \tag{2.204}$$

This corresponds to the first time a non trivial solution appear. Beyond that point, form the leaf removal process point of view, we are prescribed to take as the valid $z^*$ the largest solution of (2.201), as the point where the algorithm halts. to $z^*$ will correspond a halting time $t^* = \gamma(1 - c(z^*))$. In the particular case of Poissonian $p$-spin, the solutions of (2.201) can be recast in the particular form

$$\lambda(t) = p\left[\gamma(\gamma - t)^{p-1}\right]^{\frac{1}{p}} \quad , \tag{2.205}$$

$$c_1(t) = \lambda(t)\left[e^{-\lambda(t)} - 1 + \left(\frac{\lambda(t)}{p\gamma}\right)^{\frac{1}{p-1}}\right] \quad , \tag{2.206}$$

$$c_0(t) = 1 - \sum_{k=1}^{\infty} c_k(t) \quad . \tag{2.207}$$

where $\lambda(t) =< k >_t - c_1(t) + \lambda(t)e^{-\lambda(t)}$ is the mean degree of all the vertices of $k \geq 2$ at time $t$. As in the general case, the leaf removal algorithm stops when there are no more vertices of degree 1, so one can predict the resulting core by fixing $\lambda(t) = \lambda^*$, where $\lambda^*$ is the largest zero of the equation $c_1(t^*) = 0$ or equivalently

$$e^{-\lambda^*} - 1 + \left(\frac{\lambda^*}{p\gamma}\right)^{\frac{1}{p-1}} = 0 \quad . \tag{2.208}$$

As before, notice that once we define $z^* = [\lambda^*/(p\gamma)]^{1/(p-1)}$, eq. (2.208) can be rewritten as

$$1 - z^* = \exp\left(-p\gamma(z^*)^{p-1}\right) \quad , \tag{2.209}$$

eq. (2.203) (or its particular case (2.209)) coincides with (2.89) and (2.182), the equation for the backbone size in any 1RSB cluster, the fraction of variables $(z^*)^2 = (1 - t)$ with a non trivial distribution of cavity $u$ or $h$-fields. Incidentally, we observe here that eq. (2.203) is the same equation appearing in parity check diluted error correcting codes theory as the convergence threshold for sum-product or belief propagation (BP) algorithms in the corrupted message reconstruction process. This coincidence is not surprising from a statistical physics point of view: indeed, we will see in chapter 5 how the mapping between spin systems on diluted hypergraphs and and such kind of codes interprets the low performance of BP-like algorithms in terms of a dynamical phase transition. At $t^*$, $z^*$ gives us the size of the core. In the $l = 2$ case the leaf removal algorithm is able to delete all the edges only for tree-like graphs. As soon as there are loops in the graph, a core containing these loops arises (see fig. 2.26). In a random graph the leaf removal transition coincides with the percolation one at $\gamma_{perc} = 1/2$. The shape of the function $c_1(\lambda)$ is shown in fig. 2.24 for Poissonian graphs and is similar in the general case: For $\gamma \leq \gamma_{perc}$, there is only one zero in $\lambda^* = z^* = 0$; While, for $\gamma > \gamma_{perc}$, $\lambda^* > 0$ , $z^* > 0$ and

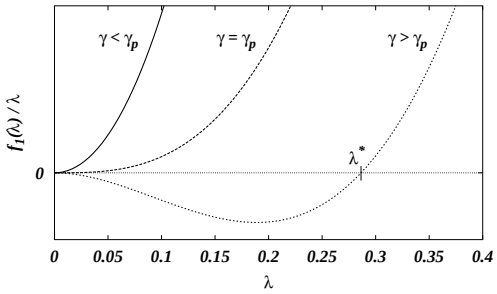



Figure 2.24: The function $c_1(\lambda)/\lambda$ for $l = 2$.

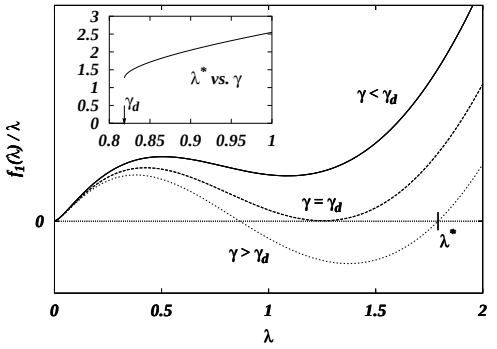



Figure 2.25: The function $c_1(\lambda)/\lambda$ for $l = 3$. Inset: function $\lambda^*(\gamma)$ for $l = 3$.

a core arises, whose size grows as $(\gamma - \gamma_{perc})^2$ near the critical point. For $l > 2$ the percolation transition, taking place for example at $\gamma_{perc} = \frac{1}{l(l-1)}$ for fixed rank, does not affect at all the leaf removal algorithm which is able to delete all the hyper-edges, even those forming loops (but not hyper-loops), far beyond $\gamma_{perc}$ (see fig. 2.27). The shape of the function $c_1(\lambda)$ for $l = 3$ and Poissonian graphs is shown in fig. 2.25. It is clear (see inset of fig.( 2.25)) that when $\lambda^*(\gamma)$ becomes different from zero it directly jumps to a finite value: $\lambda^*(\gamma_d) = 1.25643$ for $l = 3$. The core transition is therefore discontinuous unless it is driven by simple 2-loops percolation.

### 2.7.3 The core and the calculation of the $\gamma_c$ threshold

In the core, the number of vertices $N_c$ and the number of hyper-edges $M_c$ can be expressed as a function of the distributions $v$ and $c$, $\gamma$ and $z^*$ as

$$\begin{aligned} M_c &= N(\gamma - t^*) = N\gamma v(z^*) \\ N_c &= N(1 - c(0, z^*)) \\ c(0, z^*) &= c\left(1 - \frac{v'(z^*)}{v'(1)}\right) + \gamma(1 - z^*)v'(z^*) \end{aligned} \tag{2.210}$$

The first equation states that the number of hyper-edges left is the initial one minus the number of step the leaf removal algorithm has been run (during each step only one hyper-edge is deleted). The lower curves in fig. 2.28 show the normalized number of vertices $N_c/N$ and number of interactions $M_c/N$ in the core as a function of $\gamma$, for $l = 3$ and Poissonian degrees. It is natural now to study the residual problem on the core, $\hat{A}_c\,\vec{x}_c = \vec{y}_c\ mod[2]$, where $\hat{A}_c$ is the $M_c \times N_c$ sparse random matrix obtained from $\hat{A}$ deleting all the rows corresponding to removed interactions and all empty columns. In the rest of the subsection we will derive a general result

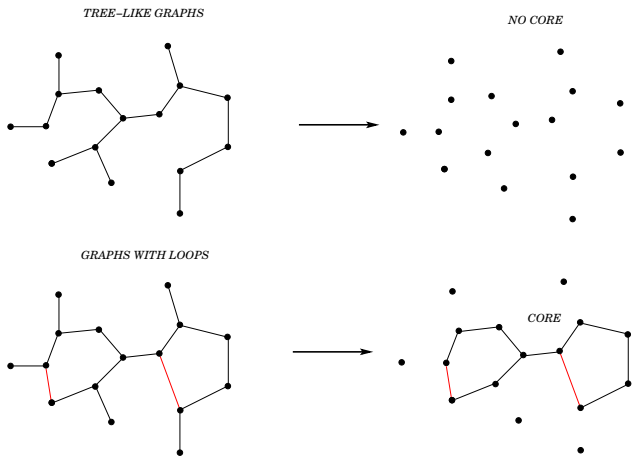



Figure 2.26: Core on $l = 2$ graphs.

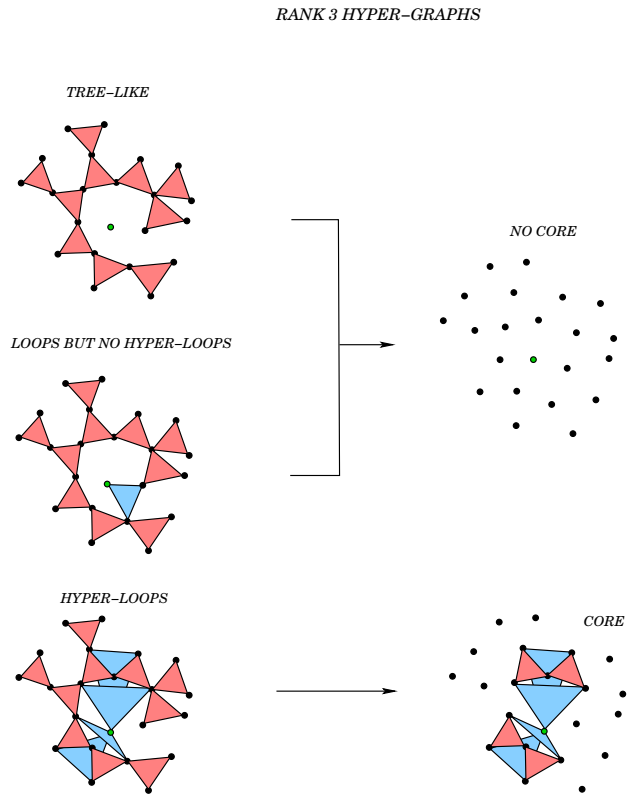



Figure 2.27: Core on hyper-graphs.

that, when applied to the problem on the core, gives a necessary and sufficient condition for the existence of solutions to the core linear system. Then we will show that, from a solution in the core, a solution for the original system can always be constructed.

Let us call $\mathcal{N}_{\mathbf{J},\mathbf{N},\mathbf{M}}$ the number of GS for a given disorder realization $\mathbf{J}$ (i.e. a given hyper-graph and couplings realization consistent with distribution $\mu(\mathbf{J})$):

$$\mathcal{N}_{\mathbf{J},N,M} = \sum_{\vec{\sigma}} \prod_{m=1}^{M} \delta(\sigma_{i_1^m} \dots \sigma_{i_p^m} = J_m) \ . \tag{2.211}$$

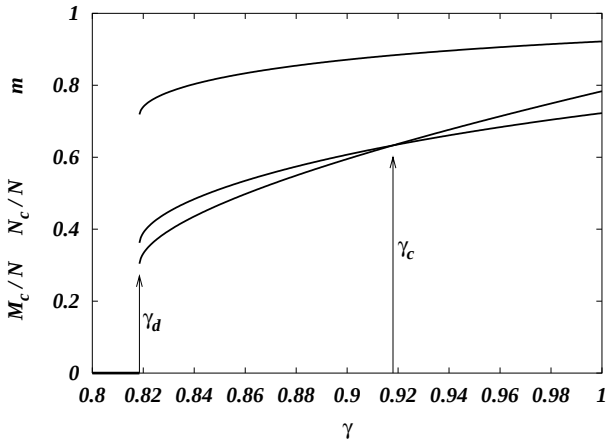



Figure 2.28: From bottom to top (on the left): For $l = 3$, normalized number of hyper-edges and vertices in the core, and fraction of frozen sites, i.e. magnetization (or backbone) in a state.

In [26] the authors show that, in the large $N$ limit, if the hyper-graph does not contain any vertex of degree less than 2, $\mathcal{N}_{\mathbf{J},\mathbf{N},\mathbf{M}}$ is a self averaging quantity, that is it does not fluctuate changing $\mathbf{J}$. In order to show self-averageness they proved that, on hyper-graphs ($p > 2$) with minimum degree at least 2, the following equalities hold

$$\overline{\mathcal{N}_{\mathbf{J},\mathbf{N},\mathbf{M}}} = 2^{N-M} \ , \ \lim_{N\to\infty} \frac{\overline{\mathcal{N}^2_{\mathbf{J},\mathbf{N},\mathbf{M}}} - \left(\overline{\mathcal{N}_{\mathbf{J},\mathbf{N},\mathbf{M}}}\right)^2}{\left(\overline{\mathcal{N}_{\mathbf{J},\mathbf{N},\mathbf{M}}}\right)^2} = 0 \ , \tag{2.212}$$

where the over-line stands for the average over the disorder ensemble, that is over the ways of choosing $M$ hyper-edges among $\binom{N}{p}$ and the ways of giving them a sign $J_m = \pm 1$. The above equalities state that the probability distribution of $\mathcal{N}_{\mathbf{J},\mathbf{N},\mathbf{M}}$ over the disorder ensemble is a delta function, and thus the quenched average equals the annealed one

$$\overline{\log \mathcal{N}_{\mathbf{J},\mathbf{N},\mathbf{M}}} = \log \overline{\mathcal{N}_{\mathbf{J},\mathbf{N},\mathbf{M}}} = \log(2)\,(N - M) \ . \tag{2.213}$$

For the interested reader that survived the calculations of the previous sections, calculating the momenta of $\mathcal{N}_{\mathbf{J},\mathbf{N},\mathbf{M}}$ following [26] should be simple. We only state the results in the general distributed hyper-graphs case: The second moment is given by

$$\overline{\mathcal{N}^2_{\mathbf{J},\mathbf{N},\mathbf{M}}} = 2^{N-M} \overline{\sum_{\vec{\tau}} \prod_{m=1}^{M} \delta(\tau_{i_1^m} \dots \tau_{i_p^m} = 1)} \to 2^{N-M} e^{-N \sum_k c_k \log\left(x_+^k + x_-^k\right)} \ , \tag{2.214}$$

in the thermodynamic limit, where $x_+, x_-$ solve the following equations

$$x_+ + x_- = \frac{1}{< l >} \sum_l l v_l \left[ \sum_k \frac{k c_k}{\langle k \rangle} \frac{x_+^{k-1} + x_-^{k-1}}{x_+^k + x_-^k} \right]^{l-1} \ , \tag{2.215}$$

$$x_+ - x_- = \frac{1}{< l >} \sum_l l v_l \left[ \sum_k \frac{k c_k}{\langle k \rangle} \frac{x_+^{k-1} - x_-^{k-1}}{x_+^k + x_-^k} \right]^{l-1} \ . \tag{2.216}$$

This is simply the output of the annealed calculation of the $p$-spin model, where the functional order parameter are replaced by scalars $x_\pm$. The annealed calculations do not make use of

replicas and are therefore rigorous. The value of $x_+$ (resp. $x_-$) is proportional to the fraction of variables taking values 1 (resp. -1) in the set of configurations which maximize the last sum in eq. (2.214). Then the typical magnetization of this model is given by $m = \frac{x_+ - x_-}{x_+ + x_-}$. Solutions to eqs.(2.215,2.216) can be classified depending on the value of magnetization $m$. In full generality there are 3 solutions: a first symmetric one ($x_+ = x_-$) with $m = 0$, a second one with large magnetization and a third one with an intermediate value of $m$. For some choices of $P(k)$ (e.g. a Poissonian) solutions with $m > 0$ may exist only for $\frac{M}{N}$ large enough. The solution with intermediate magnetization always corresponds to a minimum of $F_{N,M}$ and can be in general neglected. The symmetric solution $x_+ = x_- = 2^{-1/l}$ always exists and gives $F_{N,M} = \log(2)\,(1 - \frac{M}{N})$. For $l > 2$ and $P(0) = P(1) = 0$, i.e. for hyper-graphs with minimum degree 2, the solution with large magnetization also exist for any $\gamma$ value and has $x_+ = 1$, $x_- = 0$ and $F_{N,M} = 0$. As expected, the intermediate solution, when it exists, has negative entropy and therefore is not the physical one. Then, for $l > 2$ and $P(0) = P(1) = 0$, we can conclude that $\sum_k c_k \log\left(x_+^k + x_-^k\right) = 0$, equalities in eq. (2.212) hold, and the number of GS is a self-averaging quantity. Since the core generated by the leaf removal algorithm has minimum degree 2, we may apply the above result, and find that the SAT/UNSAT threshold is given by the condition

$$N_c(\gamma_c) = M_c(\gamma_c)\ . \tag{2.217}$$

For the Poissonian 3-spin this last condition gives precisely the ferromagnetic and the 1RSB spin-glass threshold $\gamma_c = 0.917935$.

For more complicated rank distributions, however, another ($x_\pm \neq 2^{-1/l}$) solution can appear and give a value for the entropy higher than zero. When it is the case, this solution is always the one corresponding to the continuous phase transition of the rank 2 sub-graph. The condition for the existence of a tricritical crossover point is given by the simultaneous satisfaction of (2.203), (2.204), (2.217) and $v_2 = 1/2\gamma$, that reduce to:

$$\gamma_{tricritical} = \frac{< k >^2}{2v_2 < k(k-1) >} = \frac{3 < k(k-1) >^2}{< k >< k(k-1)(k-2) >} \quad . \tag{2.218}$$

In the Poissonian degrees case this reduces to $v_2 = 3v_3 = 1/2\gamma_{tricritical}$. The presence of this continuous transition was related in previous work - in models as the $2+p$-SAT - to a crossover between problems with typical[40] P to typical NP complexity [11]. A simpler model that can be studied in full detail and shows this kind of crossover behavior is the $@+p$-XOR-SAT. Results are reported in the next chapter. It will be interesting to see (chapter 5) that a large *fauna* of models exists, due to the freedom in degree and rank distributions choices in the generalized $p$-spin model (and in principle for a wider class of Hamiltonians treatable with similar means). In some cases it is easy to see that no crossover tricritical point exists, but a general core develops at $\gamma_d$, followed by 2-loops percolation in the subgraphs *before* condition (2.217) is fulfilled on the embedding hyper-graph.

### 2.7.4 Ground States Clustering

Before the SAT/UNSAT threshold ($\gamma \leq \gamma_c$) the system is not frustrated and then a gauge transformation setting all coupling signs to 1 can always be found: Given an unfrustrated GS

[40] Notice that the notion of typical computational complexity is however not well defined and some very recent results [30, 58] seem to show no concept of NP complexity in the typical case, even though the role and nature of the phase transitions encountered are still crucial in the heuristic understanding of the hardness onset and on the clever algorithm design.

$\vec{\sigma}^0$ a possible gauge transformation is $\sigma'_i = \sigma_i \sigma_i^0$ and $J'_m = J_m \sigma_{i_1^m}^0 \ldots \sigma_{i_p^m}^0 = 1$. It is then possible to consider only the ferromagnetic system ($J_m = 1 \; \forall m$), which corresponds to the linear system $\hat{A}\,\vec{x} = \vec{0}\; mod[2]$. This is also what it will be done in a more complete study of the computational cost and memory transition of sparse systems solving algorithms in chapter 5. The solutions to the linear system we are studying form a group: The sum of 2 solutions is still a solution and the null element is the solution $\vec{x} = \vec{0}$. Therefore, if one looks at the configurational space sitting on a reference GS, the set of GS will look the same, whatever the reference GS is. An immediate consequence of this symmetry is that, *if GS form clusters, these clusters must be all of the same size.*

For $\gamma \leq \gamma_c$, hyper-loops are absent and the total number of GS (or solutions) is always given by $2^{N-M}$, i.e. their entropy is $S(\gamma) = \log(2)\,(1-\gamma)$. From the previous calculations it is possible to divide the $N$ variables in 2 sets: $\vec{x}_c$ represents the $N_c$ variables in the core, and $\vec{x}_{nc}$ the $N - N_c$ variables in the non-core part of the hyper-graph, that is variables corresponding to vertices remained isolated at the end of the leaf removal process. Thus also the entropy can be divided in 2 parts. One part is given by the solutions in the core, that is by the possible assignments of $\vec{x}_c$,

$$S_c(\gamma) = \log(2)\frac{N_c(\gamma) - M_c(\gamma)}{N} \quad , \tag{2.219}$$

which is non-negative for $\gamma_d \leq \gamma \leq \gamma_c$. The other part is given by the possible multiple assignments of $\vec{x}_{nc}$ during the reconstruction process

$$S_{nc}(\gamma) = S(\gamma) - S_c(\gamma) \quad . \tag{2.220}$$

fig. (2.29) is a pictorial representation of the $N$-dimensional hypercube (represented as a spherical surface for convenience) of variables assignments binary vectors $\vec{x} = (x_1, ...., x_2)$. The conjecture, supported by numerics, is that *solutions are concentrated in clusters, each one of them around a reference one which is one of the solutions of the core-reduced system.* By def-

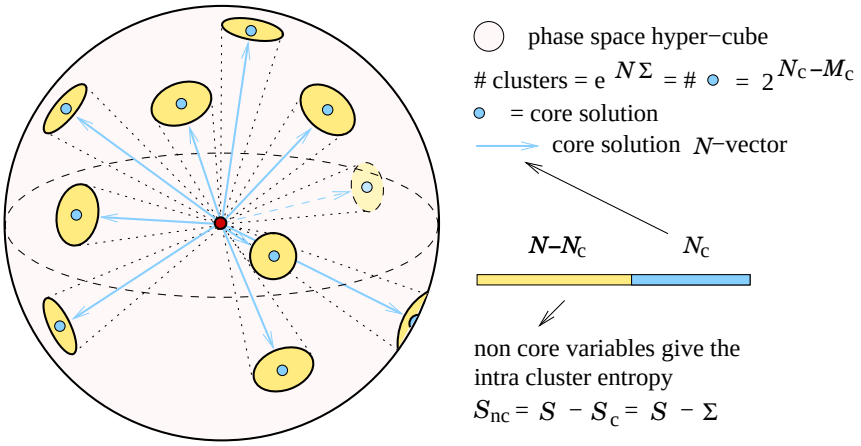



Figure 2.29: Pictorial representation of clustering of solutions in the dynamical region $[\gamma_d, \gamma_c]$.

inition, a cluster is a set of solutions with finite Hamming distance $d$ such that $d/N \to 0$ as $N \to \infty$. In virtue of the group symmetry property property, all the clusters have the same size. We call their number is $e^{N\Sigma(\gamma)}$, where $\Sigma(\gamma)$ is indeed the complexity Of the system. If the

conjecture represented in fig. (2.29) is true, the number of clusters must equal the number of solutions in the core, that is

$$\Sigma(\gamma) = S_c(\gamma) \quad . \tag{2.221}$$

The intra-cluster entropy, i.e. the normalized logarithm of the cluster size, is then given by the non-core entropy $S_{nc}(\gamma) = S(\gamma) - S_c(\gamma) = S(\gamma) - \Sigma(\gamma)$. In order to prove the validity of (2.221) the authors of [26] were able to show that:

- all the solution assignments of the core variables $\vec{x}_c$ are "well separated", that is the distance among any pair of them is extensive. This is what gives rise to the clustering, with a number of clusters which is at least as large as the number of core solutions ($\Sigma \geq S_c$).
- then, for any fixed $\vec{x}_c$, all possible assignments of non-core variables $\vec{x}_{nc}$ belong to the same cluster, and so $\Sigma = S_c$.

The first step is accomplished by calculating the probability distribution of the distance among any two solutions in the core. Thanks to the group property, one can restrict the calculation fixing one solution to the null vector $\vec{0}$, working again with the ferromagnetic model. For simplicity the authors have performed an annealed average, but this does not invalidate the exactness of the results because in can be proved via the Jensen inequality that the annealed average gives a lower bound on the core solutions distances, which is enough for the validity of the proof. These last two steps of the calculations are identical in the general and in the Poissonian 3-spin case, so we refer back to the original paper [26] where they are explained in details. As far as the complexity remains positive, the core system has an exponential number of solutions and it is therefore solvable (SAT). It is then always possible to assign values to the non core variables so that the original system is also always solvable. Since the complexity goes to zero at $\gamma_c$, beyond that threshold the core linear system only have exponentially rare solutions in $N$. We are therefore in the USAT region. Changing the values of the non core variables does not allow to find a core solution different form the starting one (absent in this case), so we cannot solve the original system if we cannot start from a core solution as a starting point: the larger system is not solvable if a core subsystem of it leads to contradiction. Having proved identity (2.221), eq. (2.217) therefore provides the exact threshold for random XOR-SAT satisfiability. We stress once more that these results coincide with the general 1RSB/cavity solution and with the heuristic derivation of the complexity curve via the study of the metastable states of the ferromagnetic model via the factorized Ansatz.

# Chapter 3

# Some particular cases of interest

## 3.1 The 2+p-XOR-SAT model: role of phase coexistence and finite-size scaling

The statistical mechanics study of random $K$-SAT have provided some geometrical understanding of the onset of complexity at the phase transition through the introduction of a functional order parameter which describes the geometrical structure of the space of solutions. The nature of the SAT/UNSAT transition for the different values of $K$ appears to be a particularly relevant prediction [31]. The SAT/UNSAT transition is accompanied by a smooth (respectively abrupt) change in the structure of the solutions of the 2-SAT (resp. 3-SAT) problem. More specifically, at the phase boundary a finite fraction of the variables become fully constrained while the entropy density remains finite. Such a fraction of frozen variables (i.e. those variables which take the same value in all solutions) may undergo a continuous (2-SAT) or discontinuous (3-SAT) growth at the critical point. This discrepancy is responsible for the difference of typical complexities of both models recently observed in numerical studies. The typical solving time of search algorithms displays an easy-hard pattern as a function of $\gamma$ with a peak of complexity close to the threshold. The peak in search cost seems to scale polynomially with $N$ for the 2-SAT problem and exponentially with $N$ in the 3-SAT case. From an intuitive point of view, the search for solutions ought to be more time-consuming in presence of a finite fraction of fully quenched variables since the exact determination of the latter requires an almost exhaustive enumeration of their configurations. To test this conjecture, a mixed $2+p$-model has been proposed, including a fraction $p$ (resp. $1-p$) of clauses of length two (resp. three) and thus interpolating between the 2-SAT ($p=0$) and 3-SAT ($p=1$) problems. The statistical mechanics analysis predicts that the SAT/UNSAT transition becomes abrupt when $p > p_0 \simeq 0.4$ [31, 13, 11, 14]. Precise numerical simulations support the conjecture that the polynomial/exponential crossover occurs at the same critical $p_0$. Though the problem is both critical ($\gamma_c = 1/(1-p)$ for $p < p_0$) and NP-complete for any $p > 0$, it is only when the phase transition becomes of the same type of the 3-SAT case that hardness shows up. An additional argument in favor of this conclusion is given by the analysis of the finite-size effects on $P_N(\gamma, K)$ and the emergence of some universality for $p < p_0$. A detailed account of these findings may be found in [31, 13, 11, 14, 9]. For $p < p_0$ the exponent $\nu$, which describes the shrinking of the critical window where the transition takes place, is observed to remain constant and close to the value expected for 2-SAT. The critical behavior is the same of the percolation transition in random graphs (see also ref. [53]). For $p > p_0$ the size of the window shrinks following some

$p$-dependent exponents toward its statistical lower bound [119] but numerical data did not allow for any precise estimate. In this section, we study an exactly solvable version of the random 2+p SAT model which displays new features and allows us to settle the issue of universality of the critical exponents. The threshold of the model can be computed exactly as a function of the mixing parameter $p$ in the whole range $p \in [0,1]$. Rare events are found to be dominant also in the low $\gamma$ phase, where a coexistence of satisfiable and unsatisfiable instances is found. A detailed analysis for the $p = 1$ case can be found in ref. [19]. The existence of a global – polynomial time – algorithm for determining satisfiability allows us to perform a finite size scaling analysis around the exactly known critical points over huge samples and to show that indeed the exponent controlling the size of the critical window ceases to maintain its constant value $\nu = 3$ and becomes dependent on $p$ as soon as the phase transition becomes discontinuous, i.e. for $p > p_0 = .25$. Above $p_0$ and below $p_1 \sim 0.5$, the exponent $\nu$ takes intermediate values between 3 and 2. Finally, above $p_1$ the critical window is determined by the statistical fluctuations of the quenched disorder [119] and so $\nu = 2$.

### 3.1.1 Model definition and outline of some results

The model we study can be viewed as the mixed $2+p$ extension of the 3-*XOR-SAT* (or hSAT) model discussed in [19], as much as the $2+p$-SAT [31] is an extension of the usual $K$-SAT model. In computer science literature and its critical behavior was still recently considered an open issue [82]. We can write an instance of our model as a mixture of 2 and 4-clauses sets defined in chapter 1 (with 50% satisfying assignments). A compact definition can be achieved by the use of the exclusive OR operator $\oplus$, e.g. $C(ijk|+1) = x_i \oplus x_j \oplus x_k$. Then, we randomly choose two independent sets $E_3$ and $E_2$ of $pM$ triples $\{i,j,k\}$ and $(1-p)M$ couples $\{i,j\}$ among the $N$ possible variable indices (see section 2.1 for definitions) and respectively $pM$ and $(1-p)M$ associated unbiased and independent random variables $T_{ijk} = \pm 1$ and $J_{ij} = \pm 1$, and we construct a Boolean expression in Conjunctive Normal Form (CNF) as

$$F = \bigwedge_{\{i,j,k\} \in E_3} C(ijk|T_{ijk}) \bigwedge_{\{i,j\} \in E_2} C(ij|J_{ij}) \ . \tag{3.1}$$

As in [19], we can build a *satisfiable* version of the model choosing clauses only of the $C(ij|+1)$ and $C(ijk|+1)$ type. For $p < p_0$ the problem is easily solved by local and global algorithms, whereas interesting behaviors are found for $p > p_0$, where the local algorithms fail. The above combinatorial definition can be recast in a simpler form as a minimization problem of a cost-energy function on a topological structure which is a mixture of a random graph (2-spin edges) and hyper-graph (3-spin hyper-edges). We end up with a diluted spin model where the Hamiltonian reads

$$H_J[\mathbf{S}] = M - \sum_{\{i,j,k\} \in E_3} T_{ijk}\, S_i S_j S_k - \sum_{\{i,j\} \in E_2} J_{ij}\, S_i S_j \ , \tag{3.2}$$

where the $S_i$ are binary spin variables and the the random couplings can be either $\pm 1$ at random. The satisfiable version is nothing but the ferromagnetic model: $T_{ijk} = 1$ and $J_{ij} = 1$ for any edge. As the average connectivity $\gamma$ of the underlying mixed graph grows beyond a critical value $\gamma_c(p)$, the *frustrated* model undergoes a phase transition from a mixed phase in which satisfiable instances and unsatisfiable ones coexist to a phase in which all instances are unsatisfiable. At the same $\gamma_c(p)$ the associated spin glass system, undergoes a zero temperature glass transition where frustration becomes effective and the ground state energy is no longer

the lowest one (i.e. that with all the interactions satisfied). At the same critical point the *unfrustrated*, i.e. ferromagnetic, version undergoes a para–ferro transition, because the same topological constraints that drive the glass (mixed SAT/UNSAT to UNSAT) transition in the frustrated model are shown to be the ones responsible for the appearance of a nonzero value of the magnetization in the unfrustrated one [19]. We shall take advantage of such coincidence of critical lines by making the analytical calculation for the simpler ferromagnetic model. Moreover, the nature of the phase transition changes from second to random first order, when $p$ crosses the critical value $p_0 = 1/4$. For $p > p_0$ the critical point $\gamma_c(p)$ is preceded by a dynamical glass transition at $\gamma_d(p)$ where ergodicity breaks down and local algorithms get stuck (local algorithms are procedures which update the system configuration only by changing a finite number of variable at the same time, e.g. all single or multi spin flip dynamics, together with usual computer scientists heuristic algorithms). The dynamical glass transition exist for both versions of the model [20] and corresponds to the formation of a locally stable ferromagnetic solution in the unfrustrated model [22] (the local stability is intimately related to the ergodicity breaking). Specializing to the present case the general results of the first chapter, we can look for a self consistent Ansatz for the zero temperature effective fields distribution $P(h)$ in the satisfiable case., which turns out to have the following simple form

$$P(h) = \sum_{l \geq 0} r_l \delta(h - l) \quad , \tag{3.3}$$

with a self-consistency equation for $r_0$:

$$r_0 = e^{-3p\gamma(1-r_0)^2 - 2(1-p)\gamma(1-r_0)} = \sum_{c_1=0}^{\infty} \sum_{c_2=0}^{\infty} e^{-3p\gamma} e^{-2(1-p)\gamma} \frac{(3p\gamma)_1^c}{c_1!} \frac{(2(1-p)\gamma)_2^c}{c_2!} (1-(1-r_0)^2)^{c_1} (r_0)^{c_2} \quad . \tag{3.4}$$

The equations for the frequency weights $r_l$ with $l > 0$ follow from the one for $r_0$ and read

$$r_l = \frac{[3p\gamma(1-r_0)^2 + 2(1-p)\gamma(1-r_0)]^l}{l!} \quad . \tag{3.5}$$

The previous self consistency equations for $r_0$ (or for the magnetization $m = 1 - r_0$) can easily be derived by the same probabilistic argument used in [19], due to the fact that the clause independence allows to treat the graph and the hyper-graph part separately. Note that in the simple limit $p = 0$ we retrieve the equation for the percolation threshold in a random graph of connectivity $\gamma$ [61, 62, 67]. The ground state entropy can be written in the SAT phase as:

$$S(\gamma) = \log(2)[r_0(1 - \log(r_0)) - \gamma(1-p)(1-(1-r_0)^2) - \gamma p(1-(1-r_0)^3)] \tag{3.6}$$

To find the value of the paramagnetic entropy we put ourself in the phase where all sets of 4- and 2-clauses act independently, each therefore dividing the number of allowed variables choice by two: the number of ground states will be $N_{gs} = 2^{N - p\gamma N - (1-p)\gamma N} = 2^{N(1-\gamma)}$. The resulting value of $S_{para} = (1-\gamma)\log(2)$ coincides with the one found setting $r_0 = 1$ in eq.(3.6). Solving the saddle point equation for $r_0$, we find that a paramagnetic solution with $r_0 = 1$ always exists, while at a value of $\gamma = \gamma_d(p)$ there appears a ferromagnetic solution in the satisfiable model. For $p = 0$, the critical value coincides as expected with the percolation threshold $\gamma_d(0) = 1/2$. As long as the model remains like 2-SAT, up to $p < p_0 = 0.25$, the threshold is the point where the ferromagnetic solution appears and also where its entropy exceeds the paramagnetic one. The critical magnetization is zero and the transition is continuous. For larger values

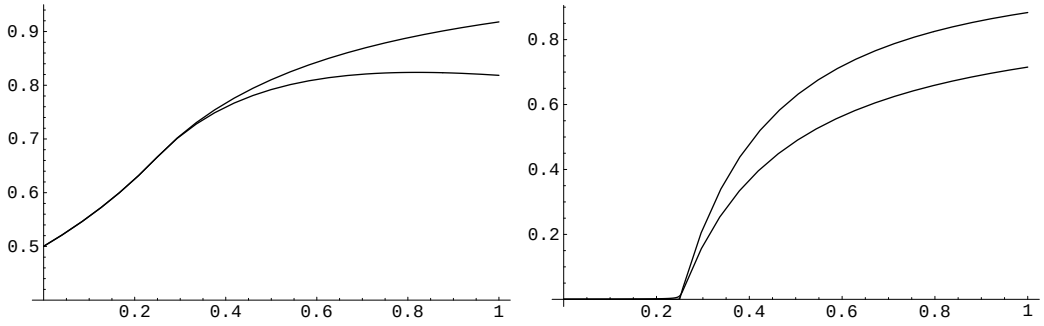



Figure 3.1: Critical lines (the upper is the static and lower the dynamic) in the $(\gamma, p)$ plane. Tricritical point point $(0.25, 0.667)$ separates continuous transitions from discontinuous ones (where $\gamma_d < \gamma_c$).

Figure 3.2: Critical magnetizations at $\gamma_d(p)$ and $\gamma_c(p)$ versus $p$.

of the control parameter $p$ the transition becomes discontinuous. There appears a dynamical transition at $\gamma = \gamma_d(p)$ where locally stable solutions appear. At $\gamma = \gamma_c(p) > \gamma_d(p)$, the non trivial $r_0 \neq 1$ solution acquires an entropy larger than the paramagnetic one and becomes globally stable. The shape of $\gamma = \gamma_d(p)$ and $\gamma = \gamma_c(p)$ as functions of $p$ are shown in fig. 3.1. The inset picture shows the magnetization of the model at the points where the dynamical and the static transitions take place.

### 3.1.2 Numerical simulations

The model can be efficiently solved by a polynomial algorithm based on a representation modulo two (i.e. in Galois field GF[2]). The same techniques will be exploited in chapter four, where we will stress the physical implication of such a mapping for the memory and CPU cost transitions met by algorithms trying to solve linear systems modulo two built in order to correspond to the spin model in the dynamical region. If a formula can be satisfied, then a solution to the following set of $M$ equations in $N$ variables exists

$$\left\{ \begin{array}{rcll} S_i S_j S_k & = & T_{ijk} & \forall \{i,j,k\} \in E_3 \\ S_i S_j & = & J_{ij} & \forall \{i,j\} \in E_2 \end{array} \right. \tag{3.7}$$

Through the mapping $S_i = (-1)^{\sigma_i}$, $J_{ij} = (-1)^{\eta_{ij}}$ and $T_{ijk} = (-1)^{\zeta_{ijk}}$, with $\sigma_i, \eta_{ijk}, \zeta_{ijk} \in \{0,1\}$, eq.(3.7) can be rewritten as a set of binary linear equations

$$\left\{ \begin{array}{rcll} (\sigma_i + \sigma_j + \sigma_k) \bmod 2 & = & \zeta_{ijk} & \forall \{i,j,k\} \in E_3 \\ (\sigma_i + \sigma_j) \bmod 2 & = & \eta_{ij} & \forall \{i,j\} \in E_2 \end{array} \right. \tag{3.8}$$

For any given set of couplings $\{\eta_{ij}, \zeta_{ijk}\}$, the solutions to these equations can be easily found in polynomial time by e.g. Gaussian substitution. The solution to the $M$ linear equations in $N$ variables can be summarized as follows: a number $N_{dep}$ of variables is completely determined by the values of the coupling $\{\eta_{ij}, \zeta_{ijk}\}$ and by the values of the $N_{free} = N - N_{dep}$ independent variables. The number of solutions is $2^{N_{free}}$ and the entropy $S(\gamma) = \log(2) N_{free}/N = \log(2)(1 - N_{dep}(\gamma)/N)$. As long as $N_{dep} = M$ we have the paramagnetic entropy $S_{para} = \log(2)(1-\gamma)$. However $N_{dep}$ may be less than $M$ when the interactions are such that one can generate linear combinations of equations where no $\sigma$'s appear, like $0 = f(\{\eta_{ij}, \zeta_{ijk}\})$. This kind of equations

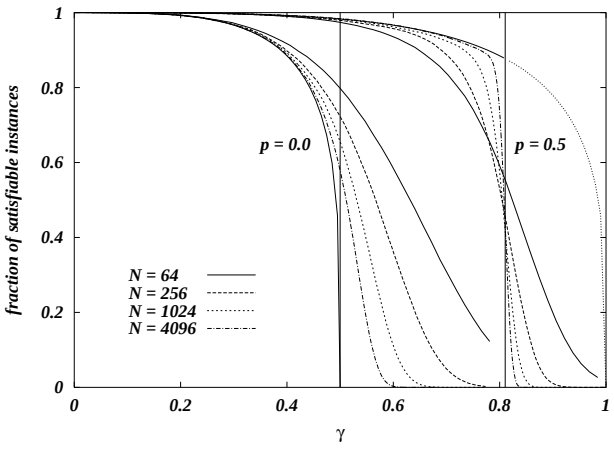



Figure 3.3: SAT probabilities $P_{SAT}(\gamma, p)$ for $p = 0$ and $p = 0.5$. Data has been averaged over $10^4$ different random hyper-graphs. Vertical straight lines are analytical predictions for critical points: $\gamma_c(p = 0) = 0.5$ and $\gamma_c(p = 0.5) = 0.810343$. Bold curves for $\gamma < \gamma_c$ are analytical predictions for the SAT probability in the large $N$ limit.

correspond to the presence of loops (resp. hyper-loops [19]) in the underlying graph (resp. hyper-graph). A hyper-loops (generalization of a loop on a hyper-graph) is defined as a set $\mathcal{S}$ of hyper-edges such that every spin (i.e. node) is "touched" by an even number of hyper-edges belonging to $\mathcal{S}$ (see fig. 3.4). Here we are interested in the fraction of satisfiable instances $P_{SAT}(\gamma, p)$, averaged over the random couplings distribution. One can show that, for any random hyper-graph, $P_{SAT}$ is given by $2^{-N_{hl}}$, where $N_{hl}$ is the number of independent hyper-loops [19]. In fig. 3.3 we show the fraction of satisfiable instances as a function of $\gamma$ for $p = 0$ and $p = 0.5$. The vertical lines report the analytical predictions for the critical points, $\gamma_c(p = 0) = 0.5$ and $\gamma(p = 0.5) = 0.810343$. In the limit of large $N$ and for $p = 0.5$ the fraction of SAT instances sharply vanishes at the critical point in a discontinuous way, that is $\lim_{\gamma \to \gamma_c^-} P_{SAT}(\gamma) > 0$ while $\lim_{\gamma \to \gamma_c^+} P_{SAT}(\gamma) = 0$. This is the usual behavior already measured in 3-SAT [31, 13] and 3-hyper-SAT [19], with the SAT probabilities measured on finite systems crossing at $\gamma_c$ and becoming sharper and sharper as $N$ increases. On the contrary for $p = 0$ and large $N$ the probability of being SAT becomes zero at $\gamma_c$ in a continuous way. The main consequence is that finite size corrections make $P_{SAT}(\gamma)$ larger than its thermodynamical limit both before and after the critical point and thus the data crossing is completely missing. Note also that for $p < 1$ the fraction of SAT instances for $\gamma < \gamma_c(p)$ is finite and less than 1 even in the thermodynamical limit, implying a *mixed phase* of SAT and UNSAT instances. This is due to the presence in the random hyper-graph of loops made only by 2-spin edges (indeed the mixed phase is absent for $p = 1$ when only 3-spin interactions are allowed [19]). The expression for the SAT probability in the thermodynamical limit (bold curves in fig. 3.3, the lower most for $p = 0$ and the uppermost for $p = 0.5$) can be calculated analytically and the final result has been obtained in [21] and reads

$$P_{SAT}(\gamma, p) = e^{\frac{1}{2}\gamma(1-p)[1+\gamma(1-p)]} \left[1 - 2\gamma(1-p)\right]^{1/4} \qquad \text{for} \quad \gamma \leq \gamma_c(p) \quad . \tag{3.9}$$

We have numerically calculated the SAT probabilities for many $p$ and $N$ values, finding a transition from a mixed to a completely UNSAT phase at the $\gamma_c(p)$ analytically calculated in

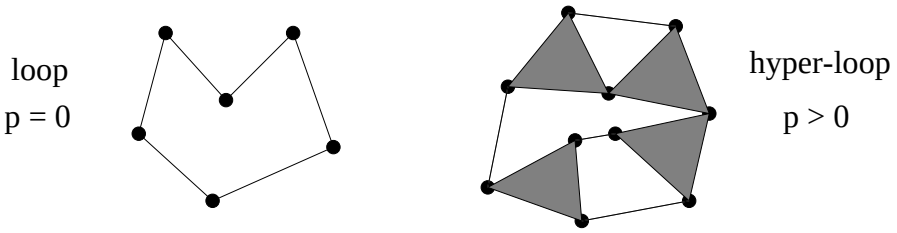



Figure 3.4: Typical loop and hyper-loop. Lines are 2-spin edges, while triangles are 3-spin edges. Note that every vertex has an even degree.

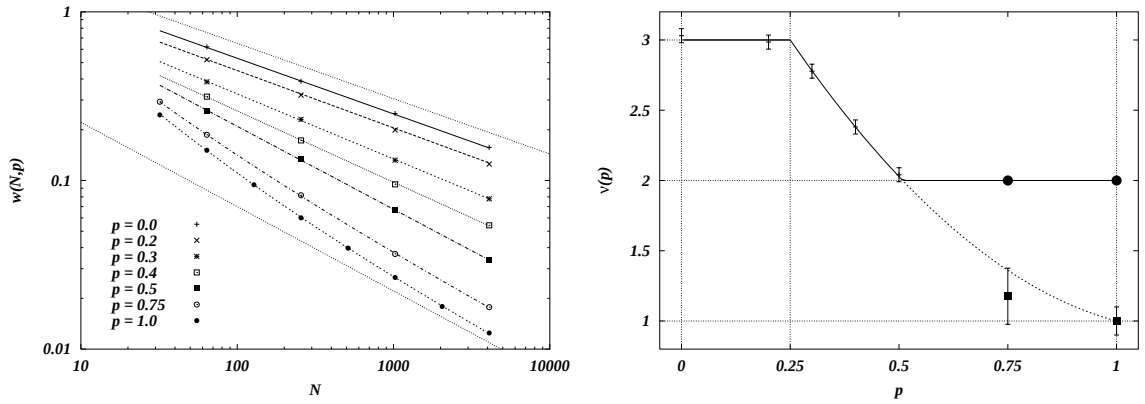



Figure 3.5: Scaling of the critical window width. Errors are smaller than symbols. Lines are fits to the data.

Figure 3.6: Critical $\nu$ exponents obtained from the fits shown in fig. 3.5. For $p = 0.75$ and $p = 1$ filled squares show the sub-leading term power exponent, the leading term one being fixed to $-1/2$ (filled circles).

the previous section. We also find, in agreement with analytical results, that the transition is continuous as long as $p \leq 1/4$ and then it becomes discontinuous in the SAT probability. Let us now concentrate on the scaling with $N$ of the critical region. We have considered several alternative definitions for the critical region. The one we present here seems to be the simplest and also the most robust, in the sense it can be safely used when the transition is both continuous ($p \leq 0.25$) and discontinuous ($p > 0.25$). We assume that the size of the critical region is inversely proportional to the derivative of the SAT probability at the critical point

$$w(N,p)^{-1} = \left. \frac{\partial P_{SAT}(\gamma,p)}{\partial \gamma} \right|_{\gamma=\gamma_c} \quad . \tag{3.10}$$

For any value of $p$ the width $w(N)$ goes to zero for large $N$ and the scaling exponent $\nu(p)$ is defined through

$$w(N,p) \propto N^{-1/\nu(p)} \quad . \tag{3.11}$$

In fig. 3.5 we show, in a log-log scale, $w(N,p)$ as a function of $N$ for many $p$ values, together with the fits to the data. The uppermost and lower-most lines have slopes $-1/3$ and $-1/2$ respectively. Data for $p \leq 0.5$ can be perfectly fitted by simple power laws (straight lines in fig. 3.5) and the resulting $\nu(p)$ exponents have been reported in fig. 3.6. We note that as long as $p \leq 0.25$ the $\nu$ exponent turns out to be highly compatible with 3, which is known to be the

right value for $p = 0$. Thus we conclude that for $p < 1/4$ the exponents are those of the $p = 0$ fixed point. For $0.25 < p \leq 0.5$ we find that the $\nu$ exponent takes non-trivial values between 2 and 3. Then one of the following two conclusions may hold. Either the transition for $p > p_0$ is driven by the $p = 1$ fixed point and the $\nu$ exponent is not universal, or more probably any different $p$ value defines a new universality class. This result is very surprising and interesting for the possibility that different universality classes are simply the consequence of the random hyper-graph topology. More complicated is the fitting procedure for $p > 0.5$. In a recent paper [119] Wilson has shown that in SAT problems there are intrinsic statistical fluctuations due to the way one construct the formula. This *white noise* induces fluctuations of order $N^{-1/2}$ in the SAT probability. If critical fluctuations decay faster than statistical ones (i.e. $\nu < 2$), in the limit of large $N$ the latter will dominate and the resulting exponent saturates to $\nu = 2$. Data for $p = 0.75$ and $p = 1$ shown in fig. 3.5 have a clear upwards bending, which we interpret as a crossover from critical (with $\nu < 2$) to statistical ($\nu = 2$) fluctuations. Then we have fitted these two data sets with a sum of two power laws, $w(N) = AN^{-1/\nu} + BN^{-1/2}$. The goodness of the fits (shown with lines in fig. 3.5) confirm the dominance of statistical fluctuations for large $N$. Moreover we have been able to extract also a very rough estimate of the critical exponent $\nu$ from the subleading term. In fig. 3.6 we show with filled squares these values, which turn out to be more or less in agreement with a simple extrapolation from $p \leq 0.5$ results.

### 3.1.3 Conclusions

The exact analysis of a solvable model for the generation of random combinatorial problems has allowed us to show that combinatorial phase diagrams can be affected by rare events leading to a mixed SAT/UNSAT phase. The energy difference between such SAT and UNSAT instances is non extensive and therefore non detectable by the usual $\beta \to \infty$ statistical mechanics studies. However, a simple probabilistic argument is sufficient to recover the correct proportion of instances. Moreover, through the exact location of phase boundaries together with the use of a polynomial global algorithm for determining the existence of solutions we have been able to give a precise characterization of the critical exponents $\nu$ depending on the mixing parameter $p$. The $p$-dependent behavior conjectured in ref. [31] for the random $2+p$ SAT case finds here a quantitative confirmation. The mixing parameter dependency also shows that the value of the scaling exponents is not completely determined by the nature of the phase transition and that the universality class the transtion belongs to is very probably determined by the topology of the random hyper-graph. The model we study has also a physical interpretation as a diluted spin glass system. It would be interesting to know whether the parameter-dependent behavior of critical exponent plays any role in some physically accessible systems. A generalization of the present model to a mixture of different rank hyper-graphs will be presented in chapter four in a computer science context . In the general case we will see that, depending on the fractions of hyper-graphs involved, phase diagrams still more complex with, for example, a continuos phase transition preceded by a dynamical one.

## 3.2 Ferromagnetic ordering on random graphs

The results of this section are the output of a joint work with Alexei Vazquez, Riccardo Zecchina and Alessandro Vespignani [98].

### 3.2.1 Introduction

The increasing evidence that many physical, biological and social networks exhibit a high degree of wiring entanglement has led to the investigation of graph models with complex topological properties[99]. In particular, the possibility that some special nodes of the cluster (hubs) posses a larger probability to develop connections pointing to other nodes has been recently identified in scale-free networks [100, 101]. These networks exhibit a power law degree distribution $p_k \sim k^{-\gamma}$, where the exponent $\gamma$ is usually larger than 2. This kind of degree distribution implies that each node has a statistically significant probability of having a large number of connections compared to the average degree of the network. Examples of such properties can be found in communication and social webs, along with many biological networks, and have led to the developing of several dynamical models aimed to the description and characterization of scale-free networks[100, 101, 102].

Power law degree distributions are the signature of degree fluctuations that may alter the phase diagram of physical processes as in the case of random percolation [105, 106] and spreading processes [107] that do not exhibit a phase transition if the degree exponent is $\gamma \leq 3$. In this perspective, it is interesting to study the ordering dynamics of the Ising model in scale-free networks. The Ising model is, indeed, the prototypical model for the study of phase transitions and complex phenomena and it is often the starting point for the developing of models aimed at the characterization of ordering phenomena. For this reason, the Ising model and its variations are used to mimic a wide range of phenomena not pertaining to physics, such as the forming and spreading of opinions in societies and companies or the evolution and competition of species. Since social and biological networks are often characterized by scale-free properties, the study of the ferromagnetic phase transition in graphs with arbitrary degree distribution can find useful application in the study of several complex interacting systems and it has been recently pursued in Ref. [108]. The numerical simulations reported in Ref [108] show that in the case of a degree distribution with $\gamma = 3$ the Ising model has a critical temperature $T_c$, characterizing the transition to an ordered phase, which scales logarithmically with the network size. Therefore, there is no ferromagnetic transition in the thermodynamic limit.

