Hiding Quiet Solutions in Random Constraint Satisfaction Problems

Florent Krzakala[1,2] and Lenka Zdeborová[2]

[1]CNRS and ESPCI ParisTech, 10 rue Vauquelin, UMR 7083 Gulliver, Paris 75000 France

[2]Theoretical Division and Center for Nonlinear Studies, Los Alamos National Laboratory, Los Alamos, New Mexico 87545 USA

(Received 16 January 2009; revised manuscript received 14 April 2009; published 8 June 2009)

We study constraint satisfaction problems on the so-called *planted* random ensemble. We show that for a certain class of problems, e.g., graph coloring, many of the properties of the usual random ensemble are quantitatively identical in the planted random ensemble. We study the structural phase transitions and the easy-hard-easy pattern in the average computational complexity. We also discuss the finite temperature phase diagram, finding a close connection with the liquid-glass-solid phenomenology.

DOI: 10.1103/PhysRevLett.102.238701 PACS numbers: 89.70.Eg, 64.70.qd, 75.50.Lk

Constraint satisfaction problems (CSPs) stand at the root of the theory of computational complexity [1] and arise in computer science, physics, engineering, and many other fields of science. Consider a set of N discrete variables and M Boolean constraints; the problem consists in finding a configuration of variables that satisfies all the constraints or in proving that no such configuration exists. Algorithmical approaches to intrinsically hard NP-complete CSPs [1] are one of the biggest challenges in today's science. Ensembles of random CSPs, where the constraints are chosen uniformly at random from some prescribed distribution, are being used to understand the average computational complexity [2]. Statistical physics techniques have shed new light on the problem and on the origin of the average algorithmical hardness [3,4].

A major point in evaluating the performance of new algorithms for hard CSPs is to be able to generate difficult instances that are guaranteed to be satisfiable. *Planting* is the most standard way to do so: one first chooses a configuration of variables and *then* considers only constraints which are compatible with this planted configuration. Many planting protocols have been introduced [5–7]; however, the understanding of when and why they provide a difficult instance is still very poor compared to what is known for the purely random ensemble [3,4]. This is because planting a solution changes the properties of the ensemble. It is moreover often anticipated that the planted solution is easier to find than a random one, as has been indeed proven for high density of constraints [8]. Hard instances with a known solution are also appealing to cryptographic application as they provide good one-way functions. Planted instances may also result from applications where only constraints compatible with an initial state of the system are added.

In this Letter we show that for a specific, yet large, class of CSPs, one can easily generate planted instances by hiding a *quiet* solution that does not have influence on most of the characteristics of the ensemble. The canonical example of a CSP where a solution can be planted in the *quiet* way is the graph q-coloring problem on which we shall illustrate our findings about the phase diagram and the average algorithmical hardness. In the conclusion, we discuss the class of problems that allow such a quiet hiding.

Hiding without changing.—The graph coloring problem [9,10] consists in deciding if the N vertices of a graph can be colored using only q colors in such a way that every two adjacent vertices have different colors. The control parameter is the average degree of variables c, and we consider the thermodynamical limit $N \to \infty$.

The way to plant a quiet solution in the graph coloring problem is actually the most natural one: One assigns a random color with equal probability to each of the N vertices, and then constructs the graph by randomly throwing links between vertices of different colors. Using the cavity method [11] we describe the phase diagram and the structure of solutions in this planted ensemble. In the large N limit, the degree distribution in the planted graphs is Poissonian with mean c, and thus they are locally treelike just as the standard random Erdös-Rényi graphs. Following the cavity approach [10,11] the Belief-Propagation (BP) equations can be written. Denote $\psi_s^{i\to j}$ the probability that the site i takes color s in the absence of the site j:

$$\psi_s^{i\to j} = f(\{\psi^{k\to i}\}) = \frac{1}{Z^{i\to j}} \prod_{k\in\partial i\setminus j} (1 - \psi_s^{k\to i}), \qquad (1)$$

where $Z^{i\to j}$ is a normalization ensuring that $\sum_{s=1}^{q} \psi_s^{i\to j} = 1$. The entropy (the logarithm of the number of proper colorings) is computed from the fixed point of Eq. (1) as

$$S = \sum_i \log\Big[\sum_{s=1}^{q} \prod_{j\in\partial i} (1 - \psi_s^{j\to i})\Big] - \sum_{(ij)} \log\Big(1 - \sum_{s=1}^{q} \psi_s^{j\to i}\psi_s^{i\to j}\Big). \qquad (2)$$