In this section we present a detailed analytical study of the Ising model in graphs with arbitrary degree distribution that heavily relies on the general results of the first chapter. By relaxing the degree homogeneity in the usual mean field (MF) approach to the Ising model, it is possible to show that the existence of a disordered phase is related to the ratio of the first two moments of the degree distribution. Motivated by this finding, we apply the replica calculation method in order to find an exact characterization of the transition to the ordered state and its associated critical behavior. We find that a disordered phase is allowed only if the second moment of the degree distribution is finite. In the opposite case, the strong degree of the hubs present in the network prevails on the thermal fluctuations, imposing a long-range magnetic order for any finite value of the temperature. Corrections to this picture are found when the minimal allowed degree is $m = 1$. The value of the critical temperature and exponents is found for any degree exponent $\gamma > 3$ and a transition to the usual infinite dimensional MF behavior is recovered at $\gamma = 5$. Moreover, in the range $3 < \gamma \leq 5$ non trivial scaling exponents are obtained.

During the completion of the present work we become aware that Dorogovtsev, Goltsev and Mendes [109] have obtained with a different approach results which partially overlap with those reported in this section.

Let us consider a network with arbitrary degree distribution $c_k$. Then consider the Ising model with a ferromagnetic coupling constant on top of this network. The Hamiltonian of this system is given by

$$\mathcal{H} = M - \sum_{i>j=1}^{N} J_{ij} s_i s_j + H_0 \sum_i \zeta_i s_i, \tag{3.12}$$

where $M = \langle k \rangle N/2$, $J_{ij} = 1(0)$ if there is (there is not) a edge connecting node $i$ and $j$, $s_i = \pm 1$ are the spin variables, and $N$ is the network size. $H_0\zeta_i$ is a general external random field with $\zeta_i$ following the a priori general probability distribution $\Lambda(\zeta_i)$. As one can easily see, this is a particularly simple case of the models introduced in the first chapter. A simple mean field approach is already able to predict the conditions for the existence of a transition temperature as a function of the characteristic moments of the degree distribution and to give a rather good estimate of its numerical value as:

$$T_c = \beta_c^{-1} = \frac{\langle k^2 \rangle}{\langle k \rangle}. \tag{3.13}$$

Hence, when $\langle k^2 \rangle / \langle k \rangle$ is finite there is a finite critical temperature as an evidence of the transition from the para-magnetic to a ferro-magnetic state. However, if $\langle k^2 \rangle$ is not finite the system is always in the ferromagnetic state. Nevertheless, the following result is only approximate, it does not take into account the full probability distribution of the effective fields in the system but it relies only on the value of the mean magnetization, which we will see not to be enough to properly describe the critical behavior of the model.

### 3.2.2 The replica approach on general random graphs

In the present section we will refine the mean field picture via a the replica calculation We will show how this method allows to calculate values of and conditions for the existence of a critical temperature of the model that we believe to be exact. Moreover, these results contain the classical mean field theory prediction in the limits where the latter is applicable. Being the system a diluted ferromagnet with only a limited number of ground states and absence of frustration we believe the replica symmetric Ansatz to be sufficient to find the correct solution of the problem. The details of the calculation of the replica free energy can be followed from the formulas of the first chapter keeping $c_k$ general and $V(\hat{l}) = \delta(\hat{l} - 2)$. We only rewrite below the saddle point equations and the corresponding free energy expression for this particular case, in order to make the section more readable:

$$P(h) = \frac{1}{< k >} \sum_k k p_k \int \prod_{t=1}^{k-1} du_t Q(u_t) \delta \left( h - \sum_t u_t - H_0 \right) \tag{3.14}$$

$$Q(u) = \int dh P(h) \delta \left[ u - \frac{1}{\beta} \tanh^{-1} (\tanh(\beta) \tanh(\beta h)) \right] \tag{3.15}$$

where $P(h)$ is the average probability distribution of effective (or cavity) fields acting on the sites and $Q(u)$ is that of the cavity fields due to the contribution of a single neighbor. We would like to stress the importance of the fact that the strong inhomogeneities present in the graph

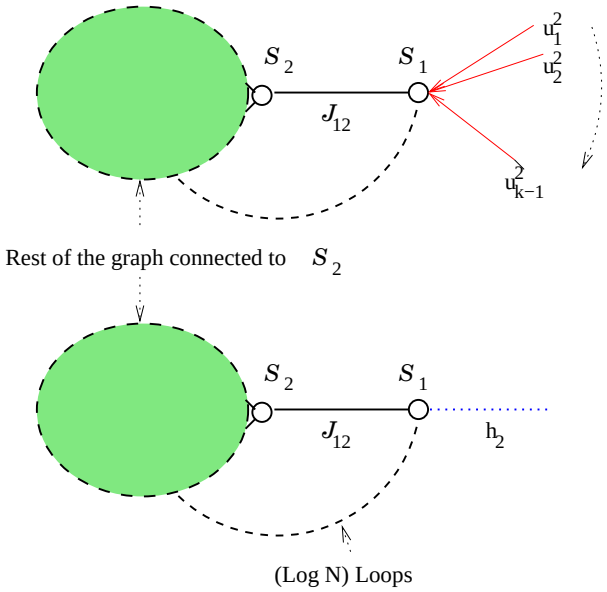



Figure 3.7: pictorial representation of the effective fields acting on site $S_1$ once its connection $J_{12}$ with $S_2$ (and therefore with the left part of the graph with probability 1 in the $N \to \infty$ limit) has been removed.

are correctly taken into account and handled via the computation of the whole probability distributions. In the Ising case we can easily work only with the $u$-fields, whose self consistent equation for the $Q(u)$ reads:

$$Q(u) = \frac{1}{< k >} \sum_k k p_k \int \prod_{t=1}^{k-1} du_t Q(u_t) \delta \left[ u - \frac{1}{\beta} \tanh^{-1} \left[ \tanh(\beta) \tanh \left( \beta \sum_t^{k-1} u_t + \beta H_0 \right) \right] \right] \tag{3.16}$$

This is an integral equation that can be solved at every value of $\beta$ using a population dynamics algorithm such as the RS simple version of that proposed in [23]. We chose to work in terms of the $u$-fields because they are connected to the local magnetization, whose mean value is the main quantity we are interested in studying around criticality. The equation for the physical magnetization probability distribution will indeed be:

$$\Pi(s) = \sum_k p_k \int \prod_{t=1}^{k} du_t Q(u_t) \delta \left[ s - \tanh \left( \beta \sum_t u_t + \beta H_0 \right) \right] \tag{3.17}$$

The equations for $< u >$ and $< s >$ follow:

$$< u >= \int u Q(u) du = \frac{1}{< k >} \sum_k k p_k \int \prod_{t=1}^{k-1} du_t Q(u_t) \frac{1}{\beta} \tanh^{-1} \left[ \tanh(\beta) \tanh \left( \beta \sum_t^{k-1} u_t + \beta H_0 \right) \right] \tag{3.18}$$

$$< s >= \int s \Pi(s) ds = \sum_k p_k \int \prod_{t=1}^{k} du_t Q(u_t) \tanh \left( \beta \sum_t^{k} u_t + \beta H_0 \right) \tag{3.19}$$

The free energy reads

$$\beta F \quad = \quad < k > \Big( \int \int dh du P(h) Q(u) \log(1 + \tanh(\beta h) \tanh(\beta u)) -$$

$$\frac{1}{2}\int\prod_{t=1}^{2}dh_t P(h_t)\log(1+\tanh(\beta)\prod_{t=1}^{2}\tanh(\beta h_t))\Big)$$
$$-\sum_k p_k\int\prod_{t=1}^{k}du_t Q(u_t)\log\left(\frac{2\cosh(\beta\sum_{t=1}^{k}u_t+\beta H_0)}{\prod_{t=1}^{k}2\cosh(\beta u_t)}\right)-$$
$$<k>\left(\log(2)+\frac{1}{2}(\beta-\log(\cosh(\beta)))\right) \tag{3.20}$$

At the saddle point the expression further simplifies. The internal energy and the specific heat at the saddle point can be calculated from eq.(3.20) through relations $< E >= \beta\frac{\partial\beta F}{\partial\beta}$ and $C = d < E > /dT$ and further exploiting (3.14) and (3.15):

$$< E >= \frac{< k >}{2} - \frac{< k >}{2}\int dh_1 dh_2 P(h_1)P(h_2)\left(\frac{\tanh(\beta)+\tanh(\beta h_1)\tanh(\beta h_2)}{1+\tanh(\beta)\tanh(\beta h_1)\tanh(\beta h_2)}\right) \tag{3.21}$$

$$C = \frac{\beta^2 < k >}{2(\cosh(\beta))^2}\int dh_1 dh_2 P(h_1)P(h_2)\left(\frac{1+(\tanh(\beta h_1)\tanh(\beta h_2))^2}{(1+\tanh(\beta)\tanh(\beta h_1)\tanh(\beta h_2))^2}\right) \tag{3.22}$$

The term $< k\beta > /2$ gauges the value of the energy to zero at $T = 0$ and no external field.

### 3.2.3 Ferromagnetic phase transition

At $T = 0$ and in the limit of non vanishing fields ($u$ and $h \sim O(1)$) it is straightforward to see that the cavity fields can take only 0 or 1 values. The equation (3.16) can be solved exactly with the Ansatz $Q(u) = q_0\delta(u) + (1-q_0)\delta(u-1)$. Plugging this Ansatz into eqs. (3.16), (3.18), and (3.19) one obtains:

$$\langle u\rangle = 1 - q_0, \tag{3.23}$$

$$\langle s\rangle = 1 - G_0(q_0), \tag{3.24}$$

$$q_0 = G_1(q_0), \tag{3.25}$$

where

$$G_0(x) = \sum_k k\ p_k\ x^k, \qquad G_1(x) = \frac{1}{< k >}\sum_k k\ p_k\ x^{k-1}, \tag{3.26}$$

are the generating functions of the degree distributions of a vertex chosen at random and a vertex arrived following an edge chosen at random [69], respectively. We point out that these equations correctly coincides with that obtained in the problem of percolation in a random graph with an arbitrary degree distribution [112, 69], where the average magnetization $\langle s\rangle$ is just the size of the giant component. Moreover, these expressions can be easily generalized to higher order hyper-graphs as it has been done in [19, 21]. From eq. (3.24) it follows that there is a finite magnetization whenever the solution $q_0$ of eq. (3.25) is less than 1. This happens whenever

$$\frac{\langle k^2\rangle}{\langle k\rangle} \geq 2, \tag{3.27}$$

that is just the condition for percolation in a random graph [112, 69]. On the contrary, for $\langle k^2\rangle / \langle k\rangle < 2$ the magnetization (the size of giant component) is 0, *i.e.* the system is in a paramagnetic state.

For random graphs satisfying the percolation condition in eq. (3.27) we are now interested in finding the value of $\beta_c$ for the ferromagnetic transition. There are few equivalent ways to do so. In the general case we can derive both sides of eq.(3.18) in $u = 0$ self consistently, obtaining

$$\frac{1}{T_c} = \beta_c = -\frac{1}{2}\log\left(1 - 2\frac{\langle k\rangle}{\langle k^2\rangle}\right). \tag{3.28}$$

In the limit $\langle k^2\rangle \gg 2\langle k\rangle$ we can expand the logarithm getting the first order condition $T_c = \langle k^2\rangle / \langle k\rangle$ which is the value found in the naive mean field approximation (3.13). Hence, the MF approach in developed in the previous section is valid for $\langle k^2\rangle \gg 2\langle k\rangle$ and, in this case, it gives the same results as those obtained using the replica approach.

### 3.2.4 Critical behavior around $\beta_c$

The critical behavior of the thermodynamical quantities $< s >$, $\chi$, $\delta C$, and $< s >_{H_0} \sim H_0^{1/\delta}$ close to $\beta_c$ can be calculated without having to explicitly solve the self consistent equations for the whole probability distributions $Q(u)$ and $\Pi(s)$. Sufficiently close to the critical point we can assume $Q(u) \sim \delta(u - < u >)$ being $< u >$ infinitesimal. In fact this Ansatz is incorrect if $\beta > \beta_c$, because it correctly takes into account the degree distribution but disregards the non trivial structure of the $Q(u)$ , which does not merely translate from the critical form $\delta(u)$ at $\beta_c$, but immediately develops a continuum structure. In the zero temperature limit the continuum shape will again collapse in a distribution of delta peaks discussed above. Nevertheless, sufficiently close to the transition we can expect only the first momenta of the $Q(u)$ to be relevant. For distributions with $< k^4 >$ finite one is left with a closed system of equations for the first three momenta all contributing to the same leading order. Defining $\mu_n =< k(k-1)...(k-n) >$ and $A = ((\tanh(\beta))^2\mu_2)/(\beta^2 < k > -(\tanh(\beta))^2\mu_1)$

$$\begin{aligned}
< u > &= \frac{\tanh(\beta)}{\tanh(\beta_c)} < u > -\frac{\beta^2 \tanh(\beta)[1-(\tanh(\beta)]^2}{3 < k >} \cdot \\
&\quad \left[\mu_1 < u^3 > +3\mu_2 < u >< u^2 > +\mu_3 < u >^3\right] \\
< u^2 > &= A < u >^2 \\
< u^3 > &= \left(\frac{(\tanh(\beta))^3 A\mu_2 + \mu_3}{\beta^3 < k > -(\tanh(\beta))^3 < \mu_1}\right) < u >^3
\end{aligned} \tag{3.29}$$

The explicit calculations are show in appendix D as a title of example. Exactly analogous calculations can be done for the the free energy, the energy and the specific heat Proportionality is found also for $< k^4 >= \infty$, where the calculation is a bit more involved because the leading momenta are to be found via an analytic continuation in the values of their order. Correctly taking into consideration the values of the leading momenta is important in case one is interested not only on calculating critical exponents, but also the amplitudes, because in general more terms at the same leading order are present, as we see in eq.(3.29). However, the exponents are determined by the lowest non trivial last analytic value of the momenta of the distribution $p_k$, and do not change in the general case because all relevant momenta of the $Q(u)$ give the same divergence in the momenta of the $p_k$. One example again is given in eq.(3.29). Since we are not interested in the calculation of amplitudes we can therefore resort to the variational Ansatz $Q(u) \sim \delta(u - < u >)$ in the proximity of the transition. However we would like to stress that

calculations can be done also in the general case. eqs.(3.18), (3.19) then become

$$< u > \sim \frac{1}{< k >} \sum_k k p_k \frac{1}{\beta} \tanh^{-1}(\tanh(\beta) \tanh(\beta(k-1) < u > +\beta H_0)) \tag{3.30}$$

$$< s > \sim \sum_k p_k \tanh(\beta k < u > +\beta H_0) \tag{3.31}$$

The corresponding expressions for the free energy, the energy and the specific heat can be retrieved in the same way and will not be written here for the sake of space. If $< k^4 >$ is finite the first non trivial term of the power series expansion of eq.(3.30) that still gives an analytic contribution is simply $< u >^3$. One finds

$$< u > \sim \left( \frac{3 < k >}{\beta_c^2 (\tanh \beta_c) < k(k-1)^3 >} \right)^{\frac{1}{2}} \tau^{\frac{1}{2}} \tag{3.32}$$

$$< s > \sim < u >, \quad \chi \sim \tau^{-1}, \quad < s > \sim H_0^{1/3} \tag{3.33}$$

where $\tau = 1 - T/T_c$ as usually defined. All exponents are the usual mean field ones. However, one finds a finite jump in the specific heat. The transition is therefore first order in the traditional sense. If we keep all the relevant momenta in our calculation, we find the expected correction to the amplitudes. For example we find

$$< u > \sim \sqrt{3}((\beta_c \tanh(\beta_c) < k >)((\mu_1 + 3\mu_2)A + \mu_3 >))^{-\frac{1}{2}} \tau^{\frac{1}{2}}. \tag{3.34}$$

This equation reduces to (3.32) if we disregard higher momenta.

### 3.2.5 Power law distributed graphs

In the following we are mostly interested in the case of a power law distribution of the type

$$p_k = c\, k^{-\gamma}, \qquad m \leq k < \infty, \tag{3.35}$$

where $c$ is a normalization constant and $m$ is the lowest degree. Note that in the case of a power law distribution

$$< k^2 > = c \sum_{k=m}^{k_{max}} k^{2-\gamma} > c\, m \sum_{k=m}^{k_{max}} k^{1-\gamma} = m < k > . \tag{3.36}$$

Hence, we have that for $m \geq 2$ the graph is always percolating for all $\gamma$ independently on the cutoff $k_{max}$. Then for $m \geq 2$ the critical temperature is always given by eq. (3.28). In particular for $m > 2$ and $\gamma \gg 1$ the critical temperature approaches the limit $T_c^{lim} = -2/\log(1 - 2/m)$ while for $m = 2$ the critical temperature tends to zero in the large $\gamma$ limit. However, for $m = 1$ there is a critical value $\gamma^\star$ beyond which the graph is no longer percolating [111]. $\gamma^\star$ is the value of $\gamma$ at which $\langle k^2 \rangle = 2 \langle k \rangle$, resulting $\frac{\zeta(\gamma^\star - 2)}{\zeta(\gamma^\star - 1)} = 2$ that have the solution $\gamma^\star = 3.47875....$ If $\gamma \geq \gamma^\star$ the system is always paramagnetic while for $\gamma < \gamma^\star$ there is a transition to a ferromagnetic state at a temperature given by eq. (3.28). In fig. 3.8 we show the phase diagram together with the critical lines for $m = 1$, 2 and 3.

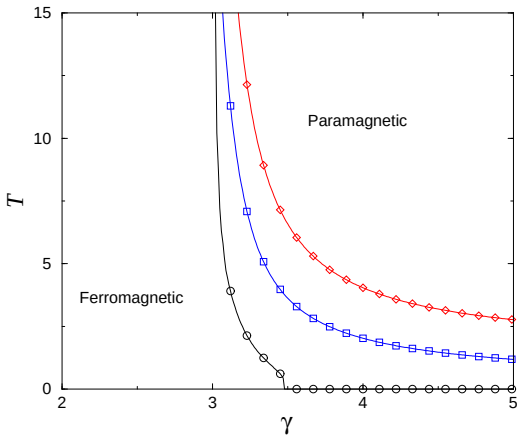



Figure 3.8: The phase diagram of the Ising model on scale-free graphs with a power law degree distribution $p_k = ck^{-\gamma}$, $m \leq k < \infty$. The ferromagnetic transition lines depends on the value of $m$, with $m = 1$ circles, 2 squares, and 3 diamonds.

### 3.2.6 $2 < \gamma \leq 3$

For $2 < \gamma \leq 3$ the second moment of the degree distribution diverges and, therefore, as discussed in previous sections, the system is always in a ferromagnetic state. In this case it is important to investigate the behavior of $\langle u \rangle$ and $\langle s \rangle$ when $\beta \to 0$. This computation can be done using either the mean-field or the replica approach obtaining the same results. In fact, in this case we have $\lim_{\beta \to 0} Q(u) = \delta(u)$ and putting this limit distribution into the self consistent equation for $< u >$ and $< s >$ we recover the mean field asymptotic behavior. For $2 < \gamma \leq 3$ the sums in eq.(3.30) are dominated by the large $k$ region. In this case these sums can be approximated by integrals resulting

$$\langle u \rangle \approx (\gamma - 2)(m\beta \langle u \rangle)^{\gamma - 2} \int_{m\beta\langle u \rangle}^{\infty} dx x^{1-\gamma} \tanh x, \tag{3.37}$$

while the magnetization, $\langle s \rangle = \sum_k p_k \tanh(\beta k \langle u \rangle)$, is simply given by

$$\langle s \rangle \approx \frac{\gamma - 1}{\gamma - 2} m\beta \langle u \rangle . \tag{3.38}$$

The above integral cannot be analytically calculated but its asymptotic behaviors for $\beta \to 0$ can be obtained. For $\gamma = 3$ the integral in the rhs of eq. (3.37) is dominated by the small $x$ behavior. Thus, approximating the $\tanh x$ by $x$ and computing $\langle u \rangle$ we obtain

$$\langle u \rangle \approx \frac{\exp(-1/m\beta)}{m\beta}, \qquad \gamma = 3. \tag{3.39}$$

On the other hand, for $\gamma < 3$ the integral in the rhs of eq. (3.37) is finite for any value of $m\beta \langle u \rangle$ and, therefore, for $m\beta \langle u \rangle \ll 1$ it follows that

$$\langle u \rangle \approx [(\gamma - 2)I]^{\frac{1}{3-\gamma}} (m\beta)^{\frac{\gamma-2}{3-\gamma}}, \qquad \gamma < 3, \tag{3.40}$$

where $I = \int_0^\infty dx x^{1-\gamma} \tanh x$. Finally, substituting eqs. (3.39) and (3.40) on eq. (3.38) we get

$$\langle s \rangle \sim \exp(-1/m\beta), \qquad \gamma = 3, \tag{3.41}$$

$$\langle s \rangle \sim (m\beta)^{\frac{1}{3-\gamma}}, \quad 2 < \gamma < 3. \tag{3.42}$$

With the same technique one can study the behavior of the other physically relevant quantities. Extracting the leading asymptotic terms from the expressions for the energy and the specific heat $T = \infty$, we find an infinite order phase transition with

$$\begin{aligned} \delta C &\sim \frac{e^{-2/m\beta}}{\beta^2}, \quad \gamma = 3, \\ \delta C &\sim \beta^{(\gamma-1)(3-\gamma)}, \quad 2 < \gamma < 3. \end{aligned} \tag{3.43}$$

Extracting from eq.(3.18) the leading behavior of $\chi_u \equiv \partial < u > /\partial H_0$ at $H_0 = 0$ and plugging the result together with eqs.(3.39), (3.40), (3.41) and (3.42) into $\chi \equiv \partial < m > /\partial H_0$ one obtains:

$$\chi \sim \frac{1}{m^2 \beta} \tag{3.44}$$

The limiting case $\gamma = 3$ corresponds with the Barabasi-Albert model studied in [108] by means of numerical simulations. The magnetization exhibits an exponential decay in agreement with our calculation in eq. (3.41). Moreover, the critical temperature was observed to increase logarithmically with the network size $N$. Computing $T_c$ in eq. (3.13) for $\gamma = 3$ we obtain $T_c \approx (m/2) \ln N$, which is in very good agreement with their numerical results. It is worth remarking that similar exponential and logarithmic dependencies have been observed for the order and control parameter in some non-equilibrium transitions [107, 110].

### 3.2.7 $3 < \gamma \leq 5$

In this case $\langle k^2 \rangle$ is finite and, therefore, there is a ferromagnetic transition temperature given by eq. (3.28). However, $\langle k^4 \rangle$ is not finite and the derivation of the MF critical exponents performed in Sec. 3.2.4 is not valid. In order to find the critical exponents we can write the functions inside the degrees sums as power series in $< u >$. The coefficients of the two series will however depend on the higher momenta of the degrees distribution and will be infinite beyond a certain power of $< u >$. This is direct consequence of the fact that the power expansion of the $\tanh(y)$ around 0 is convergent as long as the $y < \pi/2$, while for any $< u >$ in our cases there will exist an $k^\star$ such that $< u >$ lays outside the convergence radius. Nevertheless, the function is well approximated by the expansion when one truncates it up to the maximum analytical value of the exponent such that all momenta of the power law distribution taken into consideration are finite.

For $3 < \gamma < 5$ the highest analytical exponent of the expansion of eq.(3.30) in powers of $< u >$ is $n_{max} = \gamma - 2$, where the integer value has been analytically continued and so should be done with the corresponding series coefficient. In this range of values of s $n_{max}$ is lower than 3 so is to be taken as the correct value instead of $n = 3$ that leads to non analicities. With analogous calculations we are able to find all other critical exponents:

$$\begin{aligned} < u > &\sim < s > \sim \tau^{\frac{1}{\gamma-3}} \\ \delta C &\sim \tau^{(5-\gamma)/(\gamma-3)} \\ \chi &\sim \tau^{-1}, \quad < s > \sim H_0^{\beta/(1+\beta)} \sim H_0^{1/(\gamma-2)} \end{aligned} \tag{3.45}$$

As an example of this kind of calculation, the critical exponent governing the behavior of $< u >$ can be found in the appendix D, where a value for the non universal amplitude in the

$Q(u) \sim \delta(u - < u >)$ is also computed. On the other hand, for $\gamma = 5$ one can find a logarithmic correction to the previous values expanding the inverse hyperbolic tangent in eq.(3.30) to the third order in the tails of the degrees distribution. The results are:

$$\begin{aligned} < u > &\sim < s > \sim \tau^{1/2}/(-\log(\tau))^{1/2} \\ \delta C &\sim 1/(-\log(\tau)) \\ \chi &\sim \tau^{-1}, \quad < s > \sim H_0^{1/3}/(-\log(H_0))^{1/3} \end{aligned} \tag{3.46}$$

The specific heat is continuous at $\beta_c$ for $\gamma \in (3, 5]$, indicating a phase transition of order $> 1$. A part from the logarithmic corrections in the $\gamma = 5$ case, the universality relations between the exponents are satisfied.

This treatment parallels the $T = 0$ calculations done in [113] for the case of percolation critical exponents in a power law graph in presence of further dilution. If we introduce a cutoff into the degrees distribution the critical exponent very close to the transition point is always the mean field one, due to the fact that the sum over the degrees is always finite and there is no non analyticity in $< u >= 0$ for any $\gamma$. However the influence of non trivial terms is very strong (decreasing if we increase $\gamma$). eq.(3.32) is always valid but only in a very narrow region around $\beta_c$. The numerical values of $T_c$ and of the amplitudes in the critical behavior of the magnetization are also strongly affected being a function of the moments of the degrees distribution. In the infinite cutoff limit the mean field window shrinks to zero and one recovers the non trivial behavior. Indeed, if we work with large enough a cutoff at $\gamma \in (3, 5)$ and calculate the average magnetization in regions where $\beta(k-1) < u > (\beta) \sim \pi/2$, limit of the radius of convergence of the series expansions of $\tanh^{-1}(\tanh(\beta)\tanh(\beta(k-1) < u >))$, we see a contribution in the magnetization curves that goes as $(\beta - \beta_c)^{1/(\gamma-3)}$. This region becomes dominant for large values of the cutoff. In summary, we have obtained the phase diagram of the Ising model on a random graph with an arbitrary degree distribution. Three different regimes are observed depending on the moments $\langle k^2 \rangle$ and $\langle k^4 \rangle$ of the distribution. For $\langle k^4 \rangle$ finite the critical exponents of the ferromagnetic phase transition coincides with those obtained from the simple MF theory. On the contrary, for $\langle k^4 \rangle$ not finite but $\langle k^2 \rangle$ finite we found non-trivial exponents that depend on the power law exponent of the degree distribution $\gamma$. On the other hand, for $\langle k^2 \rangle$ not finite the system is always in a ferromagnetic state. Moreover, at $T = 0$ we recover the results obtained by the generating function formalism for the percolation problem on random graphs with an arbitrary degree distribution.

# Chapter 4

# Two examples of NP optimization problems

## 4.1 The Hyper-Graph Bicoloring Problem

The Bicoloring problem of a uniform rank 3 hyper-graph is defined as follows: you want to color (with 2 colors, say red and blue) the hyper-graph vertices in such a way that no hyper-edge has got all vertices of the same color an example for a small fraction of a sample hyper-graph is shown in fig. (4.1). Again, the problem could be immediately generalized to hyper-graphs of generic degree and distribution, along the same lines of the $p$-spin. In the following, however, we will show only the calculation in the Poissonian random graph case and fixed rank 3. The first choice is justified by the search of the behavior of the problem in the average case (it is proved to be NP in the worst one), and the will of testing the accuracy of the variational 1RSB factorized Ansatz for a problem in the same hardness class of the $K$-SAT. Indeed we found out that the behaviors of both models seem very similar, with some significant difference from the generalized $p$-spin. As in the $K$-SAT, the present model will undergo a sat/unsat phase transition at $T = 0$ as a function of mean degree. The second (fixed degree) choice was performed to show another case admitting an exactly factorized 1RSB solution and how this solution seems however to be here less relevant for the understanding of the general behavior.

The model Hamiltonian is nothing but the cost function of the associated combinatoric problem and reads

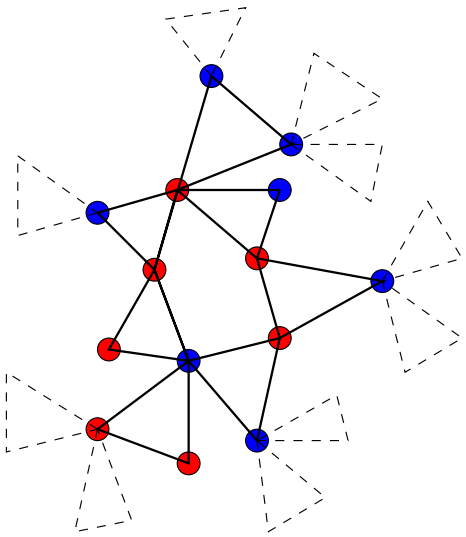
$$H = \sum_{i_1<i_2<i_3} J_{i_1 i_2 i_3} \delta_{s_1;s_2} \delta_{s_1;s_3} = \frac{1}{4} \sum_{i_1<i_2<i_3} J_{i_1 i_2 i_3} (1 + s_1 s_2 + s_2 s_3 + s_1 s_3) \tag{4.1}$$

The resulting model is an anti-ferromagnet with a peculiar type of three body interaction term, with spins connected via the following distribution of couplings

$$\prod_{i_1<i_2<i_3} P(J_{i_1 i_2 i_3}) = \prod_{i_1<i_2<i_3} \left( (1 - \frac{3!\gamma}{N^2}) \delta(J_{i_1 i_2 i_3}) + \frac{3!\gamma}{N^2} \delta(J_{i_1 i_2 i_3} - 1) \right) \tag{4.2}$$

Frustration is given by the anti-ferromagnetic couplings. Exploiting the usual replica trick one gets

$$< Z^n >_{\mathbf{J}} \sim \sum_{s_i^a} e^{-\gamma N + \frac{\gamma}{N^2} \sum_{i_1<i_2<i_3}} e^{-\frac{\beta}{4} \sum_{a=1}^{n} (1 + s_{i_1}^a s_{i_2}^a + s_{i_2}^a s_{i_3}^a + s_{i_1}^a s_{i_3}^a)} \tag{4.3}$$



and, with the usual multilevel gas picture ($\rho(\vec{\sigma}) = \frac{1}{N}\sum_{i=1}^{N}\delta(\vec{\sigma};\vec{s}_i)$)

$$< Z^n > \sim \int \prod_{\vec{\sigma}} d\rho(\vec{\sigma}) e^{-n\beta N F[\rho(\vec{\sigma})]} \tag{4.4}$$

$$n\beta F[\rho(\vec{\sigma})] = \gamma + \sum_{\vec{\sigma}} \rho(\vec{\sigma})\log(\rho(\vec{\sigma})) - \gamma \sum_{\vec{\sigma}_1,\vec{\sigma}_2,\vec{\sigma}_3} \rho(\vec{\sigma}_1)\rho(\vec{\sigma}_2)\rho(\vec{\sigma}_3) e^{-\frac{\beta}{4}\sum_{a=1}^{n}(1+\sigma_1^a\sigma_2^a+\sigma_2^a\sigma_3^a+\sigma_1^a\sigma_3^a)} \tag{4.5}$$

In the large $N$ limit we are left with the contribution at the saddle point

$$\rho(\vec{\sigma}) = e^{-3\gamma+3\gamma\sum_{\vec{\sigma}_1,\vec{\sigma}_2}\rho(\vec{\sigma}_1)\rho(\vec{\sigma}_2)e^{-\frac{\beta}{4}\sum_{a=1}^{n}(1+\sigma_1^a\sigma_2^a+\sigma_2^a\sigma_3^a+\sigma_1^a\sigma_3^a)}} \tag{4.6}$$

### 4.1.1 The RS results

Plugging the RS Ansatz into (4.6) one gets after some manipulation. A small technical difference from the $p$-spin is that here, as it will be in the $K$-SAT case, fields are originally at half integer values. They can be rescaled on integers thanks to a rescaling of $\beta \to 2\beta$, that does not influence the zero temperature properties. The final result reads:

$$\int_{-\infty}^{\infty} P(h)e^{x\beta h} \quad = \quad e^{-3\gamma}e^{3\gamma\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} dh_1 dh_2 P(h_1)P(h_2)e^{x\beta u(h_1,h_2)}} \tag{4.7}$$

with

$$u(h_1,h_2) = \quad \frac{1}{\beta}\log(\alpha_-/\alpha_+) \tag{4.8}$$

$$\alpha_\pm = \quad 2\cosh(\beta(h_1-h_2)) + 2\cosh(\beta(h_1+h_2))e^{\mp\beta} \tag{4.9}$$

or

$$P(h) \quad = \quad e^{-3\gamma}\sum_t \frac{(3\gamma)^t}{t!}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\prod_{i=1}^{t} dh_1^i dh_2^i P(h_1^i)P(h_2^i)\delta(h-\sum_{i=1}^{t}u(h_1^i,h_2^i)) \tag{4.10}$$

where $x = \sum_a \sigma_a$. The function $u(h, g)$ takes the values of the cavity biases introduced in chapter 2. An analogous equation for the free energy can be found generalizing the $p$-spin model approach from the usual Hamiltonian term $\beta \sum_a (\sigma_1^a ... \sigma_k^a - 1)$ to any $J_\beta(\sigma_1^a, ..., \sigma_k^a)$ In the Bicoloring case $J_\beta(\sigma_1^a, ..., \sigma_k^a) = J_\beta(\sigma_1^a, \sigma_2, \sigma_3^a) = -\beta/4 \sum_a (\sigma_1^a \sigma_2^a + \sigma_1^a \sigma_2^a + \sigma_1^a \sigma_2^a + 1)$. However, we are here interested in the combinatorial problem itself, and therefore in taking the zero temperature limit.

The trivial paramagnetic solution $P(h) = \delta(h)$ and $S_{para} = \log(2) - \gamma \log(4/3)$ is always present in the SAT zero energy phase. This is in contrast with the 3-SAT case and similar to the paramagnetic phase of the $p$-spin. Moreover in the RS framework, the only saddle point solution in the zero energy SAT phase is the previous one. The absence of local fields, as in the $p$-spin models, drives out the appearance of a non trivial form for the $P(h)$ at low but non zero values of $\gamma$, differently to what happens in the 3-SAT case. Indeed, in the US case we can distinguish two different regimes of effective fields scaling as $O(T)$ or tending to a fixed value in the zero temperature limit. In the first regime one can write integro-differential equations for the probability distribution of magnetizations and the ground state entropy (in the sat phase), as in 3-SAT or in the $p$-spin models. One can then solve them perturbatively, writing a series expansion in the average degree (or in $\gamma$) along the same lines of [9]. It is found that the total paramagnetic solution is stable for all $\gamma$ and the expansion collapses back to the annealed expression to all orders. However it is to be noted that this does not rule out the possibility of an intermediate cross-over region of mixed scaling of the order parameter, where replica symmetry would have to be broken in a non trivial manner. Indeed, the behavior of the Bicoloring model in degree seems to share intermediate properties between the $p$-spin models and the 3-SAT.

In the second regime the saddle point equations (4.7) reduce to

$$\begin{aligned} \int_{-\infty}^{+\infty} dh P(h) e^{\beta h x} &= \exp\left( -\frac{3\gamma}{2} + 3\gamma \int_0^{+\infty} \int_0^{+\infty} dh_1 dh_2 P(h_1) P(h_2) e^{x\beta min(1,h_1,h_2)} + \right. \\ &\left. 3\,\gamma \int_{-\infty}^{0} \int_{-\infty}^{0} dh_1 dh_2 P(h_1) P(h_2) e^{-x\beta min(1,|h_1|,|h_2|)} \right) \end{aligned} \tag{4.11}$$

Looking again for a symmetric integer fields solution of the type we get

$$p_0 = e^{-\frac{3\gamma}{2}(1-p_0)^2} I_0(\frac{3\gamma}{2}(1-p_0)^2) \tag{4.12}$$

$$p_{k>0} = p_{k<0} = e^{-\frac{3\gamma}{2}(1-p_0)^2} I_k(\frac{3\gamma}{2}(1-p_0)^2) \tag{4.13}$$

In the RS framework , the only saddle point solution in the zero energy SAT phase is the perfect paramagnetic one $P(h) = \delta(h)$. The absence of local fields, as in the $p$-spin models, drives out the appearance of a non trivial form for the paramagnetic $P(h)$ at low values of $\gamma$, differently to what happens in the 3-SAT case. No other stable integer fields solution is found to exist. A $p_0 \neq 0$ spin glass metastable solution appears for $\gamma = 2.3335$, that however initially corresponds to a non physical negative energy value. As in [9], the RS estimate for $\gamma_c$ is therefore given by the point where the energy

$$E_{GS} = 2\gamma \left( \frac{1-p_0}{2} \right)^3 - \frac{3\gamma}{4}(1-p_0)^2 r_1 \tag{4.14}$$

turns positive[1]. This gives a rough upper bound of 2.45, that can be tracked down to 2.35 by the introduction of rational fields, following again the prescription of [9]. After a long manipulation one finds the following saddle point equations, closed in the first $r$ weights:

$$p_0 = e^{-\frac{3\gamma(1-p_0)^2}{2}} \int_0^{2\pi} \frac{d\theta}{2\pi} e^{\sum_{j=1}^{r} \alpha_j \cos(j\theta)} \tag{4.15}$$

$$p_k = e^{-\frac{3\gamma(1-p_0)^2}{2}} \int_0^{2\pi} \frac{d\theta}{2\pi} \cos(k\theta) e^{\sum_{j=1}^{r} \alpha_j \cos(j\theta)} \tag{4.16}$$

with

$$\alpha_{j<r} = 6\gamma p_j (1 - 2\sum_{l=0}^{j} p_l + p_j) \tag{4.17}$$

$$\alpha_r = \frac{3\gamma}{2}(1 - 2\sum_{j=0}^{r-1} p_j)^2 \tag{4.18}$$

$$\begin{aligned} E_{GS} = {} & \frac{2\gamma}{r}\left((\frac{1-p_0}{2})^3 + \sum_{j=1}^{r-1}(\frac{1-p_0}{2} - \sum_{l=1}^{j} p_l)^3\right) - \\ & \frac{1}{r}\left(\sum_{j=1}^{r} j\alpha_j(\frac{p_0+p_j}{2} + \sum_{l=1}^{j-1} p_l)\right) + \frac{p_0}{2r}\sum_{j=1}^{r} j\alpha_j - \frac{1}{r}\sum_{j=1}^{r}\alpha_j \sum_{l=1}^{j-1}(l-j)p_l \end{aligned} \tag{4.19}$$

One would however like to go beyond scheme which is RS and furthermore does not reflect the physical phenomena taking place in the model. Indeed, There are no reasons for local fields at $T = 0$ not to have support on integer values. Even though the last solution is a legitimate variational one[2], it is believed [24, 30, 29] that in fact signals the presence of non trivial RSB phenomena.

### 4.1.2 The RSB Calculations

In order to improve the previous results we used the same RSB factorized Ansatz that was quite successful in the $p$-spin and that seems to provide a nearly exact solution for any model defined on fixed degree graphs, independently of the specific form of the Hamiltonian. We won't show all the calculations, exhaustively done for the $p$-spin case and essentially identical in this case. Let us specialize initially to fixed degree $k$-hyper-graphs The final self consistent equation reads

$$P(h) = \frac{(2\cosh\beta h)^m}{A_{l-1}} \int \prod_{i=1}^{k-1} \frac{\mathcal{D}h_i\, \mathcal{D}g_i\, W(h_i, g_i)^m}{(4\cosh(\beta h_i)\cosh(\beta g_i))^m} \cdot \delta\left(h - \sum_{i=1}^{k-1} u(h_i, g_i)\right) \quad , \tag{4.20}$$

[1] Notice the close similarity with the RS expressions for the 3-spin written in chapter 3 and the ones for the 3-SAT in [9] and easily retrievable form the 1RSB equations of the next section. In fact, the only difference seen by the RS treatment seems to be a rescaling of the hyper-graph diluteness parameter $\gamma_{3-spin} \to \gamma_{Bic}/2 \to \gamma_{3-SAT}/4$, that reflects the size of the elementary clause in the combinatorial problem (3-spin interactions correspond to 4 3-SAT like clauses, for instance). It is clear that from the RS point of view all these models are equivalent and their difference, which is well seen theoretically experimentally, needs a broader picture, that could explain for instance why in the dynamical region 3-XOR-SAT is still Polynomial thanks to a global solution procedure, while 3-SAT in NP-complete.

[2] This can be rigorously proven as an additional special case of the general calculations of chapter 6.

| $k+1$ | $e_{gs}$ | $y^*$ |
|---|---|---|
| 1–6 | 0 | $\infty$ |
| 7 | 0.003711 | 1.96611 |
| 8 | 0.027383 | 1.17118 |
| 9 | 0.058131 | 0.92887 |
| 10 | 0.093181 | 0.78746 |
| 11 | 0.131392 | 0.69315 |
| 12 | 0.172118 | 0.55338 |

Table 4.1: Energy densities at the optimal value $y^*$ of the scaling parameter for the Bicoloring model on fixed degree $K$ 3-hyper-graphs.

where $W(h,g) = \sqrt{\alpha_-\alpha_+}$ is the re-weighting function that in the exact 1RSB has been connected to LGS level crossing [23, 24]. The RS (resp. paramagnetic) equation is recovered for $m = n \to 0$ (resp. $P(h) = \delta(h)$). $A_{k-1}$ is a normalization factor. At $T = 0$:

$$p_0 = \frac{1}{g(k,y)} \sum_{t=0}^{[(k-1)/2]} \frac{(k-1)!}{(k-1-2t)!(2t)!} \frac{A^{k-1-2t} B[y]^{2t}}{2^{2t}} \tag{4.21}$$

$$F = -\frac{1}{y}\left( (1-\frac{2k}{3}) \log(g(k,y)) + \frac{2k}{3} \log(g(k-1,y)) \right) \tag{4.22}$$

with:

$$\begin{aligned} A &= 1 - \frac{(1-p_0)^2}{2} \\ B[y] &= \frac{(1-p_0)^2}{2} e^{-y} \\ g(k,y) &= \sum_{t=0}^{[(k-1)/2]} \frac{(k-1)!}{(k-1-2t)!(2t)!} \frac{A^{k-1-2t} B[y]^{2t}}{2^{2t}} + \\ &\quad 2 \sum_{r=0}^{k} e^{yr} \sum_{t=0}^{[(k-1)/2]} \frac{k! A^{k-r-2t} B[y]^{r+2t}}{(k-r-2t)!t!(r+t)!2^(r+2t)} \end{aligned}$$

Table 4.1 shows the GS energy densities $e_{gs}$ at the optimal $y^*$ for some choices of $l$.

The same Ansatz plugged into the variational free energy for poissonian degree distribution gives, after calculations similar to the $p$-spin,

$$P(h) = (2\cosh\beta h)^m \sum_{l=1} \frac{e^{-3\gamma}(3\gamma)^{k-1}}{A_{k-1}(k-1)!} \left( \int \prod_{i=1}^{k-1} \frac{\mathcal{D}h_i \mathcal{D}g_i W(h_i,g_i)^m}{(4\cosh(\beta h_i)\cosh(\beta g_i))^m} \delta\left( h - \sum_{i=1}^{k-1} u(h_i,g_i) \right) \right) \quad , \tag{4.23}$$

and, in the $T = 0$ limit,

$$p_0 = \frac{I_0(z_1)}{I_0(z_1) + 2\sum_{k>0} I_k(z_1) e^{\frac{yk}{2}}} \tag{4.24}$$

$$p_l = = p_{-l} = \frac{I_l(z_1) e^{\frac{yl}{2}}}{I_0(z_1) + 2\sum_{k>0} I_k(z_1) e^{\frac{yk}{2}}} \tag{4.25}$$

$$z_1 = \frac{3\gamma}{4\Omega}(1-p_0)^2 e^{-\frac{y}{2}} \tag{4.26}$$

$$\Omega = 1 + \frac{(1-p_0)^3}{4}(e^{-y}-1) \tag{4.27}$$

for the saddle point equations and

$$F(y) = -\frac{1}{y}(\gamma \log\Omega - \log\Lambda - z_1\cosh(y) - z_1\sinh(y)p_0) \tag{4.28}$$

$$\Lambda = \frac{1}{I_0(z_1) + 2\sum_{k>0} I_k(z_1)e^{\frac{yk}{2}}} \tag{4.29}$$

for the potential. Again, as we expected, no found RSB solution has support on non integer fields. Optimizing over $y$, we find an upper bound for the critical value of $\gamma_c$ of 2.145, very close to the numerical exact estimate [117]. This value is found maximizing the free-energy and tuning $\gamma$ and $y$ to the point where this maximum crosses to positive values for the first time, indicating the onset of positive energy density global ground states.

### Complexity results of the Bicoloring model

Using eq. (2.133) it is also possible to write a variational expression for the complexity. Obviously, the number of LGS will be overestimated because correlations between LGS, that here are neglected, can and indeed do reduce the number of states at Hamming distance of order $N$. The notion of LGS is however a subtle one, and currently under debate. For some late insights see for example [24]. The dynamical threshold for the Bicoloring model is then defined as the point where the complexity attains for the first time a non zero value. This corresponds to the point where LGS with highest energy density first appear. The factorized Ansatz gives the estimate $\gamma_d \sim 1.881$. The point where the number of LGS ceases to be extensive in $\exp^N$ coincides with the previously calculated one at $\gamma_c \sim 2.145$.

We also tried to obtain an exact value for the true zero temperature complexity, as done in the $p$-spin case thanks to the accidental equivalence with the its ferromagnetic version before the static transition. The reason for that possibility lied in the fact that in that particular case the LGS turned out to be orthogonal and uncorrelated, so that one could look at the configurational space sitting on a reference GS chosen at will. In the dynamical region clusters of solutions all of the same size and equivalent to the ferromagnetic cluster formed. Indeed, the complexity calculated as in eq. (2.187) was seen to be identical to that of the number of metastable states into the *ferromagnetic* model. Can this be done in the Bicoloring case too? No apparent gauge cluster symmetry of this kind seem to be present in this case (as well as in the $K$-SAT, graph-coloring or other models), so we expect the answer to be negative. Nevertheless, we tried to retrieve the solution of the factorized symmetric saddle point equations in the $m = 1$ case. This can be done along the same lines of the $p$-spin, leading however to the negative expected result: the $m = 1$ saddle point equations

$$p_0 = e^{-\gamma(1-p_0)^2} \tag{4.30}$$

$$p_l = p_{-l} = \frac{p_0}{2}\frac{\gamma^l(1-p_0)^{2l}}{l!} \tag{4.31}$$

give no non trivial solution before $\gamma^* = 2.454$, which is well above the transition point of the model. Therefore at the beginning of this work the exact value for the complexity was

*erroneously* thought to be zero anywhere before the static transition. Incidentally, (4.30) and (4.31) turn out to be the symmetrized version of the solutions of a ferromagnetic spin version of the Bicoloring model, built with the hamiltonian

$$H = \frac{1}{4} \sum_{i_1<i_2<i_3} J_{i_1 i_2 i_3}(1 + s_{i_1} s_{i_2} - s_{i_2} s_{i_3} - s_{i_1} s_{i_3}) \tag{4.32}$$

Contrary to the $p$-spin model, there is *no correspondence* between the saddle point equations in the frustrated and the ferromagnetic models, because the two are not related by any symmetry transformation. Consequently, counting the metastable states in the ferromagnetic model does not correspond to counting the Bicoloring LGS. Moreover, the ferromagnetic model shows an intermediate continuously magnetized phase between the paramagnetic and the backbone ferromagnetic ones. Models showing this behavior are interesting for their own sake and have been investigated in [55]. We argue that this intermediate transition reflects in the spin-glass as an indicator that also Bicolorig, as 3-SAT (see also [30]), admits a crossover region where a simple 1RSB factorized Ansatz is not sufficient. In fact, due the absence of cluster symmetry the LGS cannot be gauged to the same ferromagnetic one. A non trivial 1RSB solution can be found with the general technique recently put forward in [29, 30, 24]. In working with the factorized Ansatz approximation, an upper bound for the complexity is calculated, where the number of LGS is overestimated because correlations that can decrease the number of actually disconnected[3] clusters are not taken into account. The general solution can be explicitly found with the same techniques reviewed in chapter 2, even though the saddle point equations are slightly more complicated [114]. This solutions shows a narrower but still non zero dynamical region of positive complexity. Thresholds calculable in this way are conjectured to be exact for the Bicoloring problem. A similar picture applies to the $K$-SAT case. Moreover in the Bicoloring $T = 0$ saddle point equations, the absence of non trivial vanishing fields (as it be seen via series expansion around the perfect paramagnetic solution as well as via numerical experiments) lead us to believe the last solution to be exact for *any* value of $\gamma$ in the phase diagram of the model, even when models as $K$-SAT seem to show an $\infty$-RSB transition. This property can be traced back, in our opinion, to the absence in the model Hamiltonian to single spin-flip asymmetric terms, present for instance in the SAT models. This terms can give rise to local fluctuations that vanish only at zero temperature but can give rise to further symmetry breaking in the phase space. The same is *not* true in the $K$-SAT case [30, 89, 90], as will be discussed in the following section. In this sense the Bicoloring model lies in a somehow intermediate position between the $p$-spin and the random $K$-SAT model. Eventually, we would like to notice that, contrary to the $K$-SAT case we will mention in the following section, the factorized Ansatz gives upper bounds whose value nearly overlaps the latest estimated numerical thresholds [117].

## 4.2 Results of the variational RSB calculations for the random 3-SAT

$K$-SAT is a central problem in theoretical computer science [34]. A throughout study of random version model has been carried out by the physics community in [9, 14, 30, 12] and references

[3] Separated by a Hamming distance of order $N$.

therein , where the reader is referred to for the definition of the problem, the mapping on spin-glass like model and for various analytical and numerical approaches to its solution. Rigorous approaches can be read for example in [177, 115].

In this short section we simply want to state the results for the RSB variational calculations exploiting the factorized Ansatz, and discussing some more recent results announced in [29] and obtained in [30]. We worked directly at zero temperature. Through a computation analogous to the ones for the $p$-spin and the Bicoloring model we found, for the special 3-SAT case,

$$p_0 = \frac{I_0(z_1)}{I_0(z_1) + 2\sum_{k>0} I_k(z_1) e^{\frac{yk}{2}}} \tag{4.33}$$

$$p_l = = p_{-l} = \frac{I_l(z_1) e^{\frac{yl}{2}}}{I_0(z_1) + 2\sum_{k>0} I_k(z_1) e^{\frac{yk}{2}}} \tag{4.34}$$

$$z_1 = \frac{3\gamma}{4\Omega}(1-p_0)^2 e^{-\frac{y}{2}} \tag{4.35}$$

$$\Omega = 1 + \frac{(1-p_0)^3}{8}(e^{-y} - 1) \tag{4.36}$$

for the saddle point equations and

$$F(y) = -\frac{1}{y}(\gamma \log \Omega - \log \Lambda - z_1 \cosh(y) - z_1 \sinh(y) p_0) \tag{4.37}$$

$$\Lambda = \frac{1}{I_0(z_1) + 2\sum_{k>0} I_k(z_1) e^{\frac{yk}{2}}} \tag{4.38}$$

for the potential. Notice that for $y = 0$, re-summing the Bessel functions one immediately retrieves the RS integer fields solution of [9]:

$$p_0 = e^{-\frac{3\gamma}{4}(1-p_0)^2} I_0(\frac{3\gamma}{4}(1-p_0)^2) \ . \tag{4.39}$$

Again, closed fractional fields equations can be written as in the RS and in the $p$-spin and Bicoloring cases, but no solutions have support on non integer values. The variational expression for the complexity (2.133) leads to the presence of a dynamical region in the range of values $\gamma \in [\gamma_d, \gamma_c] = [3.94, 4.39]$. However, as in the Bicoloring model, LGS are not uncorrelated as explicitly stated in the factorized Ansatz picture. A more general solution found in [30] with the $T = 0$ cavity method [24] with a dynamical region $[\gamma_d, \gamma_c] = [3.921, 4.256]$.

The difference between the previous variational results and the zero temperature general 1RSB cavity result is both quantitative and qualitative: in ref. [14] the predicted nature of the intermediate phase is different with respect to the one predicted by the non-vanishing fields complete 1RSB solution, while in ref. [22] the structure of the order parameter is oversimplified. (as well as in [22]) the authors work directly at zero temperature ($T = 0$), which has the advantage that they do not need to study the subtle question of the limit $T \to 0$. The reason why this limit is subtle is due to the fact that some of the local fields, at low temperatures, vanish linearly in $T$, and thus contribute to the local magnetization $m = \tanh(\beta H)$ (the vanishing fields!). The local magnetization at $T = 0$ is zero for a zero field, it is equal to 1 for a finite field, and it takes an intermediate value $m \in ]-1, 1[$ for a vanishing field. The variational approach of [14] focuses onto vanishing fields, and finds a *continuous* phase transition at $\gamma_s \simeq 3.96$ where the vanishing fields in different states start to cluster. However as these are all vanishing fields,

this means that the corresponding local magnetizations, in a given state, are not frozen to $\pm 1$ but take some intermediate value, even in the $T \to 0$ limit. In the $T = 0$ cavity approach (as well as in [22]), the HSP corresponds to a *discontinuous* transition at zero temperature, involving fields which are not vanishing, but are of order one. This means that, in a given state, a finite number of local fields are non-zero integers, giving rise to magnetizations $\pm 1$, as one could expect at zero temperature. This phenomenology cannot be found by considering vanishing fields. Its study with replicas would require using a more complicated Ansatz.

Note that this approach working directly at $T = 0$ also has its limitations, for instance we are unable to determine precisely the self overlap (or the typical radius) of a state, or its internal entropy, precisely because we do not control the vanishing fields.

Moreover the 1RSB picture does not take into account the possible arising of non trivial correlations among LGS at higher values of $\gamma$. This could lead to higher RSB phenomena, as evidence is taken in [89, 90]. However, this seems not to be the case in the dynamical region and immediately beyond the static transition, where the only known phenomenon that could give rise to such further symmetry breaking is indeed the presence of vanishing fields at finite temperature. A population dynamics study of this region with the 1RSB finite temperature Ansatz of [23] shows that the distribution of local fields tend to peak on integers when the temperature goes to zero in the dynamical phase, and this is a strong argument in favor of the exactness of the 1RSB solution. Very recently [58] a solution of the long standing graph-coloring problem on random graphs has been proposed which does not suffer from the need of introducing pathological fractional fields and works at the complete 1RSB level. Similarly to the $p$-spin, Hyper-graphs Bicoloring and the $K$-SAT case, the presence of a dynamical region of metastable states is found and the authors claim the obtained dynamical and static thresholds to be exact. Notice that the calculations of chapter 6 could be in principle extended to the graph-coloring, proving results in [58] to be rigorous upper bounds.

# Chapter 5

# Phase and computational complexity transitions

## 5.1 Global algorithms transitions in linear systems over finite fields

### 5.1.1 Introduction

The methods and concepts of statistical physics of disordered systems constitute a very useful tool for the understanding of the onset of computational complexity in randomly generated hard combinatorial problems. Once the optimization problems are translated into zero temperature spin glass problems, one may study the geometrical changes in the space of solutions as symmetry breaking phenomena. In this context one may view the exponential regimes of randomized search algorithms as out-of-equilibrium phases of stochastic processes. However, combinatorial problems are not always exponentially hard: Problems that can be solved in polynomial time, even in their worst-case realizations compose the so called Polynomial (P) class [34]. Such problems are often of great practical relevance and are tackled using large scale computations. Examples can be found in all disciplines: In physics, just to make one example, one may study ground states of 2D spin glass like Hamiltonians resorting to a polynomial max-cut algorithm [121]. The major application are obviously found in engineering: Examples are design problems (finite elements methods), control theory (convex optimization), coding theory (parity check equations) and cryptography (integer factorization). Due to the practical relevance of the problems and to the typically large number of variables used for their encoding, that is the size of the problems, it is of basic interest to look at the fine structure of the class P in order to concretely optimize the computational strategies. For instance, in error correcting codes it is crucial to have algorithms that converge in *linear* time with respect to the number of encoded bits, any power larger than one being considered of no practical interest. Quite in general, the trade-off between time and memory resources is the guiding criterion which selects the algorithms used in real-world applications. Roughly speaking polynomial algorithms can be divided in different groups depending on the solving strategy they implement. The main groups are local algorithms (e.g. greedy/gradient methods), global algorithms (e.g. Gaussian elimination or Fourier transforms methods), iterative algorithms (e.g. Lanczos method) and parallel algorithms. See Ref. [122] for a basic introduction to the subject. In what follows we shall study a prototype problem of the P class, that is the problem of solving large and random

sparse systems in some Galois field GF($q$). Working in GF($q$) is completely equivalent to perform any operation modulo $q$. Firstly, we give a precise analysis of the computational features for non-trivial ensembles of random instances. By a statistical mechanics study, we look into the – symmetry breaking – geometrical structure of the space of solution thereby providing an explanation for the changes in the power law behavior observed in different algorithms. Moreover, we are able to predict and explain in terms of clustering of solutions, the memory catastrophe found in global algorithms such as Gaussian elimination. Such an effect seriously hampers application of this sort of global algorithms in many circumstances, one example being symbolic manipulations. This memory catastrophe induce in turn an even more dramatic increase in CPU time, which make large problems unaffordable above the dynamical threshold $\gamma_d$ (see below for its definition). Secondly, we consider a specific "real-world" application, namely the Integer Factorization problem used in RSA public key cryptography [123]. By a non-trivial mapping of the factoring problem on a sparse linear system modulo 2, endowed with a quite peculiar statistical distribution of matrix elements, we analyze which are the characteristic geometrical properties of solutions that are responsible for the usage of specific algorithms and constitute the possible bottleneck for the near future. Interestingly enough, the changes in both time or memory requirements during the solution process of sparse systems can be interpreted in physical terms as a dynamical transition at which the phase space of the associated physical systems becomes split into an exponential number of ergodic components. While it is to be expected that local algorithms get stuck by local minima at such phase boundary, it is less obvious to predict which is the counterpart of the dynamical transition in global algorithms, for which polynomial time convergence is guaranteed even for the hardest instances. Indeed the dynamical transition manifests itself as a phase transition in the computational requirements which in turn leads to a slowing down phenomenon that saturates the upper bound for the convergence time. Such a change of scale in memory requirements constitute a serious problem for hardware implementations of large scale simulations.

### 5.1.2 Random Linear systems in GF(2): rigorous results and statistical mechanics analysis

As is well known in the context of error correcting codes [124], solving a sparse linear system modulo 2 is equivalent to finding the zero temperature ground states of a class of multiple degree interactions $p$-spin models on diluted random graphs. Let us consider a random linear system in GF(2) in the form $\hat{A}\vec{x} = \vec{y} \ \ mod[2]$, where $\hat{A}$ is a 0-1 matrix of dimension $M \times N$. For each of its specific choices $\hat{A}$ can be interpreted as the contact matrix of a particular random hyper-graph belonging to a specific ensemble. The class of random matrices we shall deal with are defined by the fraction of rows $v_l$ with $l$ non zero elements. The latter are placed uniformly at random within each row. The notation has been chosen to be consistent with the one of the previous chapters. We focus on matrices that lead to graphs with an average rank value $\langle l \rangle = \sum_l l v_l$ finite and much less than both $M$ and $N$. We are interested to the limit of very large matrices, where we can assume $N, M \to \infty$ with a finite ratio $\gamma \equiv M/N$. This is the regime in which a study of the computational cost is important in that it applies directly to large scale computations. In the limit $N, M \to \infty$ average quantities characterizing the system (e.g. the average fraction of violated equations) are known to be equal to the most probable values (i.e. their probability distribution is strongly peaked [125]) and therefore single random large systems behave as the average over the ensemble. We will always assume $v_1 = 0$ at the beginning, since rows with a single one corresponds to trivial equations which can be removed

a priori from the set. The equivalence between linear systems and spin models is a quite straightforward generalization of the mapping used in the 2+p-XORSAT model (which by the way can in turn be seen as a particular case of the present model, where only two and three variables equations are present.). We start from a set of linear equations in GF(2), $\hat{A}\vec{x} = \vec{y}$, and we build up a spin Hamiltonian whose ground state energy $E_{gs}$ counts the minimal number of unsatisfied equations. In the case where $E_{gs} = 0$, ground state configurations will correspond to solutions of the original set of linear equations and the zero-temperature entropy will count the number of such solutions. The construction is done as follows: For every equation, labelled by $i \in [1 \dots M]$, let us define the set of variables $\vec{x}$ entering equation $i$ as

$$v(i) \equiv \{j \in [1 \dots N] : A_{ij} = 1\} \quad . \tag{5.1}$$

With the transformation $s_j = (-1)^{x_j}$ and $J_i = (-1)^{y_i}$, we have that every equation can be converted in a term of the Hamiltonian through

$$\sum_{j=1}^{N} A_{ij} x_j = y_i \Leftrightarrow \sum_{j \in v(i)} x_j = y_i \Leftrightarrow \prod_{j \in v(i)} s_j = J_i \quad , \tag{5.2}$$

where the multi-spin interaction contain at least 2 spins since we set $v_1 = 0$. Then the Hamiltonian

$$H = \frac{1}{2}\left[M - \sum_{i=1}^{M} J_i \prod_{j \in v(i)} s_j\right] \quad , \tag{5.3}$$

fits the above requirements and can be used in the analytical treatment. A better form for the above Hamiltonian can be obtained grouping together $l$-spin terms with the same $l$, that is

$$H = \frac{1}{2}\left[M - \sum_{k} \sum_{i_1 < i_2 < \dots < i_k} J_{i_1 i_2 \dots i_k} s_{i_1} \dots s_{i_k}\right] \quad , \tag{5.4}$$

where $s_i = \pm 1$ are Ising spins and the couplings $J_{i_1 i_2 \dots i_k}$ are i.i.d. quenched random variables taking values in $\{0, \pm 1\}$. The total number of interactions, that is of terms with $J \neq 0$, is M, and the energy is zero if and only if all the interactions are satisfied. For each unsatisfied interaction the energy increases by 1. The fraction of interactions of $l$-spin kind is $v_l$ and thus the probability of having $J_{i_1 i_2 \dots i_l} \neq 0$ equals $a_l M / \binom{N}{l} \simeq \gamma v_l l!/N^{l-1}$, while the sign of $J_{i_1 i_2 \dots i_l}$ depends on the probability distribution of the components of $\vec{y}$,

$$P(J_{i_1 i_2 \dots i_l}) = \left[1 - \frac{\gamma v_l l!}{N^{l-1}}\right] \delta(J_{i_1 i_2 \dots i_l}) + \frac{\gamma v_l l!}{N^{l-1}} \left[p\, \delta(J_{i_1 i_2 \dots i_l} - 1) + (1-p)\, \delta(J_{i_1 i_2 \dots i_l} + 1)\right] \quad , \tag{5.5}$$

where $p \in [0, 1]$ controls the fraction of zeros in $\vec{y}$. As long as the system admits at least one solution, it can always be brought by a gauge transformation in the form with $p = 1 \Leftrightarrow \vec{y} = \vec{0}$. This corresponds to have positive or null couplings only, like in a diluted ferromagnetic model. The liceity of the gauge transformation is a peculiarity of generalized $p$-spin models of this kind, as stated in the first chapter. In order to make a connection between the behavior of solving algorithms and the structure of the matrix $\hat{A}$, we study the geometrical properties of the space of solution, i.e. ground states of (5.4), as a function of $\gamma$ for non-trivial choices of $\{v_l\}$. We may have access to the structure of such a space by just performing the $T = 0$ statistical mechanics analysis of the spin glass model, with control parameter $\gamma$. For $\gamma$ large enough, at say $\gamma_c$,

the system of equations becomes over-determined and some of the equations can no longer be satisfied. This fact is reflected in the ground state energy of the associated spin glass model becoming positive. The interesting aspect of the problem is that, under proper conditions, there appears a clustering phenomenon with macroscopic algorithmic consequences at some intermediate value $0 < \gamma = \gamma_d < \gamma_c$. We will focus our attention on the latter transition, thus assuming a priori that at least one solution always exist. This allow us to fix $\vec{y} \equiv \vec{0}$ hereafter. The complete picture of the typical structure of the solution space can be obtained through the RS replica calculations of chapter 1 specialized to the case of Poissonian degree hyper-graph with *a priori* general choice of $v(x)$. Due to the zero energy condition ($E_{gs} = 0$ for $\gamma < \gamma_c$), the dominance of thermodynamical states is purely to be determined in entropic terms. Defining $S_0(\gamma)$ as the logarithm of the number of solutions to $\hat{A}\vec{x} = \vec{0}$ divided by $N$, we have that

$$S_0(\gamma) = S(m,\gamma) = \log(2)\left[(1-m)[1-\log(1-m)] - \gamma \sum_{l\geq 2} v_l (1-m^l)\right] \quad , \tag{5.6}$$

where $m$ solves

$$G(m) = 1 - m - e^{-\gamma \sum_{l\geq 2} l v_l m^{l-1}} = 0 \quad . \tag{5.7}$$

When more than one solution to eq.(5.7) exist, the one maximizing $S(m,\gamma)$ must be chosen. At fixed $\{v_l\}$, one can study the phase diagram as a function of $\gamma$. At low enough $\gamma$, eq. (5.7) has only the trivial solution $m = 0$ and the system is paramagnetic with entropy $S(0,\gamma) = \log(2)\,(1-\gamma)$. As long as $v_2 > 0$, the condition for the continuous phase transition of two-loops percolation in the rank 2 sub-graph is given by the instability condition:

$$\begin{aligned} &\left.\frac{\partial G(m)}{\partial m}\right|_{m=0} = 0 \\ &G(m=0) = 0 \ , \end{aligned} \tag{5.8}$$

that reduces to[1]

$$\hat{\gamma} = \frac{1}{2v_2} \tag{5.9}$$

Typically a non trivial magnetized solution for the order parameter, $m^* > 0$, appears at a value $\gamma_d$ such that

$$G(m^*) = 0 \ \ and \ \ \left.\frac{\partial G(m)}{\partial m}\right|_{m=m^*} = 0 \quad . \tag{5.10}$$

This condition gives a threshold for the onset of the dynamical region at

$$\gamma_d = \frac{1}{(1-m^*)\sum_{l\geq 2} l(l-1) v_l (m^*)^{(l-2)}} \tag{5.11}$$

and contains the condition for $\hat{\gamma}$ as a particular case. This last solution becomes entropically favored at a value $\gamma_c$ found solving

$$S(0,\gamma_c) = S(m^*,\gamma_c) \quad . \tag{5.12}$$

As in the case of the 2+p-XOR-SAT model of chapter 2, we can look for the presence of a tricritical point where $\hat{\gamma} = \gamma_d = \gamma_c$. This is given by the instability condition

$$G(m^*=0) = 0 \ \ G'(m^*=0) = 0 \ \ and \ \ G''(m^*=0) = 0 \tag{5.13}$$

[1] $\gamma = 1/2$ for $v_2 = 1$.

that reduces to

$$v_2 = 3v_3 = \frac{1}{2\gamma_{tricritical}} \ . \tag{5.14}$$

Notice that the value of the tricritical point, if it exists, does not depend on other than the fraction of two variables over three variables equations. There are obviously cases [2] where a tricritical point does not exist. In those situation the shift from a continuous to a discontinuous transition is sharp. A part of these last examples, the 2+p model retains a great deal of generality, and indeed this particular case treated in chapter 2 and in [21] retains many of the qualitative features of this more general analysis. [3]. The crucial observation is now the following. At $\gamma_d$, together with the magnetized solution, there appear other spin glass solutions to the saddle-point equation. In particular, it can be shown [26] that the difference between the paramagnetic and the ferromagnetic entropies,

$$\Sigma(\gamma) = S(0,\gamma) - S(m^*,\gamma) \quad , \tag{5.15}$$

gives the configurational entropy of the problem, that is the number of clusters of solutions [4]. There exist $\exp[\Sigma(\gamma)N]$ well separated clusters [Hamming distances $\sim \mathcal{O}(\mathcal{N})$], each one containing a number $\exp[S(m^*,\gamma)N]$ of closed solutions [Hamming distances $\sim \mathcal{O}(\infty)$]. This clusterizations has two main consequences. Local algorithms for finding solutions running in linear time in $N$ stop converging [19]: this is the typical situation for greedy algorithm which get stuck in one of the most numerous local minima at a positive energy. Global algorithms, which are guaranteed to converge in polynomial time, need to keep track along computation of this complex structure of solutions and a memory linear in $N$ turns out to be insufficient, as we will show below. For a general choice of $\{v_l\}$, the configurational entropy reads, from eq. (2.185),

$$\Sigma(\gamma) = \log(2)\left[1 - (1-m)[1-\log(1-m)] + \gamma \sum_{l\geq 2} v_l m^l\right] \quad , \tag{5.16}$$

where $m$ is the largest solution to eq. (5.7). As discussed in Ref. [21, 26], the values of $\gamma_d$ and $\gamma_c$ are found as the points where $\Sigma(\gamma)$ first appears with a non zero value and where it reaches zero again. We remind the reader that the correct expression for the complexity can be found via eq. (2.185) only due to the particular symmetry of this family of models. Moreover, even in this simple case we will see at the end of this section that there are choices of the generating function $v(x)$ for which this complexity picture is not physical, being ruled out by a previously occurring continuous transition. The algorithmic consequences of having $\Sigma(\gamma) > 0$ have been already exposed in Refs. [19, 22]: For $\gamma > \gamma_d$ a glassy state with positive energy arises, which traps any local dynamics, preventing it to converge towards the ground state of zero energy. We conjecture the counterpart on global algorithms, such as Gaussian elimination, to be that the resolution time increases with $N$ faster than linear. In the next section we will check the above conjecture with two different Gaussian elimination algorithms, none of which is able to solve the system in linear time for $\gamma > \gamma_d$.

[2] think for example to a 2+4 model where only $v_2$ and $v_4$ are different from 0.

[3] We will see in the following that there are however cases where no tricritical point is present, because condition (5.14) cannot be fulfilled by the parameters of the hyper-graph degree distribution.

[4] Two solutions belong to the same cluster (resp. to different clusters) if their Hamming distance is $\mathcal{O}(\infty)$ [resp. $\mathcal{O}(\mathcal{N})$].

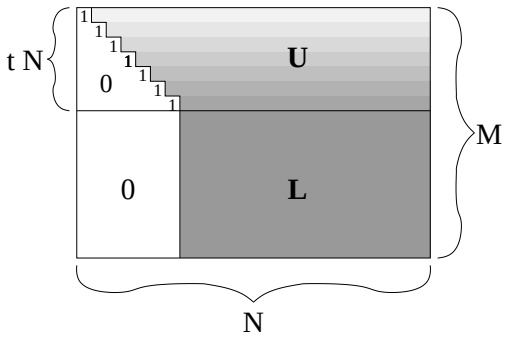



Figure 5.1: Typical shape of the $\hat{A}_t$ matrix after $tN$ steps of Gaussian elimination.

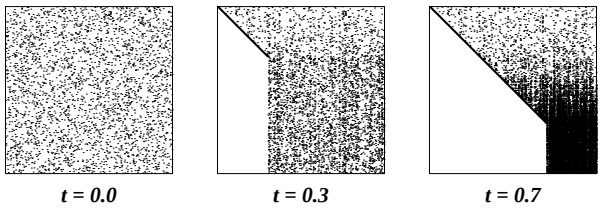



Figure 5.2: The evolution of the $\hat{A}_t$ matrix for a specific $1024 \times 1024$ random system. Every dot corresponds to a 1 entry.

### 5.1.3 Algorithms behavior

In this section we analyze the performances of a couple of different 'Gaussian elimination' algorithms, their difference being in the order equations are solved. We will measure the number of operations and the size of the memory required for the solution of a set of linear equations, that is the complexity for finding all solutions to $\hat{A}\vec{x} = \vec{y}$. We will see that, for a generic ensemble of random problems, any algorithm undergoes an easy/hard transition at a certain $\gamma$ value, which can not be pushed beyond the dynamical transition threshold $\gamma_d$. In this context we call *easy* such problems which are solvable with a CPU-time and memory of order $N$, and *hard* those requiring resources scaling with $N^\alpha$, where $\alpha > 1$. Given a set of $M$ linear equations in $N$ variables, Gaussian elimination proceeds as follows [for concreteness we will always work in GF(2)]: At each step, it takes an equation, e.g. $x_1 + x_2 + x_3 = y_1$, solves it with respect to a variable, e.g. $x_1 = x_2 + x_3 + y_1$, and then it substitutes variable $x_1$ with the expression $x_2 + x_3 + y_1$ in all the equations still unsolved. This procedure gives all the solutions to any set of linear equations in, at most, $\mathcal{O}(\mathcal{N}^\ni)$ steps and using $\mathcal{O}(\mathcal{N}^\in)$ memory. Nevertheless this bounds only holds in the worst case, namely when the matrix $\hat{A}$ is dense. Very often, in actual applications, the matrix is sparse and the algorithm is faster. We define sparse a matrix with $\mathcal{O}(\mathcal{N})$ ones and dense that with $\mathcal{O}(\mathcal{N}^\in)$ ones. In order to analyze the computational complexity of this problem, and its connections to phase transitions, we focus on a specific ensemble of random problems, generalizations to other ensembles being straightforward. We choose sets of $M = \gamma N$ linear equations, each one containing exactly $k = 3$ of the $N$ variables, taking values in GF(2). Thus the degree of a variable, defined as the number of equations this variable enters in, takes values from a Poissonian distribution of mean $3\gamma$. For very large $N$, that is in the thermodynamical limit, we are interested in how the complexity changes with $\gamma$. Moreover, for a fixed $\gamma$ such that the problem is hard, we would like to know when (in terms of the running-time $t$) and why the algorithm becomes slower and slower. The running-time $t$ is

measured as the number of equations already solved, normalized by $N$, and thus takes values in $[0, \gamma]$. $\hat{A}_t$ is the matrix representing the set of equations after $tN$ steps, and it has the form shown in fig. 5.1. See fig. 5.2 for the actual shape of $\hat{A}_t$ in a specific case with 1024 equations in 1024 variables. For ease of simplicity, we have reordered the variables and the equations of the system, such that, at the $i$-th step, we solve the $i$-th equation with respect to $x_i$. With this choice the left part of the matrix $\hat{A}_t$ has ones on the diagonal and zeros below. The right part can be naturally divided in an upper part $U$ and a lower one $L$. The density of ones in the $L$ matrix — let us call it $\rho(t;\gamma)$ — is uniform and depends on the initial $\gamma$, the time $t$ and the algorithm used for solving the linear system. The density of ones in the $U$ part is not uniform and varies from row to row, as shown in fig. 5.1 with gray tones. For continuity reasons the density at the $m$-th row of $U$ is exactly $\rho(m/N;\gamma)$. Then $U$ is sparse or dense depending on whether $L$ is. Defining $l(t;\gamma) = \rho(t;\gamma)N(1-t)$ the average number of ones per row in $L$, we have that a sparse (resp. dense) matrix corresponds to having a finite $l$ (resp. $\rho$). At each time step, the number of operations required are directly related to the density of the matrix $\hat{A}_t$ and thus to that of $L$. More specifically, solving with respect to the variable in the upper left corner of $L$, the number of operations is proportional to the number of ones in the first row of $L$, i.e. $k(t;\gamma)$, times the number of rows of $L$ having a one in the first column, i.e. $\rho(t;\gamma)N(\gamma - t)$, and thus equals

$$l(t;\gamma)\rho(t;\gamma)N(\gamma - t) = l^2 \frac{\gamma - t}{1-t} = N^2\rho^2(\gamma - t)(1-t) \quad . \tag{5.17}$$

Then, if the matrix $L$ is sparse a finite number of operations per step is enough, while $\mathcal{O}(\mathcal{N}^{\in})$ operations are required when $L$ is dense. Integrating over time $t \in [0, \gamma]$, we have that the total complexity is given by

$$N \int_0^\gamma \frac{\gamma - t}{1-t} l^2(t;\gamma)dt = N^3 \int_0^\gamma (\gamma - t)(1-t)\rho^2(t;\gamma)dt \quad . \tag{5.18}$$

Since the function $\rho(t;\gamma)$ is continuous in $t$, we conclude that

$$\left.\begin{array}{c} \rho(t;\gamma) \ \propto 1/N \\ k(t;\gamma) \ \ finite \end{array} \ \forall\ t \in [0,\gamma]\right\} \ \Leftrightarrow \rho_{max}(\gamma) = 0 \Leftrightarrow \ \left\{ \begin{array}{c} CPU \ \ time \ \propto N \\ Memory \propto N \end{array} \right. \tag{5.19}$$

$$\left.\begin{array}{c} \rho(t;\gamma) \ \ finite \\ k(t;\gamma) \ \propto N \end{array} \ \exists\ t \in [0,\gamma]\right\} \ \Leftrightarrow \rho_{max}(\gamma) > 0 \Leftrightarrow \ \left\{ \begin{array}{c} CPU \ \ time \ \propto N^3 \\ Memory \ \propto N^2 \end{array} \right. \tag{5.20}$$

where

$$\rho_{max}(\gamma) = \lim_{N\to\infty} \max_{t\in[0,\gamma]} \rho(t;\gamma) \tag{5.21}$$

is the order parameter signaling the onset of the hard regime. Having found the relation between the density of ones in $L$ and the computational complexity we are interested in, we can now run the algorithms and measure the density $\rho(t;\gamma)$. The easy/hard transition should manifest itself with $\rho_{max}(\gamma)$ becoming different from zero.

### Simplest Gaussian elimination

Let us start with the simplest algorithm, which solves the equations in the same (random) order they appear in the set and with respect to a randomly chosen variable. In this very simple case, one can easily show that the complexity for solving a set of linear equations with initial parameter $\gamma = \gamma_0$ is exactly the same as for solving a larger system with $\gamma > \gamma_0$ up to time $t = \gamma_0$. For this reason, in this case the function $\rho(t;\gamma)$ does not depend on $\gamma$ and can be

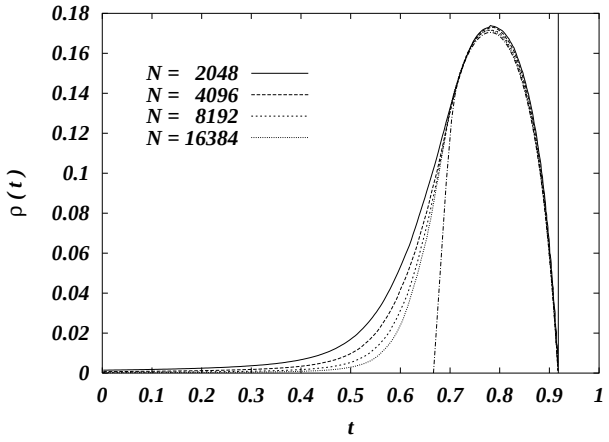



Figure 5.3: Density of ones in the $L$ matrix during the solving process with the simplest Gaussian elimination algorithm. The vertical bar marks the analytical critical point $\gamma_c = 0.918$.

calculated once for all the relevant $\gamma$ values. Moreover, it is known [19] that this algorithm, in the limit of very large $N$, keeps the matrix sparse for all $\gamma < 2/3$. In fig. 5.3 we show the function $\rho(t)$ for many large $N$ values. The dotted-dashed line is a guide to the eyes and it should not be too much different from the thermodynamical limit: It goes through the two points ($\gamma = 2/3$ and $\gamma = 0.918$) where $\rho(t)$ must vanish and coincide with numerical data in the region, where data for different sizes seem to be quite close to the asymptotic shape. In the thermodynamical limit, the algorithm keeps the matrix sparse for times $t \leq 2/3$ and so it undergoes an easy/hard transition at $\gamma = 2/3$: As long as $\gamma \leq 2/3$, $\rho_{max}(\gamma) = 0$, while $\rho_{max}(\gamma) > 0$ for $\gamma > 2/3$. As we will see below the location of the transition depends on the algorithm used and, in this case, does not correspond to any underlying thermodynamical transition. We note *en passant* that the $\gamma$ value where the $L$ matrix becomes sparse again seems to correspond to the critical point $\gamma_c = 0.918$ [19, 26, 94] (marked with a vertical line in fig. 5.3). An explanation to this observation will be given in a forthcoming publication. It implies that the value of the critical point $\gamma_c$, which is relevant e.g. in the XOR-SAT model [82] in theoretical computer science, could be obtained also by solving differential equations for $\rho(t)$.

### Smart Gaussian elimination

Now we turn to a more clever Gaussian elimination algorithm, which works as follows: At each time step, it chooses the variable $x$ having the smallest degree in $L$, i.e. that corresponding to the less dense column of $L$, and solves with respect to $x$ any of the equations where $x$ enters in. Clearly, in this case, the dynamics and thus the density of ones in $L$ depend on the initial $\gamma$ value: A smaller $\gamma$ implies that for a longer time we can choose variables of degree 1, which do not increase the average number of ones per row in $L$. It can be rigorously shown [26] using, the leaf removal procedure described in the first chapter, that this procedure keeps the density of the $L$ matrix constant, $\rho(t;\gamma) = \rho(0;\gamma)$, for times smaller than $t^* = \gamma(1 - m^3)$, where $m$ is the largest solution to $1 - m = \exp(-3\gamma m^2)$. The last equation is exactly eq. (5.7) with $\{v_3 = 1, v_{k\neq 3} = 0\}$. Running the algorithm for different $\gamma$ values we obtain the densities reported in the main panel of fig. 5.4. For $\gamma < \gamma_d = 0.818$ the density remains $\mathcal{O}(\infty/\mathcal{N})$ all along the run, while for $\gamma > \gamma_d$ there is a time when the density becomes finite and the problem

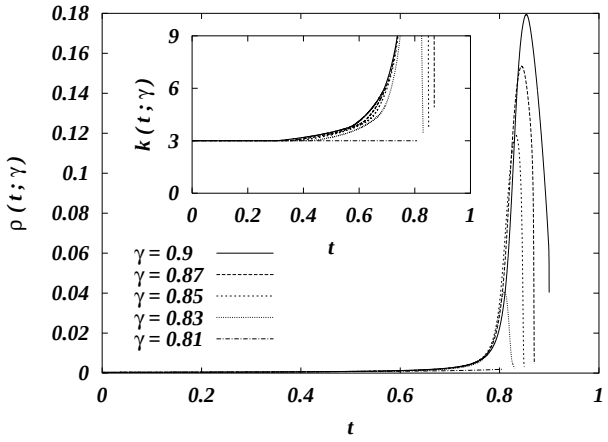



Figure 5.4: Density of ones in the $L$ matrix during the solving process with a smart Gaussian elimination algorithm ($N = 8192$). Inset: Zoom on the low-density part (with a different normalization).

hard to handle. In order to better show what happens around $t^*$, we have plotted in the inset of fig. 5.4 the mean number of ones per row, $k(t)$. It is clear that for $\gamma < \gamma_d$ this number remains constant, since one can solve the system choosing only variables of degree 1, not altering the $L$ matrix. On the contrary, for $\gamma \geq \gamma_d$ there is a time $t^*(\gamma)$ when variables of degree 1 terminate, and the algorithm has to start making substitutions in $L$, thus increasing the density of ones. Then $\gamma_d$ marks the onset of computational hardness, both in memory and CPU time. One may object that also this value for the easy/hard transition may depend on the particular algorithm. Note, however, that a completely different linear algorithm described in Ref. [19] (which firstly works with high-degree variables) seems to work up to $\gamma_d$. Moreover, as seen in the previous section, we have analytically found that at $\gamma_d$ a transition takes place, which drastically changes the structure of the solutions space, and so we argue that *any* algorithm running in linear time can converge only up to $\gamma_d$. Indeed is shown in [26] that solutions spontaneously form clusters for $\gamma > \gamma_d$ and this particular structure requires a larger memory to be stored.

### 5.1.4 The RSA cryptosystem and factorization

In this section we shall validate the above scenario on a concrete application, namely integer factorization problems arising in the RSA cryptosystem. Such problems allow for a non-trivial mapping onto huge linear systems in GF(2) with a rather peculiar structure of the underlying contact matrix. In order to be as self-contained as possible, we firstly give a short review of the problem and the methodology (a detailed description of the RSA cryptosystem can be found in [123]). The only known method for breaking RSA implies factorization of the private key, which consists in a natural number which is the product of two big prime numbers, $n = p \cdot q$, with $p$ and $q$ approximately of the same size $\simeq \sqrt{n}$. Keys currently used in applications are numbers $n$ ranging from 1024 bits (309 decimal digits) to 2048 bits (617 digits) length. The first attempt at a massive parallel factorization was the RSA129 (129 digits, 428 bits) challenge, solved in 1994 with the *quadratic sieve* (QS) algorithm. More recently, in August, 1999 the RSA155 challenged was solved using the *general number field sieve* (*GNFS*) algorithm. This has forced to abandon the 512-bit (155 digits) length for sensitive information security. There are now several sub-exponential algorithms for solving the factorization problem, the faster of which is *GNFS*. *QS*

and *GNFS* share the same structure, consisting of two phases: a first one in which a big (the size depending mostly on the size of $n$) linear system in GF(2) is produced, and a second one in which this system is solved. Although the first phase is definitely more costly, the solving phase (which affect this section) takes a respectable part of the total time and memory requirement. Especially as numbers get bigger this becomes a limitation, because the fastest solving methods used employ a sole workstation, with the consequent memory restriction. Moreover, in recent factorizations a new filtering phase has been placed between the previous two, in which pieces of the system (specifically columns of the $\{0,1\}-$matrix) get discarded in order to simplify the solving phase, effectively transferring part of the total time from the second phase to the first one.

### The QS algorithm

For a nice description of the QS algorithm see [126]. Synthetically, QS works at follows. It builds a list of integer numbers $\{y_i\}_{i\in I}$ such that:

- $y_i \equiv x_i^2 \ mod[n]$ for some $x_i$ and $y_i \neq x_i$;
- $y_i$ is completely factorizable in a given (relatively small) subset of $B$ primes called the factor-base.

This is called the *sieving* phase. The algorithm then searches a subset $J \subset I$ of elements of the list such that $\prod_{i\in J} y_i = z^2$ is a square (*solving* phase). Once found, $z^2 \equiv x^2 \ mod[n]$ (here $x = \prod_{i\in J} x_i$) and this implies that $n$ divides $(x+z)(x-z)$ and then $gcd(x-z,n)$ will likely (further trials will increase the probability) be a non-trivial factor of $n$. In order to find element pairs $x_i$,$y_i$ such that $y_i \equiv x_i^2 \ mod[n]$ we can use the polynomial $y = f(x) = x^2 - n$ and evaluate it at different values of $x$, keeping only values of $y$ which completely factorize between the first $B$ primes (the factor-base). The sieving will allow us to do this efficiently. The idea is that, given $p$, it is easy to find which are the values of $f(x)$ which are divisible by $p$, because $p$ divides $f(x)$ if and only if $f(x) = x^2 - n \equiv 0 \ mod[n]$ and this is a quadratic equation in GF(p), having at most 2 solutions. These solutions are nothing but the square roots of $n$ modulo $p$ (if they exist). This has a first consequence, i.e. that a prime $p$ will not divide $f(x)$ if $n$ is not a square $mod[p]$ independently of the value of $x$. So if we can detect these primes, we can eliminate them directly from our set of primes. Detecting them is very easy: Using Fermat's little theorem, we know that

$$n^{p-1} \equiv 1 \ mod[p] \ , \tag{5.22}$$

assuming that $p$ do not divide $n$ (which is trivially a reasonable assumption, anyway, because we are searching a divisor of $n$). If $p$ is an odd prime, i.e. not 2 (all $n$ are a squares $mod[2]$), then calling $m = n^{\frac{p-1}{2}}$ we have that $m^2 \equiv 1 \ mod[p]$, so $m \equiv \pm 1 \ mod[p]$. This $m$ will prove to be handy. If $n \equiv s^2 \ mod[p]$ then $m \equiv s^{p-1} \equiv 1 \ mod[p]$. Conversely, if $m \equiv 1$ then $n$ is a square modulo $p$ (not proven here). The number $m$ is called the Lagrange symbol and can be computed efficiently in one of the firsts stages of the algorithm. Useful primes (those with $m = 1$) are roughly a random half of all the first $B$ primes. So now we will keep only this half and redefine "the first $B$ primes" as "the first $B$ primes with $m = 1$". Computing the square root modulo $p$ is a bit more difficult than knowing that it exists, but can also be done efficiently. For instance, the easiest case is when $\frac{p+1}{4}$ is an integer, then $\left(n^{\frac{p+1}{4}}\right)^2 = n^{\frac{p+1}{2}} \equiv mn \ mod[p]$. As $m = 1$ (or else there is no solution) then $\pm n^{\frac{p+1}{4}} \ mod[p]$ are the required square roots. Once we

have computed the two solutions $f(x_p^{1,2}) \equiv 0\ mod[p]$, then adding $p, 2p, 3p, \ldots$ to them we will obtain *all* $x$ such that $f(x)$ is divisible by $p$. The sieve idea is to initialize an array with values of $f(x)$ for consecutive $x \in [[\sqrt{n}], [\sqrt{n}] + M]$ indexed by $x$, and then for each $p$ in our factor base to divide the corresponding arithmetic progression of $\{f(x_p^{1,2} + kp), k = 1, \ldots\}$ by $p$. At the end those values which are completely factored between the primes in the factor base will become 1 (Well, not exactly. Some of them can have multiple times the same prime factor. But we can set up a threshold instead of 1 below which we consider the number completely factored. We can recheck afterwards). We take those values and put their factorization in an array

$$\begin{array}{c} \\ p_1 \\ \vdots \\ p_B \end{array} \begin{array}{c} \begin{array}{ccc} f(x_1) & \cdots & f(x_m) \end{array} \\ \left[\begin{array}{ccc} \alpha_1^{(1)} & \cdots & \alpha_1^{(m)} \\ \vdots & \ddots & \vdots \\ \alpha_B^{(1)} & \cdots & \alpha_B^{(m)} \end{array}\right] \end{array} \quad mod[2]$$

The *solving* phase is conceptually simple: A solution of the homogeneous linear system $\hat{A}v = 0$ is a $\{0, 1\}$vector $v$ which represent correctly the subset $J$, in the sense that $v_i = 1$if and only if $i \in J$.

### The matrix ensemble

### Correlations

We have implemented the simplest QS described in [126] in order to analyze the output matrix ensemble. We attempted to look for correlations in the presence/absence of different primes in the set of divisors of the variables $y_i$. Specifically we checked that there is virtually no correlation between rows of the matrix: We have taken one such output matrix (resulting from the factorization of a product of two 20 digits primes) and computed the covariance between the corresponding spin variables $s_1, s_2$ of two rows $r_1, r_2$, the averages being taken along different columns,

$$\langle s_1 s_2 \rangle - \langle s_1 \rangle \langle s_2 \rangle \quad .$$

Once repeated for all $r_1 < r_2$, we found that all pairs have correlations in the interval $0 \pm 0.06$, a proportion of 0.9999 pairs having correlations in $0 \pm 0.02$.

### Dependence on "factorization hardness"

We then examined dependence of the resulting distributions of ones per row on the "factorization hardness" of the number $n$. Typically (depending on the algorithm) the complexity of factorization depends on the size of the smallest prime divisor of $n$ [5]: For instance, *trial division* ends in exactly this amount of steps. It was conjectured that this would be reflected in the structure of the output matrix. We have constructed 25 numbers $n$ with different factor sizes (from now on, factor type 10+10+10 will mean a 30 digit number constructed as a product of tree 10-digit primes) organized as follows:

- 5 of type 20+20
- 5 of type 10+30

[5] This is why in RSA we choose $n = p \cdot q$ with $p, q \simeq \sqrt{n}$.

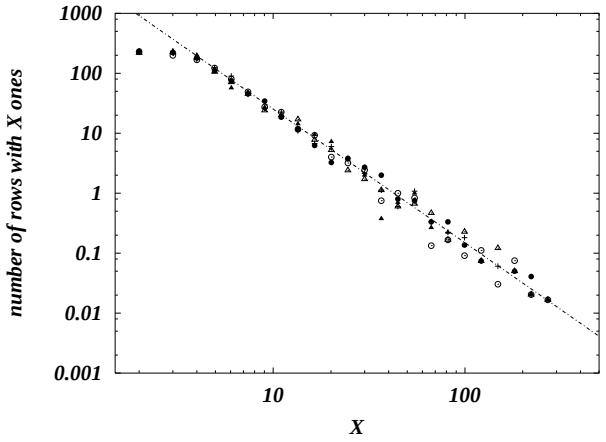



Figure 5.5: Probability distribution of the number of ones per row in 5 different matrices of size around 1300. The line is the best power law fit on $X > 3$ data, giving an exponent $\sim -2.2$.

- 5 of type 13+13+13
- 5 of type 10+10+10+10
- 5 of type 5+5+5+5+5+5+5+5

All 25 numbers differed between them in less than a 0.01%. We then made QS compute the factorization matrices, with a factor base of size 1500. This value for the size of the factor base has been chosen experimentally in order to minimize the sieving phase duration. The resulting matrices were of size $1500 \times 1510$ and were then post-processed in order to remove rows and columns with a single 1. The final size is thus reduced of about 200 columns and rows. The resulting distributions of ones per row are plotted in fig. 5.5, showing very little variations. They can be very well described by a unique distribution, which is substantially a power law with some little deviations in the range of type-2 and type-3 rows. The best fit in the region $X > 3$ gives an exponent $\sim -2.2$. Our conclusion is that statistical properties of the resulting matrix do not depend on the factorization hardness. The bottleneck for factorizing a large hard number is mainly determined by the time required by QS to generate the matrix, which indeed strongly depends on the size of the smallest factor. In the rest of the section we will analyze the solving phase, assuming the factorization matrix to have uncorrelated rows and the number of ones per row to be a random variable extracted from distribution in fig. 5.5. These two assumptions have been experimentally verified.

### Linear solving methods

Plain standard Gaussian elimination execution time is cubic in the size of the matrix (our matrices are almost square). Fortunately, we can pack 32 matrix entries in a single 4-byte word, and then the sum operation is implemented as the low-cost bit-wise logical XOR operation, saving a factor 32 in time. As also the matrix is very sparse, instead of keeping in memory all of it, we can memorize only the position of 1's. This forbid us to use the factor-32 trick, but allows us to do the first steps very quickly. At some time in the Gaussian elimination process (typically more than half of the process), the remaining (non eliminated) part will be very dense, and then it will be convenient to switch to the standard method above. This is

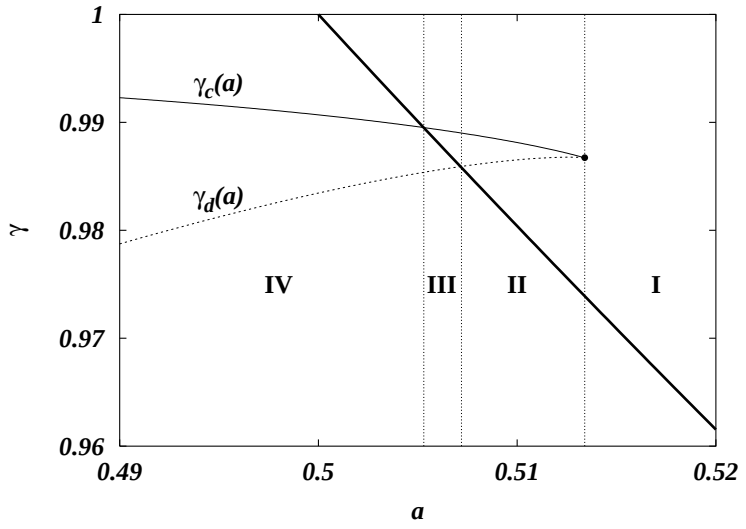



Figure 5.6: Phase diagram $(a,\, \gamma)$ for a typical choice of $s = 2.2$ and $l_{max} = 200$. The bold line $1/(2a)$ represents the continuous transition, while $\gamma_d(a)$ and $\gamma_c(a)$ corresponds respectively to the spinodal and the critical lines of a first order transition. The dot marks the origin of these lines.

what was done in the solving phase of RSA129. Another option is to use in one of the stages an iterative algorithms, like the discrete Lanczos. The Lanczos method has the advantage of having a stable $\mathcal{O}(\mathcal{N}^{\in})$ total time for a sparse matrix, but finds only one solution (or a prefixed quantity in the block-Lanczos variant) instead of all of them. For factorization this is not a problem, because we need only a few solutions to have a reasonable chance. This is the method that was used in the solving phase of RSA155.

**Power law distributed $\{v_l\}$: Phase diagram and comparison with real application data**

The previous analysis leads to the construction of matrices whose density of non zero entries follows quite well a power law distribution with light deviations due to rows with a small number of ones and a cutoff, $l_{max}$, of some hundreds. Then we use the following distribution in the analytical treatment:

$$v_2 = a \quad , \tag{5.23}$$

$$v_k = \epsilon\, l^{-s} \quad for \;\; 3 \leq l \leq l_{max} \quad , \tag{5.24}$$

where $\epsilon$ is a normalizing factor equal to $(1-a)/\sum_{l=3}^{l_{max}} l^{-s}$. The factorized integers considered in the previous section lead to an exponent $s \simeq 2.2$ and to a non zero support up to $l_{max} \sim 200$. The choice of keeping $v_2$, and only $v_2$, as an independent parameter is dictated by the very difference in the physical behavior of 2-spin terms and $l$-spin terms with $l > 2$. The study of the phase diagram in the control parameter $\gamma$ for choices of $a$, $s$ and $l_{max}$ retrieved from real data reveals a non trivial behavior. In fig. 5.6 we show the phase diagram for $s = 2.2$ and $l_{max} = 200$. Only part of the entire phase diagram ($a \in [0,1]$, $\gamma \in [0,1]$) is shown for clarity. The lines further go on smoothly outside the drawn portion. If $a$ is high enough, we are in the rightmost region **I** of the phase diagram, where algorithms smoothly find solutions to the system and do not undergo any critical slowing down. Indeed, crossing the bold hyperbole $\gamma = 1/(2a)$ given by

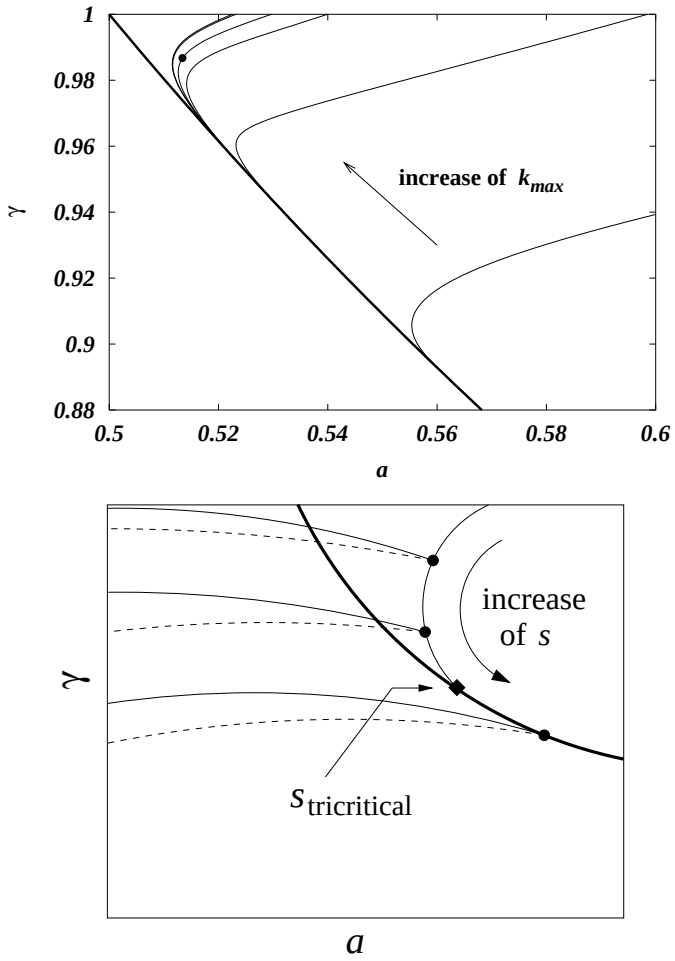



Figure 5.7: Dependence on $s$ and $l_{max}$ of the origin of first order critical lines. The bold curve is the continuous phase transition $\gamma = 1/(2a)$. Each solid bell-shaped curve in the left plot is the ensemble of such origins, defined as the point where, decreasing $a$, another non trivial solution to the saddle point equations appears. Each curve from right to left is indexed by a different value of $l_{max} = 10, 30, 100, 200, 1000, 2000, 10000$. Each point on the curve corresponds to a particular value of $s$ (the dot is for $s = 2.2$ and $l_{max} = 200$ as in fig. 5.6). Along the curve $s$ increases for decreasing $\gamma$ (see right plot). From each point of the curve originate the two first order critical lines shown for $s = 2.2$ and $l_{max} = 200$ in fig. 5.6, and pictorially drawn for different $s$ values in the right plot. When the origin joins the second order hyperbole the system is at a tricritical point. $s_{tricritical}$ scales very rapidly with $l_{max}$ converging to $\sim 2.73 - 2.74$ already for $l_{max} \sim 100$.

the condition $\partial G(m)/\partial m|_{m=0} = 0$, the system undergoes a continuous transition in the order parameter $m$, representing the fraction of variables taking the same value in all the solutions. The problem of finding solutions is always easy, as for the case $\{a = 1; v_{k\neq 2} = 0\}$. Decreasing $a$ we meet a first intermediate region **II**, where the birth of a meta-stable non-trivial saddle-point solution at $\gamma = \gamma_d(a)$ is given by the solution of eq. (5.10). However, algorithms should not be much affected by this meta-stable state, because the system starts magnetizing continuously before, crossing the bold line. Increasing $\gamma$ up to the critical value $\gamma_c(a)$ one meets a first order transition, where the magnetization, that was already non-zero, undergoes a further jump. The second central region **III** shows an inversion between $\gamma_d(a)$ and the bold line $1/(2a)$. These two intermediate regions have not been exhaustively studied yet, because real data all fall in the leftmost one. The shape of the central part of the phase diagram is very sensitive to the choice of the control parameters $s$ and $k_{max}$, as shown in fig. (5.7). The $\gamma_c(a)$ curve in the second and third regions is found solving

$$S(m^*, \gamma_c) = S(m_*, \gamma_c) \quad , \tag{5.25}$$

where $m_*$ is the smallest positive solution to $G(m) = 0$, which corresponds to the magnetization of the ferromagnetic state arisen from the second order transition (bold line). The points of crossing showing the onset of different regions, from right to left, are found respectively as: $\frac{\partial G(m)}{\partial m} = 0$ & $S(m^*, \gamma) = S(m_*, \gamma)$, $\frac{\partial G(m)}{\partial m} = 0$ & $\gamma = \frac{1}{2a}$ and $S(m^*, \gamma) = S(0, \gamma)$ & $\gamma = \frac{1}{2a}$. The leftmost part **IV** shows the typical behavior described in [19]. Increasing $\gamma$ the system never reaches the continuous transition on the bold line, but it undergoes a first dynamical transition at $\gamma_d(a)$ and second thermodynamical one at $\gamma_c(a)$, found via eq. (5.25) with $m_* = 0$ since we are still below the second order transition line. Configurational entropy is non-zero between $\gamma_d(a)$ and $\gamma_c(a)$, and solving algorithms are affected by it. There are typically other spinodal lines in the phase diagram, but they always correspond to sub-optimal solutions, and were, therefore, not shown in the picture. The corresponding behavior of the magnetization in regions **I**, **II**, **III** and **IV** as well as at the boundaries are shown in fig.( 5.8). There, the lower curve represents the continuous phase transitions typical of loops percolation in rank 2 graphs. Indeed, if the fraction $v_2$ is high enough, all the previous cluster separation and orthogonality arguments do not hold, because in region **II**, prior to clustering, the rank 2 sub-graph one big enough to form an extensive connected component where usual percolation is attained. In region **III** clustering appears before, but that the rank 2 subgraph percolates for a value of $\gamma$ where the complexity of metastable states is still extensive. Therefore, In region **II** the dynamical phese transition is shielded by the continuos one, while in **III** a first dynamical transition is present, but the static one is again due to simple 2 loops percolation phenomenon. In real data the fraction of 2-variables equations is typically of the order of 0.2 and $\gamma \simeq 1$. So we always work deep into phase **IV** where, during the solving procedure, the system undergoes a first dynamical transition, that corresponds to a slowing down of the solving algorithms, before finding solutions. Notice that whenever the first physical static transition is the continuous one, the value of the complexity drops to zero. The typical curves for the complexity of the highest energy density metastable states as a function of $\gamma$ is exemplified if fig. (5.9) for regions **III** and **IV**. For the particular form of the $v(x)$ studied in this section and for the limit $l_{max} \to \infty$, it is easy to see that condition (2.218) reads:

$$v_2 = \frac{3^{1-s}}{\zeta(s) - 2^{-s} - 1 + 3^{1-s}} \tag{5.26}$$

The full phase diagram of the model studied in this section can be also retrieved in two different ways: The first one [26] uses the leaf removal equation for the general $p$-spin model introduced

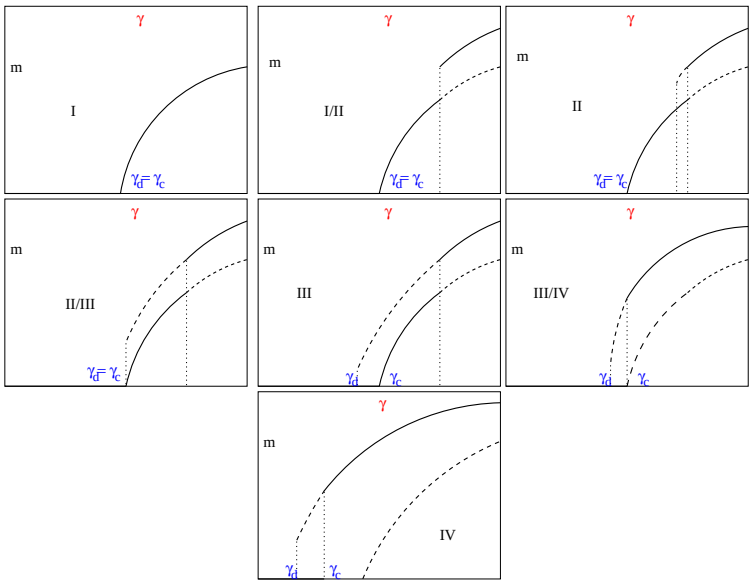



Figure 5.8: magnetization in typical regions of phase diagram 5.6. The lower curves represent the continuous transition due to two loops percolation in the rank 2 sub-graph.