The entropy per site $s = S/N$ can thus be computed if the distribution $P(\psi)$ over the graph is known. Assuming the absence of long range correlations, recursive equations on this distribution can be written and solved via the population dynamics technique [11]. In the planted ensemble one needs to distinguish between the sites that were planted with different colors; we thus consider q distributions:

$$P_s(\psi) = \sum_{k=0}^{\infty} \frac{e^{-c} c^k}{k!} \frac{1}{(q-1)^k} \sum_{s_1,\ldots,s_k \neq s} \int \prod_{i=1}^{k} [P_{s_i}(\psi^i) d\psi^i] \times \delta[\psi - f(\{\psi^i\})], \quad (3)$$

where s is taking values $1, \ldots, q$, and function $f(\cdot)$ was defined in Eq. (1). The fixed point of (3) may depend on the initial conditions. One might initialize $P_s(\psi)$ randomly or in the planted solution [where all the elements in $P_s(\psi)$ are vectors fully oriented in the direction of the color s]. The dependence on initial conditions is a generic sign for the appearance of different Gibbs states.

Let us first review the properties of the purely random ensemble. The space of solutions in the coloring of random graphs undergoes several transitions as average degree c is increased [3,10]: For low degree $c < c_d$ almost all solutions (proper colorings of the graph) belong to a single Gibbs state and the problem can be studied using the BP approach. For $c > c_d$, the space of solutions shatters into exponentially many different clusters, each corresponding to a different Gibbs state. In this case, a technique called one-step replica symmetry breaking (1RSB) [3,11] is used to describe the phase space. To focus on clusters of a given size we introduce the Parisi 1RSB parameter m, clusters are then weighted by their size to the power of m [10,12]. For $c < c_c$ a typical solution belongs to a cluster corresponding to the value $m = 1$. For $c > c_c$, although exponentially many clusters exist, a random solution will with high probability belong to one of the few largest clusters, corresponding to $0 < m < 1$, while the $m = 1$ clusters do not exist anymore; this is called the condensed phase [3]. Finally for $c > c_s$ the last cluster disappears and no solutions exist anymore. On top of this geometrical behavior in the space of solutions, a remarkable phenomenon appears within the clusters themselves. In some of them a finite fraction of variables are allowed only one color (a phenomenon call *freezing)* [10,13]. To the best of our knowledge, no existing algorithm is able to find solutions in the frozen clusters in polynomial time [4,10,14], and since in a region near to the colorability threshold all clusters are frozen this provides a bound on the algorithmically hard phase.

Coming back to the planted ensemble, notice that Eq. (3) is nothing else but the 1RSB equation for the coloring of purely random graphs at $m = 1$ [compare, e.g., with Eq. (C4) in [10], or with the equations for the reconstruction on trees [15]]. It is known from [15] that if (3) is initialized in the planted configuration then in the fixed point the distribution P_s is biased towards color s above the reconstruction threshold, i.e., for average degree $c > c_d$ [15]. The value c_d is then a spinodal point for the existence of a *planted* Gibbs state containing the planted configuration. From the equivalence of Eq. (3) with the 1RSB equation at $m = 1$ for the purely random ensemble it also follows that both the planted and the purely random ensembles admit the so-called liquid solution where all $\psi_s = 1/q$. A linear stability analysis shows that the liquid solution is locally stable against small perturbations towards the planted solution for $c < c_l = (q-1)^2$ [16]. Above c_l the only stable fixed point of (3) is strongly biased towards the planted configuration and c_l is therefore a spinodal point for the liquid state. The fact that the liquid solution is stable for $c < c_l$ also means that the properties of the phase space are not affected by the very existence of the planted state. This leads us to the important conclusion—which we call *quiet* planting—that in this region the properties of the planted ensemble are exactly the same as the properties of the purely random ensemble, up to the existence of the planted state [17].