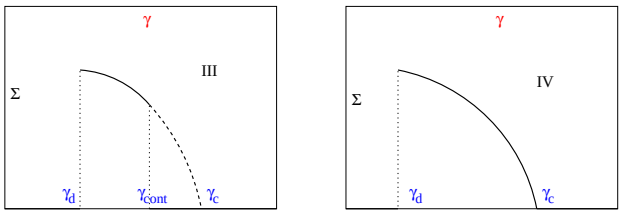



Figure 5.9: Complexity of GGS in regions **III** and **IV**.

in the first chapter. Specializing the form of the generating function $v(x)$ to the present case we immediately find the equivalence between eq.(2.203) and the self consistent condition (5.7) for the magnetization of the ferromagnetic model, as it was already noted in chapter 1. The instability condition for $\gamma$ analogously follows from eq.(2.204). Moreover, it can be shown that condition (2.217) is equivalent to the vanishing ferromagnetic complexity threshold used in this section. The same is obviously true for the continuous threshold $\hat{\gamma}$ and for $\gamma_{tricritical}$, when present. The second alternative way to solve this model with statistical physics tools is the general 1RSB-like solution via the cavity method at $T = 0$. Its general strategy was presented in [23] and [24], applied to the particular case of the $p$-spin model on uniform rank Poissonian degree hyper-graphs in [26] and straightforwardly extended in the multiple rank case in chapter 1. The method has been shown to be equivalent to the replica method on average samples. Although it is not proven to be exact yet, it can be proven along the same lines of the calculations presented in chapter 5 to give rigorous upper bounds to the thresholds. Since these values coincide with the exact ones found via the generalized leaf-removal method, and since the clustering property of the $p$-spin in the dynamical region implies the physical exactness of a 1RSB picture without further symmetry breaking phenomena, we are very confident in the results.

Overall, we have analyzed the behavior of different type of polynomial algorithms in the solutions of large-scale linear systems over finite fields. The connection between memory requirements and clustering phase transitions as been made clear on both artificially generated problem as well as on a "real-world" applications. While the role of the dynamical glass transition in local search algorithm was already well known (trapping in local minima), we have provided a clear example of the role of such type of glass transition in global dynamical processes which are guaranteed to converge to the global optimum in some polynomial time. The memory catastrophe found is such cases constitutes a concrete limitation for the performance of single-machine programs.

## 5.2 The dynamic phase transition for decoding algorithms

The content of this section is the output of a collaboration with Andrea Montanari, Silvio Franz and Federico Ricci-Tersenghi [127].

### 5.2.1 Introduction

Recently there has been some interest in studying "complexity phase transitions", i.e. abrupt changes in the computational complexity of hard combinatorial problems as some control parameter is varied [128]. These phenomena are thought to be somehow related to the physics of glassy systems, where the physical dynamics experiences a dramatic slowing down as the temperature is lowered [129].

Complexity is a central issue also in coding theory [130, 131]. Coding theory [132, 134, 133] deals with the problem of communicating information reliably through an unreliable channel of communication. This task is accomplished by making use of *error correcting codes*. In 1948 Shannon [135] proved that almost any error correcting code allows to communicate without errors, as long as the rate of transmitted information is kept below the *capacity* of the channel. However decoding is an intractable problem for almost any code. Coding theory is therefore a rich source of interesting computational problems.

On the other hand it is known that error correcting codes can be mapped onto disordered spin models [38, 136, 137, 138, 139]. Remarkably there has recently been a revolution in coding theory which has brought to the invention of new and very powerful codes based on random constructions: turbo codes [140], low density parity check codes (LDPCC) [141, 142], repetition accumulated codes [143], etc. As a matter of fact the equivalent spin models have been intensively studied in the last few years. These are diluted spin glasses, i.e. spin glasses on random hyper-graphs [12, 23, 22, 20].

The new codes are decoded by using approximate iterative algorithms, which are closely related to the TAP-cavity approach to mean field spin glasses [144, 145]. We think therefore that a close investigation of these systems from a statistical physics point of view, having in mind complexity (i.e. dynamical) issues, can be of great theoretical interest[6].

Let us briefly recall the general setting of coding theory [132] in order to fix a few notations (cf. fig. 5.10 for a pictorial description). A source of information produces a stream of symbols.

[6]The reader is invited to consult Refs. [146, 147, 148, 149, 150, 151, 152, 153, 154, 155] for a statistical mechanics analysis of the optimal decoding (i.e. of static issues).

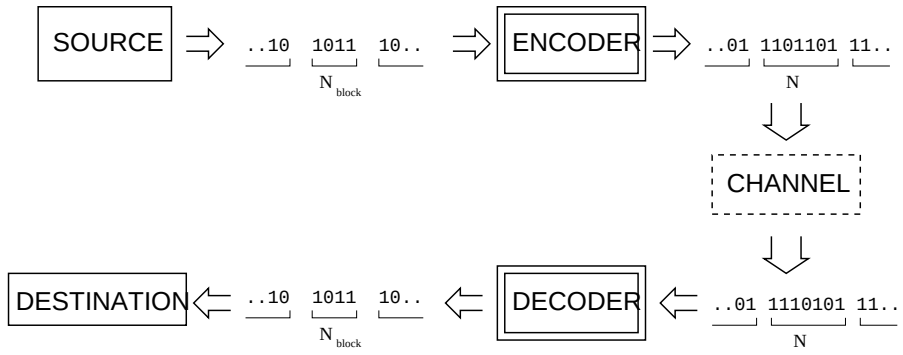



Figure 5.10: A schematic description of how error correcting codes work.

Let us assume, for instance, that the source produces unbiased random bits. The stream is partitioned into *blocks* of length $N_{\rm block}$. Each of the possible $2^{N_{\rm block}}$ blocks is mapped to a *codeword* (i.e. a sequence of bits) of length $N > N_{\rm block}$ by the *encoder* and transmitted through the channel. An error correcting code is therefore defined either as a mapping $\{0,1\}^{N_{\rm block}} \to \{0,1\}^N$, or as a list of $2^{N_{\rm block}}$ codewords. The *rate* of the code is defined as $R = N_{\rm block}/N$.

Let us denote[7] the transmitted codeword by $\underline{\mathtt{x}}^{\rm in} = [\mathtt{x}_1^{\rm in}, \dots, \mathtt{x}_N^{\rm in}]^{\intercal}$. Due to the noise, a different sequence of symbols $\underline{\mathtt{x}}^{\rm out} = [\mathtt{x}_1^{\rm out}, \dots, \mathtt{x}_N^{\rm out}]^{\intercal}$ is received. The decoding problem is to infer $\underline{\mathtt{x}}^{\rm in}$ given $\underline{\mathtt{x}}^{\rm out}$, the definition of the code, and the properties of the noisy channel.

It is useful to summarize the general picture which emerges from our work. We shall focus on Gallager codes (both *regular* and *irregular*). The optimal decoding strategy (maximum-likelihood decoding) is able to recover the transmitted message below some noise threshold: $p < p_c$. Iterative, linear time, algorithms get stuck (in general) at a lower noise level, and are successful only for $p < p_d$(alg.), with $p_d$(alg.) $\le p_c$. In general the "dynamical" threshold $p_d$(alg.) depends upon the details of the algorithm. However, it seems to be always smaller than some universal (although code-dependent) value $p_d$. Moreover, some "optimal" linear-time algorithms are successful up to $p_d$ (i.e. $p_d$(alg.) $= p_d$). The universal threshold $p_d$ coincides with the dynamical transition [129] of the corresponding spin model.

The plan of the section is the following. In Subsection 5.2.2 we introduce low density parity check codes (LDPCC), focusing on Gallager's *ensembles*, and we describe *message passing* decoding algorithms. We briefly recall the connection between this algorithms and the TAP-cavity equations for mean-field spin glasses. In Subsec. 5.2.3 we define a spin model which describes the decoding problem, and introduce the replica formalism. In Subsec. 5.2.4 we analyze this model for a particular choice of the noisy channel (the *binary erasure channel*). In this case calculations can be fully explicit and the results are particularly clear. Then, in Subsec. 5.2.5, we address the general case. The Appendices of [127] collect some details of our computations that we have not included here not to overload this thesis[8].

### 5.2.2 Error correcting codes, decoding algorithms and the cavity equations

This Subsection introduces the reader to some basic terminology in coding theory. In the first part we define some *ensembles* of codes, namely *regular* and *irregular* LDPCC. In the second one we describe a class of iterative decoding algorithms. These algorithms have a very clear physical interpretation, which we briefly recall. Finally we explain how these algorithms are analyzed in the coding theory community. This Section does not contain any original result. The interested reader may consult Refs. [156, 141, 134, 145] for further details.

[7] We shall denote transmitted and received symbols by typographic characters, with the exception of symbols in $\{+1,-1\}$. In this case use the physicists notation and denote such symbols by $\sigma$. When considering binary symbols we will often pass from the $\mathtt{x}$ notation to the $\sigma$ notation, the correspondence $\sigma = (-1)^{\mathtt{x}}$ being understood. Finally vectors of length $N$ will be always denoted by underlined characters: e.g. $\underline{\mathtt{x}}$ or $\underline{\sigma}$.

[8] The reader should notice that in [127] the notations for the hyper-graph rank and degree probability distribution and generating funtions are reversed.

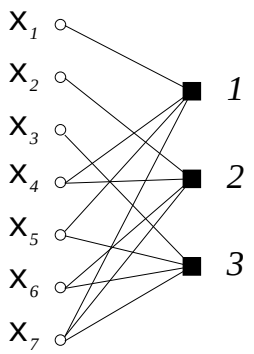



Figure 5.11: The Tanner graph for the $\mathcal{H}_2(3)$ Hamming code.

**Encoding** ...

Low density parity check codes are defined by assigning a binary $N \times M$ matrix $\hat{H} = \{H_{ij}\}$, with $H_{ij} \in \{0, 1\}$. All the codewords are required to satisfy the constraint

$$\hat{H}\,\underline{\mathtt{x}} = 0 \pmod 2 \,. \tag{5.27}$$

The matrix $\hat{H}$ is called the *parity check matrix* and the $M$ equations summarized in eq. (5.27) are the *parity check equations* (or, for short, *parity checks*). If the matrix $\hat{H}$ has rank $M$ (this is usually the case), the rate is $R = 1 - M/N$.

There exists a nice graphic representation of eq. (5.27) which is often used in the coding theory community: the *Tanner graph* representation [64, 65]. One constructs a bipartite graph by associating a left-hand node to each one of the $N$ variables, and a right-hand node to each one of the $M$ parity checks. An edge is drawn between the *variable node* $i$ and the *parity check node* $\alpha$ if and only if the variable $\mathtt{x}_i$ appears with a non-zero coefficient in the parity check equation $\alpha$.

Let us for instance consider the celebrated $\mathcal{H}_2(3)$ Hamming code (one of the first examples in any book on coding theory). In this case we have $N = 7$, $M = 3$ and

$$\hat{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} . \tag{5.28}$$

This code has $2^4 = 16$ codewords $\underline{\mathtt{x}}^{(\alpha)} = [\mathtt{x}_1^{(\alpha)}, \ldots, \mathtt{x}_7^{(\alpha)}]^{\mathtt{T}}$, with $\alpha \in \{1, \ldots, 16\}$. They are the solutions of the three parity check equations: $\mathtt{x}_1 + \mathtt{x}_4 + \mathtt{x}_5 + \mathtt{x}_7 = 0$; $\mathtt{x}_2 + \mathtt{x}_4 + \mathtt{x}_6 + \mathtt{x}_7 = 0$; $\mathtt{x}_3 + \mathtt{x}_5 + \mathtt{x}_6 + \mathtt{x}_7 = 0$ (mod2). The corresponding Tanner graph is drawn in fig. 5.11.

In general one considers *ensembles* of codes, by defining a random construction of the parity check matrix. One of the simplest *ensembles* is given by *regular* $(k, l)$ *Gallager codes*. In this case one chooses the matrix $\hat{H}$ randomly among all the $N \times M$ matrices having $k$ non-zero entries per row, and $l$ per column. The Tanner graph is therefore a random bipartite graph with fixed degrees $k$ and $l$ respectively for the parity check nodes and for the variable nodes. Of course this is possible only if $M/N = l/k$.

Amazingly good codes [158, 159, 157] where obtained by slightly more sophisticated *irregular* constructions. In this case one assigns the distributions of the degrees of parity check nodes and variable nodes in the Tanner graph. Accordingly to the notations introduced in the first chapter, We shall denote by $\{v_l\}$ the degree distribution of the check nodes and $\{c_k\}$ the degree

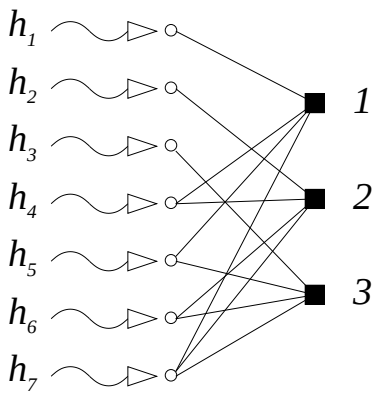



Figure 5.12: The information coming from the channel must be used for decoding the $\mathcal{H}_2(3)$ Hamming code: a pictorial view.

distribution of the variable nodes. This means that there are $Nc_k$ bits of the codeword belonging to $k$ parity checks and $Nv_l$ parity checks involving $l$ bits for each $k$ and $l$. In this case, we shall always assume $v_l = 0$ for $l < 3$ and $c_k = 0$ for $k < 2$ It is useful to redefine here the generating polynomials

$$c(x) \equiv \sum_{k=3}^{\infty} c_k x^k \,, \quad v(x) \equiv \sum_{l=2}^{\infty} v_l x^l \,, \tag{5.29}$$

which satisfy the normalization condition $c(1) = v(1) = 1$. Moreover we define the average check and variable degrees $< l > \equiv \overline{l} = v'(1)$ and $< k > \equiv \overline{k} = c'(1)$. Particular examples of this formalism are the regular codes, whose generating polynomials are $c(x) = x^k$, $v(x) = x^l$.

### ... and decoding

The codewords are transmitted trough a noisy channel. We assume antipodal signalling: one sends $\sigma^{\rm in} \in \{+1, -1\}$ signals instead of $\mathtt{x}^{\rm in} \in \{0, 1\}$ through the channel (the correspondence being given by $\sigma = (-1)^{\mathtt{x}}$). At the end of the channel, a corrupted version of this signals is received. This means that if $\sigma^{\rm in} \in \{+1, -1\}$ is transmitted, the value $\mathtt{x}^{\rm out}$ is received with probability density $Q(\mathtt{x}^{\rm out}|\sigma^{\rm in})$. The information conveyed by the received signal $\mathtt{x}^{\rm out}$ is conveniently described by the log-likelihood[9]:

$$h(\mathtt{x}^{\rm out}) = \frac{1}{2} \log \frac{Q(\mathtt{x}^{\rm out}|+1)}{Q(\mathtt{x}^{\rm out}|-1)} \,. \tag{5.30}$$

We can represent this information by wavy lines in the Tanner graph, cf. fig. 5.12.

The decoding problem is to compute the probability for each transmitted bit $\sigma_i^{\rm in}$ to take the value $\sigma_i$, given the structure of the code and the received message $\underline{\mathtt{x}}^{\rm out} = [\mathtt{x}_1^{\rm out}, \ldots, \mathtt{x}_N^{\rm out}]^{\mathtt{T}}$. This is in general an intractable problem [130, 131]. Recently there has been a great interest in dealing with this problem using approximate *message passing* algorithms.

Message passing algorithms are iterative: at each step $t$ one keeps track of $M\overline{k}$ messages from the variable nodes to the check nodes $\{y_{\alpha\to i}^{(t)}\}$ and vice-versa $\{x_{i\to\alpha}^{(t)}\}$. Messages can be

[9]Notice the unconventional normalization: the factor 1/2 is inserted to make contact with the statistical mechanics formulation.

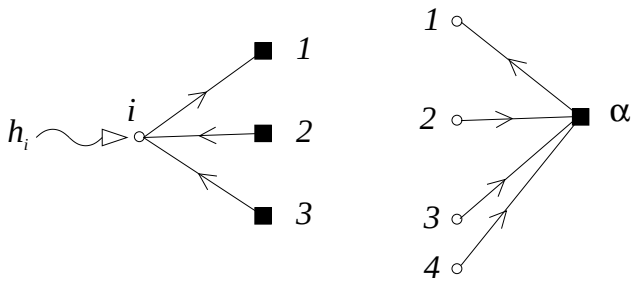



Figure 5.13: A graphic representation of the operations executed in a message passing algorithm. At the variable node $i$ (on the left): $x_{i\to 1}^{(t+1)} = F(y_{2\to i}^{(t)}, y_{3\to i}^{(t)}; h_i)$. At the check node $\alpha$ (on the right): $y_{\alpha\to 1}^{(t+1)} = G(x_{2\to\alpha}^{(t)}, x_{3\to\alpha}^{(t)}, x_{4\to\alpha}^{(t)})$.

thought to travel along the edges and computations to be executed at the nodes. A node computes the message to be sent along each one of the edges, using the messages received from the other (!) edges at the previous iteration (the variable nodes make also use of the log-likelihoods $h(\mathtt{x}_i^{\rm out})$), cf. fig. 5.13. At some point the iteration is stopped (there exists no general stopping criterion), and a choice for the bit $\sigma_i$ is taken using all the incoming messages (plus the log-likelihood $h(\mathtt{x}_i^{\rm out})$).

The functions which define the "new" messages in terms of the "old" ones, can be chosen to optimize the decoder performances. A particularly interesting family is the following:

$$x_{i\to\alpha}^{(t+1)} = h_i + \sum_{\alpha'\ni i:\, \alpha'\neq\alpha} y_{\alpha'\to i}^{(t)} \tag{5.31}$$

$$y_{\alpha\to i}^{(t+1)} = \frac{1}{\zeta}\,\mathrm{arctanh}\left[\prod_{j\in\alpha:\, j\neq i} \tanh\zeta\, x_{j\to\alpha}^{(t)}\right], \tag{5.32}$$

where we used the notation $i\in\alpha$ whenever the bit $i$ belongs to the parity check $\alpha$. The messages $\{x_{i\to\alpha}^{(\cdot)}\}$ and $\{y_{\alpha\to i}^{(\cdot)}\}$ can be rescaled in such a way to eliminate the parameter $\zeta$ everywhere except in front of $h_i$. Therefore $\zeta$ allows to tune the importance given to the information contained in the received message.

After the convergence of the above iteration one computes the *a posteriori* log-likelihoods as follows:

$$H_i = h_i + \sum_{\alpha\ni i} y_{\alpha\to i}^{(\infty)}\,. \tag{5.33}$$

The meaning of the $\{H_i\}$ is analogous to the one of the $\{h_i\}$ (but for the fact that the $H_i$ incorporate the information coming from the structure of the code): the best guess for the bit $i$ is $\sigma_i = +1$ or $\sigma_i = -1$ depending whether $H_i > 0$ or $H_i < 0$.

The most popular choice for the free parameter $\zeta$ is $\zeta = 1$: this algorithm has been invented separately by R. G. Gallager [141] in the coding theory context (and named the *sum-product* algorithm) and by D. Pearl [160] in the artificial intelligence context (and named the *belief propagation* algorithm). Also $\zeta = \infty$ is sometimes used (the *max-product* algorithm).

The alerted reader will notice that the eqs. (5.31)-(5.32) are nothing but the cavity equations at inverse temperature $\zeta$ for a properly constructed spin model. This remark is the object of Refs. [161, 144].

In the analysis of the above algorithm it is convenient to assume that $\sigma_i^{\rm in} = +1$ for $i = 1,\ldots,N$. This assumption can be made without loss of generality if the channel is symmetric

(i.e. if $Q(\mathtt{x}|+1) = Q(-\mathtt{x}|-1)$). With this assumption the $h_i$ are i.i.d. random variables with density

$$p(h) \equiv Q(\mathtt{x}(h)|+1)|\mathtt{x}'(h)|\,, \tag{5.34}$$

where $\mathtt{x}(h)$ is the function which inverts eq. (5.30). In the following we shall consider two particular examples of noisy channels, the generalization being straightforward:

- The binary erasure channel (BEC). In this case a bit can either be received correctly or erased[10]. There are therefore three possible outputs: $\{+1,-1,0\}$. The transition probability is:

$$Q(\mathtt{x}^{\rm out}|+1) = \begin{cases} (1-p) & \text{if } \mathtt{x}^{\rm out} = +1\,, \\ p & \text{if } \mathtt{x}^{\rm out} = 0\,, \\ 0 & \text{if } \mathtt{x}^{\rm out} = -1\,, \end{cases} \qquad Q(\mathtt{x}^{\rm out}|-1) = \begin{cases} 0 & \text{if } \mathtt{x}^{\rm out} = +1\,, \\ p & \text{if } \mathtt{x}^{\rm out} = 0\,, \\ (1-p) & \text{if } \mathtt{x}^{\rm out} = -1\,. \end{cases} \tag{5.35}$$

  We get therefore the following distribution for the log-likelihoods: $p(h) = (1-p)\,\delta_\infty(h) + p\,\delta(h)$ (where $\delta_\infty$ is a Dirac delta function centered at $+\infty$). Let us recall that the capacity of the BEC is given by $C_{BEC} = 1-p$: this means that a rate-$R$ code cannot assure error correction if $p > 1-R$.

- The binary symmetric channel (BSC). The channel flips each bit independently with probability $p$. Namely

$$Q(\mathtt{x}^{\rm out}|+1) = \begin{cases} (1-p) & \text{if } \mathtt{x}^{\rm out} = +1\,, \\ p & \text{if } \mathtt{x}^{\rm out} = -1\,, \end{cases} \qquad Q(\mathtt{x}^{\rm out}|-1) = \begin{cases} p & \text{if } \mathtt{x}^{\rm out} = +1\,, \\ (1-p) & \text{if } \mathtt{x}^{\rm out} = -1\,. \end{cases} \tag{5.36}$$

  The corresponding log-likelihood distribution is $p(h) = (1-p)\,\delta(h-h_0) + p\,\delta(h+h_0)$, with $h_0 = \operatorname{arctanh}(1-2p)$. The capacity of the BSC is[11] $C_{BSC} = 1-\mathtt{h}(p)$: a rate-$R$ code cannot correct errors if $p > \delta_{GV}(R)$.

It is quite easy [162, 156] to write a recursive equations for the probability distributions of the messages $\pi_t(x)$ and $\widehat{\pi}_t(y)$:

$$\pi_{t+1}(x) = \frac{1}{\overline{k}} \sum_{k=2}^{\infty} c_k k \int \prod_{i=1}^{k-1} dy_i\, \widehat{\pi}_t(y_i) \int dh\, p(h)\, \delta\left(x - h - \sum_{i=1}^{k-1} y_i\right)\,, \tag{5.37}$$

$$\widehat{\pi}_{t+1}(y) = \frac{1}{\overline{l}} \sum_{l=3}^{\infty} v_l l \int \prod_{i=1}^{l-1} dx_i\, \pi_t(x_i)\, \delta\left(y - \frac{1}{\zeta} \operatorname{arctanh}\left[\prod_{i=1}^{l-1} \tanh \zeta x_i\right]\right)\,. \tag{5.38}$$

These equations (usually called the *density evolution* equations) are correct for times $t \ll \log N$ due to the fact that the Tanner graph is locally tree-like. They allow therefore to predict whether, for a given *ensemble* of codes and noise level (recall that the noise level is hidden in $p(h)$) the algorithm is able to recover the transmitted codeword (for large $N$). If this is the case, the distributions $\pi_t(x)$ and $\widehat{\pi}_t(y)$ will concentrate on $x = y = +\infty$ as $t \to \infty$. In the opposite case the above iteration will converge to some distribution supported on finite values of $x$ and $y$. In Tab. 5.1 we report the threshold noise levels for several regular codes, obtained using the

[10] This is what happens, for instance, to packets in the Internet traffic.

[11] We denote by $\mathtt{h}(p)$ the binary entropy function $\mathtt{h}(p) = -p\log_2 p - (1-p)\log_2(1-p)$. It is useful to define its inverse: we denote by $\delta_{GV}(R)$ (the so-called Gilbert-Varshamov distance) the smallest solution of $\mathtt{h}(\delta) = 1-R$.

| | BEC | | BSC | | | |
|---|---|---|---|---|---|---|
| $(l,k)$ | $p_c$ | $p_d$ | $p_c$ | $p_d(\zeta=1)$ | $p_d(\zeta=2)$ | $p_d(\zeta=\infty)$ |
| $(6,3)$ | 0.4882 | 0.4294 | 0.100 | 0.084 | 0.078 | 0.072 |
| $(10,5)$ | 0.4995 | 0.3416 | 0.109 | 0.070 | 0.056 | 0.046 |
| $(14,7)$ | 0.5000 | 0.2798 | 0.109 | 0.056 | 0.039 | 0.029 |
| $(6,5)$ | 0.8333 | 0.5510 | 0.264 | 0.139 | 0.102 | 0.078 |

Table 5.1: The static and dynamical points for several regular codes and decoding algorithms, cf. eqs. (5.31), (5.32).

density evolution method, together with the thresholds for the optimal decoding strategy, see Ref. [154].

Finally let us notice that the fixed point of the iteration (5.37)-(5.38) is the replica symmetric order parameter for the equivalent spin model.

### 5.2.3 Statistical mechanics formulation and the replica approach

We want to define a statistical mechanics model which describes the decoding problem. The probability distribution for the input codeword to be $\underline{\sigma} = (\sigma_1, \ldots, \sigma_N)$ conditional to the received message, takes the form

$$P(\underline{\sigma}) = \frac{1}{Z}\delta_{\hat{H}}[\underline{\sigma}] \, \exp\left\{\sum_{i=1}^{N} h_i \sigma_i\right\} , \tag{5.39}$$

where $\delta_{\hat{H}}[\underline{\sigma}] = 1$ if $\underline{\sigma}$ satisfies the parity checks encoded by the matrix $\hat{H}$, cf. eq. (5.27), and $\delta_{\hat{H}}[\underline{\sigma}] = 0$ otherwise. Since we assume the input codeword to be $\underline{\sigma}^{\rm in} = (+1, +1, \ldots, +1)$, the $h_i$ are i.i.d. with distribution $p(h)$.

We modify the probability distribution (5.39) in two ways:

1. We multiply the fields $h_i$ by a weight $\hat{\zeta}$. This allows us to tune the importance of the received message, analogously to eqs. (5.31) and (5.32). This modification was already considered in Ref. [154]. Particularly important cases are $\hat{\zeta} = 1$ and $\hat{\zeta} = 0$.

2. We relax the constraints implied by the characteristic function $\delta_{\hat{H}}[\underline{\sigma}]$. More precisely, let us denote each parity check by the un-ordered set of bits positions $(i_1, \ldots, i_k)$ which appears in it. For instance the three parity checks in the Hamming code $\mathcal{H}_2(3)$, cf. eq. (5.28), are $(1,4,5,7)$, $(2,4,6,7)$, $(3,5,6,7)$. Moreover let $\Omega_k$ be the set of all parity checks involving $k$ bits (in the irregular *ensemble* the size of $\Omega_k$ is $Nc_k$). We can write explicitly the characteristic function $\delta_{\hat{H}}[\underline{\sigma}]$ as follows:

$$\delta_{\hat{H}}[\underline{\sigma}] = \prod_{l=3}^{\infty} \prod_{(i_1 \ldots i_l) \in \Omega_l} \delta(\sigma_{i_1} \cdots \sigma_{i_l}, +1) , \tag{5.40}$$

   where $\delta(\cdot,\cdot)$ is the Kronecker delta function. Now it is very simple to relax the constraints by making the substitution $\delta(\sigma_{i_1} \cdots \sigma_{i_l}, +1) \to \exp\{\beta[\sigma_{i_1} \cdots \sigma_{i_l} - 1]\}$.

Summarizing the above considerations, we shall consider the statistical mechanics model defined by the Hamiltonian

$$H(\sigma) = -\sum_{l=3}^{\infty} \sum_{(i_1 \ldots i_l) \in \Omega_l} (\sigma_{i_1} \cdots \sigma_{i_l} - 1) \quad - \frac{\hat{\zeta}}{\beta} \sum_{i=1}^{N} h_i \sigma_i , \tag{5.41}$$

at inverse temperature $\beta$.

We address this problem by the replica approach [163] The replicated partition function reads

$$\langle Z^n \rangle \sim \int \prod_{\vec{\sigma}} d\lambda(\vec{\sigma}) d\widehat{\lambda}(\vec{\sigma})\, e^{-NS[\lambda,\widehat{\lambda}]}\,, \tag{5.42}$$

with the action

$$\begin{aligned} S[\lambda,\widehat{\lambda}] \;=\; & \overline{k} \sum_{\vec{\sigma}} \lambda(\vec{\sigma})\widehat{\lambda}(\vec{\sigma}) - \frac{\overline{k}}{\overline{l}} \sum_{l=3}^{\infty} v_l \sum_{\vec{\sigma}_1 \dots \vec{\sigma}_l} J_\beta(\vec{\sigma}_1,\dots,\vec{\sigma}_l)\lambda(\vec{\sigma}_1)\cdots\lambda(\vec{\sigma}_l) - \\ & - \sum_{k=2}^{\infty} c_k \log\left[\sum_{\vec{\sigma}} \widehat{\lambda}(\vec{\sigma})^k \mathcal{H}(\vec{\sigma})\right] - \overline{k} + \frac{\overline{k}}{\overline{l}}\,, \end{aligned} \tag{5.43}$$

where

$$J_\beta(\vec{\sigma}_1,\dots,\vec{\sigma}_k) \equiv e^{\beta \sum_a (\sigma_1 \dots \sigma_k - 1)}\,, \qquad \mathcal{H}(\vec{\sigma}) = \langle e^{\hat{\zeta} h \sum_a \sigma_a} \rangle_h\,, \tag{5.44}$$

$\langle\cdot\rangle_h$ being the average over $p(h)$. The order parameters $\lambda(\vec{\sigma})$ and $\widehat{\lambda}(\vec{\sigma})$ are closely related, at least in the replica symmetric approximation, to the distribution of messages in the decoding algorithm [154], cf. eqs. (5.37), (5.38).

In the case of the BEC an irrelevant infinite constant must be subtracted from the action (5.43) in order to get finite results. This corresponds to taking

$$\mathcal{H}_{BEC}(\vec{\sigma}) \equiv p + (1-p)\delta_{\vec{\sigma},\vec{\sigma}_0}\,, \tag{5.45}$$

where $\vec{\sigma}_0 = (+1,\dots,+1)$.

### 5.2.4 Binary erasure channel: analytical and numerical results

The binary erasure channel is simpler than the general case. Intuitively this happens because one cannot receive misleading indications concerning a bit. Nonetheless it is an important case both from the practical [164] and from the theoretical point of view [165, 156, 158].

#### The decoding algorithm

Iterative decoding algorithms for irregular codes were first introduced and analyzed within this context [158]. Belief propagation becomes particularly simple. Since the knowledge about a received bit is completely sure, the log-likelihoods $\{h_i\}$, cf. eq. (5.30), take the values $h_i = +\infty$ (when the bit has been received[12]) or $h_i = 0$ (when it has been erased). Analogously the messages $\{x^{(t)}_{i\to\alpha}\}$ and $\{y^{(t)}_{\alpha\to i}\}$ must assume the same two values. The rules (5.31), (5.32) become

$$x^{(t+1)}_{i\to\alpha} \;=\; \begin{cases} +\infty & \text{if either } h_i = +\infty \text{ or } y^{(t)}_{\alpha'\to i} = +\infty \text{ for some } \alpha' \ni i \text{ (with } \alpha' \neq \alpha), \\ 0 & \text{otherwise,} \end{cases} \tag{5.46}$$

$$y^{(t+1)}_{\alpha\to i} \;=\; \begin{cases} +\infty & \text{if } x^{(t)}_{j\to\alpha} = +\infty \text{ for all the } j \in \alpha \text{ (with } j \neq i), \\ 0 & \text{otherwise.} \end{cases} \tag{5.47}$$

[12] Recall that we are assuming the channel input to be $\sigma^{\rm in}_i = +1$ for $i = 1,\dots,N$.

There exists an alternative formulation [158] of the same algorithm. Consider the system of $M$ linear equations (5.27) and eliminate from each equation the received variables (which are known for sure to be 0). You will obtain a new linear system. In some cases you may have eliminated all the variables of one equation, the equation is satisfied and can therefore be eliminated. For some of the other equations you may have eliminated all the variables but one. The remaining variable can be unambiguously fixed using this equation (since the received message is not misleading, this choice is surely correct). This allows to eliminate the variable from the entire linear system. This simple procedure is repeated until either all the variables have been fixed, or one gets stuck on a linear system such that all the remaining equations involve at least two variables (this is called a *stopping set* [165]).

Let us for instance consider the linear system defined by the parity check matrix (5.28). Suppose, in a first case, that the received message was $(0, *, 0, *, 0, *, 0)$ (meaning that the bits of positions 2, 4, 6 were erased). The decoding algorithm proceeds as follows:

$$\left\{\begin{array}{rcl} \mathtt{x}_1+\mathtt{x}_4+\mathtt{x}_5+\mathtt{x}_7 &=& 0 \\ \mathtt{x}_2+\mathtt{x}_4+\mathtt{x}_6+\mathtt{x}_7 &=& 0 \\ \mathtt{x}_3+\mathtt{x}_5+\mathtt{x}_6+\mathtt{x}_7 &=& 0 \end{array}\right. \Rightarrow \left\{\begin{array}{rcl} \mathtt{x}_4 &=& 0 \\ \mathtt{x}_2+\mathtt{x}_4+\mathtt{x}_6 &=& 0 \\ \mathtt{x}_6 &=& 0 \end{array}\right. \Rightarrow \left\{\begin{array}{rcl} 0 &=& 0 \\ \mathtt{x}_2 &=& 0 \\ 0 &=& 0 \end{array}\right. . \tag{5.48}$$

In this case the algorithm succeeded in solving the decoding problem. Let us now see what happens if the received message is $(*, 0, *, 0, *, 0, *)$:

$$\left\{\begin{array}{rcl} \mathtt{x}_1+\mathtt{x}_4+\mathtt{x}_5+\mathtt{x}_7 &=& 0 \\ \mathtt{x}_2+\mathtt{x}_4+\mathtt{x}_6+\mathtt{x}_7 &=& 0 \\ \mathtt{x}_3+\mathtt{x}_5+\mathtt{x}_6+\mathtt{x}_7 &=& 0 \end{array}\right. \Rightarrow \left\{\begin{array}{rcl} \mathtt{x}_1+\mathtt{x}_5+\mathtt{x}_7 &=& 0 \\ \mathtt{x}_7 &=& 0 \\ \mathtt{x}_3+\mathtt{x}_5+\mathtt{x}_7 &=& 0 \end{array}\right. \Rightarrow \left\{\begin{array}{rcl} \mathtt{x}_1+\mathtt{x}_5 &=& 0 \\ 0 &=& 0 \\ \mathtt{x}_3+\mathtt{x}_5 &=& 0 \end{array}\right. . \tag{5.49}$$

The algorithm found a stopping set. Notice that the resulting linear system may well have a unique solution (although this is not the case in our example), which can be found by means of simple polynomial algorithms [166]. Simply the iterative algorithm is unable to further reduce it.

The analysis of this algorithm [156] uses the density evolution equations (5.37), (5.38) and is greatly simplified because the messages $\{x_{i\to\alpha}^{(t)}\}$ and $\{y_{\alpha\to i}^{(t)}\}$ take only two values. Their distributions have the form:

$$\pi_t(x) = \rho_t\,\delta(x) + (1-\rho_t)\,\delta_\infty(x) \quad , \widehat{\pi}_t(x) = \hat{\rho}_t\,\delta(y) + (1-\hat{\rho}_t)\,\delta_\infty(y)\,, \tag{5.50}$$

where $\delta_\infty(\cdot)$ is a delta function centered at $+\infty$. The parameters $\rho$ and $\hat{\rho}$ give the fraction of zero messages, respectively from variables to checks and from checks to variables. Using eqs. (5.37) and (5.38), we get:

$$\rho_{t+1} = p\,\frac{c'(\hat{\rho}_t)}{c'(1)}\ , \qquad \hat{\rho}_{t+1} = 1 - \frac{v'(1-\rho_t)}{v'(1)}\,. \tag{5.51}$$

The initial condition $\rho_0 = \hat{\rho}_0 = 1$ converges to the perfect recovery fixed point $\rho = \hat{\rho} = 0$ if $p < p_d$. This corresponds to perfect decoding. For $p > p_d$ the algorithm gets stuck on a non-trivial linear system: $\rho_t \to \rho_*$, $\hat{\rho}_t \to \hat{\rho}_*$, with $0 < \rho_*, \hat{\rho}_* < 1$. The two regimes are illustrated in fig. 5.14.

### Static transition

In the spin model corresponding to the situation described above, we have two types of spins: the ones corresponding to correctly received bits, which are fixed by an infinite magnetic field $h_i = +\infty$; and the ones corresponding to erased bits, on which no magnetic field acts: $h_i = 0$.

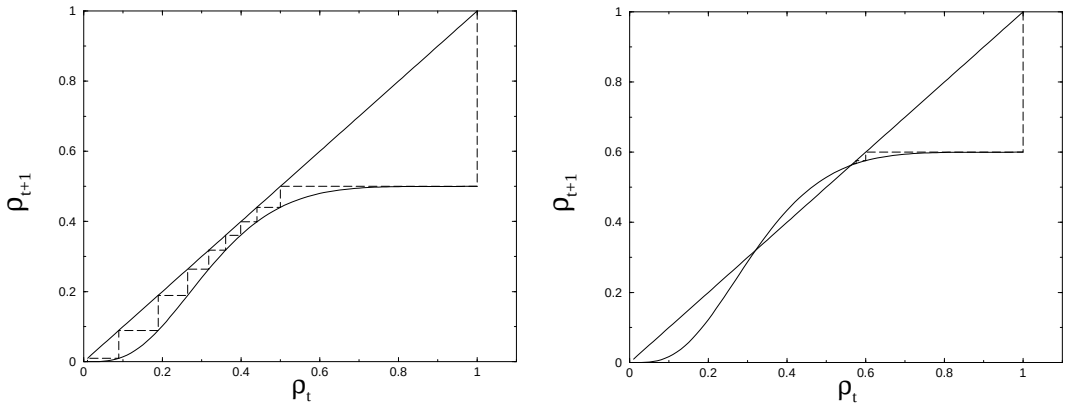



Figure 5.14: The evolution of the iterative decoding algorithm on the BEC, cf. eqs. (5.51). Here we consider the $(6,5)$ code: $\rho_{t+1} = p[1-(1-\rho_t)^5]^4$. On the left $p = 0.5 < p_d$, on the right $p = 0.6 > p_d$.

We can therefore consider an effective model for the erased bits once the received ones are fixed to $+1$. This correspond somehow to what is done by the decoding algorithm: the received bits are set to their values in the very first step of the algorithm and remain unchanged thereafter.

Let us consider the zero temperature limit. If the system is in equilibrium, its probability distribution will concentrate on zero energy configurations: the codewords. We will have typically $\mathcal{N}_{\rm words}(p) \sim 2^{N s_{\rm words}(p)}$ codewords compatible with the received message. Their entropy $s_{\rm words}(p)$ can be computed within the replica formalism as it was explicitly done in [127]. The result is

$$s_{\rm words}(\rho,\hat\rho;p) = \overline{k}\rho(1-\hat\rho) + \frac{\overline{k}}{\overline{l}}\,c(1-\rho) + p\,v(\hat\rho) - \frac{\overline{k}}{\overline{l}}\,, \tag{5.52}$$

which has to be maximized with respect to the order parameters $\rho$ and $\hat\rho$. The saddle point equations have exactly the same form as the fixed point equations corresponding to the dynamics (5.51), namely $\rho = pc'(\hat\rho)/c'(1)$ and $\hat\rho = 1 - v'(1-\rho)/v'(1)$

The saddle point equations have two stable solutions, i.e. local maxima of the entropy (5.52): $(i)$ a completely ordered solution $\rho = \hat\rho = 0$, with entropy $s_{\rm words}(0,0) = 0$ (in some cases this solution becomes locally unstable above some noise $p_{loc}$); $(ii)$ (for sufficiently high noise level) a paramagnetic solution $\rho_*, \hat\rho_* > 0$. The paramagnetic solution appears at the same value $p_d$ of the noise above which the decoding algorithm gets stuck.

The fixed point to which the dynamics (5.51) converges coincides with the statistical mechanics result for $\rho_*, \hat\rho_*$. However the entropy of the paramagnetic solution $s_{\rm words}(\rho_*,\hat\rho_*)$ is negative at $p_d$ and becomes positive only above a certain critical noise $p_c$. This means that the linear system produced by the algorithm continues to have a unique solution below $p_c$, although our linear time algorithm is unable find such a solution.

The "dynamical" critical noise $p_d$ is the solution of the following equation

$$p\frac{c''(\hat\rho_*)v''(1-\rho_*)}{v'(1)c'(1)} = -1\,, \tag{5.53}$$

where $\rho_*$ and $\hat\rho_*$ solve the saddle point equations. The static noise can be obtained setting

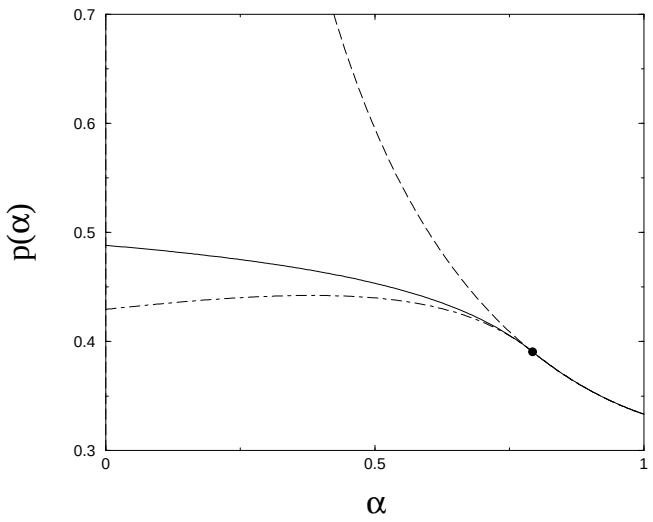



Figure 5.15: The phase diagram of the family of codes with generating polynomials $v(x) = \alpha x^4 + (1-\alpha)x^6$, $c(x) = \alpha x^2 + (1-\alpha)x^3$. The dashed line gives the local stability threshold for the completely ordered ferromagnetic phase. The continuous and dot-dashed lines refer (respectively) to the static and dynamic critical points $p_c(\alpha)$ and $p_d(\alpha)$.

$s_{\rm words}(\rho_*, \hat{\rho}_*) = 0$. Finally the completely ordered solution becomes locally unstable for

$$p_{loc} = \frac{c'(1)v'(1)}{c''(0)v''(1)}\,. \tag{5.54}$$

As an example let us consider the one-parameter family of $R = 1/2$ codes specified by the following generating polynomials: $v(x) = \alpha x^4 + (1-\alpha)x^6$, $c(x) = \alpha x^2 + (1-\alpha)x^3$. This is an irregular code which smoothly interpolates between the regular $(6,3)$ and $(4,2)$ codes. The local stability threshold is given by

$$p_{loc}(\alpha) = \frac{(3-\alpha)^2}{6\alpha(5-3\alpha)}\,. \tag{5.55}$$

The dynamical and critical curves $p_d(\alpha)$ and $p_c(\alpha)$ are reported in fig. 5.15. Notice that the $\alpha$ value where $p_d(\alpha)$ reaches its maximum, corresponding to the best code in this family, is neither 0 nor 1. This is a simple example showing that irregular codes ($0 < \alpha < 1$) are generally superior to regular ones ($\alpha = 0$ or $\alpha = 1$ in this example). Notice also that above the tricritical point $\alpha_t \approx 0.79301412$, $p_t \approx 0.39057724$ the three curves $p_{loc}(\alpha)$, $p_c(\alpha)$ and $p_d(\alpha)$ coincide. In the following we shall study in some detail the $\alpha = 0$ case, which corresponds to a regular $(6,3)$ code, the corresponding critical and dynamical points $p_c$ and $p_d$ are given in Tab. 5.1.

### Dynamical transition

The dynamical transition is not properly described within the replica symmetric treatment given above. Indeed, the paramagnetic solution cannot be considered, between $p_d$ and $p_c$, as a metastable state because it has negative entropy. One cannot therefore give a sensible interpretation of the coincidence between the critical noise for the decoding algorithm, and the appearance of the paramagnetic solution.

Before embarking in the one step replica symmetry-breaking (1RSB) calculation, let us review some important concepts on configurational complexuty [7, 167] already introduced and exploited in the second chapter. Let us call $m\phi(\beta, m)$ the free energy of $m$ weakly coupled "real" replicas times beta. This quantity can be computed in 1RSB calculation. In the limit $\beta \to \infty$, with $m\beta = y$ fixed, we have $m\phi(\beta, m) \to \mu\phi(y)$. The number of metastable states with a given energy density $\epsilon$ is

$$\mathcal{N}_{MS}(\epsilon) \sim e^{N\Sigma(\epsilon)} , \tag{5.56}$$

where the complexity $\Sigma(\epsilon)$ is the Legendre transform of the $m$ replicas free energy:

$$\Sigma(\epsilon) = \mu\epsilon - \mu\phi(y)|_{\epsilon=\partial[y\phi(y)]} . \tag{5.57}$$

The (zero temperature) dynamic energy $\epsilon_d$ and the static energy $\epsilon_s$ are[13], respectively, the maximum and the minimum energy such that $\Sigma(\epsilon) \geq 0$.

The static energy is obtained by solving the following equations:

$$\begin{cases} \epsilon_s = \phi(y) , \\ \partial\phi(y) = 0 , \end{cases} \tag{5.58}$$

which corresponds to the usual prescription of maximizing the free energy over the replica symmetry breaking parameter $m$ [163]. The dynamic energy is given by

$$\begin{cases} \epsilon_d = \partial[y\phi(y)] , \\ \partial^2[y\phi(y)] = 0 . \end{cases} \tag{5.59}$$

Finally, if $\epsilon_s = 0$ the complexity of the ground state is $\Sigma(0) = -\lim_{y\to\infty} y\phi(y)$.

At the time the calculation were done we weren't able to exactly compute the 1RSB free energy $\phi(y)$. After results of [24, 30, 26], exact 1RSB calculations could be redone. However excellent results can be obtained within an "almost factorized" variational Ansatz, cf. [127]. The picture which emerges is essentially not changed by the exact 1RSB solution , as we have checked numerically, and is the following:

- In the low noise region ($p < p_d$), no metastable states exist. Local search algorithms should therefore be able to recover the erased bits.

- In the intermediate noise region ($p_d < p < p_c$) an exponentially large number of metastable states appears. They have energy densities $\epsilon$ in the range $\epsilon_s < \epsilon < \epsilon_d$, with $\epsilon_s > 0$. Therefore the transmitted codeword is still the only one compatible with the received message. Nonetheless a large number of extremely stable *pseudo-codewords* stop local algorithms. The number of violated parity checks in these codewords cannot be reduced by means of local moves.

- Above $p_c$ we have $\epsilon_s = 0$: a fraction of the metastable states is made of codewords. Moreover $\Sigma(0)$ (which gives the number of such codewords) coincides with the paramagnetic entropy $s_{\text{words}}(\rho_*, \hat{\rho}_*)$ computed in the previous Section.

As an illustration, let us consider the $(6, 3)$ regular code. In fig. 5.16 we plot the resulting complexity curves $\Sigma(\epsilon)$ for three different values of the erasure probability $p$. In fig. 5.17, left

[13]Notice that one can give (at least) three possible definitions of the dynamic energy: $(i)$ from the solution of the non-equilibrium dynamics: $\epsilon_d^{(d)}$; $(ii)$ imposing the replicon eigenvalue to vanish: $\epsilon_d^{(r)}$; $(iii)$ using, as in the text, the complexity $\Sigma(\epsilon)$: $\epsilon_d^{(c)}$. The three results coincide in the $p$-spin spherical fully connected model, however their equality in the present case is, at most, a conjecture.

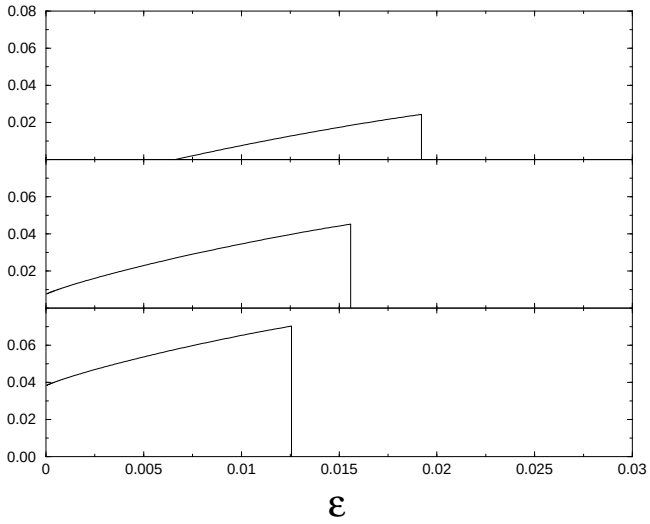



Figure 5.16: The complexity $\Sigma(\epsilon)$ for (from top to bottom) $p = 0.45$ (below $p_c$), $p = 0.5$, and $p = 0.55$ (above $p_c$).

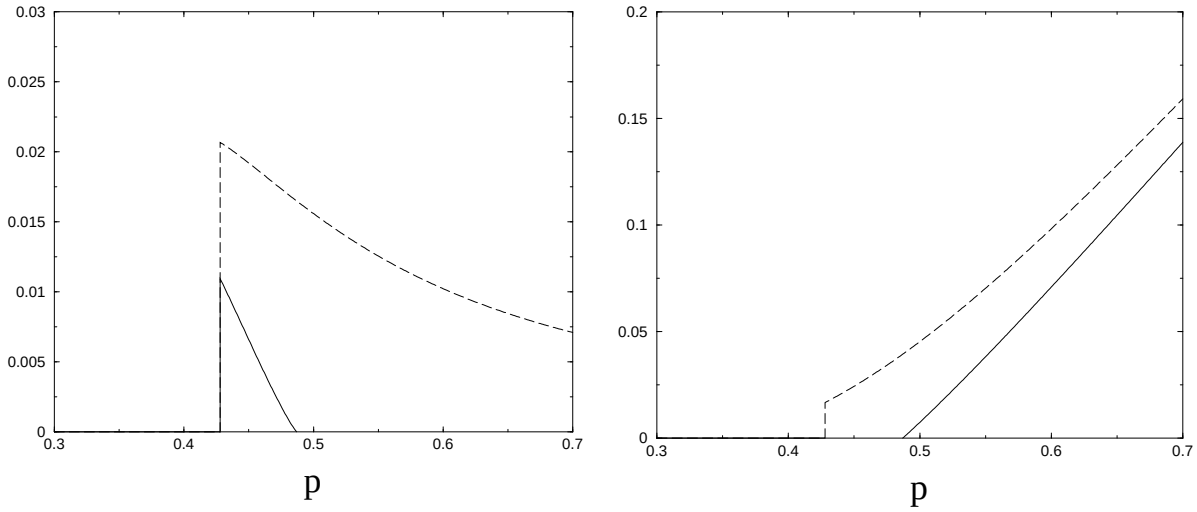



Figure 5.17: Left-hand frame: the static and dynamic energies $\epsilon_s$ and $\epsilon_d$ of the metastable states (respectively, solid and dashed lines). Right-hand frame: the total complexity $\max_\epsilon \Sigma(\epsilon)$ and the zero energy complexity $\Sigma(0)$.

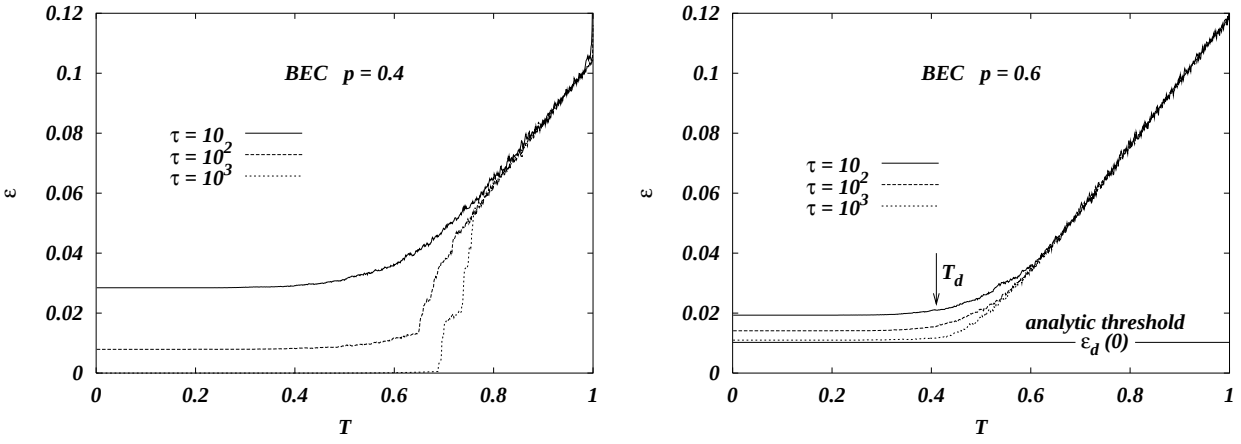



Figure 5.18: Energy relaxation for the Hamiltonian of the (6,3) regular code during the simulated annealing with $\tau$ MCS per temperature and 1000 equidistant temperatures in $[0, 1]$

frame, we report the static and dynamic energies $\epsilon_s$ and $\epsilon_d$ as functions of $p$. In the right frame we present the total complexity $\Sigma_{\rm tot} \equiv \max_\epsilon \Sigma(\epsilon) = \Sigma(\epsilon_d)$, and the zero energy complexity $\Sigma(0)$.

### Numerical results

In order to check analytical predictions and to better illustrate the role of metastable states, we have run a set of Monte Carlo simulations, with Metropolis dynamics, on the Hamiltonian (5.41) of the (6,3) regular code for the BEC. Notice that local search algorithms for the decoding problem have been already considered by the coding theory community [168].

We studied quite large codes ($N = 10^4$ bits), and tried to decode it (i.e. to find a ground state of the corresponding spin model) with the help of simulated annealing techniques [169]. For each value of $p$, we start the simulation fixing a fraction $(1 - p)$ of spins to $\sigma_i = +1$ (this part will be kept fixed all along the run). The remaining $pN$ spins are the dynamical variables we change during the annealing in order to try to satisfy all the parity checks. The energy of the system counts the number of unsatisfied parity checks.

The cooling schedule has been chosen in the following way: $\tau$ Monte Carlo sweeps (MCS) [14] at each of the 1000 equidistant temperatures between $T = 1$ and $T = 0$. The highest temperature is such that the system very rapidly equilibrates on the paramagnetic energy $\epsilon_P(T)$. Typical values for $\tau$ are from 1 to $10^3$.

Notice that, for any fixed cooling schedule, the computational complexity of the simulated annealing method is linear in $N$. Then we expect it to be affected by metastable states of energy $\epsilon_d$, which are present for $p > p_d$: the energy relaxation should be strongly reduced around $\epsilon_d$ and eventually be completely blocked.

In order to illustrate how the system relaxes during the simulated annealing we show in fig. 5.18 the energy density as a function of the temperature for $p = 0.4$ (left) and $p = 0.6$ (right) and various cooling rates, $\tau = 10, 10^2, 10^3$ (each data set is the average over many different samples).

[14] Each Monte Carlo sweep consists in $N$ proposed spin flips. Each proposed spin flip is accepted or not accordingly to a standard Metropolis test.

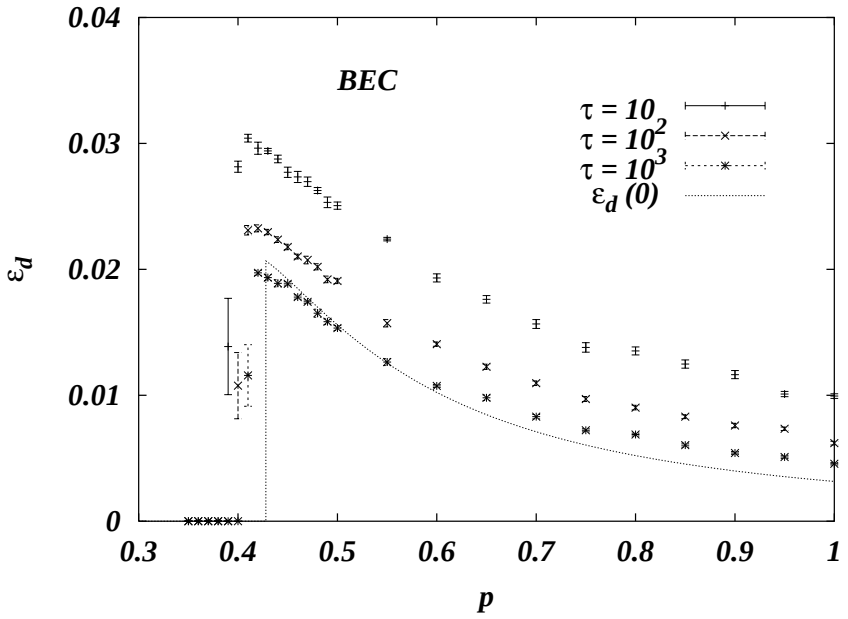



Figure 5.19: Lowest energies reached by the simulated annealing. Errors are sample to sample fluctuations.

For $p = 0.4 < p_d$ the final energy strongly depends on the cooling rate and the slowest cooling procedure is always able to bring the system on the ground state, corresponding to the transmitted codeword. Decoding by simulated annealing is therefore successful.

For $p = 0.6 > p_d$ the situation drastically changes. Below a temperature $T_d$ (marked by an arrow in fig. 5.18, right frame) there is an almost complete stop of the energy relaxation. $T_d$ marks the dynamical transition and the corresponding energy $\epsilon_d(T_d) = \epsilon_P(T_d)$ is called the threshold energy. The energy of threshold states still varies a little bit with temperature, $\epsilon_d(T)$, and the final value reached by the simulated annealing algorithm is its zero-temperature limit $\epsilon_d(0) = \epsilon_d$. Remember that, by construction, ground states of zero energy are present for any $p$ value, but they become unreachable for $p > p_d$, because they become shielded by metastable states of higher energy.

We show in fig. 5.19 the lowest energy reached by the simulated annealing procedure for different $p$ and $\tau$ values. While for $p < p_d$ all parity checks can be satisfied and the energy relaxes to zero in the limit of a very slow cooling, for $p \geq p_d$ the simulation get stuck in a metastable state of finite energy, that is with a number of unsatisfied parity checks of order $N$. The agreement with the analytic prediction (dotted line) is quite good everywhere, but very close to $p_d$.

Discrepancies between analytical predictions and numerical results may be very well due to finite-size effects in the latter. One possible explanation for large finite-size effects near the dynamic critical point $p_d$ is the following. Metastable states of energy $\epsilon_d$ are stable under any local dynamic, which may flip simultaneously only a finite number of spins, and under global dynamics flipping no more than $\omega N$ spins simultaneously. Physical intuition (threshold states become more robust increasing $p$) imply that the function $\omega(p)$ must monotonously increase for $p \in [p_d, 1]$. Moreover, continuity reasons tell us that $\omega(p_d) = 0$. The fact that $\omega(p)$ is very small close to $p_d$, together with the fact that in numerical simulations we are restricted to finite values of $N$, allow the local Monte Carlo dynamic to relax below the analytical predicted

threshold energy. A more detailed characterization of this effect is presently under study and will be presented in a forthcoming publication.

### 5.2.5 The general channel: analytical and numerical results

We considered the case of a general noisy channel using two different approaches: a finite-temperature and a zero-temperature approach. While the first one offers a clear connection with the dynamics of decoding-by-annealing algorithm, the second one gives a nice geometrical picture of the situation.

#### Finite temperature

Suppose you received some message encoded using a Gallager code and you want to decode it, but no one explained to you the belief propagation algorithm, cf. eqs. (5.31), (5.32).

A physicist idea would be the following. Write the corresponding Hamiltonian $H(\underline{\sigma})$, see eq. (5.41), and run a Monte Carlo algorithm at inverse temperature $\beta$. If you wait enough time, you will be able to sample the configuration $\underline{\sigma}$ according to the Boltzmann distribution $P_\beta(\underline{\sigma}) \propto e^{-\beta H(\underline{\sigma})}$. Then cool down the system adiabatically: i.e. change the temperature according to some schedule $\{\beta_1, \beta_2, \dots, \}$ with $\beta_k \uparrow \infty$, waiting enough time at each temperature for the system to equilibrate.

As $\beta \to \infty$ the Boltzmann measure of the Hamiltonian (5.40) concentrates on the codewords (for which the exchange term in eq. (5.40) is equal to zero). Moreover each codeword is given a weight which depends on its likelihood. In formulae:

$$\lim_{\beta\to\infty} P_\beta(\underline{\sigma}) = \frac{1}{Z_{\hat{\zeta}}}\, P(\underline{\sigma}|\underline{\mathtt{x}}^{\rm out})^{\hat{\zeta}}\,, \tag{5.60}$$

where $P(\underline{\sigma}|\underline{\mathtt{x}}^{\rm out})$ is the probability for $\underline{\sigma}$ to be the transmitted codeword, conditional to the received message $\underline{\mathtt{x}}^{\rm out}$, and $Z_{\hat{\zeta}}$ is a normalization constant. Therefore when $\beta \gg 1$, our algorithm will sample a codeword with probability proportional to $P(\underline{\sigma}|\underline{\mathtt{x}}^{\rm out})^{\hat{\zeta}}$. For good codes below the critical noise threshold $p_c$, the likelihood $P(\underline{\sigma}|\underline{\mathtt{x}}^{\rm out})$ is strongly concentrated[15] on the correct input codeword. Therefore the system will spend most of its time on the correct codeword as soon as $\beta \gg 1$ and $\hat{\zeta} \geq 1$ (for $\hat{\zeta} < 1$, $p_c$ has a non-trivial dependence on $\hat{\zeta}$, cf. Ref. [154]).

This algorithm will succeed as long as we are able to keep the system in equilibrium at all temperatures down to zero. If some form of ergodicity breaking is present this may take an exponentially (in the size $N$) long time. Let us suppose to spend an $O(N)$ computational time at each temperature $\beta_i$ of the annealing schedule (this is what happens in Nature). We expect to be able to equilibrate the system only at low enough noise (let us say for $p < p_d(\hat{\zeta})$), when the magnetic field in eq. (5.41) is strong enough for single out a unique ergodic component.

#### The random linear code limit

Some intuition on the static phase diagram can be gained by looking at the $k, l \to \infty$ limit with rate $R = 1 - k/l$ fixed, cf [127]. Unhappily, in this limit the dynamic phase transition disappears: the decoding algorithm is always unsuccessful, as can be understood by looking at eqs. (5.31)-(5.32). This phenomenon is analogous to what happens in the random energy

[15] Namely we have $P(\underline{\sigma}^{\rm in}|\underline{\mathtt{x}}^{\rm out}) = 1 - O(e^{-\alpha N})$. This happens because there is a minimum $O(N)$ Hamming distance between distinct codewords [141].

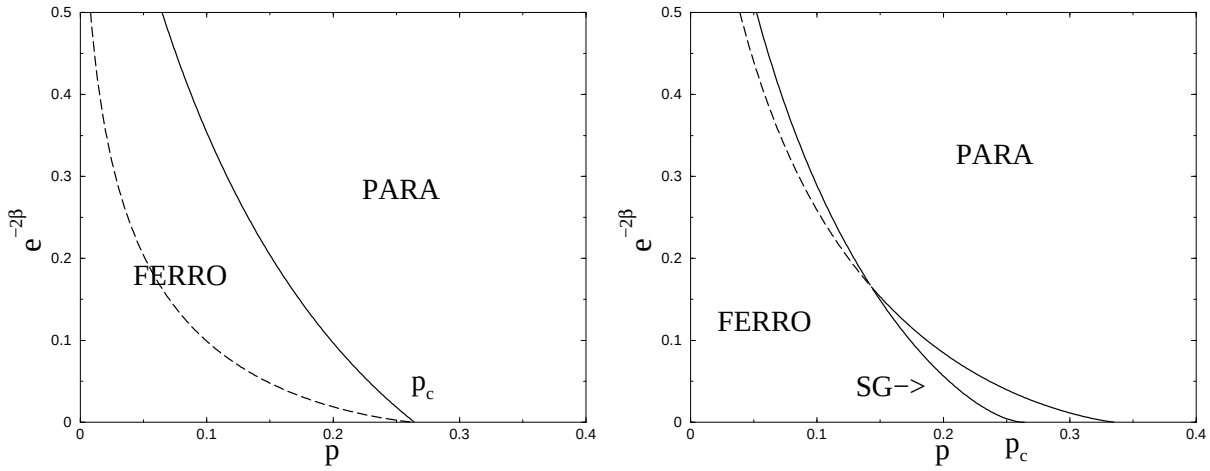



Figure 5.20: The phase diagram for the model (5.40) in the limit $k, l \to \infty$ with $R = 1 - k/l$ fixed. Here we consider $R = 1/6$ and $\hat{\zeta} = 1$ (on the left) and 1.5 (on the right). The rightmost (i.e. noisier) point for which the ferromagnetic phase is globally stable is always at $\beta = \infty$, $p = \delta_{GV}(R) \approx 0.264$. Along the dashed line the entropy of the paramagnetic phase vanishes.

model (REM) [170]: the dynamic transition is usually said to occur at infinite temperature. We refer to Sec. 5.2.5 for further clarifications of this point.

There exist a paramagnetic and a ferromagnetic phases, with free energy densities

$$f_P = -\frac{1}{\beta}\langle \log(2\cosh\hat{\zeta}h)\rangle_h + \frac{1-R}{\beta}\log(1+\tanh\beta)\,, \tag{5.61}$$

$$f_F = -\frac{\hat{\zeta}}{\beta}\langle h\rangle_h\,. \tag{5.62}$$

One must be careful in computing the entropy because of the explicit dependence of the Hamiltonian (5.40) upon the temperature. The result is that the ferromagnetic phase has zero entropy $s_F = 0$, while the entropy of the paramagnetic phase is

$$\begin{aligned} s_P = {} & \langle \log(2\cosh\hat{\zeta}h)\rangle_h - \langle \hat{\zeta}h\tanh\hat{\zeta}h\rangle_h - \\ & -(1-R)\log(1+\tanh\beta) + (1-R)\beta(1-\tanh\beta)\,. \end{aligned} \tag{5.63}$$

In the low-temperature, low-noise region the paramagnetic entropy $s_P$ becomes negative. This signals a REM-like glassy transition [170]. The spin glass free energy is obtained by maximizing over the RSB parameter $m$ (with $0 \le m \le 1$) the following expression

$$f_{SG}(m) = -\frac{(1-R)}{\beta m}\log(1+e^{-2\beta m}) - \frac{1}{m}\langle \log(2\cosh m\hat{\zeta}h)\rangle_h\,. \tag{5.64}$$

The generic phase diagram is reported in fig. 5.20. At high temperature, as the noise level is lowered the system undergoes a paramagnetic-ferromagnetic transition and concentrates on the correct codeword. At low temperature an intermediate glassy phase may be present (for $\hat{\zeta} > 1$): the system concentrates on a few incorrect configurations.

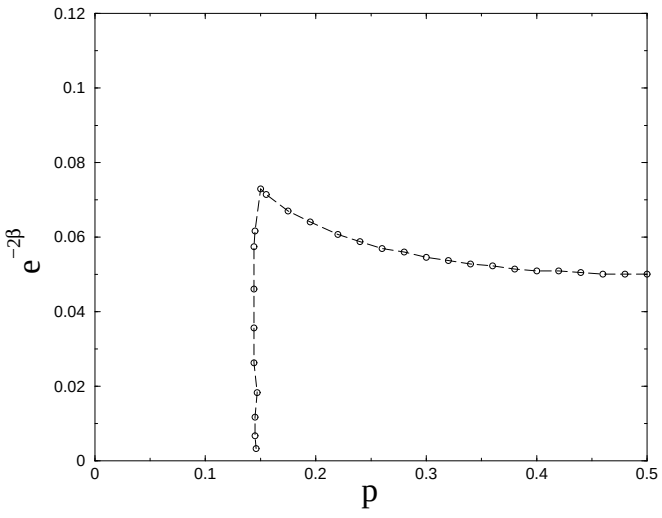



Figure 5.21: The dynamical phase transition for a regular $(6, 5)$ code (cf. eq. (5.40) with $k = 6$ and $l = 5$) with $\hat{\zeta} = 1$.

### Theoretical dynamical line

The existence of metastable states can be detected within the replica formalism by the so-called marginal stability condition. One considers the saddle point equations for the 1RSB order parameter, fixing the RSB parameter $m = 1$, cf. [127]. The dynamical temperature $T_d(p)$ is the highest temperature for which a "non-trivial" solution of the equation exists. At this temperature ergodicity of the physical dynamics breaks down (at least this is what happens in infinite connectivity mean field models) and we are no longer able to equilibrate the system within an $O(1)$ physical time (i.e. an $O(N)$ computational time).

We looked for a solution of eqs. (**B-3-B-3**) in [127] using the population dynamics algorithm of Ref. [23]. We checked the "non-triviality" of the solution found by considering the variance of the distributions $\rho(x)$, $\hat{\rho}(y)$ (more precisely of the *populations* which represent such distributions in the algorithm).

We consider the $(6, 5)$ regular code because it has well separated static and dynamical thresholds $p_c$ and $p_d$, cf. Tab. 5.1. The resulting dynamical line for the Hamiltonian (5.40) with $\hat{\zeta} = 1$, is reported in fig. 5.21. The dynamic temperature $T_d(p)$ drops discontinuously below a noise $p_d(\hat{\zeta})$: for $p < p_d(\hat{\zeta})$ the dynamical transition disappears and the system can be equilibrated in linear computational time down to zero temperature. We get $p_d(1) \approx 0.14$, which is in good agreement with the coding theory results, cf. Tab. 5.1

### Numerical experiments

We have repeated for the BSC the same kind of simulations already presented at the end of Sec. 5.2.4 for the BEC.

We have run a set of simulated annealings for the Hamiltonian 5.41 of the (6,5) regular code. System size is $N = 12000$ and the cooling rates are the same as for the BEC, the only difference being the starting and the ending temperatures, which are now $T = 1.2$ and $T = 0.2$ (plus a quench from $T = 0.2$ to $T = 0$ at the end of each cooling). This should not have any relevant effect because $0.2 \ll T_d \approx 0.6$.

The important difference with respect to the BEC case is that now we have no fixed

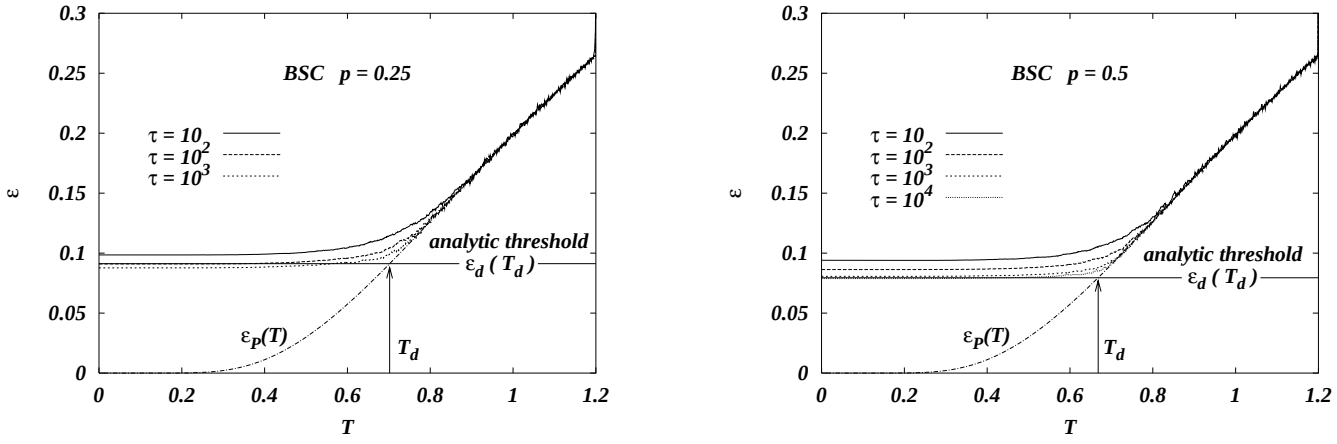



Figure 5.22: Energy relaxation for the Hamiltonian of the (6,5) regular code during the simulated annealing with $\tau$ MCS per temperature and 1000 equidistant temperatures in $[0.2, 1.2]$. Notice that, in both cases $p > p_d$. The dot-dashed line is the theoretical prediction for the paramagnetic exchange energy.

spins, all $N$ spins are dynamical variables subject to a random external field of intensity $h = (1/\beta)\text{arctanh}(1-2p)$, cf. eq. (5.41).

Also here, as in the case of the BEC, the energy relaxation for $p > p_d$ undergoes a drastic arrest when the temperature is reduced below the dynamical transition at $T_d$, see fig. 5.22.

Unfortunately, in this case, we are not able to calculate analytically the threshold energy $\epsilon_d(0)$, but only the dynamical critical temperature $T_d$ and then the threshold energy at the transition $\epsilon_d(T_d)$ which is higher than $\epsilon_d(0)$. The difference $\Delta\epsilon = \epsilon_d(T_d) - \epsilon_d(0)$ is usually not very large (see e.g. the BEC case), but it becomes apparent when $p$ is decreased towards $p_d$. Indeed for $p = 0.25$ (fig. 5.22 left) the Metropolis dynamics is still able to relax the system for temperatures below $T_d$ and then it reaches an energy well below $\epsilon_d(T_d)$. On the other hand for $p = 0.5$ (fig. 5.22 right), where $\Delta\epsilon$ is small the relaxation below $T_d$ is almost absent and the analytic prediction is much more accurate. Notice that for this case we have run a still longer annealing with $\tau = 10^4$: the asymptotic energy is very close to that for $\tau = 10^3$ and hardly distinguishable from the analytical prediction.

In fig. 5.23 we report the lowest energy reached by the simulated annealing for many values of $p$ and $\tau = 10, 10^2, 10^3$, together with the analytic calculation for the threshold energy at $T_d$. This analytical value is an upper bound for the true threshold energy $\epsilon_d(0)$ where linear algorithms should get stuck, but it gives very accurate predictions for large $p$ values where $\Delta\epsilon$ is very small. In the region of small $p$ a more complete calculation is needed.

### Zero temperature

This approach follows from a physical intuition that is slightly different from the one explained in the previous paragraphs. Once again we will formulate it algorithmically. For sake of simplicity we shall refer, in this Section, to the BSC. We refer to the Appendices of [127] for more general formulae.

The overlap between the transmitted codeword and the received message

$$q^{\text{in,out}} = \frac{1}{N}\sum_{i=1}^{N} \sigma_i^{\text{in}}\sigma_i^{\text{out}} , \tag{5.65}$$

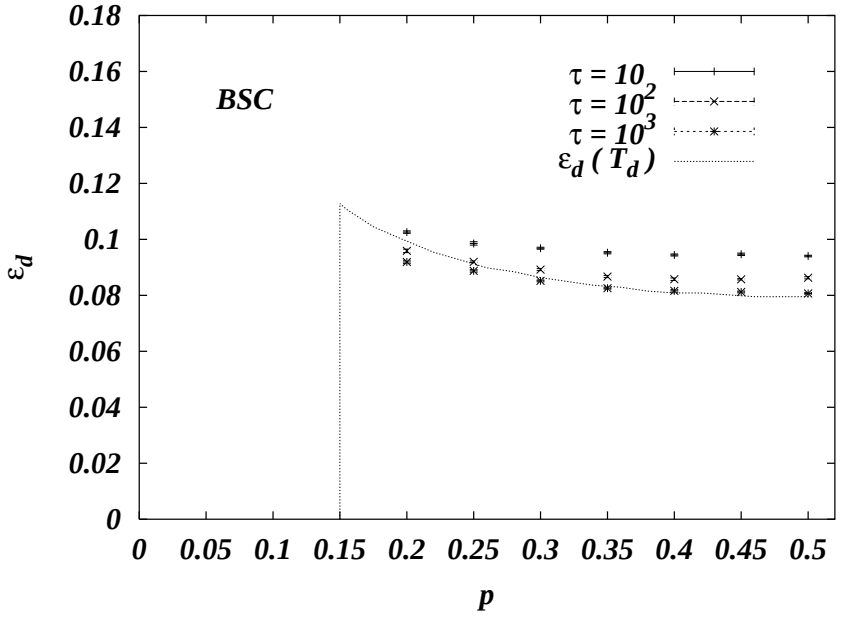



Figure 5.23: Lowest energies reached by the simulated annealings. Errors are sample to sample fluctuations. The theoretical prediction $\epsilon_d(T_d)$ is computed using the results in fig. 5.21 for $T_d(p)$.

is, typically, $q^{\rm in,out} = 1-2p$. Given the received message, one can work in the subspace of all the possible configurations which have the prescribed overlap with it[16], i.e. all the $\underline{\sigma}$ such that $(1/N)\sum_{i=1}^{N}\sigma_i\sigma_i^{\rm out} \approx (1-2p)$. Once this constraint has been imposed (for instance in a Kawasaki-like Monte Carlo algorithm) one can restrict himself to the exchange part of the Hamiltonian (5.40) $H_{\rm exch}(\underline{\sigma}) = -\sum_l \sum_{(i_1\dots i_l)} \sigma_{i_1}\cdots\sigma_{i_l}$ and apply the cooling strategy already described in the previous Section.

Below the static transition $p_c$ there exists a unique codeword having overlap $(1-2p)$ with the received signal. This is exactly the transmitted one $\underline{\sigma}^{\rm in}$. This means that $\underline{\sigma}^{\rm in}$ is the unique ground state of $H_{\rm exch}(\underline{\sigma})$ in the subspace we are considering. If we are able to keep our system in equilibrium down to $T=0$, the cooling procedure will finally yield the correct answer to the decoding problem. Of course, if metastable states are encountered in this process, the time required for keeping the system in equilibrium diverges exponentially in the size.

We expect the number of such states to be exponentially large[17]:

$$\mathcal{N}_{MS}(\epsilon, q|p) \sim e^{N\Sigma_p(\epsilon,q)}\,, \tag{5.66}$$

where $\epsilon$ is the exchange energy density $H_{\rm exch}(\underline{\sigma})/N$. Notice that we emphasized the dependence of these quantities upon the noise level $p$. In fact the noise level determines the statistics of the received message $\underline{\sigma}^{\rm out}$. The static threshold is the noise level at which an exponential number of codewords with the same overlap as the correct one ($q=1-2p$) appears: $\Sigma_p(0,1-2p)>0$. The dynamic transition occurs where metastable states with the same overlap begin to exist: $\Sigma_p(\epsilon,1-2p)>0$ for some $\epsilon>0$.

[16] Of course this is true up to $O(N^{-1/2})$ corrections. For instance one can work in the space of configurations $\underline{\sigma}$ such that $(1-2p-\delta)N < \sum_{i=1}^{N}\sigma_i\sigma_i^{\rm out} < (1-2p+\delta)N$, for some small number $\delta$.

[17] For a related calculation in a fully connected model see Ref. [171].

**The random linear code limit**

It is quite easy to compute the complexity $\Sigma_p(\epsilon, q)$ in the limit $k, l \to \infty$ with rate $R = 1 - k/l$ fixed. In particular, the zeroth order term in a large $k, l$ expansion can be derived by elementary methods.

In this limit we expect the regular $(l, k)$ *ensemble* to become identical to the random linear code (RLC) *ensemble*. The RLC *ensemble* is defined by taking each element of the parity check matrix $\hat{H}$, cf. eq. (5.27) to be 0 or 1 with equal probability. Distinct elements are considered to be statistically independent.

Let us compute the number of configurations $\underline{\sigma}$ having a given energy and overlap with the received message $\underline{\sigma}^{\rm out}$. Given a bit sequence $\underline{\mathtt{x}} \neq \underline{\mathtt{0}}$, the probability that $L$ out of $M$ equations $\hat{H}\underline{\mathtt{x}} = \underline{\mathtt{0}}$ are violated is

$$P_{L,\underline{\mathtt{x}}} = \left( \begin{array}{c} M \\ L \end{array} \right) 2^{-M} \, . \tag{5.67}$$

Therefore the expected number of configurations $\underline{\mathtt{x}}$ which violate $L$ checks and have Hamming distance $W$ from the received message $\underline{\mathtt{x}}^{\rm out}$ is

$$\overline{\mathcal{N}_{W,L}} = \delta_{W,W_{\underline{\mathtt{x}}^{\rm out}}} \delta_{L,0} [1 - 2^{-M}] + \left( \begin{array}{c} N \\ W \end{array} \right) \left( \begin{array}{c} M \\ L \end{array} \right) 2^{-M} \, , \tag{5.68}$$

where $W_{\underline{\mathtt{x}}^{\rm out}}$ is the *weight* of $\underline{\mathtt{x}}^{\rm out}$, i.e. its Hamming distance from $\underline{\mathtt{0}}$. Notice that, up to exponentially small corrections, the above expression does not depend on $\underline{\mathtt{x}}^{\rm out}$.

Introducing the overlap $q = 1 - 2W/N$ and the exchange energy density $\epsilon = 2L/N$, we get $\overline{\mathcal{N}_{W,L}} \sim 2^{N\tilde{\Sigma}(\epsilon,q)}$ with

$$\tilde{\Sigma}(\epsilon, q) = \mathtt{h}[(1-q)/2] + (1-R)\, \mathtt{h}[\epsilon/2(1-R)] - (1-R) \, . \tag{5.69}$$

The typical number $\mathcal{N}^{\rm typ}_{W,L}$ of such configurations can be obtained through the usual REM construction: $\mathcal{N}^{\rm typ}_{W,L} \sim 2^{N\tilde{\Sigma}(\epsilon,q)}$ when $\tilde{\Sigma}(\epsilon, q) \geq 0$ and $\mathcal{N}^{\rm typ}_{W,L} = 0$ otherwise.

Now we are interested in picking, among all the configurations having a given energy density $\epsilon$ and overlap $q$, the metastable states. In analogy with the REM, this can be done by eliminating all the configurations such that $\partial_\epsilon \tilde{\Sigma}(\epsilon, q) < 0$. In other words, the number of metastable states is $\mathcal{N}_{MS}(\epsilon, q) \sim 2^{N\Sigma(\epsilon,q)}$ with $\Sigma(\epsilon, q) = \tilde{\Sigma}(\epsilon, q)$ when $\tilde{\Sigma}(\epsilon, q), \partial_\epsilon \tilde{\Sigma}(\epsilon, q) > 0$, $\Sigma(\epsilon, q) = -\infty$ otherwise.

In fig. 5.24 we plot the region of the $(\epsilon, q)$ plane for which $\Sigma(\epsilon, q) > 0$, for $R = 1/2$ codes. Notice that, in this limit $\Sigma(\epsilon, q)$ does not depend on the received message $\underline{\sigma}^{\rm out}$ (and, therefore, is independent of $p$). As expected we get $p_c = \delta_{GV}(R)$ and $p_d = 0$.

In order to get the first non-trivial estimate for the dynamical point $p_d$, we must consider the next term in the above expansion. This correction can be obtained within the replica formalism, see [127]. In fig. 5.25 we reproduce contour of the region $\{(\epsilon, q) : \Sigma_p(\epsilon, q) > 0\}$ for a few regular codes of rate $R = 1/2$: $(l, k) = (6, 3)$,$(10, 5)$,$(14, 7)$. The main difference between these curves and the exact results, cf. Sec. 5.2.5, is the convexity of the upper boundary of the $\Sigma_p(\epsilon, q) > 0$ region (dashed lines in figs. 5.24 and 5.25).

The corresponding estimates for $p_c$ and $p_d$ are reported in Tab. 5.2.

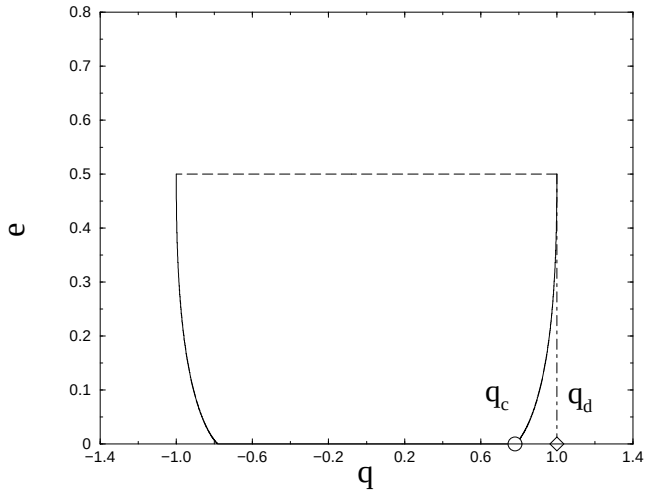



Figure 5.24: Metastable states in the random linear code limit for $R = 1/2$: their number is exponential between the continuous and the dashed lines. It vanishes discontinuously when the dashed line is crossed and continuously when the continuous line is crossed. The critical and dynamical overlaps are related to the statical and critical noise by $q_{c,d} = 1 - 2p_{c,d}$. In this limit $p_d = 0$ and $p_c = \delta_{GV}(1/2) \approx 0.110025$.

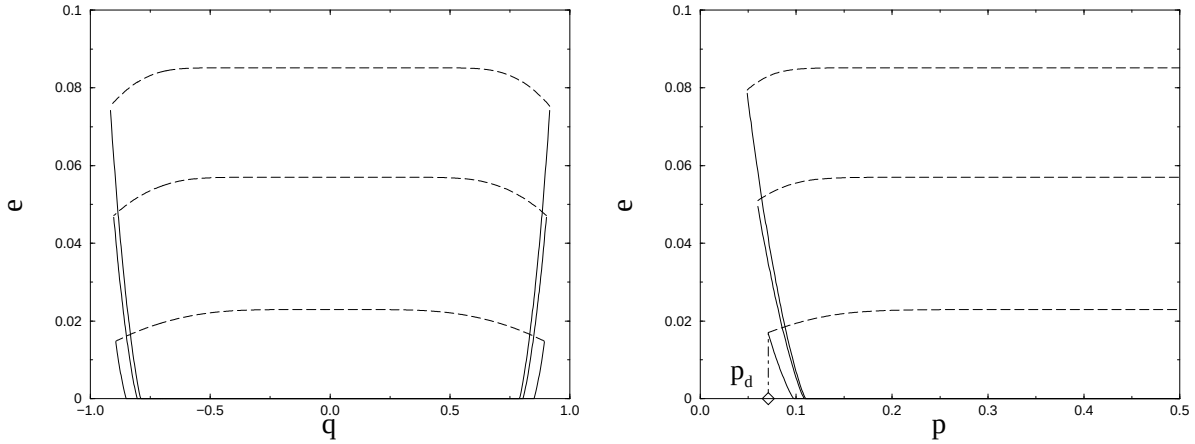



Figure 5.25: Metastable states for regular $(l, k)$ codes in a large-$k$,$l$ expansion, at fixed rate $R = 1/2$. We consider (from bottom to top) $(l, k) = (6, 3)$, $(10, 5)$, $(14, 7)$. On the left we show the region where $\Sigma_{p=0}(\epsilon, q) > 0$. On the right we consider instead $\Sigma_p(\epsilon, 1 - 2p)$.

| $(l, k)$ | $p_c$ | $p_d(1)$ |
|---|---|---|
| $(6, 3)$ | 0.097 | 0.071 |
| $(10, 5)$ | 0.108 | 0.060 |
| $(14, 7)$ | 0.109 | 0.049 |
| $(6, 5)$ | 0.264 | 0.108 |

Table 5.2: Dynamical and static thresholds at the first nontrivial order in a large $k$,$l$ expansion, cf. Tab. 5.1.

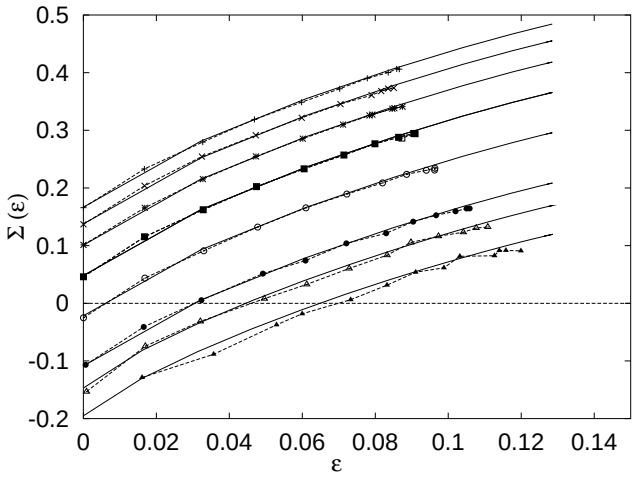



Figure 5.26: The configurational entropy versus the energy for the $(6, 5)$ regular code. Symbols refer to various noise levels. From top to bottom $p = 0.5, 0.4, 0.35, 0.3, 0.25,\ 0.2, 0.18, 0.155$. Continuous lines give the result of a variational computation, cf. App. E.

### The complete calculation

The full 1RSB solution for can be obtained through the population dynamics method [23]. Here, as in Sec. 5.2.5, we focus on the example of the $(6, 5)$ code. In fig. 5.26 we plot the configurational entropy as a function of the energy of the states along the lines of constant $q$, together with the corresponding results obtained within a simple variational approach, briefly introduced in the Appendix. The approximate treatment is in quantitative agreement with the complete calculation for $\epsilon < \epsilon_d$, but predicts a value for the threshold energy which is larger than the correct one: $\epsilon_d^{var} > \epsilon_d$. Here $\epsilon_d^{var} \approx 0.127$ and almost $p$-independent.

Unhappily the estimate of the dynamic energy obtained from this curves is not very precise. Moreover, at least two more considerations prevent us from comparing these results with the ones of simulated annealing simulations, cf. Sec. 5.2.5: $(i)$ In our annealing experiments the overlap with the received message $\underline{\sigma}^{\rm out}$ is free to fluctuate; $(ii)$ We cannot exclude the 1RSB solution to become unstable at low temperature.

However the population dynamics solution give the estimate $p_d \leq 0.155$. This allows us to confirm that the point $p_d = 0.139$ where the decoding algorithm fails to decode, cf. Tab. 5.1, coincides with the point where the metastable states appear.

## 5.2.6 Conclusions

We studied the dynamical phase transition for a large class of diluted spin models in a random field, the main motivation being their correspondence with very powerful error correcting codes.

In a particular case, we were able to show that the dynamic critical point coincides exactly with the critical noise level for an important class of decoding algorithms, cf. Sec. 5.2.4. For a general model of the noisy channel, we couldn't present a completely explicit proof of the same statement. However, within numerical precision, we obtain identical values for the algorithmic and the statistical mechanics thresholds.

It may be worth listing a few interesting problems which emerge from our work:

- Show explicitly that the identity between statistical mechanics and algorithmic thresholds holds in general. From a technical point of view, this is a surprising fact because the two

thresholds are obtained, respectively, within a replica symmetric, cfr. eqs. (5.37), (5.38), and a one-step replica symmetry breaking calculations.

- We considered message-passing and simulated annealing algorithms. Extend the above analysis to other classes of algorithm (and, eventually, to any linear time algorithm).
- Message passing decoding algorithms get stuck because they are unable to decode some fraction of the received message, the "hard" bits, while they have been able to decode the other ones, the "easy" bits. A closer look at this heterogeneous behavior would be very fruitful.

# Chapter 6

# Determining bounds

## 6.1 Variational bounds for optimization problems and spin systems

In this final chapter we generalize to the case of diluted spin models and random combinatorial optimization problems a technique recently introduced by Guerra (cond-mat/0205123) to prove that the replica method generates variational bounds for disordered systems. We analyze a family of models that includes the Viana-Bray model, the diluted $p$-spin model or random XOR-SAT problem, and the random $K$-SAT problem, showing that the replica method provides an improvable scheme to obtain lower bounds of the free-energy at all temperatures and of the ground state energy. In the case of $K$-SAT the replica method thus gives upper bounds of the satisfiability threshold. The replica method [176, 2], originally devised as a trick to compute thermodynamical quantities of physical systems in presence of quenched disorder, has found applications in the analysis of systems of very different nature, as Neural Networks, Combinatorial optimization problems [2, 35, 27], Error Correction Codes [27] etc. Although many physicists believe that the method, within the Replica Symmetry Breaking scheme of Parisi [2], is able to potentially give the exact solution of any problem treatable as a mean field theory, the necessary mathematical foundation of the theory is still lacking, after more then 20 years from its introduction in theoretical physics. The last times have seen a growing interest of the mathematical community in the method, leading to important but still partial results, confirming in certain cases the replica analysis, with more conventional and well established techniques [177]. Apart the remarkable exception of the analysis of the fully connected $p$-spin model in ref. [178] and the rigorous analysis of Random Energy Models [179], the analysis of the mathematicians has been, as far as we know, restricted to the high temperature regions and/or to problem of replica symmetric nature. Very welcomed have been the techniques recently introduced by Guerra and Toninelli [60] which allow rigorous analysis not relying on the assumption of high temperature, and valid even in problems with replica symmetry breaking. Along these lines, an important step towards the rigorous comprehension of the replica method, has been undertaken in [60], where it has been shown how in the case of the Sherrington-Kirkpatrick model, and its $p$-spin generalizations, the replica free-energies with arbitrary number of replica symmetry breaking steps constitute variational lower bounds to the true free-energy of the model. As stated in that paper, the analysis is restricted to fully-connected models, whose replica mean field theory can be formulated in terms of a single $n \times n$ matrix. However, in recent times, many of the more interesting problems analyzed with

replica theory pertain to the so called "diluted models" where each degree of freedom interacts with a finite number of neighbors. The introduction of a "population dynamics algorithm" [23] has allowed to treat in full generality -within statistical precision- complicated sets of probabilistic functional equations appearing in the one step symmetry broken framework of diluted models. The same algorithm has been used as a starting point of a generalized "belief propagation" algorithm for optimization problems [145, 30]. Furthermore, at the analytic level, simplifications due to graph homogeneities in some cases [22], and to the vanishing temperature limit in some other cases [9] have led to supposedly exact solutions of the ground state properties of diluted models, culminated in the resolution of the random XOR-SAT on uniform graphs in [22] and the random $K$-SAT problem in [30] within the framework of "one-step replica symmetry breaking" (1RSB). The aim of this chapter, is to show that the replica analysis of diluted models provides lower bounds for the exact free-energy density, and ground state energy density. We analyze in detail the cases of the diluted $p$-spin model on the Poissonian degree hyper-graphs also known as random XOR-SAT problem and the random $K$-SAT problems. We expect that along similar lines free-energy lower bounds can be found for many other diluted cases. The Guerra method we use sheds some light on the meaning of the replica mean field theory. The physical idea behind the method is that within mean field theory one can modify the original Hamiltonian weakening the strength of the interaction couplings or removing them partially or totally, and compensate this removal by some auxiliary external fields. In disordered systems these fields should be random fields, taken from appropriate probability distributions and possibly correlated with the original values of the quenched variables eliminated from the systems. One is then led to consider Hamiltonians interpolating between the original model and a pure paramagnet in a random field, and by means of these models achieving free-energy lower bounds. We will see that the RS case corresponds to assuming independence between the random fields and the quenched disorder. The Parisi RSB scheme, assumes at each breaking level a peculiar kind of correlations, and gives free-energy bounds improving the RS one. The chapter is organized in this way: in section 6.1.1 we introduce some notations that will be extensively used in the following sections. In section 6.1.2 we introduce the general strategy to get the replica bounds We then specialize to the replica symmetric and the one step replica symmetry broken bounds, giving the results in the $p$-spin and the $K$-SAT cases. Conclusions are drawn in section 6.1.5. In the appendices some details of the calculations in both the $p$-spin and the $K$-SAT cases are shown. Our results will be issue of explicit calculations. Although at the end we will get bounds, formalizable as mathematical theorems, the style and most of the notations of the chapter will be the ones of theoretical physics.