For completeness let us mention that, just as in the purely random ensemble [10], the liquid solution in the planted ensemble decomposes further into 1RSB states for $c > c_d$. Properties of these states can be obtained by solving the 1RSB equations. In the planted ensemble, the 1RSB equations have only one nontrivial solution, independent from the planted configuration, and identical to the 1RSB solution in the purely random ensemble. Since the liquid state is identical in the two ensembles, it is not so surprising that the glassy states are identical as well.

Phase diagram of planted coloring.—We now describe the phase diagram of the planted ensemble (Fig. 1). Up to the average degree c_d almost all solutions belong to one single large cluster or state of entropy $s_{\mathrm{BP}} = \log q + (c/2)\log(1 - 1/q)$. Above c_d the space of solutions splits into exponentially many clusters, as in the purely random ensemble. As the planted cluster or state is described by the solution of (3) it has all the properties of the $m = 1$ clusters from the purely random ensemble. In particular, for $c_d < c < c_c$ the planted cluster is one of the exponentially many equilibrium clusters and thus for $c < c_c$ the purely random and planted ensembles of random graphs are asymptotically equivalent. Interestingly, this equivalence has been rigorously proven in [18], however only up to an average degree $c_q < c_c$ [19] with $c_q \to c_c$ as $q \to \infty$.

For $c > c_c$ all the nonplanted $m = 1$ clusters disappear and the size of the planted cluster becomes larger than the total size of the remaining clusters. A first order transition happens and the planted state dominates the total number of solution. The entropy is thus given by the ''planted'' fixed point of (3) plugged into (2). Another transition appears at c_s (the colorability threshold in the purely random ensemble) beyond which all clusters disappears *except* the planted one. The values of c_d, c_c, and c_s given q are identical to those in the purely random ensemble (see [10]).

The properties of the planted cluster can be studied numerically on a single graph (as was done for satisfiability in [7]). We checked on many instances that the BP equations (1) initialized in the planted configuration converge to the liquid fixed point for $c < c_d$, and to the planted one for $c > c_d$, while when initialized randomly they converge to the planted fixed point only for $c > c_l$. We have checked that the appearance of frozen variables [10,13] follows exactly the theoretical prediction (see Fig. 2).

Easy-hard-easy pattern.—If one does not discover the planted cluster, the planted and the purely random graphs

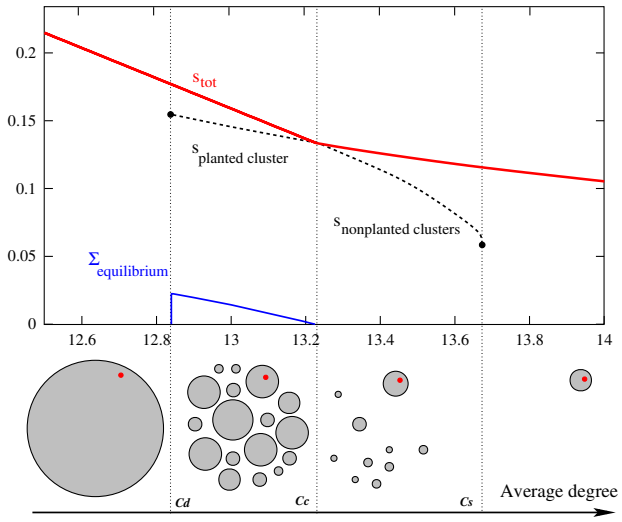

FIG. 1 (color online). Phase diagram on the 5-coloring on the planted ensemble. Bottom: Sketches of the clustering. At an average degree c_d the space of solutions shatters into exponentially many clusters, the planted cluster being one of them. Beyond c_c the planted cluster contains more solutions than all the others together. At c_s the last nonplanted cluster disappears. Top: Total entropy s_{tot} with the subdominant part (dashed). The equilibrium complexity $\Sigma_{\mathrm{equilibrium}}$ (logarithm of the number of dominant clusters), the entropy of the nonplanted clusters and critical degrees are taken from [10].