### 6.1.1 Notations

Since the aim of this chapter is to obtain rigorous results, it is necessary to review and extend here some notations already introduced at beginning. The spin models we will consider in this work are defined by a collection of $N$ Ising $\pm 1$ spins $\mathbf{S} = \{S_1, ..., S_N\}$, interacting through Hamiltonians of the kind

$$\mathcal{H}^{(\alpha)}(\mathbf{S}, \mathbf{J}) = \sum_{\mu=1}^{M} H_{J^{(\mu)}}(S_{i_1^\mu}, ..., S_{i_p^\mu}) \tag{6.1}$$

where the indices $i_l^\mu$ are i.i.d. quenched random variables chosen uniformly in $\{1, ..., N\}$. We will call each term $H_{J^{(\mu)}}$ a clause. The subscript $J^{(\mu)}$ in the clauses indicates the dependence on a single or a set of quenched random variables, as it will be soon clear. The number of

clauses $M$ will be taken to be proportional to $N$. For convenience we will choose it to be for each sample a Poissonian number with distribution $\pi(M, \alpha N) = e^{-\alpha N}\frac{(\alpha N)^M}{M!}$. The fluctuations of $M$ will not affect the free-energy in the thermodynamic limit, and this choice, which slightly simplify the analysis, will be equivalent to choosing a fixed value of $M$ equal to $\alpha N$. The clauses themselves will be random. The $p$-spin model[19] has clauses of the form

$$H_{J^{(\mu)}}(S_{i_1^\mu}, ..., S_{i_p^\mu}) = J^\mu S_{i_1^\mu} \cdot ... \cdot S_{i_p^\mu} \ . \tag{6.2}$$

This form reduces to $H_{J^{(\mu)}}(S_{i_1^\mu}, S_{i_2^\mu}) = J^\mu S_{i_1^\mu} S_{i_2^\mu}$ in the case of the Viana-Bray spin glass $p = 2$. In both cases the $J^\mu$ will be taken as i.i.d. random variable with regular symmetric distribution $\mu(J) = \mu(-J)$. Notice that for $\mu(J) = 1/2[\delta(J+1)+\delta(J-1)]$ the model reduces to the random XOR-SAT problem [82] of computer science. The random $K$-SAT clauses have the form [9]

$$H_{J^{(\mu)}}(S_{i_1^\mu}, ..., S_{i_p^\mu}) = \prod_{l=1}^{p} \frac{1 + J^\mu_{i_l^\mu} S_{i_l^\mu}}{2} \ , \tag{6.3}$$

where the $J^\mu_{i_l^\mu} = \pm 1$ are i.i.d. with symmetric probability. (The number $p$ of spin appearing in a clause is usually called $K$ in the $K$-SAT problem, for uniformity of notation we will deviate from this convention). Notice that in all cases, on average each spin participate to $\alpha = \frac{M}{N}$ clauses, and that the set of spins and interactions defines a random diluted hyper-graph of uniform rank $p$ and random local degree with Poissonian statistics in the thermodynamic limit. At high enough temperature, the existence of the free-energy in the thermodynamic limit for models of this kind has been proved in by Talagrand in [180], together with the validity of the RS solution. A proof valid at all temperature based on the ideas presented in this chapter, can be obtained for even $p$ in analogy of the analysis in [60] for long range models. We sketch it in appendix C in the case of the $p$-spin model.

In establishing the free-energy bounds we will need several kind of averages:

- The Boltzmann-Gibbs average for fixed quenched disorder: given an observable $A(\mathbf{S})$

$$\omega(A) = \frac{\sum_{\mathbf{S}} A(\mathbf{S}) \exp(-\beta \mathcal{H}(\mathbf{S}, \mathbf{J}))}{Z} \tag{6.4}$$

  where $Z = \sum_{\mathbf{S}} \exp(-\beta \mathcal{H}(\mathbf{S}, \mathbf{J}))$ and $\beta$ is the inverse temperature. Obviously, $\omega(A)$, as well as $Z$ will be functions of the quenched variables, the size of the system and the temperature. This dependence will be made explicit only when needed.

- The disorder average: given an observable quantity $B$ dependent on the quenched variables appearing in the Hamiltonian, we will denote as $E(B)$ its average. This will include the average with respect to the $J$ variables and the choice of the random indices in the clauses as well as with respect to other quenched variables to be introduced later.

- We will need in several occasion the "replica measure"

$$\Omega(A_1, ..., A_n) = E(\omega(A_1)...\omega(A_n)) \tag{6.5}$$

  and some generalizations that we will specify later.

- We will occasionally use other kinds of averages, as well as other notations, for which we will use an angular bracket notation, with a subscript indicating the variable(s) over

which the average is performed. e.g. an average over a random variable $u$ with probability distribution $Q(u)$ will be denoted equivalently as $\int duQ(u)(\cdot) \equiv \int dQ(u)(\cdot) \equiv \langle\cdot\rangle_u$. Analogously, averages over distribution families of $Q(u)$ will be denoted as $\int dQ\,\mathcal{Q}(Q)(\cdot) \equiv \int \mathcal{D}\mathcal{Q}(Q)(\cdot) \equiv \langle\cdot\rangle_Q$. Subscripts will be omitted whenever confusion is not possible.

- Another notation we will have the occasion to use in the one for the overlaps among $l$ spin configurations $\{S_i^{a_1}, ..., S_i^{a_l}\}$, out of a population of $n$ $\{S_i^1, ..., S_i^n\}$:

$$q^{(a_1,...,a_l)} = \frac{1}{N}\sum_{i=1}^{N} S_i^{a_1} \cdot ... \cdot S_i^{a_l} \quad (1 \le a_r \le n \quad \forall r), \tag{6.6}$$

and in particular

$$q^{(n)} = q^{(1,...,n)} = \frac{1}{N}\sum_{i=1}^{N} S_i^1 \cdot ... \cdot S_i^n \ , \tag{6.7}$$

This notation will be extended to multi-overlaps in the 1RSB case, as we will specify in section 6.1.4.

In the following we will need to consider averages where some of the variables are excluded, e.g. the averages when a variable $u_i^{k_i}$ is erased. These average will be denoted with a subscript $-u_i^{k_i}$ e.g. if an $\omega$ average is concerned the notation will be $\omega(\cdot)_{-u_i^{k_i}}$. Other notations will be defined later in the text whenever needed.

Our interest will be confined to bounds to the free-energy density $F_N = -\frac{1}{\beta N} E \log Z$ and the ground state energy density $U_{GS} = \lim_{N\to\infty} 1/NE\left[min\left(U_N\right)\right]$ valid in the thermodynamic limit, so that $O(1/N)$ will be often implicitly neglected in our calculations.

### 6.1.2 The general strategy

The strategy to get the replica bound is a generalization of the one introduced by Guerra in the case of fully connected models [60]. We will consider models which will interpolate between the original ones we want to analyze and pure paramagnet in random fields with suitably chosen distribution. The underlying idea is that, given the mean field nature of the models involved, if one was able to reconstruct the real local fields acting on a given spin variable via a given hyper-edge, and to introduce auxiliary fields acting on that variable in such a way to energetically balance the deletion of the hyper-edge, then it would be possible to have an exact expression for the free-energy in terms of such auxiliary fields even when the whole edge set was emptied. A single step in the iteration procedure is exemplified in fig (6.1), where the deletion of a clause parallels the insertion of a spin variable in the original formulation of the cavity method. Indeed, the two procedures can be seen to be equivalent on average on poissonian hyper-graphs, as the results of this chapter will confirm. However, if the replacement is done with some approximate form of the auxiliary fields distribution function, the real free-energy will be the one calculated using the approximate fields plus an excess term at every step of the graph deletion process. The proof of the definite sign of this excess term gives a way to determine bounds for the thermodynamic quantities. We will prove the existence of replica lower bounds to the free-energy density of the $p$-spin model and the random $K$-SAT problem. In this last case our result proves that the recent replica solution of [30] gives a lower bound to the ground state energy and therefore an upper bound for the satisfiability threshold. The proofs will strictly hold in the $N \to \infty$ limit, due to the presence of corrections of order $1/N$

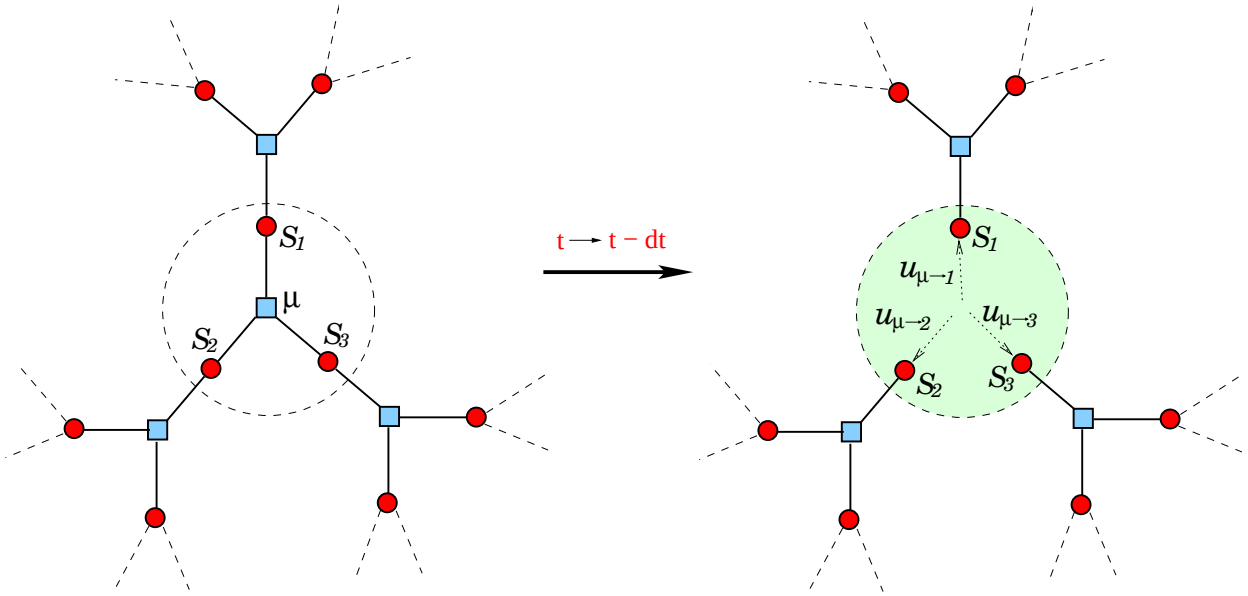



Figure 6.1: Erasure of a clause and corresponding injection of balancing fields for the particular case of function nodes of degree three.

in the calculated expressions for any finite size graph. Moreover, our proofs will be restricted to the $p$-spin model the the $K$-SAT with even $p$. In the cases of odd $p$ the same bound would hold if one could rely on some physically reasonable assumptions on the overlap distribution (see below). Our analysis will start from the TAP (Cavity) equations for the models [181, 23], and their probabilistic solutions implied by the cavity, or equivalently the replica method at various degrees of approximation. We will consider in particular the replica symmetric (RS) and one step replica symmetry broken solutions, but it should be clear from our analysis how to generalize to more steps of replica symmetry breaking. In the TAP/cavity equations one singles out the contribution of the clauses and the sites to the free-energy and defines cavity fields $h_i^{(\mu)}$ and $u_\mu^{(i)}$ respectively as the local field acting on the spin $i$ in absence of the clause $\mu$ and the local field acting on $i$ due to the presence of the clause $\mu$ only. If we define $Z_N[S_i]$ as the partition function of a given sample with $N$ spins where all but the spin $i$ are integrated, $F_{N,-i}$ the free-energy of the corresponding systems where the spin $S_i$ and all the clauses it belongs to are removed, we can write,

$$\begin{aligned} Z_N[S_i] &= e^{-\beta F_{N,-i}} \prod_{\mu \in T_i} \sum_{S_{i_2^\mu},\ldots,S_{i_p^\mu}} e^{-\beta H_{J(\mu)}(S_{i^\mu},S_{i_2^\mu},\ldots,S_{i_p^\mu}) + \sum_{l=2}^{p} h_{i_l^\mu}^{(\mu)} S_{i_l^\mu}} \\ &= e^{-\beta F_{N,-i}} \prod_{\mu \in T_i} B_\mu^{(i)} e^{\beta u_\mu^{(i)} S_i} \end{aligned} \tag{6.8}$$

where $T_i$ is the set of clauses containing the spin $i$, and the constant $B_\mu^{(i)} = e^{-\beta \Delta F_\mu^{(i)}}$ can be interpreted as suitable shifts in the free-energy due to the contribution of the clause $\mu$ for fixed value of the spin $i$. We notice that denoting $J^\mu$ as $J$, and renaming the fields in (6.8) into $h_1, \ldots, h_{p-1}$, eq. (6.8) defines functions

$$u_J(h_1, \ldots, h_{p-1}) \text{ and } B_J(h_1, \ldots, h_{p-1}) \,. \tag{6.9}$$

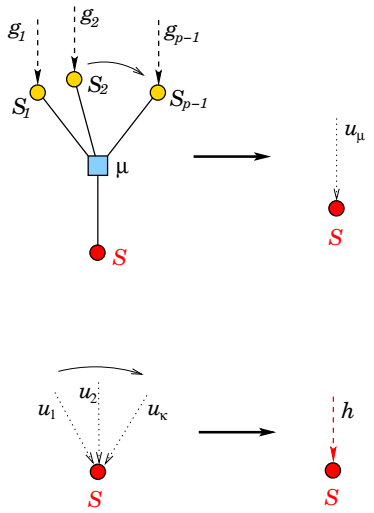



Figure 6.2: Diagrammatic representation of the relations for $g$, $u$ and $h$ fields acting on spin $S$. The cavity solution closes under the condition $g \to h$. The hyper-edge interaction is drawn in the factor-graph notation.

The equation are closed by the self-consistent condition:

$$h_i^{(\mu)} = \sum_{\nu \in \{T_i - \mu\}} u_\nu^{(i)} \tag{6.10}$$

These equations are at the basis of iterative algorithms such as the "belief propagation" or "sum-product" know for a long time in statistical inference [160] and coding theory [141] and the more recently proposed algorithm of "survey propagation"[30]. Conditions (6.8) and (6.10) can be diagrammatically represented as in fig.(6.2). The cavity fields solutions of (6.8,6.10) are random variables which fluctuate for two reasons [2, 23, 24]. First, they differ from sample to sample. Second, within the same sample the equations can have several solutions which can level-cross. The cavity/replica method provides under certain assumption probabilistic solutions. In the RS approximation, one just supposes a single solution to give the relevant contribution in a given sample. The sample to sample fluctuation induce probability distributions $P(h)$ and $Q(u)$ whose relations implied by (6.8,6.10) are:

$$P(h) = \sum_k e^{-\alpha p} \frac{(\alpha p)^k}{k!} \int du_1\, Q(u_1) ... du_k\, Q(u_k) \delta(h - \sum_{i=1}^k u_k) \tag{6.11}$$

$$Q(u) = \int dh_1\, P(h_1) ... dh_{p-1}\, P(h_{p-1}) \langle \delta(u - u_J(h_1, ..., h_{p-1})) \rangle_J \tag{6.12}$$

where $\langle \cdot \rangle_J$ denotes the average over the random variables appearing in a clause. In addition to sample to sample fluctuations, the 1RSB solution assumes fluctuations of the fields from solution to solution of the equations, so that the functions $P(h)$ and $Q(u)$ will be themselves randomly distributed according to some functional probability distributions $\mathcal{P}(P)$ and $\mathcal{Q}(Q)$ related by the self-consistency equations [12]

$$\mathcal{Q}(Q) = \int \mathcal{D}P_1 \mathcal{P}(P_1) ... \mathcal{D}P_{p-1} \mathcal{P}(P_{p-1}) \langle \delta(Q(\cdot) - Q(\cdot | P_1, ..., P_{p-1}, J)) \rangle_J \tag{6.13}$$

$$\mathcal{P}(P) = \sum_{k=0}^{\infty} e^{-\alpha p} \frac{(\alpha p)^k}{k!} \int \prod_{l=1}^{k} \mathcal{D}Q_l \mathcal{Q}(Q_l) \delta(P(\cdot) - P(\cdot|Q_1, ..., Q_k)) \tag{6.14}$$

where:

$$\begin{aligned} Q(u|P_1, ..., P_{p-1}, H) &= \mathcal{N}_P[P_1, ..., P_{p-1}] \int dh_1 \; P_1(h_1) ... dh_{p-1} \; P_1(h_{p-1}) B_{\mathbf{J}}(h_1, ..., h_{p-1})^m \cdot \\ &\quad \delta(u - u_{\mathbf{J}}(h_1, ..., h_{p-1})) \end{aligned} \tag{6.15}$$

$$\begin{aligned} P(h|Q_1, ..., Q_k) &= \mathcal{N}_{Q,k}[Q_1, ..., Q_k] \; (2\cosh(\beta h))^m \int \prod_{l=1}^{k} du_l \; \frac{Q_l(u_l)}{(2\cosh(\beta u_l))^m} \cdot \\ &\quad \delta(h - \sum_{l=1}^{k} u_l) \end{aligned} \tag{6.16}$$

where $\mathcal{N}_{Q,k}[Q_1, ..., Q_k]$ and $\mathcal{N}_G[G_1, ..., G_{p-1}]$ insure normalization and $B_{\mathbf{J}}(g_1, ..., g_{p-1})$ is a rescaling term of the form (6.9) that can be re-absorbed in the normalization in the case of the $p$-spin model. Its form for the $K$-SAT case is given in the appendix. $m$ is a number in the interval $(0, 1]$, which within the formalism selects families of solutions at different free-energy levels. The physical free-energy is estimated maximizing over $m$.

The interpretation of these equations has been discussed many times in the literature [2, 23, 24]. We will show here, that such choices in the field distributions result in lower bounds for the free-energy analogous to the ones first proved by Guerra in fully connected models. In order to prove these bounds, we will have to consider auxiliary models where the number of clauses $\alpha N$ will be reduced to $\alpha t N$ $(0 \leq t \leq 1)$, while this reduction will be compensated in average by some external field terms of the kind:

$$\mathcal{H}_{ext}^{(t)} = \sum_i \sum_{l_i=1}^{k_i} u_i^{l_i} S_i \tag{6.17}$$

where the numbers $k_i$ will be i.i.d. Poissonian variables with average $\alpha p(1-t)$. The diagrammatic picture is similar to the cavity one, as seen in

As the notation suggests, the fields $u_i^l$ will play the role of the cavity fields $u_\mu^{(i)}$ of the TAP approach, and they will be i.i.d. random variables with suitable distribution. Indeed, for each field $u_i^{l_i}$ we will chose in an independent way $p-1$ primary fields $g_i^{l_i,n}$ $(n = 1, ..., p-1)$ and clause variables $J_i^{l_i,n}$ such that the relation

$$u_i^{l_i} = u_{J_i^{l_i,n}}(g_i^{l_i,1} ... g_i^{l_i,p-1}) \tag{6.18}$$

is verified. Notice that the compound Hamiltonian

$$\mathcal{H}_{tot}^{(t)}[\mathbf{S}] = \mathcal{H}^{(\alpha t)}[\mathbf{S}] + \mathcal{H}_{ext}^{(t)}[\mathbf{S}] \tag{6.19}$$

will constitute a sample with the original distribution for $t = 1$, while it will consist in a system of non interacting spins for $t = 0$. The key step of the procedure, consists in the choice of the distribution of the primary fields $g_i^{l_i}$. We will also find useful to define fields $h_i$ verifying

$$h_i = \sum_{l=1}^{k_i} u_i^l. \tag{6.20}$$

The field $u$ are related to the $g$'s by a relation similar to (6.8), while the $h$'s are related to the $u$'s by a relation similar to (6.10). Of course, the statistics of the fields $h$ and the $g$'s

do coincide in the TAP approach. It is interesting to note that the bounds we will get, are optimized precisely when their statistical ensemble coincide. As we mentioned, various Replica bounds are obtained assuming for the fields $g_i^{l_i}$ the type of statistics implied by the different replica solution. So, the Replica Symmetric bound is got just supposing the field as quenched variables completely independent of the quenched disorder and with distribution $G(g)$. For the one-step RSB bound on the other hand the distribution $G$ will itself be considered as random, subject to a functional probability distribution $\mathcal{G}[G]$. More complicated RSB estimates, not considered in this chapter, can be obtained along the same lines. The case of the fully connected models considered by Guerra can be formalized in this way where the various field distributions involved are Gaussian.

### 6.1.3 The RS bound

We consider in this case i.i.d. fields $u$ and $h$ distributed according probabilities $Q(u)$ and $P(h)$ verifying the following relation with the distribution $Q(g)$ of the primary fields.

$$\begin{aligned} Q(u) &= \int dg_1\, G(g_1)...dg_{p-1}\, G(g_{p-1})\langle\delta(u - u_J(g_1, ..., g_{p-1}))\rangle_J && (6.21)\\ P(h) &= P(h|k)\pi(k, \alpha p(1-t)) && (6.22)\\ P(h|k) &= \int du_1\, Q(u_1)...du_k\, Q(u_k)\delta(h - \sum_{i=1}^{k} u_k) && (6.23) \end{aligned}$$

The distribution $G(g)$ will be chosen to be symmetric under change of sign of $g$, and regular enough for all the expression below to make sense. The RS bound can now be obtained following a procedure to the one of Guerra for the SK model, and considering the $t$ dependent free-energy; with obvious notation:

$$F(t) = \lim_{N\to\infty} F_N(t) = \lim_{N\to\infty} -\frac{1}{\beta N} E \log Z_N(t) \tag{6.24}$$

where $E$ represents the average over all the quenched variables, the one defining the clauses and the external fields. We then consider the $t$ derivative of $F_N$

$$\frac{d}{dt}F_N(t) = -\frac{1}{N\beta}\frac{d}{dt}E(\log Z_N). \tag{6.25}$$

As in [60] we will then write

$$F(1) = F(0) + \int_0^1 dt\, \frac{d}{dt}F(t) \tag{6.26}$$

and show, by an explicit computation, that, up to $O(1/N)$ terms that will be systematically neglected, the expression coincides with the variational RS free-energy plus a remainder. In fortunate cases this term will have negative sign and neglecting it will immediately result in a lower bound for the free-energy. This happens in the Viana-Bray model, the $p$-spin and the $K$-SAT for even $p$. In the cases of odd $p$ we were not able to prove the sign definiteness of the remainder, although as we will discuss we believe this to be the case on a physical basis.

The time derivative of $F$ take contributions from the derivative of the distribution of the number of clauses $M$

$$\frac{d\pi(M, \alpha t N)}{dt} = -N\alpha(\pi(M, \alpha t N) - \pi(M-1, \alpha t N)) \tag{6.27}$$

and the distribution of the number of $u$ fields on each site

$$\frac{d\pi(k_i, \alpha p(1-t))}{dt} = \alpha p(\pi(k_i, \alpha p(1-t)) - \pi(k_i - 1, \alpha p(1-t))) \tag{6.28}$$

so that:

$$\begin{aligned}\frac{d}{dt}E\log Z(t) = \quad & -N\alpha \sum_M (\pi(M, \alpha t N) - \pi(M-1, \alpha t N))E' \log Z(t) \\ & +\alpha p \sum_i \sum_{k_i} (\pi(k_i, \alpha p(1-t)) - \pi(k_i - 1, \alpha p(1-t)))E_i'' \log Z(t)\end{aligned} \tag{6.29}$$

where we have denoted as $E'$ the average with respect to all the quenched variables except $M$ and with $E_i''$ the average with respect to all the quenched variables except $k_i$, and simply $Z(t)$ the partition function of the $N$ spin system $Z_N(t)$.

In the first term of (6.29) we can single out the $M$-th clause, and write

$$Z(t) = Z_{-M}(t)\omega(e^{-\beta H_M(S_{i_1^M}, \ldots, S_{i_p^M})})_{-M} \ , \tag{6.30}$$

where by $Z_{-M}(t)$ we denote the partition function of the system in absence of the $M$-th clause, and $\omega(\cdot)_{-M}$ is the canonical average in absence of the $M$-th clause. In the following terms we single out the $k_i$-th field $u$ term, $Z(t) = Z_{-u_i^{k_i}}(t)\omega(e^{\beta u_i^{k_i} S_i})_{-u_i^{k_i}}$, where $Z_{-u_i^{k_i}}(t)$ is the partition function in absence of the field $-u_i^{k_i}$ and analogously for the average $\omega(\cdot)_{-u_i^{k_i}}$. Finally, rearranging all terms we find

$$\begin{aligned}\frac{d}{dt}E\log Z(t) = \quad & N\alpha \sum_M (\pi(M-1, \alpha t N))E' \log[\omega(e^{-\beta H_{J(M)}(S_{i_1^M}, \ldots, S_{i_p^M})})_{-M})] \\ & -p\alpha \sum_i \sum_{k_i} \pi(k_i - 1, \alpha p(1-t))E_i'' \log[\omega(e^{\beta u_i^{k_i} S_i})_{-u_i^{k_i}}].\end{aligned} \tag{6.31}$$

where we have used $\sum_M \pi(M-1, \alpha t N)E' \log Z_{-M} = \sum_{k_i} \pi(k_i - 1, \alpha p(1-t))E_i'' \log Z_{-u_i^{k_i}} = E\log Z$. We notice at this point that the statistical ensemble defined by $\pi(M-1, \alpha t N))E'$ can be substituted with the original one $E$ and the average of the variables appearing in the clause we have singled out. To be more precise, we remark that the average $\omega(\cdot)$ depends on the quenched variables $D = \{\mathbf{J}, \mathbf{u}\}$ appearing in the Hamiltonian. Writing explicitly this dependence as $\omega(\cdot|D)$, and denoting as $D_{-M}$ all the quenched variables except the ones appearing in the $M$-th clause, our statement is that thanks to the Poissonian distribution of $M$ and the uniform choice of the indices of each clause,

$$\sum_M (\pi(M-1, \alpha t N))E' \log[\omega(e^{-\beta H_{J(M)}(S_{i_1^M}, \ldots, S_{i_p^M})}|D_{-M})] = \tag{6.32}$$

$$E\left(\frac{1}{N^p}\sum_{i_1, \ldots, i_p} \langle \log[\omega(e^{-\beta H_J(S_{i_1}, \ldots, S_{i_p})}|D)]\rangle_J\right).$$

where by $\langle\cdot\rangle_J$ we denote the average with respect to the random variables appearing in the clause. This is a crucial step in our analysis, in fact, similar considerations apply to the term in the second line of (6.31), which can be written as

$$\sum_{k_i} \pi(k_i - 1, \alpha p(1-t))E_i'' \log[\omega(e^{\beta u_i^{k_i} S_i})_{-u_i^{k_i}}] = \quad E\left\langle \log\omega\left(e^{\beta u S_i}\right)\right\rangle_u \ . \tag{6.33}$$

The same kind of averages $E$ and $\omega$ appear in the two terms which can be therefore directly compared as we will do in the next section. This property, linked to the Poissonian character of the graph defined by the model would not hold for other ensembles of random graphs and the analysis would be technically more involved. Substituting in (6.31) we find:

$$\frac{1}{N}\frac{d}{dt}E\log Z(t) = \alpha E\left[\frac{1}{N^p}\sum_{i_1,\ldots,i_p}\langle\log[\omega(e^{-\beta H(S_{i_1},\ldots,S_{i_p})})]\rangle_H - \frac{p}{N}\sum_i\langle\log\omega(e^{\beta u S_i})\rangle_u\right] \tag{6.34}$$

Rearranging terms and using (6.26) we finally find that the free-energy $F_N$ can be written as

$$F_N = F_{var}[G] + \int_0^1 dt\; R_{RS}[G,t] + O(1/N) \tag{6.35}$$

where $F_{var}[G]$ coincides the expression of the variational free-energy in the replica treatment under condition $G[h] = P[h]\ \forall\ h$ at $t = 0$ and $\int_0^1 dt\; R_{RS}[G,t]$ is a remainder term. Instead of writing the formulae for general clauses, in order to keep the notations within reasonable simplicity, we specialize now to the specific cases of the $p$-spin model and the $K$-SAT. Notice that in all models

$$F[0] = -\frac{1}{\beta}\langle\log(2\cosh(\beta h))\rangle_h|_{t=0} \tag{6.36}$$

### $p$-spin

In the case of the $p$-spin $H_J(S_{i_1},...,S_{i_p}) = J\,S_{i_1}\cdot\ldots\cdot S_{i_p}$. Substituting in eq.(6.34) and rearranging terms one immediately finds:

$$\begin{aligned} F_{var}^{p-spin}[G] \;=\; & \frac{1}{\beta}\left[\alpha\left(p\left\langle\log(\cosh\beta u)\right\rangle_u - \left\langle\log(\cosh\beta J)\right\rangle_J\right) - \left\langle\log(2\cosh\beta h)\right\rangle_h + \right. \\ & \left.\alpha(p-1)\left\langle\log\left(1+\tanh(\beta J)\prod_{t=1}^{p}\tanh(\beta g_t)\right)\right\rangle_{\{g_t\},J}\right] \end{aligned} \tag{6.37}$$

while the remainder is the $t$ integral of

$$\begin{aligned} R_{RS}^{p-spin}[G,t] = \quad & -\frac{\alpha}{\beta}\left[\frac{1}{N^p}\sum_{i_1,\ldots,i_p}E\left\langle\log(1+\tanh(\beta J)\omega(S_{i_1}\ldots S_{i_p}))\right\rangle_J - \right. \\ & pE\left\langle\log(1+\tanh(\beta u)\omega(S_i))\right\rangle_u + \\ & \left.(p-1)E\left\langle\log(1+\tanh(\beta J)\prod_{t=1}^{p}\tanh(\beta g_p))\right\rangle_{\{g_t\},J}\right]. \end{aligned} \tag{6.38}$$

The expression for $F_{var}^{p-spin}[G]$ coincides with the RS free energy once extremized over the variational space of probability distributions, as proven in the appendix. Terms have been properly added and subtracted in order to get a remainder which equal to zero if maximization over $G$ is taken, and the temperature is high enough for replica symmetry to be exact [180]. As we will see, the remainder turns out to be positive. $F_{var}^{p-spin}[G]$ is therefore, for all $G$ for which its expression makes sense, a lower bound to the free-energy. At saturation the condition

$$G[h] = P[h]|_{t=0}\ \forall\ h \tag{6.39}$$

should hold, which is simply the self-consistency RS equation.

By using equation

$$E\left\langle \log(1+\tanh(\beta u)\omega(S_i))\right\rangle_u = E\left\langle \log(1+\tanh(\beta J)\prod_{t=1}^{p-1}\tanh(\beta g_r)\omega(S_i))\right\rangle_{\{g_t\},J} \tag{6.40}$$

we can establish that the remainder is positive for even $p$. We expand the logarithm of the three terms in (absolutely converging) series of $\tanh(\beta J)$, and notice that thanks to the parity of the $J$ and the $g$ distributions, they will just involve negative terms. We can then take the expected value of each terms and write

$$R_{RS}^{p-spin}[G,t] = \frac{1}{\beta}\sum_{n=0}^{\infty}\langle\tanh^{2n}\beta J\rangle_J \frac{1}{n}\Omega\left[(q^{(2n)})^p - pq^{(2n)}\langle\tanh^{2n}\beta g\rangle_g^{p-1} + (p-1)\langle\tanh^{2n}\beta g\rangle_g^p\right] \tag{6.41}$$

where we have introduced the overlap $q^{(l)}$ and the replica measure $\Omega$ defined in section 2. The series in (6.41) is an average of positive terms in the case of the Viana-Bray model $p=2$, where we get perfect squares, and more in general for all even $p$, as we can easily, starting from the observation that in this case $x^p - pxy^{p-1} + (p-1)y^p$ is positive or zero for all $x = q^{(2n)}$ ,$y = \langle\tanh^{2n}\beta J\rangle_J$ real.

In the case of $p$ odd, the same term is positive only if $x$ is itself positive or zero. The bound of the free-energy would therefore be established if we were able to prove that the probability distributions of the $q^{(2n)}$ has support on the positives.[1] This property, which tells that anti-correlated states are not possible, is physically very sound whenever the Hamiltonian is not symmetric under change of sign of all spins. In fact, one expects the probability of negative values of the overlaps to be exponentially small in the size of the system for large $N$. Unfortunately however we have not been able to prove this property in full generality. Notice that upon maximization on $G$, the results of [180] imply that the remainder is exactly equal to zero if the temperature is high enough for replica symmetry to hold.

### $K$-SAT

In the case of the $K$-SAT, using def.(6.3) for the clause $H$, we find relation:

$$u_{\mathbf{J}}(h_1,...,h_{p-1}) \equiv u_J(\{J_t\},\{h_t\}) = \frac{J}{\beta}\tanh^{-1}\left[\frac{\frac{\xi}{2}\prod_{t=1}^{p-1}\left(\frac{1+J_t\tanh(\beta h_t)}{2}\right)}{1+\frac{\xi}{2}\prod_{t=1}^{p-1}\left(\frac{1+J_t\tanh(\beta h_t)}{2}\right)}\right], \tag{6.42}$$

where $\xi \equiv e^{-\beta}-1<0$. Via direct inspection, the variational free-energy coincides with the RS expression [9]

$$\begin{aligned} F_{var}^{K-SAT}[G] \;=\; & \frac{1}{\beta}\left[\alpha(p-1)\left\langle\log\left(1+(e^{-\beta}-1)\prod_{t=1}^{p}\left(\frac{1+\tanh(\beta g_t)}{2}\right)\right)\right\rangle_{\{g_t\},\{J_t\}} - \right. \\ & \langle\log(2\cosh(\beta h))\rangle_h + \alpha p\langle\log(2\cosh(\beta u))\rangle_u - \\ & \left.\alpha p\left\langle\log\left(1+\frac{(e^{-\beta}-1)}{2}\prod_{t=1}^{p-1}\left(\frac{1+\tanh(\beta g_t)}{2}\right)\right)\right\rangle_{\{g_t\},\{J_t\}}\right] \end{aligned} \tag{6.43}$$

[1] A different sufficient condition for the series to have positive terms is that $|q^{(2n)}| \geq \langle\tanh(\beta g)^{2n}\rangle_g$, but it is not clear its physical meaning.

while the remainder is the $t$ integral of

$$\begin{aligned} R_{RS}^{K-SAT}[G,t] &= -\frac{\alpha}{\beta}E\left[\frac{1}{N^p}\sum_{i_1,\dots,i_p}\left\langle\log\left(1+(e^{-\beta}-1)\omega(\prod_{t=1}^{p}\frac{1+J_tS_{i_t}}{2})\right)\right\rangle_{\{J_t\}} - \right. \\ &\frac{p}{N}\sum_i\left\langle\log\left(1+\xi\omega\left(\frac{1+JS_i}{2}\prod_{t=1}^{p-1}\frac{1+J_t\tanh(\beta g_t)}{2}\right)\right)\right\rangle_{\{g_t\},J,\{J_t\}} + \\ &\left.(p-1)\left\langle\log\left(1+\xi\prod_{t=1}^{p}\frac{1+J_r\tanh(\beta g_t)}{2}\right)\right\rangle_{\{g_t\},\{J_t\}}\right]. \end{aligned} \tag{6.44}$$

Considerations analogous to the case of the $p$-spin, have led us to add and subtract terms from eq.(6.34) to single out the proper remainder term. Expanding in series the logarithms, exploiting the symmetry of the probabilities distribution functions and taking the expectation of each term of the absolutely convergent series we finally obtain:

$$R_{RS}^{K-SAT}[G,t] = \frac{\alpha}{\beta}\sum_{n\geq 1}\frac{(-1)^n}{n}(\xi^*)^n\Omega\left[\tilde{R}(Q_n,p)\right] \tag{6.45}$$

with

$$\tilde{R}(Q_n,p) = (1+Q_n)^p - p(1+Q_n)\langle(1+J\tanh(\beta g))^n\rangle_{J,g}^{p-1} + (p-1)\langle(1+J\tanh(\beta g))^n\rangle_{J,g}^{p} \tag{6.46}$$

where we have defined $\xi^* \equiv \xi/(2^p) < 0$ and $Q_n \equiv \sum_{l=1}^{n}\langle J^l\rangle_J \sum_{a_1<\dots<a_l}^{1,n} q^{a_1\dots a_l}$. Detailed calculations are given in the appendix. As in the $p$-spin case, the previous sum is obviously positive for $p$ even. For $p$ odd we should again rely on the physical wisdom that all $q^{(a_1,\dots,a_l)}$ have positive support and so have the functions $1+Q_n \geq 0$. Again, the variational free-energy coincides with the RS expression once extremized over $G$ at the condition $P = G$ at $t = 0$.

### 6.1.4 The 1RSB Bound

We establish here a more complex estimate, in a larger variational space of functional probability distributions. The general strategy will be here to consider the same form for the auxiliary Hamiltonian, but now with a more involved choice for the fields distribution. The fields on different sites or different index $l_i$ will be still independent, but each site field distribution $G_i^{l_i}(g_i^{l_i})$ will be itself random i.i.d., chosen with a probability density functional $\mathcal{G}[G]$, with support on symmetric distributions $G(-g) = G(g)$. It will be assumed that $\mathcal{G}$ is such that all the expressions below make sense. In this case, the variational approximation for the free-energy will be obtained from an estimate of

$$-\beta F_N[m,t] = \frac{1}{mN}E_1\log E_2(Z^m(t)) \tag{6.47}$$

where we have denoted with:

- $E_2$ the average w.r.t. $g_i^{l_i,n}$ for fixed distributions $G_i^{l_i,n}$ according to the measure

$$C\prod_{i=1}^{N}\prod_{l_i=1}^{k_i}\prod_{n=1}^{p-1}dg_i^{l_i,n}\,G_i^{l_i,n}(g_i^{l_i,n})\left(\frac{B_{J_i^{l_i,n}}(g_i^{l_i,1}\dots g_i^{l_i,p-1})}{2\cosh(\beta u_{J_i^{l_i,n}}(g_i^{l_i,1}\dots g_i^{l_i,p-1}))}\right)^m \tag{6.48}$$

  where $C$ ensures the normalization.

- $E_1$ the average with respect to the quenched clause variable, distributions the $G_i^{l_i}$'s and the Poissonian variables $k_i$'s, which will be i.i.d. with probabilities $\mu(J)$, $\mathcal{G}(G_i^{l_i})$ and $\pi(k_i,(1-t)\alpha)$ respectively.

The number $m$ is real in the interval (0,1]. The statistical ensemble of the auxiliary fields $u$ and $h$ will be now related to the one of the $g$ by:

$$\mathcal{Q}(Q)=\int \mathcal{D}G_1\mathcal{G}(G_1)...\mathcal{D}G_{p-1}\mathcal{G}(G_{p-1})\langle\delta(Q(\cdot)-Q(\cdot|G_1,...,G_{p-1},J))\rangle_J \tag{6.49}$$

$$\mathcal{P}(P)=\sum_{k=0}^{\infty}e^{-\alpha p(1-t)}\frac{(\alpha p(1-t))^k}{k!}\int\prod_{l=1}^{k}\mathcal{D}Q_l\mathcal{Q}(Q_l)\delta(P(\cdot)-P(\cdot|Q_1,...,Q_k)) \tag{6.50}$$

where:

$$\begin{aligned}Q(u|G_1,...,G_{p-1},J) &= \mathcal{N}_G[G_1,...,G_{p-1}]\int dg_1\,G_1(g_1)...dg_{p-1}\,G_1(g_{p-1})B_J(g_1,...,g_{p-1})^m\cdot\\ &\quad \delta(u-u_J(g_1,...,g_{p-1}))\end{aligned} \tag{6.51}$$

$$\begin{aligned}G(g|Q_1,...,Q_k) &= \mathcal{N}_{Q,k}[Q_1,...,Q_k]\,(2\cosh(\beta g))^m\int\prod_{l=1}^{k}du_l\,\frac{Q_l(u_l)}{(2\cosh(\beta u_l))^m}\\ &\quad \delta(g-\sum_{l=1}^{k}u_l)\end{aligned} \tag{6.52}$$

where $\mathcal{N}_{Q,k}[Q_1,...,Q_k]$, $\mathcal{N}_G[G_1,...,G_{p-1}]$ and $B_J(g_1,...,g_{p-1})$ have been previously defined. With notations similar to the ones of the RS case, we can write

$$\frac{d}{dt}(-\beta F_N[m,t])=-\alpha\sum_M(\pi(M,\alpha tN)-\pi(M-1,\alpha tN))E_1'\frac{1}{Nm}\log E_2Z(t)^m+ \tag{6.53}$$

$$\frac{\alpha p}{N}\sum_i\sum_{k_i}(\pi(k_i,\alpha p(1-t))-\pi(k_i-1,\alpha p(1-t)))E_{1,i}''\frac{1}{Nm}\log E_2Z(t)^m$$

which, extracting explicitly the contribution from the $M$-th close in the first term and the $k_i$-th field $u$ in the second, following considerations similar to the RS case we find:

$$\frac{d}{dt}(-\beta F_N[m,t])=\alpha\sum_M(\pi(M-1,\alpha tN))\frac{1}{m}E_1'\log\left[\frac{E_2Z_{-M}^m\omega(e^{-\beta H_{J(\mu)}(S_{i_1^M},...,S_{i_p^M})})_{-M}^m}{E_2Z_{-M}^m}\right]-$$

$$\frac{p\alpha}{N}\sum_i\sum_{k_i}\pi(k_i-1,\alpha p(1-t))\frac{1}{m}E_{1,i}''\log\left[\frac{E_2Z_{-u_i^{k_i}}^m\omega(e^{\beta u_i^{k_i}S_i})_{-u_i^{k_i}}^m}{E_2Z_{-u_i^{k_i}}^m}\right]. \tag{6.54}$$

Again it can be recognized that the primed averages coincide with the averages over the original ensembles plus the averages on the variables appearing in the terms we extracted. Finally we get:

$$\begin{aligned}\frac{d}{dt}(-\beta F_N[m,t]) &= \frac{\alpha}{m}E_1\left[\frac{1}{N^p}\sum_{i_1,...,i_p}\left\langle\log\left(\frac{E_2Z^m\omega(e^{-\beta H_J(S_{i_1},...,S_{i_p})})^m}{E_2Z^m}\right)\right\rangle_J\right.\\ &\quad \left.-\frac{p}{N}\sum_i\left\langle\log\left(\frac{E_2Z^m\langle\omega(e^{\beta uS_i})^m\rangle_u}{E_2Z^m}\right)\right\rangle_Q\right].\end{aligned} \tag{6.55}$$

Rearranging all terms one finds the estimate:

$$F_N = F_{var}[\mathcal{G}] + \int_0^1 dt\; R_{1RSB}[\mathcal{G}, t] + O(1/N) \tag{6.56}$$

where this time $F_{var}[\mathcal{G}]$ coincides with $F_{1RSB}[\mathcal{G}]$, the expression of the variational free-energy in the 1RSB treatment at the saddle point $\mathcal{G} = \mathcal{P}$ at $t = 0$, and $\int_0^1 dt\; R_{1RSB}[\mathcal{G}, t]$ is the remainder. Notice that the derivation immediately suggests how to generalize the analysis to more steps of replica symmetry breaking. Let us now specialize the formulae for the $p$-spin model and the $K$-SAT. Again, in this case we will need the expression for $F[0]$:

$$F[0] = \frac{1}{\beta m}\left[\left\langle \log\left\langle \left(\frac{1}{2\cosh(\beta h)}\right)^m \right\rangle_h \right\rangle_P\right]_{|_{t=0}} . \tag{6.57}$$

### $p$-spin

In this case, plugging def.(6.2) in eq.(6.55) rearranging, adding and subtracting terms one finds:

$$\begin{aligned} F_{var}^{p-spin}[\mathcal{G}] \;=\; & \frac{1}{\beta m}\left[\left\langle \log\left\langle \left(\frac{1}{2\cosh(\beta h)}\right)^m \right\rangle_h \right\rangle_P - \right. \\ & \alpha m \left\langle \log(2\cosh(\beta J))\right\rangle_J \alpha p \left\langle \log\left\langle \left(\frac{1}{2\cosh(\beta u)}\right)^m \right\rangle_u \right\rangle_Q + \\ & \left. \alpha(p-1)\left\langle \log\left\langle (1+\tanh(\beta J)\tanh(\beta g_1)...\tanh(\beta g_p))^m \right\rangle_{g_1,...,g_p} \right\rangle_{G_1,...,G_p;J}\right] \end{aligned} \tag{6.58}$$

while the remainder is the $t$ integral of

$$\begin{aligned} R_{1RSB}^{p-spin}[\mathcal{G}, t] = \quad & -\frac{\alpha}{\beta m} E_1 \left[\frac{1}{N^p}\sum_{i_1,...,i_p}\left\langle \log\left(\frac{E_2 Z^m (1+\omega(S_{i_1}...S_{i_p})\tanh(\beta J))^m}{E_2 Z^m}\right)\right\rangle_J - \right. \\ & \frac{p}{N}\sum_i \left\langle \log\left(\frac{E_2 Z^m \left\langle (1+\omega(S_i)\tanh(\beta u))^m\right\rangle_u}{E_2 Z^m}\right)\right\rangle_Q + \\ & \left. (p-1)\left\langle \log\left\langle (1+\tanh(\beta J)\tanh(\beta g_1)...\tanh(\beta g_p))^m \right\rangle_{g_1,...,g_p}\right\rangle_{G_1,...,G_p;J}\right] \end{aligned} \tag{6.59}$$

The expression for $F_{var}^{p-spin}[\mathcal{G}]$ coincides with the 1RSB free-energy, as proven in the appendix. once maximized over the variational space of probability distribution functionals $\mathcal{G}$. The maximization condition reads:

$$\mathcal{G}[P] = \mathcal{P}[P]\;|_{t=0}\;\forall\; P\;, \tag{6.60}$$

which is simply the self consistency 1RSB condition. For even $p$ (and in particular for $p = 2$ that corresponds to the Viana-Bray case), one can check that the remainder is positive just expanding the logarithm in series and exploiting the parity of the $J$ and the $g$ distributions. As this is considerably more involved then in the RS case, we relegate this check to appendix A.

### $K$-SAT

In the $K$-SAT case the expression for function $B_{\mathbf{J}}(h_1, ..., h_{p-1})$ reads:

$$B_{\mathbf{J}}(h_1, ..., h_{p-1}) \equiv B(\{J_t\}, \{h_t\}) = 1 + \frac{\xi}{2}\prod_{t=1}^{p-1}\left(\frac{1 + J_t \tanh(\beta h_t)}{2}\right)\;, \tag{6.61}$$

while the corresponding one for $u_{\mathbf{J}}(h_1, ..., h_{p-1})$ is the same as in the RS case. The corresponding replica free-energy and remainder read

$$\begin{aligned} F_{var}^{K-SAT}[\mathcal{G}] &= \frac{1}{m\beta}\Bigg[\alpha(p-1)\left\langle \log\left\langle\left(1+\xi\prod_{t=1}^{p}\left(\frac{1+J_t\tanh(\beta g_t)}{2}\right)\right)^m\right\rangle_{\{g_t\}}\right\rangle_{\{G_t\},\{J_t\}} - \\ &\quad \alpha p\left\langle \log\left\langle\left(\frac{B(\{J_t\},\{g_t\})}{2\cosh(\beta u_J(\{J_t\},\{g_t\}))}\right)^m\right\rangle_{\{g_t\}}\right\rangle_{\{G_t\},\{J_t\},J} + \\ &\quad \left\langle \log\left\langle\left(\frac{1}{2\cosh(\beta h)}\right)^m\right\rangle_h\right\rangle_P\Bigg] \end{aligned} \tag{6.62}$$

The remainder is the $t$ integral of

$$\begin{aligned} R_{1RSB}^{K-SAT}[\mathcal{G},t] &= -\frac{\alpha}{\beta m}E_1\Bigg[\frac{1}{N^p}\sum_{i_1,...,i_p}\left\langle \log\left(\frac{E_2 Z^m\left(1+\xi\omega\left(\prod_{t=1}^{p}\frac{1+J_tS_{i_t}}{2}\right)\right)^m}{E_2 Z^m}\right)\right\rangle_{\{J_t\}} - \\ &\quad \frac{p}{N}\sum_i\left\langle \log\left(\frac{E_2 Z^m\left\langle\left(1+\xi\frac{1+J\omega(S_i)}{2}\prod_{t=1}^{p-1}\frac{1+J_t\tanh(\beta g_t)}{2}\right)^m\right\rangle_{\{g_t\}}}{E_2 Z^m}\right)\right\rangle_{\{G_t\},\{J_t\},J} + \\ &\quad (p-1)\left\langle \log\left\langle\left(1+\xi\prod_{t=1}^{p}\left(\frac{1+J_t\tanh(\beta g_t)}{2}\right)\right)^m\right\rangle_{\{g_t\}}\right\rangle_{\{G_t\},\{J_t\}}\Bigg] \end{aligned} \tag{6.63}$$

The expression for $F_{var}^{K-SAT}[\mathcal{G}]$ coincides with the 1RSB free energy once extremized under condition (6.60), with the corresponding $K$-SAT probability distribution functionals. Notice that The proof of the positivity of (6.63) for even $p$ is again dove via series expansion, all the detail are explained in Appendix B.

At this point we can take the zero temperature limit, finding that the resulting expression gives us a lower bound for the ground-state energy of the system, i.e. the minimal number of unsatisfied clauses. Notice that the $T \to 0$ limit of the replica free-energy is not trivial. The necessary assumptions on the field distributions to get it correct are well known in the physical literature, and have been recently reviewed in [24]. Recently Mézard, Parisi and Zecchina [30] have worked out the $K$-SAT 1RSB solution for $p = 3$ predicting a non zero ground-state energy for values of $\alpha$ above a satisfiability threshold of $\alpha_c = 4.256$, very well in agreement with the numerical simulations. Our results, together with the additional hypothesis of positivity of the support of the overlap functions imply that this value is an upper bound to the true threshold.

### 6.1.5 Summary and conclusions

In this chapter we have established that the free-energy of some families of diluted random spin models can be written as the sum of a term identical to the ones got in the cavity/replica plus an error term. Both the replica term and the remainder are different in different replica scheme, corresponding to the choice of statistical ensemble of the cavity fields. We believe that the sign of the remainder is in general negative in the model we have considered, although we have been able to prove that only in the case of even $p$. For odd $p$ our belief is supported by the physical wisdom that the overlap distributions are supported on the positives in the large $N$ limit.

We have considered the cases of replica symmetry and one step of replica symmetry breaking. It is clear that the analysis could be extended to further levels of replica symmetry breaking, although the complexity of the analysis would greatly increase. The 1RSB level is thought to give the exact scheme to treat the $p$ spin model and the $K$-SAT problem for $p \geq 3$. For the Viana-Bray model on the other hand it is believed that no finite RSB scheme furnish the exact solution, and one needs to consider the limit of infinite number of replica symmetry breaking. It is not clear to us how to generalize the analysis to this case.

Our analysis of the diluted models underlines a strong link between the Guerra method and the cavity method which remained rather hidden in the fully connected case. In the cavity approach one considers incomplete graphs in which either sites or clauses are removed from the complete graph. Then, with the aid of precise physical hypothesis, consistency equations are written that allow to compute the free-energy from the comparison between the site and clause contributions. In the approach presented in this chapter the removal of clauses is compensated in average by the addition of some external fields which have precisely the statistics which is assumed with cavity. The novelty of the approach is that it gives some control on the approximation involved, and proves the variational nature of the replica free-energies. Of course a complete control on the remainder in various situations would result in rigorous solutions. Although we have mainly worked at finite temperature, the zero temperature limit can be considered without harm. This is particularly relevant in random satisfiability problem, where it is typically found a SAT-UNSAT transition where the ground state energy passes from zero to non zero values.

# Conclusions and perspectives

In this thesis a quite extensive exploration of replica methods for the study of statistical properties of spin systems on diluted random hyper-graphs was performed. We hope to have been able to show a relevant number of examples, that have been under our direct investigation, where this method turns out to be very powerful.

The starting body of the calculations was shown quite in details at least for some particular classes of models, so that the interested reader should be able to retrieve the expressions shown in the text quite easily, at least for the replica symmetric and the 1RSB variational factorized case.

We also hope to have given at least a flavour of the equivalence between the cavity and the replica techniques, even though the cavity formulation was only sketched.

It was stressed along the whole thesis that the replica/cavity method main assumption is that of absence of non trivial correlations between the spin variables, once the system is studied in a particular thermodynamic state. This property applies to mean field-like systems as the one studied, where the method is in still in principle non exact, but can be shown to lead at least to a rigorous variational approach. Moreover, this variational approach is systematic and can be applied to a wide class of problems of interest not only in modern statistical physics, but also in combinatorial optimization theory, information theory and theoretical computer science. A proof of the well founded variational nature of the cavity/replica method was achieved in the last part of this work, even though more work is needed to formulate it in full generality.

For disordered systems rigorous calculations that do not make use of the cavity/replica method are usually very hard. In the lucky simple cases where rigorous treatment is possible, as for example the XOR-SAT case, the equivalence between the rigorous results and the replica/cavity ones was stressed, as well as the physical interpretation of the such results in terms of geometrical changes in the space of solutions of the models studied.

The deeper understanding of the replica/cavity method has led to the possibility of extending in algorithmic terms to single problem instances. This opens the road to applications to real natural systems, as for instances a novel interpretation of message flow and organization in realistic diluted neural networks. One of our future aims is to work in that direction.

Very recently, a full study of the 1RSB solution of the random 3-SAT, $p$-XOR-SAT and graph $q$-coloring problems have been achieved. This results are very promising, and one further step that is currently under study is to investigate the possibility of extending it to systems in presence of more complex geometrical structure and non trivial correlations between the hyper-graph vertices. Indeed, the replica/cavity method corresponds to the Bethe approximation in the case of disordered systems. Since this Ansatz can be seen as a first order expansion of a more systematic variational approach to the study of non pure mean field statistical systems that goes under the name of *Cluster Variation Method* (CVM), a formulation of the CVM for disordered systems seems to be necessary.

We would like to conclude this thesis with a consideration: recent numerical results on the performance of the Survey Propagation algorithm deep in the random 3-SAT dynamical region, the so called *hard/sat phase*, seem to confirm[2] that the complexity of the algorithm scales as $\mathcal{O}(N \log N)$ all the way up to the SAT/UNSAT threshold. The early study of the arising of complexity in the typical case were motivated in the past by the conviction of the existence of a deep link between the onset of phase transitions in the random version of computationally hard problems and the NP complexity in the worst case. If confirmed, this last results seem to open a path in a different direction, and typical case complexity may turn out to have little to say in the long standing P versus NP debate. Worst case instances of an NP complete problem could eventually form an elusive set of highly non-typical cases, most probably very dependent on the particular *ad hoc* algorithm built for their solution. Nevertheless, for a wide class of computational problems spontaneously emerging in Nature, the study of typical case complexity will probably still be a very relevant issue.

[2] Alfredo Braunstein and Riccardo Zecchina, private communication.

# Appendix A

# Factor graphs

The duality property in hyper-graphs is made evident when working in the **factor-graph** formalism (see for instance [65, 66, 64]), where each hyper-edge is substituted by a *function node* (otherwised called *check node* or *clause node*, depending on the context), whose incidence edges connect it to the *variable nodes* that belong to the original hyper-edge, as in fig. (A.1). This formalism is particularly handy when one is interested in message passing procedures on the hyper-graphs, and more in general whenever one is interested in computing physical quantities referring to the hyper-edges as a whole and not to single vertices. This formalism is explicitly used in chapters 5 and 6 and is implicit throughout the whole work. Notice that the rank distribution of the direct hyper-graph is the function node degree distribution of the factor graph.

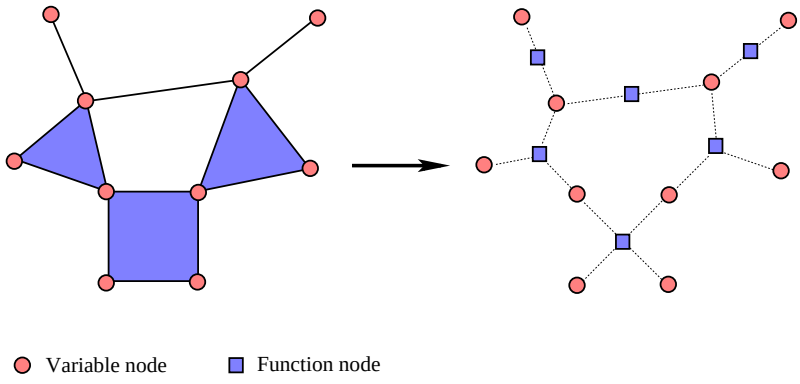



Figure A.1: From the hyper-graph to the factor graph picture.

# Appendix B

# Normalization factor $\xi[P(k)]$

The calculation is equivalent to that of the numerator in the calculation of the averages. We can rewrite eq. (2.23) in the form

$$\begin{aligned}
\xi[P(k)] &= \int \prod_i (\frac{d\psi_i}{2\pi}) \exp(-i\sum_i \psi_i k_i) \int \prod_l \prod_{i_1<\ldots<i_l} \left[ \left(1 - \frac{l!\gamma_l}{N^{l-1}}\right) \delta(J_{i_1,\ldots,i_l}) + \right. \\
&\left. \frac{l!\gamma_l}{N^{l-1}} \mu(|sign(J_{i_1,\ldots,i_l})|) \right] \exp(i \sum_l \sum_{i_1<\ldots<i_l} (\sum_{j=1}^{l} \psi_{i_j}) J_{i_1,\ldots,i_l}) \\
&= \int \prod_i (\frac{d\psi_i}{2\pi}) \exp(-i\sum_i \psi_i k_i) \int \prod_l \prod_{i_1<\ldots<i_l} \left[ 1 - \frac{l!\gamma_l}{N^{l-1}} + \frac{l!\gamma_l}{N^{l-1}} \exp(i \sum_{j=1}^{l} \psi_{i_j}) \right] \\
&\sim_{N\to\infty} \int \prod_i (\frac{d\psi_i}{2\pi}) \exp(-i\sum_i \psi_i k_i) \exp\left[ -N \sum_l \gamma_l \left( 1 - \frac{1}{N^l} \sum_{i_1,\ldots,i_l} e^{\psi_{i_1}+\ldots+\psi_{i_l}} \right) \right] \\
&= \int \prod_i (\frac{d\psi_i}{2\pi}) \exp(-i\sum_i \psi_i k_i) \exp\left[ -N \frac{< k >}{< l >} + N \sum_l \gamma_l \left( \frac{1}{N} \sum_i e^{\psi_i} \right)^l \right]
\end{aligned} \tag{B.1}$$

plus terms of order $\mathcal{O}(1/N)$. Defining

$$\rho \equiv \frac{1}{N} \sum_i e^{\psi_i} \tag{B.2}$$

and again expressing the constraint on $\rho$ in integral form we get

$$\begin{aligned}
&\int \frac{d\rho d\hat{\rho}}{2\pi N} \int \prod_i (\frac{d\psi_i}{2\pi}) \exp\left[ -N \left( \rho\hat{\rho} + \frac{i\sum_i \psi_i k_i}{N} + \frac{< k >}{< l >} - \frac{< k >}{< l >} \sum_l v_l \rho^l - \frac{\hat{\rho}}{N} \sum_i e^{i\psi_i} \right) \right] \\
&= \sum_{t=0}^{\infty} \int \frac{d\rho d\hat{\rho}}{2\pi N} e^{-N\rho\hat{\rho}} \int \prod_i (\frac{d\psi_i}{2\pi}) \exp\left[ -i\sum_i \psi_i k_i - N\frac{< k >}{< l >} + N\frac{< k >}{< l >} \sum_l v_l \rho^l \right] \frac{\hat{\rho}^t}{t!} e^{it\psi_i} \\
&= \int \frac{d\rho d\hat{\rho}}{2\pi N} \exp\left[ -N\rho\hat{\rho} - N\frac{< k >}{< l >} + N\frac{< k >}{< l >} \sum_l v_l \rho^l + N \sum_k c_k \log\left( \frac{\hat{\rho}^k}{k!} \right) \right]
\end{aligned} \tag{B.3}$$

we can evaluate this expression at the saddle point, getting

$$\rho\hat{\rho} = < k > \tag{B.4}$$

$$\frac{\sum_l l v_l \rho^l}{< l >} = 1 \tag{B.5}$$

For the case of hyper-graphs of uniform rank $l$, eq.(B.5) implies that we must have $\rho = 1$. This is not automatically true for multiple rank hyper-graphs. However, the assumption $\rho = 1$ is self consistent also in the general case, leading to the final expression

$$\xi[P(k)] \sim e^{-N\left(<k>-\sum_k c_k log\left(\frac{<k>^k}{k!}\right)\right)} \tag{B.6}$$

In assuming $\rho = 1$ we make the same normalization error we make in the computation of the numerator, assuming the functional order parameter $\rho(\vec{\sigma})$ to be normalized to one. As we see in the text, this error is at most )(1) in the free energy potential in the physically relevant limit $n \to 0$. If we redo the previous calculation taking into explicit account the constraints over the rank distribution, expression (B.3) becomes:

$$\int \frac{d\rho d\hat{\rho}}{2\pi N} \exp\left[-N\rho\hat{\rho} - N\frac{<k>}{<l>} + N\frac{<k>}{<l>}\sum_l v_l \log\left(\frac{\rho^l}{l!}\right) + N\sum_k c_k \log\left(\frac{\hat{\rho}^k}{k!}\right)\right] \sim \tag{B.7}$$

$$\exp\left[-N\left(<k> + \frac{<k>}{<l>} + <k>\log(<k>) + \frac{<k>}{<l>}\sum_l v_l \log(l!) + \sum_k c_k \log(k!)\right)\right]$$

where $\rho$ and $\hat{\rho}$ cancel out automatically. The same holds for the numerator, where the functional order parameters can be taken as normalized due to the homogeneity of the free energy.

# Appendix C

# On the choice of the functional order parameter

In choosing the functional order parameter we can adopt two variations on the same analytical formalism. Either one can be used, depending on the way we choose to look at the hyper-graph. A first way is that of treating every fixed degree sub-hyper-graph independently, assigning to each of them its own degree distribution. Let's call this choice $(\alpha)$. Under $(\alpha)$, all sub-structures will be merged assigning to each of them a given fraction of all interactions. Sub-hyper-graphs are independent, and any one is allowed a generic degree distribution. The overall degree distribution is the convolution of all distributions of sub-graphs. An alternative way of proceeding $((\beta))$ considers the hyper-graph as a whole and works directly with the overall degree distribution. The two routes are equivalent, but they can lead to easier or more difficult relative notations depending on the kind of graph we work with. In particular, $(\alpha)$ leads (see for instance appendices C.1 and C.2) to the introduction of a whole set of order parameters, one for each degree, and allows to easily write a special exact one replica symmetry broken solution in the case of uniform rank and constant degree, as well as in mixtures of single degree and rank sub-graphs, as the one shown in figure (C.1). In the case of hyper-graphs of the type of fig. (C.1), factorization is still possible because all sites keep being equivalent, even though the elementary "plaquette" can now be seen as a more complex entity made of regular groups of hyper-edges of different ranks. Moreover, given a certain hyper-graph structure, we recall that it is possible to build its **dual** counterpart in the following way: to every interaction plaquette there corresponds a site on the dual hyper-graph. Every two new sites are connected if their corresponding plaquettes of the direct hyper-graph have a common spin. The dual of a given hyper-graph is therefore a structure where the rank and the degree interaction distributions are exchanged. This leads to the possibility of finding a factorized exact solution also for fixed rank hyper-graphs with a non trivial albeit very peculiar degree distribution. The dual of fig. (C.1), for instance is a uniform rank 3 hyper-graph with bimodal 2 and 3 degrees, but structured in such a way that again it can be seen as a more complex structure where the fundamental building blocs are triplets of triplets, as shown in fig. (C.2).

A spin model on this graph could be solved through duality. Moreover, duality can be helpful any time calculating some properties of the studied model is hard in terms of degree distribution, but easy in terms of the rank distribution of the dual (The two interchange through duality). An example could be the calculation of metastable states complexity in the spin models associated to Binary Channel in Error Correcting Codes, even though that quantity has been found by different means in chapter 5. On the other hand, if one is interested only in

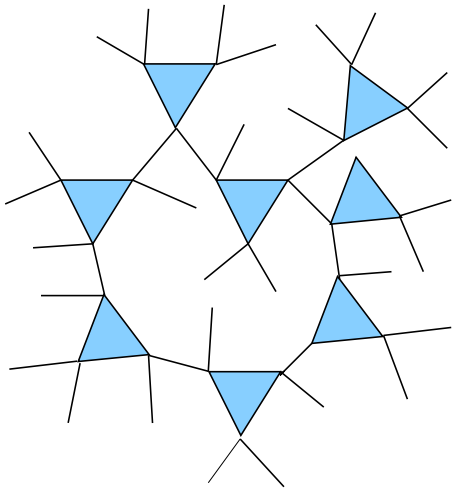


Figure C.1: mixed 2 and 3-hyper-graph with constant 2 and 1 sub-degrees.

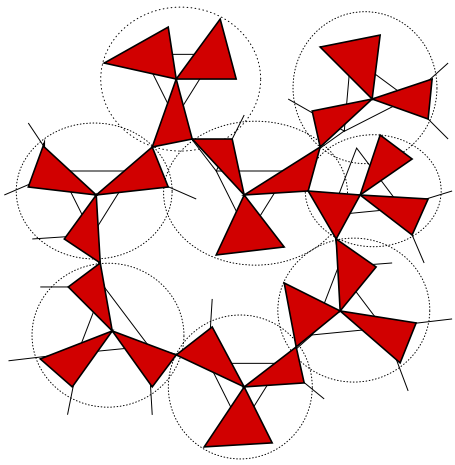


Figure C.2: Superimposed dual of the previous hyper-graph. Note that it can be seen as a decorated hype-graph of fixed degree, where decorated plaquettes are the circled ones.

fixing the overall ranks and degrees, formalism ($\beta$) is more compact and appropriate. In fixed rank and degree random graphs ($\alpha$) and ($\beta$) are equivalent. However, we will work with the formalism ($\beta$), unless otherwise stated.

## C.1 The degree sub-distributions: an alternative calculation

The constraint on the whole hyper-graph degree distribution is now substituted with a constraint on the degrees of each single rank $l$ sub-hyper-graph we can divide the structure into:

$$\prod_i \prod_k \delta(\sum_{<i_2,...,i_k>_i} J_{ii_2...i_k} - l_i^k) \tag{C.1}$$

All coupling constants probabilities are still treated as independent. This will lead to the introduction of a set of auxiliary variables $\psi_i^k$ and eventually to a whole set of functional order parameters in $\{\rho_k(\vec{\sigma}) = \frac{1}{N}\sum_i \delta(\vec{\sigma} - \vec{s}_i)e^{i\psi_i^k}, \hat{\rho}_k(\vec{\sigma})\}_{\forall k}$. Caculations are then formally equivalent to those in the text.

### C.1.1 RS results

The resulting set of replica symmetric saddle point equations reads

$$\begin{aligned}
\rho_l(\vec{\sigma}) &= \frac{1}{N_l}\sum_{\vec{k}} P(\vec{k})k_l \frac{\prod_{l'\neq l}\hat{\rho}_{l'}(\vec{\sigma})^{k_{l'}}\hat{\rho}_l(\vec{\sigma})^{k_l-1}}{\sum_{\vec{\sigma}}\prod_l \hat{\rho}_l(\vec{\sigma})^{k_l}} && \text{(C.2)}\\
N_l &= \sum_{\vec{\sigma}} \rho_l(\vec{\sigma}) && \text{(C.3)}\\
\hat{\rho}_l(\vec{\sigma}) &= \frac{1}{<l>} l v_l \sum_{\vec{\sigma}_1,...,\vec{\sigma}_{l-1}} \rho_l(\vec{\sigma}_1)...\rho_l(\vec{\sigma}_{l-1})e^{\beta\sum_{a=1}^n \sigma^a\sigma_1^a...\sigma_{l-1}^a} && \text{(C.4)}\\
P(\vec{k}) &\cong P(k_1,...,k_{l_{max}}) && \text{(C.5)}
\end{aligned}$$

and the free energy

$$\begin{aligned}
-n\beta F &= -\sum_l <k_l> \sum_{\vec{\sigma}} \rho_l(\vec{\sigma})\hat{\rho}_l(\vec{\sigma}) + \sum_{\vec{k}} P(\vec{k}) \log(\sum_{\vec{\sigma}}\prod_l \rho_l(\vec{\sigma})^{k_l}) + \\
&\quad \frac{1}{<l>}\sum_l <k_l> v_l \sum_{\vec{\sigma_1},...,\vec{\sigma_l}} \rho_l(\vec{\sigma_1})...\rho_l(\vec{\sigma_l})e^{\beta\sum_{a=1}^n \sigma_1^a...\sigma_l^a} && \text{(C.6)}\\
<k_l> &\cong \int d\vec{k} P(\vec{k})k_l && \text{(C.7)}
\end{aligned}$$

### C.1.2 Factorized 1RSB results: 1

The similar calculations in the 1RSB case factorized Ansatz lead to

$$\rho_l(\vec{\sigma}) = \frac{1}{N_l}\sum_{\vec{k}} P(\vec{k})k_l \frac{\prod_{l'\neq l}\hat{\rho}_{l'}(\vec{\sigma})^{k_{l'}}\hat{\rho}_l(\vec{\sigma})^{k_l-1}}{\sum_{\vec{\sigma}}\prod_l \hat{\rho}_l(\vec{\sigma})^{k_l}} \tag{C.8}$$

$$N_l = \sum_{\vec{\sigma}} \rho_l(\vec{\sigma}) \tag{C.9}$$

$$\hat{\rho}_l(\vec{\sigma}) = \frac{1}{\hat{N}_l}\frac{1}{<l>} l v_l \frac{\sum_{\vec{\sigma}_1,...,\vec{\sigma}_{l-1}} \rho_l(\vec{\sigma}_1)...\rho_l(\vec{\sigma}_{l-1}) e^{\beta \sum_{a=1}^{m} \sigma^a \sigma_1^a ... \sigma_{l-1}^a}}{\sum_{\vec{\sigma_1},...,\vec{\sigma_l}} \rho_l(\vec{\sigma}_1)...\rho_l(\vec{\sigma}_l) e^{\beta \sum_{a=1}^{m} \sigma_1^a ... \sigma_l^a}} \tag{C.10}$$

$$\hat{N}_l = \sum_{\vec{\sigma}} \vec{\rho}_l(\vec{\sigma}) \tag{C.11}$$

where the functional parameter is taken within a replica group, and

$$-m\beta F(m,\beta) = -\sum_l <k_l> \log(\sum_{\vec{\sigma}} \rho_l(\vec{\sigma})\hat{\rho}_l(\vec{\sigma})) - m\sum_l <k_l> \sum_{\vec{k}} P(\vec{k}) \log(\sum_{\vec{\sigma}} \prod_l \rho_l(\vec{\sigma})^{k_l}) +$$

$$\frac{1}{<l>}\sum_l <k_l> v_l \log(\sum_{\vec{\sigma_1},...,\vec{\sigma_l}} \rho_l(\vec{\sigma_1})...\rho_l(\vec{\sigma_l}) e^{\beta \sum_{a=1}^{m} \sigma_1^a ... \sigma_l^a}) + \frac{m\sum_l v_l <k_l>}{<l>} \tag{C.12}$$

From this point on, one could proceed again with the formalism in the main text, keeping in mind that the overall graph will be the interconnections of the $l$-substructures, and the overall degree distribution the convolution of the partial ones. This will reflect also on different distributions on the magnetic fields acting on spins.

## C.2 Factorized 1RSB results: 2

The factorized Ansatz formulas are valid in the slightly more general case of a mixture of hyper-graphs of fixed sub-degree, as for instance the example of In that case, with the same formalism of appendix C.1 we obtain self consistent replica equations:

$$\rho(\vec{\sigma}) = \frac{B_l^{k_l-1}(\vec{\sigma}) \prod_{l' \neq l} B_{l'}^{k_{l'}}(\vec{\sigma})}{\sum_{\vec{\sigma}} B_l^{k_l-1}(\vec{\sigma}) \prod_{l' \neq l} B_{l'}^{k_{l'}}(\vec{\sigma})} \tag{C.13}$$

$$B_l(\vec{\sigma}) = \sum_{\vec{\sigma}_1,...,\vec{\sigma}_{l-1}} \rho(\vec{\sigma}_1)...\rho(\vec{\sigma}_{l-1}) e^{\beta \sum_{a=1}^{m} \sigma^a \sigma_1^a ... \sigma_{l-1}^a} \tag{C.14}$$

recast in a familiar form:

$$-m\beta F(m,\beta) = \left(1 - \sum_l \frac{k_l(l-1)}{l}\right) \log(\sum_{\vec{\sigma}} \prod_l B_l^{k_l}(\vec{\sigma})) + \sum_l \frac{k_l(l-1)}{l} \log(B_l^{k_l-1}(\vec{\sigma}) \sum_{\vec{\sigma}} \prod_{l' \neq l} B_{l'}^{k_{l'}}(\vec{\sigma})) \tag{C.15}$$

If $k_l = k \ \forall l$, we obtain

$$\rho(\vec{\sigma}) = \frac{B_l^{k-1}(\vec{\sigma}) \prod_{l' \neq l} B_{l'}^{k}(\vec{\sigma})}{\sum_{\vec{\sigma}} B_l^{k-1}(\vec{\sigma}) \prod_{l' \neq l} B_{l'}^{k}(\vec{\sigma})} \tag{C.16}$$

and

$$-m\beta F(m,\beta) = \left(1 - k\sum_l \frac{(l-1)}{l}\right) \log(\sum_{\vec{\sigma}} \prod_l B_l^k(\vec{\sigma})) + k\sum_l \frac{(l-1)}{l} \log(B_l^{k-1}(\vec{\sigma}) \sum_{\vec{\sigma}} \prod_{l' \neq l} B_{l'}^k(\vec{\sigma})) \tag{C.17}$$

that reduce to the equations in the text (with $B(\vec{\sigma}) = \hat{\rho}(\vec{\sigma})$).

# Appendix D

# Critical exponents and non universal amplitudes

## D.1 Case $< k^4 >$ finite

In this appendix we show the explicit calculations leading to eq. (3.34) in the text. Using eq. (3.19) for the case $H_0 = 0$ and assuming all $u$'s to fluctuate around the zero value we can write:

$$\begin{aligned}
< u > &= \frac{1}{\beta < k >} \sum_k k c_k \int \prod_{t=1}^{k-1} du_t Q(u_t) \tanh^{-1} \left( \tanh(\beta) \tanh(\beta \sum_{t=1}^{k-1} u_t) \right) \\
&\sim \frac{1}{< k >} \sum_k k c_k \int \prod_{t=1}^{k-1} du_t Q(u_t) \left[ \tanh(\beta) \left( \sum_{t=1}^{k-1} u_t \right) \right. \\
&\quad \left. -\frac{\beta^2}{3} \tanh(\beta)(1 - \tanh^2(\beta)) \left( \sum_{t=1}^{k-1} u_t \right)^3 \right] + \mathcal{O}(< u >^5) \\
&= \frac{1}{< k >} \sum_k k c_k \left[ \tanh(\beta)(k-1) < u > \right. \\
&\quad \left. -\frac{\beta^2}{3} \tanh(\beta)(1 - \tanh^2(\beta)) \int \prod_{t=1}^{k-1} du_t Q(u_t) \left( \sum_{t=1}^{k-1} u_t \right)^3 \right] \\
&= \frac{1}{< k >} \sum_k k c_k \left[ \tanh(\beta)(k-1) < u > \right. \\
&\quad -\frac{\beta^2}{3} \tanh(\beta)(1 - \tanh^2(\beta))(k-1) < u^3 > +3(k-1)(k-2) < u^2 >< u > \\
&\quad \left. +(k-1)(k-2)(k-3) < u >^3 \right] \\
&= \frac{\tanh(\beta)}{\tanh(\beta_c)} < u > -\frac{\beta^2}{3} \frac{\tanh(\beta)(1 - \tanh^2(\beta))}{< k >} \left[ < k(k-1) >< u^3 > \right. \\
&\quad +3 < k(k-1)(k-2) >< u >< u^2 > \\
&\quad \left. + < k(k-1)(k-2)(k-3) >< u >^3 \right]
\end{aligned} \tag{D.1}$$

where we have exploited the second of the identities:

$$\int \prod_{t=1}^{k-1} du_t Q(u_t) \left( \sum_{t=1}^{k-1} u_t \right)^2 = (k-1) < u^2 > +(k-1)(k-2) < u >^2 \tag{D.2}$$

$$\int \prod_{t=1}^{k-1} du_t Q(u_t) \left(\sum_{t=1}^{k-1} u_t\right)^3 = (k-1) < u^3 > +3(k-1)(k-2) < u^2 >< u > +(k-1)(k-2)(k-3) < u >^3 \quad \text{(D.3)}$$

We assume now that

$$\begin{aligned} < u^2 > &\sim < u >^2 \\ < u^3 > &\sim < u >^3 \end{aligned} \quad \text{(D.4)}$$

We will see this Ansatz to be self consistent in the following. Indeed, the second and third momenta can be written as

$$\begin{aligned} < u^2 > &= \frac{1}{< k > \beta^2} \sum_k k c_k \int \prod_{t=1}^{k-1} du_t Q(u_t) \left(\tanh^{-1}(\tanh(\beta)\tanh(\beta \sum_{t=1}^{k-1} u_t))\right)^2 \\ &\sim \left[\frac{\tanh^2(\beta) < k(k-1)(k-2) >}{\beta^2 < k > - \tanh^2(\beta) < k(k-1) >}\right] < u >^2 \end{aligned} \quad \text{(D.5)}$$

$$< u^3 >= \frac{1}{< k > \beta^3} \sum_k k c_k \prod_{t=1}^{k-1} du_t Q(u_t) \left(\tanh^{-1}(\tanh(\beta)\tanh(\beta \sum_{t=1}^{k-1} u_t))\right)^3 \sim \left[\frac{tanh^3(\beta)\left(\frac{\tanh^2(\beta) < k(k-1)(k-2) >^2}{\beta^2 < k > - \tanh^2(\beta) < k(k-1) >}\right) + < k(k-1)(k-2)(k-3) >}{\beta^3 < k > - \tanh^3(\beta) < k(k-1) >}\right] < u >^3$$

where we have made use of Ansatz (D.4) and identities (D.3) and rearranged the terms. Putting all together we find eq.(3.34). As one can see, the critical exponent is the usual mean field one (1/3) and its value does not depend on taking into consideration higher momenta of the distribution $Q(u)$.

## D.2 Scale free networks: case $3 < \gamma < 5$

We show here the explicit calculations leading to the non trivial mean field critical exponent $\beta = 1/(\gamma - 3)$ in absence of a cutoff on high degrees of the distribution, together with an approximate expression for the non universal amplitude. Under the approximation $Q(u) = \delta(u - < u >)$ we can still expand

$$F_\beta(< u >) \equiv \frac{c}{\beta < k >} \sum_k k^{1-\gamma} \tanh^{-1}\left(\tanh(\beta)\tanh(\beta(k-1) < u >)\right) \quad \text{(D.6)}$$

where $c$ is the probability degree distribution normalization constant, but since the convergence radius of the hyperbolic tangent is $\pi/2$ the series will converge as long as $\beta(k-1) < u > \leq \pi/2$ only. For any value of the temperature and the cavity magnetization it is then possible to find a $k$ such that the argument of the tangent lies outside of the convergence radius. Nevertheless, the function $F_\beta(< u >)$ is still asymptotic approximable by a polynomial whose maximum degree will be a function of the exponent $\gamma$. If we call $S_\beta^{(n)}(k, < u >)$ the $n^{th}$ degree truncation of the series expansion of the $k^{th}$ term of $F_\beta(< u >)$, we can write

$$\begin{aligned} &\left|F_\beta(< u >) - \frac{c}{\beta < k >} \sum_k k^{1-\gamma} S_\beta^{(\hat{n})}(k, < u >)\right| \sim \\ &\left|F_\beta(< u >) - \mathcal{P}_\beta^{(\hat{n})}(< u >)\right| \sim \mathcal{O}(< u >^{2\hat{n}+3}) \end{aligned} \quad \text{(D.7)}$$

where $\hat{n}$ is the maximum degree s.t. the coefficients of $\mathcal{P}_\beta^{(\hat{n})}(< u >)$ are finite and the polynomial has degree $2\hat{n}+1$ due to the antisymmetry of the hyperbolic tangent. The convergence condition summing over $k$ for the polynomial coefficient of maximum degree translates in the one for the convergence of the new power series:

$$(1-\gamma) + 2\hat{n} + 1 < -1 \tag{D.8}$$

so that one finds

$$\hat{n} < \frac{\gamma - 3}{2} \tag{D.9}$$

For $\gamma > 5$ the first non trivial term of the series expansion of $< u >$ is therefore simply $\hat{n} = 1$, and one retrieves the simple mean field result. But for the range of the exponent we are interested in in this appendix the first non trivial term will indeed be the analytical continuation (D.9). It is immediate to see how the desired exponent value is retrieved. The calculation of the amplitude proceeds in a similar way. We can write again from the power expansion of the self-consistent expression for $< u >$ up to the highest converging term

$$< u > \sim C(\beta,\gamma) < u >^{\gamma-2} = C(\beta,\gamma) < u >^{2\hat{n}+1} \tag{D.10}$$

where $C(\beta,\gamma)$ is the analytic continuation of

$$\frac{c\tanh(\beta)}{< k >} \sum_k k^{1-\gamma}(k-1) \sum_{t=0}^{\infty} \frac{(-1)^t(1-\tanh^2(\beta))^t}{2^{2t}} \cdot \sum_{r=0}^{2t} C_r^{2t}(-1)^r \frac{2^{2\hat{n}+1}((t-r)(k-1)\beta)^{2\hat{n}+1}}{(2\hat{n}+1)!} \tag{D.11}$$

The series in $k$ has, as a dominant term:

$$\frac{(-1)^{2\hat{n}+1}}{(2\hat{n}+1)!} \sum_k k^{(2-\gamma)+(2\hat{n}+1)} \quad \sim \quad \Gamma(3-\gamma) \tag{D.12}$$

as one can easily see from the series expansion of the integral representation of the Gamma function. Putting all together one finds

$$\begin{aligned} C(\beta,\gamma) \quad &\sim \quad \frac{c\tanh(\beta_c)(-2\beta)_c^{\gamma-3}\Gamma(3-\gamma)}{< k >} \sum_{t=0}^{\infty} \frac{(-1)^t(1-\tanh^2(\beta))^t}{2^{2t}} \sum_{r=0}^{2t} C_r^{2t}(t-r)^{s-3} \\ < u > \quad &\sim \quad \left(\frac{1-\tanh^2(\beta_c)}{|C(\beta,\gamma)|\tanh(\beta)}\right)^{\frac{1}{s-3}} |\beta - \beta_c|^{\frac{1}{s-3}} \end{aligned} \tag{D.13}$$

In fact, in order to find the exact value of the non universal amplitudes we would need to extend the calculation of the previous paragraph. The mean value of the cavity magnetization can be written as

$$\begin{aligned} < u > \quad &= \quad \frac{1}{< k > \beta} \sum_k k c_k \int \prod_{t=1}^{k-1} du_t Q(u_t) \sum_n a_n \tanh^n(\beta) \left(\tanh(\beta \sum_t u_t)\right)^n \\ &= \quad \frac{1}{< k > \beta} \sum_k k c_k \int \prod_{t=1}^{k-1} du_t Q(u_t) \sum_n a_n \tanh^n(\beta) \\ &\quad \sum_m \left( \sum_m \sum_{l_1,\ldots,l_n} \prod_{t=1}^{n} b_{l_t} \delta\left(m; \sum_t l_t\right)\right) \beta^m \left(\sum_{t=1}^{k-1} u_t\right)^m \end{aligned} \tag{D.14}$$

where $a_n$ and $b_{l_t}$ are numerical coefficients of the Taylor expansions of the inverse hyperbolic tangent and the hyperbolic tangent respectively and

$$\left\langle \left( \sum_{t=1}^{k-1} u_t \right)^m \right\rangle = \sum_{n_1,\ldots,n_{k-1}}^{n_1+\ldots.+n_{k-1}=m} \frac{m!}{n_1!\ldots.n_{k-1}!} < u^{n_1} > \ldots. < u^{n_{k-1}} > \tag{D.15}$$

The process is now a little more involved since it is necessary to find a close form for the analytic continuation of the momenta of the distribution $Q(u)$, where $m$ takes real values $m(\gamma)$. Using Newton's expansion for real exponents eq.(D.15) becomes:

$$\left\langle \left( \sum_{t=1}^{k-1} u_t \right)^m \right\rangle = \sum_{n_1,\ldots,n_{k-2}=0}^{\infty} \prod_{t=1}^{n_1+\ldots n_{k-2}} \frac{(m-t)}{n_1!\ldots.n_{k-2}!} \prod_{s=1}^{k-2} < u^{n_s} >< u^{m-\sum_s n_s} > \tag{D.16}$$

Consequently, it can still be immediately seen that for any value of $m$ the proportionality relation

$$\left\langle \left( \sum_{t=1}^{k-1} u_t \right)^m \right\rangle \propto < u >^m \tag{D.17}$$

still holds under the assumption $< u^r > \propto < u >^r \; \forall \; r \in R$, and one is left this time with an infinite system of equations for the non integer moments that can be iteratively solved and give the desired correction to expression for the non universal amplitude. Moreover, the value of critical exponent is not changed. Similar expansions can be done for all other physical quantities.

# Appendix E

# E.C.Codes: BSC, A T=0 variational calculation

The zero temperature equations simplify in the limit $y \to \infty$, corresponding to vanishing exchange energy. In that case, a finite value of $q$ is obtained if the magnetic field $h_0$ is kept finite, and it can be proved that the relation $q = \tanh(h_0)$ holds. In this limit, a direct inspection of the saddle point equations reveals that only the values $\pm(l-1)$ are possible for the cavity fields $x$, and the values $\pm 1$ for the $y$'s. More explicitly, the order parameters $Q[\rho]$ and $\widehat{Q}[\hat{\rho}]$ are supported on distributions of the form

$$\rho(x) = \rho_+ \delta(x - l + 1) + \rho_- \delta(x + l - 1)\,, \qquad \hat{\rho}(z) = \hat{\rho}_+ \delta(z-1) + \hat{\rho}_- \delta(z-1)\ . \tag{E.1}$$

The functional order parameter $\widehat{Q}[\hat{\rho}]$, reduces to the probability distributions of a single number $\hat{\rho}_+$ representing the probability of $z = +1$.

A simple approximation is obtained by using (E.1) and neglecting the fluctuations of $\hat{\rho}_+$, in the spirit of the *factorized Ansatz*. This is exact [1] for $h_0 = 0$, where our model reduces to the one analyzed in [22]. It can be proved that, for $y = \infty$ and $h_0 \neq 0$, this approximation gives the same result as the $k, l \to \infty$ limit, cf. Sec. 5.2.5. For instance in the case of $(k, l) = (6, 5)$ we get $p_c^{var} = 0.264$ which coincides with the exact result.

[1] This assertion is true only for even values of $l$, but actually it is a very good approximation for any value of $l$.

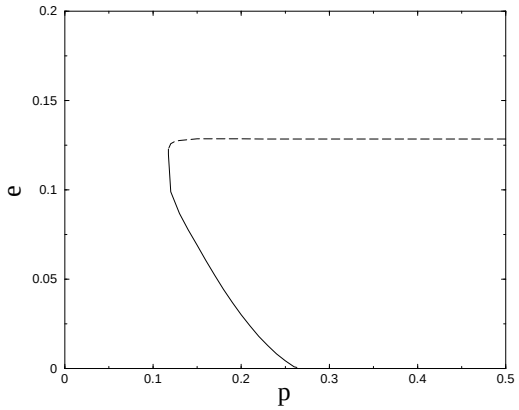



Figure E.1: The region of metastability as predicted by the approximated Ansatz (E.1) for the (6,5) code.

The same form for the functional order parameter can also be used as a variational approximation for $y$ finite, although in this case it is not justified to assume $z = \pm 1$. In Fig. E.1, we indicate the region of the $(p, \epsilon)$ plane such that $\Sigma_p(\epsilon, 1-2p) > 0$, as obtained from this simple approach.

# Appendix F

# Details of the calculations of Chapter 6

## F.1 $p$-spin

### F.1.1 Check of the positive sign of $R_{1RSB}^{p-spin}$

In this appendix we will explicitly show that expression (6.59) has positive definite sign. The notations will be those of the general $p$-spin case. Specific results in the Viana-Bray case are immediately retrieved if one assigns $p = 2$. We proceed expanding in series each of the three sub-terms and showing that every element of the sum of the resulting series is positive semidefinite.

The first term writes:

$$E_1 \left\langle \log \frac{E_2 Z^m (1+\tanh(\beta J)\omega(S_{i_1}...S_{i_p}))^m}{E_2 Z^m} \right\rangle_J = \sum_{l\geq 1} \frac{(-1)^{l+1}}{l} \sum_{k_1,...,k_l}^{1,\infty} \prod_{u=1}^{l} \left( \frac{m(-1)^{k_u-1}}{k_u!} \prod_{r_u=1}^{k_u-1} (r_1 - m) \right) \left\langle (\tanh(\beta J)^{\sum_{s=1}^{l} k_s} \right\rangle_J \cdot E_1 \left( \prod_{s=1}^{l} \frac{E_2(Z^m \omega(S_{i_1}...S_{i_p})^{k_s})}{E_2(Z^m)} \right) \tag{F.1}$$

where the term $E_1(\,\cdot\,)$ in the last line of eq.(F.1) can be written as

$$\Omega^{(l)} \left[ (q^{(k_1,...,k_l)})^p \right] \equiv \tag{F.2}$$

$$E_1 \left( \frac{E_2^{(1)}...E_2^{(l)} Z_{(1)}^m ... Z_{(l)}^m \omega_{(1)}(S_{i_1}^{1,1}...S_{i_p}^{1,1}...S_{i_1}^{k_1,1}...S_{i_p}^{k_1,1}) ... \omega_{(l)}(S_{i_1}^{1,l}...S_{i_p}^{1,l}...S_{i_1}^{k_l,l}...S_{i_p}^{k_l,l})}{(E_2 Z^m)^l} \right) .$$

where each $\omega_{(s)}$ $(s = 1, ..., l)$ is a product of $k_s$ Gibbs measure with independent fields (variables appearing in the $E_2^{(s)}$ averages), and same fields distributions and quenched disorder (variables appearing in $E_1$). The quantities $q^{(k_1,...,k_l)}$ have been defined as:

$$q^{(k_1,...,k_l)} = \frac{1}{N} \sum_i S_i^{1,1} \cdot ... \cdot S_i^{k_1,1} \cdot ... \cdot S_i^{1,l} \cdot ... \cdot S_i^{k_l,l} \tag{F.3}$$

and in this case the averages are performed using a a generalized replica measure, defined as:

$$\Omega^{(l)}[(q^{(k_1,...,k_l)})^n] = E_1 \left[ \frac{\prod_{s=1}^{l} E_2^{(s)} Z_{(s)}^m \omega_{(s)}(S_{i_1}...S_{i_n})^{k_s}}{(E_2 Z^m)^l} \right] \tag{F.4}$$

for any integer $n$. The average over $J$ selects the terms with even $\sum_{s=1}^{l} k_l$ in (F.1) so that we finally find

$$-\sum_{l\geq 1}\frac{m^l}{l}\sum_{\substack{k_1,\ldots,k_l \\ \sum_{s=1}^{l} k_s \text{even}}}^{1,\infty}\prod_{s=1}^{l}\left(\frac{\prod_{r_s=1}^{k_s-1}(r_s-m)}{k_s!}\right)\left\langle(\tanh(\beta J))^{\sum_{s=1}^{l}k_s}\right\rangle_J \Omega^{(l)}\left[(q^{(k_1,\ldots,k_l)})^p\right] \tag{F.5}$$

notice that $(r_s - m) \geq 0 \ \forall$ integer $r_s > 0$ only in the current hypothesis that $m \in [0,1]$. Analogously, the term

$$E_1\left\langle\log\frac{E_2 Z^m\left\langle(1+\tanh(\beta u)\omega(S_i))^m\right\rangle_u}{E_2 Z^m}\right\rangle_Q \tag{F.6}$$

writes

$$-\sum_{l\geq 1}\frac{m^l}{l}\sum_{\substack{k_1,\ldots,k_l \\ \sum_{s=1}^{l} k_s \text{even}}}^{1,\infty}\prod_{s=1}^{l}\left(\frac{\prod_{r=1}^{k_s-1}(r-m)}{k_s!}\right)\left\langle\prod_{s=1}^{l}\left\langle\tanh(\beta u)^{k_s}\right\rangle_u\right\rangle_Q \Omega^{(l)}\left[(q^{(k_1,\ldots,k_l)})\right] \tag{F.7}$$

or, making use of the definition of $G(g)$,

$$-\sum_{l\geq 1}\frac{1}{l}\sum_{\substack{k_1,\ldots,k_l \\ \sum_{s=1}^{l} k_s \text{even}}}^{1,\infty}\prod_{s=1}^{l}\left(\frac{\prod_{r=1}^{k_s-1}(r-m)}{k_s!}\right)\left\langle\prod_{s=1}^{l}\left\langle(\tanh(\beta g))^{k_s}\right\rangle_g\right\rangle_G^{p-1}\cdot \tag{F.8}$$

$$\left\langle(\tanh(\beta J))^{\sum_{s=1}^{l}k_s}\right\rangle_J \Omega^{(l)}\left[(q^{(k_1,\ldots,k_l)})\right]$$

Eventually, following analogous manipulations, the last term

$$\left\langle\log\left\langle\left(1+\tanh(\beta J)\prod_{t=1}^{p}\tanh(\beta g_t)\right)^m\right\rangle_{\{g_t\}}\right\rangle_{J,\{G_t\}} \tag{F.9}$$

can be written as

$$-\sum_{l\geq 1}\frac{m^l}{l}\sum_{\substack{k_1,\ldots,k_l \\ \sum_{s=1}^{l} k_s \text{even}}}^{1,\infty}\prod_{s=1}^{l}\left(\frac{\prod_{r=1}^{k_s-1}(r-m)}{k_s!}\right)\left\langle\prod_{s=1}^{l}\left\langle(\tanh(\beta g))^{k_s}\right\rangle_g\right\rangle_G^{p}\left\langle(\tanh(\beta J))^{\sum_{s=1}^{l}k_s}\right\rangle_J. \tag{F.10}$$

Invoking (6.49) and collecting all

$$R_{1RSB}^{p-spin}[\mathcal{G},t] = \frac{\alpha}{\beta m}\sum_{l\geq 1}\frac{m^l}{l}\sum_{\substack{k_1,\ldots,k_l \\ \sum_{s=1}^{l} k_s \text{even}}}^{1,\infty}\prod_{s=1}^{l}\left(\frac{\prod_{r=1}^{k_s-1}(r-m)}{k_s!}\right)\left\langle(\tanh(\beta J))^{\sum_{s=1}^{l}k_s}\right\rangle_J\cdot$$

$$\Omega^{(l)}\left[(q^{(k_1,\ldots,k_l)})^p - pA(k_1,\ldots,k_l)^{p-1}(q^{(k_1,\ldots,k_l)}) + (p-1)A(k_1,\ldots,k_l)l^p\right] \tag{F.11}$$

where we have defined:

$$A(k_1,\ldots,k_l) \equiv \left\langle\prod_{s=1}^{l}\left\langle(\tanh(\beta g))^{k_s}\right\rangle_g\right\rangle_G \tag{F.12}$$

Each inner term of the series (F.11)

$$\Omega^{(l)}\left[(q^{(k_1,...,k_l)})^p - pA(k_1,...,k_l)^{p-1}(q^{(k_1,...,k_l)}) + (p-1)A(k_1,...,k_l)^p\right] \tag{F.13}$$

is always positive semidefinite for $p$ even while we need the condition conditions $q^{(k_1,...,k_l)} \geq 0$ for $p$ odd. For $p = 2$ one retrieves the Viana-Bray result where (F.13) is a perfect square. As in the RS case, one can now integrate eq.(F.11) and recognize that once more the total true free-energy can be written as variational term plus a positive extra one. The variational term coincides with the 1RSB free-energy at stationarity and under condition

$$\mathcal{G}(P) \;=\; \mathcal{P}(P)|_{t=0} \quad \forall \; P\,. \tag{F.14}$$

### F.1.2 Check of $F^{p-spin}_{var}[\mathcal{P}] = F^{p-spin}_{1RSB}[\mathcal{P}]$

In this appendix we want to show explicitly that

$$\begin{aligned} F^{p-spin}_{1RSB}[\mathcal{P}] \;=\; & \alpha\left\langle\log(\cosh(\beta J))+\right\rangle \frac{1}{\beta m}\left[\alpha p\left\langle\log\left\langle\left(\frac{2\cosh(\beta(h+u))}{2\cosh(\beta h)2\cosh(\beta u)}\right)^m\right\rangle_{u,h}\right\rangle_{Q,P} - \right. \\ & \alpha\int dJ\mu(J)\left\langle\log\left\langle(1+\tanh(\beta J)\prod_{t=1}^{p}\tanh(\beta h_t))^m\right\rangle_{h_1,...,h_p}\right\rangle_{P_1,...,P_p} - \\ & \left.\sum_k e^{-\alpha p}\frac{(\alpha p)^k}{k!}\left\langle\log\left\langle\left(\frac{2\cosh(\beta\sum_{l=1}^k u_l)}{\prod_{t=1}^k 2\cosh(\beta u_t)}\right)^m\right\rangle_{u_1,...,u_k}\right\rangle_{Q_1,...,Q_k}\right] \end{aligned} \tag{F.15}$$

coincides with the variational expression

$$\begin{aligned} F^{p-spin}_{var}[\mathcal{G}] \;=\; & \frac{1}{\beta m}\Big[\left\langle\log\left\langle\left(\frac{1}{2\cosh(\beta h)}\right)^m\right\rangle_h\right\rangle_P - \alpha m\left\langle\log(2\cosh(\beta J))\right\rangle_J - \\ & \alpha p\left\langle\log\left\langle\left(\frac{1}{2\cosh(\beta u)}\right)^m\right\rangle_u\right\rangle_Q + \\ & \alpha(p-1)\left\langle\log\left\langle(1+\tanh(\beta J)\tanh(\beta g_1)...\tanh(\beta g_p))^m\right\rangle_{g_1,...,g_p}\right\rangle_{G_1,...,G_p;J}\Big] \end{aligned} \tag{F.16}$$

found in section 6.1.4, once this last expression is extremized with respect to $\mathcal{G}$. For a derivation of (F.15) in the replica formalism see the first chapter. Substituting in (F.17) the 1RSB self consistent conditions for $u_J(h_1,...,h_{p-1})$ and $\mathcal{G}[P] = \mathcal{P}[P]\;\forall P$, we can write:

$$\begin{aligned} & \left\langle\log\left\langle\left(\frac{2\cosh(\beta(h+u))}{2\cosh(\beta h)2\cosh(\beta u)}\right)^m\right\rangle_{u,h}\right\rangle_{Q,P} = \\ & -\alpha p\log 2 + \alpha p\left\langle\log\left\langle\left(1+\tanh(\beta J)\prod_{t=1}^{p}\tanh(\beta h_t)\right)^m\right\rangle_{\{h_t\}}\right\rangle_{\{P_t\},J} \end{aligned} \tag{F.17}$$

To condense the expressions we can define

$$p_k = e^{-\alpha p}\frac{(\alpha p)^k}{k!} \tag{F.18}$$

Using the trivial identity

$$\alpha p \left\langle \log \left\langle \left( \frac{1}{2\cosh(\beta u)} \right)^m \right\rangle_u \right\rangle_Q = \sum_k p_k \left\langle \log \left\langle \left( \frac{1}{\prod_{t=1}^k 2\cosh(\beta u_t)} \right)^m \right\rangle_{\{u_t\}} \right\rangle_{\{Q_t\}} \quad \text{(F.19)}$$

and the relation

$$\begin{aligned} \left\langle \log \left\langle \left( \frac{1}{2\cosh(\beta h)} \right)^m \right\rangle_h \right\rangle_P = & \sum_k p_k \left\langle \log \left\langle \left( \frac{2\cosh(\beta \sum_{l=1}^k u_l)}{\prod_{t=1}^k 2\cosh(\beta u_t)} \right)^m \right\rangle_{u_1,\ldots,u_k} \right\rangle_{Q_1,\ldots,Q_k} + \\ & \sum_k p_k \left\langle \log \left\langle \left( \frac{1}{\prod_{t=1}^k 2\cosh(\beta u_t)} \right)^m \right\rangle_{\{u_t\}} \right\rangle_{\{Q_t\}} \end{aligned} \quad \text{(F.20)}$$

given by eqs. (6.50) and (6.52) and putting all pieces together we finally find

$$F_{var}^{p-spin}[\mathcal{P}] = F_{1RSB}^{p-spin}[\mathcal{P}] \quad \text{(F.21)}$$

at the 1RSB saddle point. The equivalence of the corresponding RS expressions is even simpler at it is done along the same lines of calculation, exploiting the RS self consistency condition $G(h) = P(h)\ \forall h$.

## F.2 K-SAT

### F.2.1 Check of the positive sign of $R_{RS}^{K-SAT}$ ...

The aim of this appendix is to show that the expression for the remainder $R_{RS}[G,t]$ in (6.35) for the $K$-SAT model case as positive sign. For the $K$-SAT $R_{RS}[G,t]$ specializes to:[1]

$$\begin{aligned} R_{RS}^{K-SAT}[G,t] = & -\frac{\alpha}{\beta} E \left[ \left\langle \log \left( \omega \left( \exp^{-\beta \prod_{r=1}^p \frac{1+J_r S_r}{2}} \right) \right) \right\rangle_{\{J_t\}} - \right. \\ & p \left\langle \log \left( 1 + \omega(S) \tanh(\beta u) \right) \right\rangle_u - \\ & p \left\langle \log \left( 1 + \frac{\xi}{2} \prod_{t=1}^{p-1} \left( \frac{1 + J_t \tanh(\beta g_t)}{2} \right) \right) \right\rangle_{\{g_t\},\{J_t\}} + \\ & \left. (p-1) \left\langle \log \left( 1 + \xi \prod_{t=1}^{p} \frac{1 + J_r \tanh(\beta g_t)}{2} \right) \right\rangle_{\{g_t\},\{J_t\}} \right] \end{aligned} \quad \text{(F.22)}$$

which thanks to the relation between $Q(u)$ and $G(g)$, rewrites as

$$\begin{aligned} R_{RS}^{K-SAT}[G,t] = & -\frac{\alpha}{\beta} E \left[ \left\langle \log \left( 1 + (e^{-\beta} - 1) \omega \left( \prod_{t=1}^{p} \frac{1 + J_t S_t}{2} \right) \right) \right\rangle_{\{J_t\}} - \right. \\ & p \left\langle \log \left( 1 + \xi \omega \left( \frac{1 + JS}{2} \prod_{t=1}^{p-1} \frac{1 + J_t \tanh(\beta g_t)}{2} \right) \right) \right\rangle_{\{g_t\},J,\{J_t\}} + \\ & \left. (p-1) \left\langle \log \left( 1 + \xi \prod_{t=1}^{p} \frac{1 + J_r \tanh(\beta g_t)}{2} \right) \right\rangle_{\{g_t\},\{J_t\}} \right] \end{aligned} \quad \text{(F.23)}$$

[1] The sum of the site indices has been eliminated by symmetry.

The last term has been added and subtracted from eq.(6.35) in order to extract a remainder that would vanish if replica symmetry holds, and maximization is performed on $G(g)$. As in the $p$-spin case, we will proceed in a Taylor expansion of expression (F.23) in powers of $\xi$, and rely on absolute convergence to average each term of the series.

Expanding the first term in (F.23) we can write

$$
\begin{aligned}
&E\left[\left\langle \log\left(1+\xi\omega(\prod_{t=1}^{p}\frac{1+J_tS_t}{2})\right)\right\rangle_{\{J_t\}}\right] = \\
&\sum_{n\geq 1}\frac{(-1)^{n+1}}{n}(\xi^*)^n E\left[\left\langle \omega\left(\prod_{t=1}^{p}(1+J_tS_t)\right)^n\right\rangle_{\{J_t\}}\right] = \\
&\sum_{n\geq 1}\frac{(-1)^{n+1}}{n}(\xi^*)^n\Omega\left[\prod_{t=1}^{p}\left(1+\sum_{l=1}^{n}\left\langle J_t^l\right\rangle_{J_t}\sum_{a_1<\ldots<a_l}^{1,n}S_t^{a_1}\ldots S_t^{a_l}\right)\right] = \\
&\sum_{n\geq 1}\frac{(-1)^{n+1}}{n}(\xi^*)^n\Omega\left[\prod_{t=1}^{p}\left(1+\sum_{l=1}^{n}\left\langle J_t^l\right\rangle_{J_t}\sum_{a_1<\ldots<a_l}^{1,n}q^{a_1\ldots a_l}\right)\right] = \\
&\sum_{n\geq 1}\frac{(-1)^{n+1}}{n}(\xi^*)^n\Omega[(1+Q_n)^p]
\end{aligned}
\tag{F.24}
$$

where we have defined $\xi^*\equiv(e^{-\beta}-1)/(2^p)$ and $\sum_{l=1}^{n}\left\langle J^l\right\rangle_J\sum_{a_1<\ldots<a_l}^{1,n}q^{a_1\ldots a_l}\equiv Q_n$. Notice that due to the negative sign of $\xi^*$, the coefficients $(-1)^{n+1}(\xi^*)^n$ are all negative.

The analogous expansion of the second term is:

$$
\begin{aligned}
&E\left[\left\langle \log\left(1+\xi\omega\left(\frac{1+JS}{2}\prod_{t=1}^{p-1}\frac{1+J_t\tanh(\beta g_t)}{2}\right)\right)\right\rangle_{\{J_t\},J,\{g_t\}}\right] = \\
&\sum_{n\geq 1}\frac{(-1)^{n+1}}{n}(\xi^*)^n\Omega\left[\left(1+\sum_{l=1}^{n}\langle J^l\rangle_J\sum_{a_1<\ldots<a_l}^{1,n}q^{a_1\ldots a_l}\right)\left\langle\prod_{t=1}^{p-1}\prod_{l=1}^{n}(1+J_t\tanh(\beta g_t))\right\rangle_{\{J_t\},\{g_t\}}\right] = \\
&\sum_{n\geq 1}\frac{(-1)^{n+1}}{n}(\xi^*)^n\Omega\left[(1+Q_n)\left\langle(1+J\tanh(\beta g))^n\right\rangle_{J,g}^{p-1}\right]
\end{aligned}
\tag{F.25}
$$

Finally, the third terms in eq.(F.23) immediately reads

$$
\left\langle \log\left(1+\xi\prod_{t=1}^{p}\frac{1+J_t\tanh(\beta g_t)}{2}\right)\right\rangle_{\{J_t\},\{g_t\}} = \sum_{n\geq 1}\frac{(-1)^{n+1}}{n}(\xi^*)^n\langle(1+J\tanh(\beta g))^n\rangle_{J,g}^{p} \tag{F.26}
$$

The sum of the three pieces in eq.(F.23) gives:

$$
R_{RS}^{K-SAT}[G,t] = \frac{\alpha}{\beta}\sum_{n\geq 1}\frac{(-1)^n}{n}(\xi^*)^n\Omega\left[\tilde{R}(Q_n,p)\right] \tag{F.27}
$$

with

$$
\tilde{R}(Q_n,p) = (1+Q_n)^p - p(1+Q_n)\langle(1+J\tanh(\beta g))^n\rangle_{J,g}^{p-1} + (p-1)\langle(1+J\tanh(\beta g))^n\rangle_{J,g}^{p} \tag{F.28}
$$

The previous sum is always positive semidefinite for $p$ even while we need $1+Q_n\geq 0$ for $p$ odd.

### F.2.2 ...and of $R_{1RSB}^{K-SAT}$

We proceed in the same way as in the $p$-spin case. The algebra is elementary but more tedious and involved, therefore we will only list the final results of the calculation. Starting from eq.(6.63), we again expand in series the first term, getting, with a treatment similar to the RS case:

$$R_{1RSB}^{K-SAT}[\mathcal{G},t] = \sum_{l\geq 1}\frac{m^l}{l}\sum_{k_1,...,k_l}^{1,\infty}(-\xi^*)^{\sum_{s=1}^l k_s}\prod_{s=1}^{l}\left(\frac{\prod_{r=1}^{k_s-1}(r-m)}{k_s!}\right)\Omega^{(l)}\left[(1+\mathbf{Q}(k_1,...,k_l))^p\right] \quad \text{(F.29)}$$

where we have defined:

$$\mathbf{Q}(k_1,...,k_l) \equiv \sum_{s=1}^{l}\sum_{r_1,...,r_s}^{k_1,...,k_s}\left\langle J^{(r_1+...+r_s)}\right\rangle_J \prod_{t=1}^{s}\sum_{a_1<...<a_{r_t}=1}^{k_1,...,k_s} q^{(a_{r_1},...,a_{r_s})} \quad \text{(F.30)}$$

Analogous steps give for the second term in eq.(6.63)

$$\sum_{l\geq 1}\frac{m^l}{l}\sum_{k_1,...,k_l}^{1,\infty}(-\xi^*)^{\sum_{s=1}^l k_s}\prod_{s=1}^{l}\left(\frac{\prod_{r=1}^{k_s-1}(r-m)}{k_s!}\right)$$
$$\Omega^{(l)}\left[1+\mathbf{Q}(k_1,...,k_l)\right]\left\langle\prod_{s=1}^{l}\left\langle\left(1+J\tanh(\beta g)\right)^{k_l}\right\rangle_g\right\rangle_{G,J}^{p-1} \quad \text{(F.31)}$$

and for the third term

$$\sum_{l\geq 1}\frac{m^l}{l}\sum_{k_1,...,k_l}^{1,\infty}(-\xi^*)^{\sum_{s=1}^l k_s}\prod_{s=1}^{l}\left(\frac{\prod_{r=1}^{k_s-1}(r-m)}{k_s!}\right)\left\langle\prod_{s=1}^{l}\left\langle\left(1+J\tanh(\beta g)\right)^{k_l}\right\rangle_g\right\rangle_{G,J}^{p}, \quad \text{(F.32)}$$

where in the last two terms we can further expand

$$\left\langle\prod_{s=1}^{l}\left\langle\left(1+J\tanh(\beta g)\right)^{k_l}\right\rangle_g\right\rangle_{G,J}^{n} = \left(\sum_{r_1,...,r_l=1}^{k_1,...,k_l}\prod_{s=1}^{l}\binom{k_s}{r_s}\left\langle J^{(r_1+...+r_l)}\right\rangle_J\left\langle\prod_{s=1}^{l}\left\langle\left(\tanh(\beta g)\right)^{r_s}\right\rangle_g\right\rangle_G^{n}\right)$$

with $n$ equal to $p-1$ and $p$ respectively. Since $\xi^*<0$ it is easy to see how only positive terms of the series survive.

Collecting all, we eventually find the complete power expansion for $R_{1RSB}^{K-SAT}$:

$$\frac{\alpha}{\beta m}\sum_{l\geq 1}\frac{m^l}{l}\sum_{k_1,...,k_l}^{1,\infty}(-\xi^*)^{\sum_{s=1}^l k_s}\prod_{s=1}^{l}\left(\frac{\prod_{r=1}^{k_s-1}(r-m)}{k_s!}\right) \cdot \quad \text{(F.33)}$$
$$\Omega^{(l)}\left[(1+\mathbf{Q}(k_1,...,k_l))^p - p(1+\mathbf{Q}(k_1,...,k_l))\mathbf{A}(k_1,...,k_l)^{p-1} + (p-1)\mathbf{A}(k_1,...,k_l)^p\right]$$

where we have defined

$$\mathbf{A}(k_1,...,k_l) \equiv \left\langle\prod_{s=1}^{l}\left\langle\left(1+J\tanh(\beta g)\right)^{k_l}\right\rangle_g\right\rangle_G \quad \text{(F.34)}$$

Again, every term of the expansion is positive for even $p$ and for $p$ odd under condition $1+\mathbf{Q}(k_1,...,k_l)\geq 0$.

### F.2.3 Check of $F_{var}^{K-SAT}[\mathcal{P}] = F_{1RSB}^{K-SAT}[\mathcal{P}]$

As in the case of the $p$-spin, we can show the equivalence of $F_{1RSB}^{K-SAT}[\mathcal{P}]$ and $F_{var}^{K-SAT}[\mathcal{P}]$ at the 1RSB saddle point. We recall that $K \to p$ and $\xi \equiv e^{-\beta} - 1 < 0$ in our notation. In the $K$-SAT case we obtain the specific relations:

$$B_H(h_1, ..., h_{p-1}) \equiv B(\{J_t\}, \{h_t\}) = 1 + \frac{\xi}{2} \prod_{t=1}^{p-1} \left( \frac{1 + J_t \tanh(\beta h_t)}{2} \right) \tag{F.35}$$

$$u_H(h_1, ..., h_{p-1}) \equiv u_J(\{J_t\}, \{h_t\}) = \frac{J}{\beta} \tanh^{-1} \left[ \frac{\frac{\xi}{2} \prod_{t=1}^{p-1} \left( \frac{1+J_t \tanh(\beta h_t)}{2} \right)}{1 + \frac{\xi}{2} \prod_{t=1}^{p-1} \left( \frac{1+J_t \tanh(\beta h_t)}{2} \right)} \right] \tag{F.36}$$

to plug in in eq.(6.52) Along the same line of the general 1RSB computation of chapter 1 we can write the 1RSB free energy as

$$\begin{aligned} F_{1RSB}^{K-SAT}[\mathcal{P}] = \frac{1}{m\beta} \Bigg[ & -\alpha \left\langle \log \left\langle \left( 1 + \xi \prod_{t=1}^{p} \left( \frac{1 + \tanh(\beta h_t)}{2} \right) \right)^m \right\rangle_{h_1,...,h_p} \right\rangle_{P_1,...,P_p} + \\ & \alpha p \left\langle \log \left\langle (1 + \tanh(\beta h) \tanh(\beta u))^m \right\rangle_{u,h} \right\rangle_{Q,P} - \\ & - \sum_k p_k \left\langle \log \left\langle \left( \frac{2 \cosh(\beta \sum_{l=1}^k u_l)}{\prod_{t=1}^k 2 \cosh(\beta u_t)} \right)^m \right\rangle_{u_1,...,u_k} \right\rangle_{Q_1,...,Q_k} \Bigg] \end{aligned} \tag{F.37}$$

where $p_k$ is defined by eq.(F.18), and we already performed the average over the quenched disorder $\mathbf{J}$ exploiting the symmetry of the probability distributions. On the other hand

$$\begin{aligned} F_{var}^{K-SAT}[\mathcal{G}] = \frac{1}{m\beta} \Bigg[ & \alpha(p-1) \left\langle \log \left\langle \left( 1 + \xi \prod_{t=1}^{p} \left( \frac{1 + J_t \tanh(\beta g_t)}{2} \right) \right)^m \right\rangle_{\{g_t\}} \right\rangle_{\{G_t\},\{J_t\}} - \\ & \alpha p \left\langle \log \left\langle \left( \frac{B(\{J_t\}, \{g_t\})}{2 \cosh(\beta u_J(\{J_t\}, \{g_t\}))} \right)^m \right\rangle_{\{g_t\}} \right\rangle_{\{G_t\},\{J_t\},J} + \\ & \left\langle \log \left\langle \left( \frac{1}{2 \cosh(\beta h)} \right)^m \right\rangle_h \right\rangle_P \Bigg] \end{aligned} \tag{F.38}$$

Under the symmetric 1RSB saddle point conditions we can average out the quenched disorder, as before. Thanks to eqs.(6.52), (F.36) and the condition $\mathcal{G} = \mathcal{P}$ we observe that

$$\begin{aligned} \left\langle \log \left\langle \left( \frac{B(g_1, ..., g_{p-1})}{2 \cosh(\beta u(g_1, ..., g_{p-1}))} \right)^m \right\rangle_{\{g_t\}} \right\rangle_{\{G_t\}} = & \left\langle \log \left\langle (1 + \tanh(\beta h) \tanh(\beta u))^m \right\rangle_{u,h} \right\rangle_{Q,P} + \\ & \left\langle \log \left\langle B(h_1, ..., h_{p-1})^m \right\rangle_{\{h_t\}} \right\rangle_{\{P_t\}} \end{aligned} \tag{F.39}$$

Moreover, we can exploit the relations (valid at the saddle point)

$$\begin{aligned} \left\langle \log \left\langle \left( \frac{1}{2 \cosh(\beta u)} \right)^m \right\rangle_u \right\rangle_Q = & \left\langle \log \left\langle \left( \frac{B(g_1, ..., g_{p-1})}{2 \cosh(\beta u(g_1, ..., g_{p-1}))} \right)^m \right\rangle_{\{g_t\}} \right\rangle_{\{G_t\}} - \\ & \left\langle \log \left\langle B(h_1, ..., h_{p-1})^m \right\rangle_{\{h_t\}} \right\rangle_{\{P_t\}} \end{aligned} \tag{F.40}$$

and

$$\left\langle \log \left\langle \left( \frac{1}{2\cosh(\beta h)} \right)^m \right\rangle_h \right\rangle_P = \sum_k p_k \left\langle \log \left\langle \left( \frac{2\cosh(\beta \sum_{l=1}^k u_l)}{\prod_{t=1}^k 2\cosh(\beta u_t)} \right)^m \right\rangle_{u_1,\ldots,u_k} \right\rangle_{Q_1,\ldots,Q_k} - \alpha p \left\langle \log \left\langle \left( \frac{1}{2\cosh(\beta u)} \right)^m \right\rangle_u \right\rangle_Q \quad \text{(F.41)}$$

The proper rescaling with $m$ of the probability distributions (6.52) is crucial in the calculation. Using the last expressions and rearranging terms we eventually find

$$F_{var}^{K-SAT}[\mathcal{P}] = F_{1RSB}^{K-SAT}[\mathcal{P}] \quad \text{(F.42)}$$

at the 1RSB saddle point. Again, the corresponding RS check is even simpler and can be performed along the same lines.

### F.2.4 Existence of the free-energy of the $p$-spin model

Let us briefly sketch the proof of the existence of the thermodynamic limit of free-energy of the $p$-spin model for $p$ even. Let us define a model which interpolates between two non interacting systems with $N_1$ and $N_2$ spins respectively, and a system of $N = N_1 + N_2$ spins. Each clause $\mu = 1, ..., M$ will belong to the total system with probability $t$, to the first subsystem with probability $N_1/N(1-t)$ and to the second subsystem with probability $N_2/N(1-t)$. We chose the indices $i_1^\mu, ..., i_p^\mu$ in the following way: for each clause the indices will be i.i.d. with probability $t$, the indices will be chosen uniformly in the set $\{1, ..., N\}$, with probability $(1-t)N_1/N$ the indices will be chosen in $\{1, ..., N_1\}$ and with probability $(1-t)N_2/N$ in the set $\{N_1+1, ..., N\}$. Let us consider the free-energy $F_N(t) = \frac{-1}{N\beta} \log Z(t)$. A direct calculation of its $t$-derivative

$$\frac{dF_N(t)}{dt} = -\frac{1}{\beta} \left[ \frac{1}{N^p} \sum_{i_1,\ldots,1_p}^{1,N} + \frac{N_1}{N} \frac{1}{N_1^p} \sum_{i_1,\ldots,1_p}^{1,N_1} + \frac{N_2}{N} \frac{1}{N_2^p} \sum_{i_1,\ldots,1_p}^{N_1+1,N} \right] E\langle \log(1 + \tanh(\beta J)\omega(S_{i_1}...S_{i_p})) \rangle_J. \quad \text{(F.43)}$$

Expanding the logarithm in series, observing that thanks to the symmetry of the $J$ distribution the odd term vanish, introducing the replica measure and using the convexity of the function $x^p$ for even $p$ one proves that $\frac{dF_N(t)}{dt} \leq 0$ which implies sub-additivity $F_N \leq \frac{N_1}{N} F_{N_1} + \frac{N_2}{N} F_{N_2}$; this is in turn is a sufficient condition to the existence of the free-energy density. The same prove applies to the even $p$ random $K$-SAT model. For odd $p$ we face a difficulty similar to the one in the replica bounds. We can not prove sub-additivity due to the need to consider negative values of the overlaps, and non convexity of $x^p$ for negative $x$.

# List of Tables

# List of Figures

# Bibliography


[1] T. Morita , J. Phys. Soc. Jap., **12**, 753 (1957); T. Morita , J Math Phys. **13**, 116 (1972); T. Morita , Physica A **83**, 411 (1976); T. Morita , Physica **15**, 951 (1977); T. Morita , Physica A **87**, 117 (1977); S. Katsura, S. Inawashiro and S. Fujiki, Physica A **99**, 193 (1979); L. Viana and A. J. Bray, J. Phys. C, **18**, 3037 (1985); D.J. Thouless, Phys. Rev. Lett. **56**, 1082 (1986); A. Bray and S. Feng, Phys. Rev. B **36**, 8456 (1987); M. Mézard and G. Parisi, Europhys. Lett. **3**, 1067 (1987); I. Kanter and H. Sompolinsky, Phys. Rev. Lett. **58**, 164 (1987); C. De Dominicis and P. Mottishaw, J. Phys. A, **20** L1267 (1987); Y. Y., Goldschmidt, Europhys. Lett., **6**, 7 (1988); J.M. Carlson, J.T. Chayes, L. Chayes, J.P. Sethna and D.J. Thouless, Europhys. Lett. **5**, 355 (1988); K. Y. M. Wong and D. Sherrington, J. Phys. A, **21**, L459 (1988); Y. Y., Goldschmidt and P.-Y. Lai, J. Phys. A, **21** L1043 (1988); Y. Y., Goldschmidt, J. Phys. A, **22** L157 (1989); Y. Y., Goldschmidt and C. De Dominicis, ] J. Phys. A, **22** L775 (1989); Y.Y. Goldschmidt and P.Y. Lai, J. Phys. A **23**, L775 (1990); Y. Y., Goldschmidt and C. De Dominicis, Phys. Rev. B, **41**, 2184 (1990); H. Rieger and T.R. Kirkpatrick, Phys. Rev. B **45**, 9772 (1992);

[2] M. Mézard, G. Parisi, M.A. Virasoro, *Spin Glass Theory and Beyond*, World Scientific, Singapore, (1987).

[3] D. Gross, M. Mézard, *Nuclear Phys. B* **240**, 431 (1984).

[4] E. Gardner, *Nucl. Phys.* **B 257**, 747 (1985).

[5] *Spin glasses and random fields*, A. P. Young ed., World Scientific, Singapore, (1997).

[6] D. J. Amit, *Modeling brain function: the world of attractor neural networks*, Cambridge, University Press, (1989).

[7] R. Monasson, Phys. Rev. Lett., **75**, 2847 (1995).

[8] R. Monasson Phil. Mag. B **77**, 1515, (1998).

[9] R. Monasson and R.Zecchina, *Phys. Rev. Lett.* **76**, 3881 (1996); *Phys. Rev.* **E 56**, 1357 (1997).

[10] R. Monasson, R. Zecchina, S. Kirkpatrick, B. Selman and L. Troyansky, Proceedings of PhysComp 96, T. Toffoli, M. Biafore, J. Leao eds., Boston (1996).

[11] R. Monasson and R. Zecchina, J. Phys. A **31**, 9209 (1998).

[12] R. Monasson, J. Phys. A: Math. Gen. **31**, 513 (1998).

[13] R. Monasson, R. Zecchina, S. Kirkpatrick, B. Selman and L.Troyansky, Random Structures and Algorithms **3**, 414 (1999).

[14] G. Biroli, R. Monasson, M. Weigt, *Europ. Phys. J*, **B 14**, 551 (2000).

[15] J. Berg and M. Sellitto, Phys. Rev. E **65**, 016115 (2002).

[16] A. Lefevre and D. S. Dean, Eur. Phys. J. B **21**, 121 (2001); D. S. Dean, Eur. Phys. J. **15** 493.

[17] A. Barrat and R. Zecchina, Phys. Rev. E **59**, R1200 (1999).

[18] F. Ricci-Tersenghi and R. Zecchina, Phys. Rev. E **62**, R7567 (2000).

[19] F. Ricci-Tersenghi, M. Weigt and R. Zecchina, Phys. Rev. E **63**, 026702 (2001).

[20] S. Franz, M. Mézard, F. Ricci-Tersenghi, M. Weigt and R. Zecchina, Europhys. Lett. **55**, 465 (2001).

[21] M. Leone, F. Ricci-Tersenghi and R. Zecchina, J. Phys. A **34**, 4615 (2001).

[22] S. Franz, M. Leone, F. Ricci-Tersenghi and R. Zecchina, Phys. Rev. Lett. **87**, 127209 (2001).

[23] M. Mézard and G. Parisi, Eur. J. Phys. B **20**, 217 (2001).

[24] M. Mezard, G. Parisi, *The cavity method at zero temperature* cond-mat/0207121.

[25] S. Caracciolo and A. Sportiello, cond-mat/0206352.

[26] M. Mezard, F. Ricci-Tersenghi and R. Zecchina, cond-mat/0207140.

[27] H. Nishimori, *Statistical Physics of Spin Glasses and Information Processing: An Introduction* Oxford, 2001.

[28] P. Poirazi and B. W. Mel, Neuron **29**, 779 (2001).

[29] M. Mezard, G. Parisi and R. Zecchina, *Science*, **297**, 812 (2002).

[30] M. Mezard and R. Zecchina, cond-mat/0207194, to be published in Phys. Rev. E..

[31] R. Monasson, R. Zecchina, S. Kirkpatrick, B. Selman, L.Troyansky, *Nature* **400**, 133 (1999)

[32] M. Weigt, A. K. Hartmann, Phys. Rev. E **63**, 056127 (2001).

[33] M. Weigt, A. K. Hartmann, Phys. Rev. Lett. **84**, 6118 (2000).

[34] M. Garey, and D.S. Johnson, *Computers and Intractability; A guide to the theory of NP–completeness*, W.H. Freeman and Co., San Francisco, 1979; C. Papadimitriou, *Computational Complexity*, Addison–Wesley, 1994;

[35] O. C. Martin, R. Monasson and R. Zecchina, Theoret. Comput. Sci., **265** (2001) 3.

[36] S. Mertens, Computing in Science & Engineering, **4**, 31 (2002) and references therein; Theor. Comp. Science, **265**, 79 (2001); Phys. Rev. Lett. **84**, 1347 (2000); Phys. Rev. Lett., **81**, 4281 (1998).

[37] D. S. Dean, S. N. Majumdar, J. Phys. A. **35**, L501 (2002).

[38] N. Sourlas. Nature **339**, 693-694 (1989).

[39] S. Franz, M. Leone, A. Montanari and F. Ricci-Tersenghi, cond-mat/0205051, To be published in Phys. Rev. E.

[40] H., Jeong et al. Nature **411**, 41 (2001) and references therein; Fickett, J.W. & Wasserman, W.W. *Discovering and modeling of transcriptional regulatory regions.* Curr. Opin. Biotechnol. **11** 19 (2000); Pilpel Y., Sudarsanam P., & Church G.M. *Identifying regulatory networks by combinatorial analysis of promoter elements.* Nature Genetics (2001); Bussemaker, H.J., Li, H. & Siggia, E.D. *Regulatory element detection using correlation with expression.* Nature Genetics (2001); Alberts B. et al. *The Molecular Biology Of The Cell*, **IV** edition, Garland (2002); H. Jeong, S. P. Mason, A.-L. Barabasi and Z. N. Oltvai, cond-mat/0105306; J. Podani, Z. N. Oltvai, H. Jeong, B. Tombor, A.-L. Barabasi, E. Szathmary, cond-mat/0110370; I.J. Farkas, H. Jeong, T. Vicsek, A.-L. Barabasi and Z.N. Oltvai, cond-mat/0205181; M. Caselle, F. Di Cunto, P. Provero, BMC Bioinformatics 3:7, (2002); M. Caselle, F. Di Cunto, M. Pellegrino, P. Provero, physics/0201033; Cheng T., Filkov V. and Skiena S. S., Nec Research Index: http://citeseer.nj.nec.com/chen99identifying.html; A. Vazquez, A. Flammini, A. Maritan and A. Vespignani, cond-mat/0108043; J. Berg, M. Lässig and A. Wagner, cond-mat/0207711 and references therein;

[41] E. Ravasz, A.L. Somera, D.A. Mongru, Z.N. Oltvai and A.-L. Barabasi, Science **297** 1551 (2002) and references therein.

[42] *"The answer is 42."* D. Adams, *The Hitchhiker's Guide to the Galaxy.*

[43] R. Albert and A.-L. Barabasi, Rev. Mod. Phys. **74**, 47 (2002) and references therein;

[44] A. Vazquez, R. Pastor-Satorras, A. Vespignani, Phys. Rev. E **65**, 066130 (2002); A. Vazquez, R. Pastor-Satorras, A. Vespignani, Phys. Rev. Lett. **87**, 258701 (2001).

[45] A. Vazquez, R. Pastor-Satorras, A. Vespignani, cond-mat/0206084;

[46] A. Vazquez, *Degree correlations and clustering hierarchy in networks: measures, origin and consequences*, Ph.D. Thesis (2002) and references therein.

[47] S.A. Cook, *The complexity of theorem–proving procedures* , in *Proc. 3rd Ann. ACM Symp. on Theory of Computing*, Assoc. Comput. Mach., New York, 151 (1971).

[48] Y.-T. Fu, and P.W. Anderson, in *Lectures in the Sciences of Complexity*, D. Stein (ed.), (Addison-Wesley, 1989), p. 815.

[49] D. Mitchell, B. Selman and H. Levesque, "Hard and Easy Distributions of SAT problems," *Proc. of Am. Assoc. for Artif. Intell. AAAI-92*, 456-465 (1992).

[50] S. Kirkpatrick and B. Selman, *Science* **264**, 1297 (1994)

[51] Issue 1–2, *Artificial Intelligence* **81**, T. Hogg, B. A. Huberman, and C. Williams, Eds., (1996)

[52] D. Achlioptas, C. Gomes, D. Liang, H. Kautz, B. Selman, "Generating Satisfiable Problem Instances", preprint.

[53] B. Bollobás, C. Borgs, J.T. Chayes, J.H. Kim, D.B. Wilson, `arXiv:math.CO/9909031` .

[54] A. Goerdt, in *Proc. 7th Int. Symp. on Mathematical Foundations of Computer Science*, 264 (1992); *Journal of Computer and System Sciences*, **53**, 469 (1996)
V. Chvàtal and B. Reed, in *Proc. 33rd IEEE Symp. on Foundations of Computer Science*, 620 (1992)

[55] W. Barthel, A.K. Hartmann, M. Leone, F. Ricci-Tersenghi, M. Weigt and R. Zecchina, Phys. Rev. Lett. **88**, 188701 (2002).

[56] A. Braunstein, M. Mézard and R. Zecchina, in preparation.

[57] J. van Mourik and D. Saad, cond-mat/0207453.

[58] R. Mulet, A. Pagnani, M. Weigt and R. Zecchina, cond-mat/0208460; R. Mulet, A. Pagnani, M. Weigt and R. Zecchina, in preparation; A. Braunstein, M. Weigt and R. Zecchina, in preparation.

[59] G. Parisi, Talk given at "New programs and open problems in the foundation of mathematics and of its applications, in year 2000", Paris. preprint cond-mat/0207334, and references therein.

[60] F. Guerra and F. L. Toninelli, cond-mat/0201092; F. Guerra and F. L. Toninelli,cond-mat/0204280; F. Guerra, cond-mat/0205123; F. Guerra and F. L. Toninelli, cond-mat/0208579.

[61] P. Ërdos and A. Rényi, Publ. Math. Inst. Hung. Acad. Sci., **5**, 17 (1960).

[62] B. Bollobás, *Random Graphs*, Academic Press, London, (1985).

[63] C. Berge, *Graphs and Hypergraphs*, North-Holland, Amsterdam, (1973).

[64] R. M. Tanner, IEEE Trans. Infor. Theory, **27**, 533-547 (1981).

[65] G. D. Forney, Jr., IEEE Trans. Inform. Theory, **47** 520-548 (2001).

[66] F. R. Kschischang, B. Frey and H.-A. Loeliger, submitted to IEEE Trans. Inform. Theory, (1998). Also available at http://www.comm.utoronto.ca/frank/factor/

[67] J. Spencer, *Random Graphs*, Lectures of the 2002 School on "Statistical Physics, Probability Theory and Computational Complexity", I.C.T.P., Trieste (2002).

[68] V.F. Kolchin, *Random graphs* (Cambridge University Press, 1999).

[69] M. E. J. Newman, to appear in Handbook of Graphs and Networks, S. Bornholdt and H. G. Schuster (eds.), Wiley-VCH, Berlin (2002), also available on cond-mat/0202208, and references therein; M. E. J. Newman, S. H. Strogatz and D. J. Watts, Phys. Rev. E **64**, 026118 (2001) and references therein.

[70] M. E. J. Newman, cond-mat/0205405.

[71] J. Berg and M. Lässig, cond-mat/0205589.

[72] A. Vazquez and M. Weigt, cond-mat/0207035.

[73] M. E. J. Newman, Phys. Rev. E **64**, 025102 (2001). D. S. Callaway, J. E. Hopcroft, J. M. Kleinberg, M. E. J. Newman, and S. H. Strogatz, Phys. Rev. E **64**, 041902 (2001); A. Vazquez, M. Boguna, Y. Moreno, R. Pastor-Satorras and A. Vespignani, cond-mat/0209183 and references therein.

[74] G. Biroli and M. Mézard, Phys. Rev. Lett. **88**, 025501 (2002).

[75] G. Toulouse, Comm. Phys. **2**, 115 (1977).

[76] F. Y. Wu, Rev. Mod. Phys. **54**, 235 (1982).

[77] D. Achlioptas and M. Molloy, Electr. J. Comb **6**, R39 (1999).

[78] S. Boettcher and A. G. Percus, Phys. Rev. E **64**, 026114 (2001).

[79] M. Mézard, *Theory of random solid states*, http://ipnli5.in2p3.fr/ lptms/membres/mezard/.

[80] J. Berg and A. Metha, Europhys. Lett. **56**, 784 (2001); J. Berg and A. Metha, Phys. Rev. E **65**, 031305 (2002); J. Berg, S. Franz and M. Sellitto, Eur. Phys. J. B **26** , 349 (2002);

[81] C.A. Angell, Science **267**, 1924 (1995).

[82] T.J. Schaefer, in Proc. 10th STOC, San Diego (CA, USA), ACM, 216 (1978); N. Creignou, H. Daudé, and O. Dubois, preprint `arXiv:cs.DM/0106001`.

[83] A. Gliozzi, Degree Thesis (1998).

[84] E. J. Gumbel, *Statistics of extremes*, Columbia Univ. Press, NY (1958).

[85] C.P. Gomes, B. Selman, N. Crato, K. Kautz, J. of Automated Reasoning **24**, 67 (2000); C.P. Gomes, B. Selman, and H. Kautz. Proc. AAAI-98, 431, Madison, WI, July (1998).

[86] A. Montanari and R. Zecchina, Phys. Rev. Lett. **88**, 178701 (2002).

[87] C. P. Gomes, B. Selman, K. McAloon and C. Tret, Proc. AIPS-98, Pittsburgh, PA, June (1998); C. P. Gomes, B. Selman, and H. Kautz. Proc. AAAI-98, Madison, WI, July (1998).

[88] S. Cocco and R. Monasson, submitted to Annals of Math and Artificial Intelligence, also available at cond-mat/0206242, and references therein.

[89] L. Leuzzi and G. Parisi, J. STAT. PHYS. **103**, 679 (2001).

[90] A. Crisanti, L. Leuzzi and G. Parisi J. Phys. A: Math. Gen. **35**, 481 (2002).

[91] M. Davis, H. Putnam, *J. Assoc. Comput. Mach.*, **7**, 201 (1960)

[92] B. Selman, H. Levesque and D. Mitchell, Proceedings AAAI-92 (1992); B. Selman, H. Kautz and B. Cohen, Proceedings of DIMACS, 661 (1993);
see also http://www.cs.cornell.edu/home/selman/papers-ftp/papers.html;
http://www.cs.cornell.edu/gomes/Papers.htm;
http://www.cs.washington.edu/homes/kautz/walksat/;
http://www.cs.washington.edu/homes/kautz/ and references therein.
Search for SAT related articles at: http://citeseer.nj.nec.com/

[93] S. Cocco and R. Monasson submitted to Phys.Rev.E, also available at cond-mat/0012191, and references therein.

[94] S. Cocco, O. Dubois, J. Mandler and R. Monasson, cond-mat/0206239.

[95] M. Weigt, Eur. Phys. J. B **28**, 369 (2002).

[96] B. Pittel, J. Spencer, and N. Wormald, J. Comb. Theory B **67**, 111 (1996).

[97] M. Bauer and O. Golinelli, Eur. Phys. J. B **24**, 339 (2001).

[98] M. Leone, A. Vazquez, A. Vespignani and R. Zecchina, Eur. Phys. J. B **28**, 191 (2002).

[99] S.H Strogatz, Nature, **410** , 268 (2001).

[100] R. Albert and A.-L. Barabási, Rev. Mod. Phys. **74**, 47 (2002), also available at cond-mat/0106096.

[101] S. N. Dorogovtsev AND J. F. F. Mendes, Adv. Phys. **51**, 1079 (2002), also available at cond-mat/0106144.

[102] A.-L. Barabási and R. Albert, Science **286**, 509 (1999);

[103] A.-L. Barabási, R. Albert, and H. Jeong, Physica A **272**, 173 (1999).

[104] L. A. N. Amaral, A. Scala, M. Barthélémy, and H. E. Stanley, Proc. Nat. Acad. Sci. **97**, 11149 (2000).

[105] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Phys. Rev. Lett. **86**, 3682 (2001).

[106] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Phys.Rev. Lett. **85**, 5468 (2000)

[107] R. Pastor-Satorras, A. Vespignani, Phys. Rev. Lett. **87**, 258701 (2001). Phys. Rev. E 63, 066117 (2001).

[108] A. Aleksiejuk, J. A. Holyst, and D. Stauffer, cond-mat/0112312.

[109] S. N. Dorogovtsev, A. V. Goltsev, and J. F. F. Mendes, Phys.Rev. E **66**, 016104 (2002).

[110] Y. Moreno-Vega and A. Vazquez, cond-mat/0108494.

[111] W. Aiello, F. Chung and L. Lu, Proceedings of the Thirtysecond Annual ACM Symposium on Theory of Computing (2000), 171-180.

[112] M. Molloy and B. Reed, Random Structures and Algorithms **6**, 161 (1995); Combin. Probab. Comput. **7**, 295 (1998).

[113] R. Cohen, D. ben-Avraham and S. Havlin, preprint `cond-mat/0202259`

[114] V. Napolano and R. Zecchina, work in progress

[115] L. Kirousis, E. Kranakis, D. Krizanc, in Proceedings of the 4th European Symposium on Algorithms, 27 (1992); O. Dubois, Y. Boufkhad, Journal of Algorithms **24**, 395 (1997).

[116] T.R. Kirkpatrick and D. Thirumalai, *Phys. Rev. Lett.* **58**, 2091 (1987)

[117] D. Achlioptas, "Setting two variables at a time yields a new lower bound for random 3-SAT", proceedings of STOC 00, p.28 (2000); D. Achlioptas, J. H. Kim, M. Krivelevich and P. Tetali, "Two-Coloring Random Hypergraphs", Random Structures & Algorithms, **20** (2), 249 (2002); D. Achlioptas, A. Chtcherba, G. Istrate, and C. Moore, "The Phase Transition in NAESAT and 1-in-k SAT", in Proceedings of SODA 01, p.721-722, (2001); For a more complete bibliography of D. Achlioptas work, see for instance: http://research.microsoft.com/ optas/work.html.

[118] M.-T. Chao, J. Franco, *Inform. Sci.* **51**, 289 (1990)

[119] D.B. Wilson, preprint at arXiv:math/0005136.

[120] A. Braunstein, M. Leone, F. Ricci-Tersenghi and R. Zecchina, J. Phys. A: Math. Gen. **35**, 7559 (2002).

[121] M.J. Alava et al., in *Phase Transitions and Critical Phenomena*, Vol. 18, C. Domb and J.L. Lebowitz eds. (Academic Press, San Diego, 2001).

[122] T.H. Cormen, C.E. Leiserson, R.L.Rivest, *Introduction to Algorithms* (MIT Press, 1990).

[123] R.L. Rivest, A. Shamir, and L. Adleman, *"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"* (1978). http://mit.edu/ rivest/rsapaper.ps

[124] N. Sourlas, Statistical mechanics and error-correcting codes in "From Statistical Physics to Statistical Inference and Back", Proc. Cargèse 1992, eds. P. Grassberger, J.P. Nadal, 1994, Kluwer Academic, pp. 195-204.

[125] A.Z. Broder, A.M. Frieze, E. Upfal, Proc. 4th Annual ACM-SIAM Symp. on Discrete Algorithms, 322 (1993).

[126] C. Pomerance and S. Goldwasser, *Cryptology and computational number theory.* Factoring (pp 27-48). AMS Proceedings of symposia in applied mathematics, v.42 (1990).

[127] S. Franz, M. Leone, A. Montanari and F. Ricci-Tersenghi, in press in PRE, also available at cond-mat/0205051.

[128] O. Dubois, R. Monasson, B. Selman and R. Zecchina (eds.), Theor. Comp. Sci. **265**, issue 1-2 (2001).

[129] J.-P. Bouchaud, L. F. Cugliandolo, J. Kurchan and M. Mézard, in *Spin Glasses and Random Fields*, A. P. Young ed., (World Scientific, Singapore, 1997)

[130] A. Barg, in *Handbook of Coding Theory*, edited by V. S. Pless and W. C. Huffman, (Elsevier Science, Amsterdam, 1998).

[131] D. A. Spielman, in *Lecture Notes in Computer Science* **1279**, pp. 67-84 (1997).

[132] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, (Wiley, New York, 1991).

[133] A. J. Viterbi and J. K. Omura, *Principles of Digital Communication and Coding*, (McGraw-Hill, New York, 1979).

[134] R. G. Gallager *Information Theory and Reliable Communication* (Wiley, New York, 1968)

[135] C. E. Shannon, Bell Syst. Tech. J. **27**, 379-423, 623-656 (1948)

[136] N. Sourlas, in *Statistical Mechanics of Neural Networks* Lecture Notes in Physics **368**, edited by L. Garrido (Springer, New York, 1990).

[137] N. Sourlas, in *From Statistical Physics to Statistical Inference and Back,* edited by P. Grassberger and J.-P. Nadal (Kluwer Academic, Dordrecht, 1994).

[138] P. Ruján, Phys.Rev.Lett. **70**, 2968-2971 (1993).

[139] N. Sourlas. Europhys.Lett. **25**, 159-164 (1994).

[140] C. Berrou, A. Glavieux, and P. Thitimajshima. Proc. 1993 Int. Conf. Comm. 1064-1070.

[141] R. G. Gallager, *Low Density Parity-Check Codes* (MIT Press, Cambridge, MA, 1963)

[142] D. J. .C. MacKay, IEEE Trans. Inform. Theory **45**, 399-431 (1999).

[143] S. M. Aji, G. B. Horn and R. J. McEliece, Proc. 1998 IEEE Intl. Symp. Inform. Theory (Cambridge, MA), p.276.

[144] J. S. Yedidia, W. T. Freeman, Y. Weiss, in *Advances in Neural Information Processing Systems 13*, edited by T. K. Leen, T. G. Dietterich, and V. Tresp, (MIT Press, Cambridge, MA, 2001)

[145] J. S. Yedidia, W. T. Freeman, and Y. Weiss, *Understanding Belief Propagation and its Generalizations*, 2001. MERL technical report TR 2001-22, available at `http://www.merl.com/papers/TR2001-22`

[146] I. Kanter and D. Saad, Phys. Rev. Lett. **83**, 2660-2663 (1999).

[147] R. Vicente, D. Saad and Y. Kabashima, Phys. Rev. E. **60**, 5352-5366 (1999).

[148] I. Kanter and D. Saad, Phys. Rev. E. **61**, 2137-2140 (1999).

[149] A. Montanari and N. Sourlas, Eur. Phys. J. B **18**, 107-119 (2000).

[150] A. Montanari, Eur. Phys. J. B **18**, 121-136 (2000).

[151] Y. Kabashima, T. Murayama and D. Saad, Phys. Rev. Lett. **84**, 1355-1358 (2000).

[152] I. Kanter and D. Saad, Jour. Phys. A. **33**, 1675-1681 (2000).

[153] R. Vicente, D. Saad and Y. Kabashima. Europhys. Lett. **51**, 698-704 (2000).

[154] A. Montanari, Eur. Phys. J. B **23**, 121-136 (2001).

[155] Y. Kabashima, N. Sazuka, K. Nakamura and D. Saad, *Tighter Decoding Reliability Bound for Gallager's Error-Correcting Codes*, `cond-mat/0010173`.

[156] T. Richardson and R. Urbanke, in *Codes, Systems, and Graphical Models*, edited by B. Marcus and J. Rosenthal (Springer, New York, 2001).

[157] S.-Y. Chung, G. D. Forney, Jr., T. J. Richardson and R. Urbanke, IEEE Comm. Letters, **5**, 58–60 (2001).

[158] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, IEEE Trans. on Inform. Theory, **47**, 569-584 (2001)

[159] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman. IEEE Trans. on Inform. Theory, **47** 585-598 (2001)

[160] J. Pearl, *Probabilistic reasoning in intelligent systems: network of plausible inference* (Morgan Kaufmann, San Francisco,1988).

[161] Y. Kabashima and D. Saad, Europhys. Lett. **44**, 668-674 (1998).

[162] T. Richardson and R. Urbanke, IEEE Trans. Inform. Theory, **47**, 599–618 (2001).

[163] M. Mezard, G. Parisi and M. A. Virasoro, *Spin Glass Theory and Beyond* (World Scientific, Singapore, 1987).

[164] See, for instance, `http://www.digitalfountain.com/technology/index.htm`

[165] C. Di, D. Proietti, E. Telatar, T. Richardson and R. Urbanke, *Finite length analysis of low-density parity-check codes*, submitted IEEE Trans. on Information Theory, (2001)

[166] W. H. Press, B. P. Flannery, S. A. Teukolsky, and W. T. Vetterling, *Numerical Recipes*, (Cambridge University Press, Cambridge, 1986).

[167] S. Franz, G. Parisi, J. Phys. I (France) **5** (1995) 1401

[168] M. Sipser and D. A. Spielman, IEEE Trans. on Inform. Theory, **42**, 1710-1722 (1996).

[169] S. Kirkpatrick, C.D. Vecchi, and M.P. Gelatt, Science **220**, 671 (1983)

[170] B. Derrida. Phys. Rev. B **24**, 2613-2626 (1981).

[171] A. Cavagna, J. P. Garrahan, and I. Giardina, J. Phys. A, **32**, 711 (1999).

[172] H. Nishimori. J. Phys. C **13**, 4071-4076 (1980).

[173] H. Nishimori. Prog. Theor. Phys. **66**, 1169-1181 (1981).

[174] H. Nishimori and D. Sherrington, *Absence of Replica Symmetry Breaking in a Region of the Phase Diagram of the Ising Spin Glass*, `cond-mat/0008139`.

[175] S. Franz and M. Leone, submitted to J. Stat. Phys., also available at cond-mat/0208280.

[176] S. F. Edwards and P. W. Anderson, J. Phys. F: Metal Phys. **5**, 965 (1975).

[177] For a review on the work of mathematicians on spin glass systems see: A. Bovier and P. Picco (eds.) *Mathematical Aspects of Spin Glasses and Neural Networks*, Progress in Probability, Vol. 41, Birkhauser, Boston, 1997.
M. Talagrand, Proceedings of the Berlin international Congress of Mathematicians. Doc. Math., Extra Volume I, (1998) 1 and references therein. We refer to the web page of M. Talagrand for the comprehensive list of references on the work of this author: http://www.math.ohio-state.edu/ talagran/

[178] M. Talagrand Probab. Theory and Relat. Fields **117**, (2000), 303. and *On the p-spin interaction model at low temperature* C. R. A. S., to appear.

[179] A. Bovier and I. Kurkova *Rigorous results on some simple spin glass models* cond-mat/0206562 and references therein.

[180] M. Talagrand Probab. Theory and Relat. Fields **119**, (2001), 187.

[181] K. Nakanishi, Phys. Rev. B **23** (1981) 3514.

# Acknowledgments

Thanks over all to Riccardo, who has always believed in me and trusted me more as a friend than as a simple student.

To Amos, for accepting me in his group even if I was doing completely different things(!).

To the Statistical Mechanics and Interdisciplinary Applications Group at ICTP, that has been so kindly hosting me for such a long time.

Thanks to Riccardo, Silvio, Federico and Martin, who taught me what I know and helped me in every part of this thesis, and are both teachers and friends.

To Marc, for hosting me in Orsay and for being the inspirer of many lines of research my thesis just superficially touches.

To Johannes, for the (not only) scientific discussions and all the good time spent together in Trieste and in Israel; for the tactical choice of Youth Hostels in Jerusalem, the idea to cross the Jordan border at night and the snorkeling in the Red Sea.

To Nicoletta, for standing two "casinisti" office neighbors like Mauro and I, and for solving all administrative and technical problems (very few) I had during my stay at ictp.

To "Gesù Cristo" Mulet for "obvious political reasons" and because it is fun to be with him, always.

To Anna Delin for the amazing determination that leads her to go running three times a week and for her colorful T-shirts: I wish I had one, but I probably have to go to Sweden to find it.

To Andrea and Marcus that reminded me (if there was the need) that no matter where you go the Big-Brains are there.

To Mauro, the only quiet "napolitano" that I got to know. It was a pleasure sharing the office with him this last year.

To Alfredo, the only quiet Argentinian that I got to know, because he is simply the sweetest guy around here and he is truly modest, regardless of his amazing intelligence.

To Marco, for being such a discrete house-mate, but especially a true friend, for the only time we played chess at the Caffè San Marco, for his culture and his intellectual honesty and curiosity. You'll have a happy life.

To Andrea Pagnani, especially for the googd tome spent together in Paris

To Katia, who hosted me in Paris and introduced me to the world of the "fine arts" and the interesting zoology of people that populate it.

To Margherita, that gave me a bed when I had no place to stay; and a glimpse of the multitute of worlds outside physics.

To Gianluca, who standed for a large part of my PhD studies and was always generous in advices and encouragements (and also in good food), especially when I was feeling down; and to his family, that made immediately me feel in Bari as one of them, and whose stories enjoyed me all the time.

To Mario: you were always there to listen to my complaints, *scusate se é poco*. I hope you'll find your way in Brrrlin.

To Davide MIT-"Zoccolansgi" and "il subcomandante" Mario, for the car tours Trieste-Torino-Trieste and to the Italian rail to be always late, as if a seven hours journey was not already long enough.

Thanks to "El Marenduzzo" because you have to be really a *good man* to stand me at lunch time at ICTP every day while I am moaning all the time.

Thanks to Davide, Cristina, Fabio and Sara, Anna and Biri, Angelo, Laura, Andemar, the " Cavaliere Jada", Alessandro M., Vincenzo, Valeria, Katrin, Alexei, Boost and all my other friends at SISSA and ICTP that I have not mentioned but I would have to write a second thesis to explain the whos and whys for everyone.

To "sensitive" Zeljca for her deep feelings, for being "hopelessly ..." and for constantly reminding me what really counts in life.

To Padhu for his Hollywood-Indian style, his "gargarismi", his Indian food that saved me more than once when I came home late and hungry and with nothing in the icebox. It has been a pleasure to share the apartment with him for one year.

To Francesco "Frank" for his dinners and coffee breaks, his encouragements and vitality.

Thanks to Cristina and all my friends met in Boulder, especially the Longs Peak group. I can share memories with them that I'll never forget.

Thanks to "Kill-the-rock" Martin and his checkian-style sense of humor, to Katka for standing him and to Matjei for probably standing both of them. Martin, going climbing with you has been a part of my life I'll tell my grand children about. thanks for saving my life coming down Netopir, in Osp! And thanks not to have killed me when I was belaying you the wrong side!! I hope we'll climb together again.

Thanks to Flaminia and Riccardo, for the "Tigelle", the wonderful time climbing and singing together, and the days in Paklenica.

To Alessandro, for the good times climbing and saying foolish things together. And thanks in particular for the mythical September 1st ascension to the Jôf Fuart: the real crucial step in the writing of this Thesis.

Thanks to Raffaella, that showed me how immense sweetness and steadiness can coexist in the same person.

Thanks to Eric, Serena, Marco and to the Olympic Rock team that remind me that in life, beyond all, you must pursue what you like to do and that at the end the happy man is the one who surrender to his passions. Teaching rock climbing was one of them.

Thanks to my parents and my family, who never ask me why am I doing this and are always happy with the choices I make. To my mom for being so profound and for having taught me the beauty of nature around me, to my dad for being hopelessly like me (or vice-versa ?), to Nonna for her optimism about life, and overwhelming vitality, to Fely and Ago for their love and to Luca for being not a cousin but a brother.

Thanks to Antonio and Alberto for always being my best friends.

Thanks to Cecilia, for sharing her life with me even through troubled times.

Thanks to the Hungarian fried mushrooms for breakfast in Sopron, that reminded me that home is there wherever one feels to be at home.

*"So long, and thanks for all the fish."*