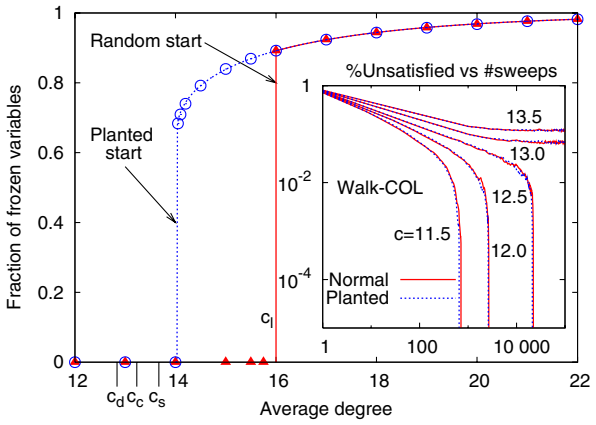

FIG. 2 (color online). Fraction of variables frozen in their planted colors in 5-coloring of a $N = 10^5$ graph. Data obtained from the BP fixed point when initialized randomly (full triangles) and in the planted configuration (also called the whitening [20], empty circles), compared to the theoretical predictions [10,13] (full and dashed lines). For $c > c_l = 16$ BP converges spontaneously to the planted fixed point. For $c < 14.04$ [13] there are no frozen variables in the planted cluster. Inset: Fraction of monochromatic edges versus the number of sweeps of the Walk-COL algorithm [10] in 5-coloring of a purely random and a planted graph, $N = 10^5$. Quiet planting does not seem to affect the computational hardness in the region $c < c_s$.

are indistinguishable and we expect that they have comparable algorithmic difficulty. This is indeed what we observed in experiments with several solvers. Figure 2 shows results of the Walk-COL algorithm [10] on both the planted and purely random graphs. No difference is visible; thus (unless the planted cluster intervenes), the easy-hard pattern observed in the colorable phase $c < c_s$ is the same in both the ensembles. It has been empirically argued this transition is related to the freezing of clusters [10].

On the other hand, for very large degree $c \gg c_s$ it is known that even simple message passing algorithms find a solution near the planted one [8]; therefore, a second hard-easy transition must exist. This is due to the aforementioned linear instability at c_l: Since for $c > c_l$ BP (1) converges spontaneously towards the planted fixed point (as shown in Fig. 2) it is easy to find solutions from the planted cluster above c_l (e.g., BP decimation algorithm finds solutions in linear time). For $c < c_l$, however, without prior knowledge of the planted configuration BP converges to the uniform liquid fixed point. Applying the state of art algorithms (BP decimation, BP reinforcement, Walk-COL, simulated annealing, etc.) to planted instances for $c_s < c < c_l$ we were indeed not able to find solutions in polynomial time. This suggests that the hard-easy algorithmic transition in the planted ensemble arises exactly at c_l. Note at this point that since $c_d = c_l$ for $q = 3$, the planted 3-coloring is algorithmically easy for all degrees.

Phase diagram at finite temperature.—It is finally of interest to consider the properties of the problem at finite temperature T, using a unit energy cost for every monochromatic edge. The BP and the 1RSB equations can be easily extended to this situation as, e.g., in [10]. Note, however, that at $T > 0$ the equations for the planted ensemble do not correspond anymore to the 1RSB equations at $m = 1$, making the finite temperature problem richer. In fact, the system behaves just as a usual mean field glass problem, with its liquid-glass transition, where the planted state acts as a solidlike (or crystal) phase. This solid or planted phase exists below an upper spinodal temperature T_1 (that starts at c_d, see Fig. 3), and the liquid solution $\psi_s = 1/q$ becomes unstable towards this solid state as it encounters a spinodal point at

$$T_2 = -1/\log\left[\frac{c-(q-1)^2}{q-1+c}\right], \tag{4}$$

which starts at c_l at $T = 0$ (see Fig. 3). As usual in first order phase transitions, the free energy of the liquid and solid state have to be compared to draw the equilibrium phase transition line, starting at c_c at $T = 0$. As in the purely random ensemble the liquid state undergoes a dynamical and Kauzmann glass transition (Fig. 3). The 3-coloring is particular: the two spinodals coincide, making the equilibrium transition of a second order. A similar phase diagram as in Fig. 3 was found in [21] for the ferromagnetic p-spin model, in fact that model is just a particular case of our quiet planting setting. In [21], however, the liquid state is always stable and finding the ground state is polynomial due to the linearity of the problem.

The inset of Fig. 3 shows the behavior of Monte Carlo annealing for $c > c_l$ to illustrate the liquid-glass-solid

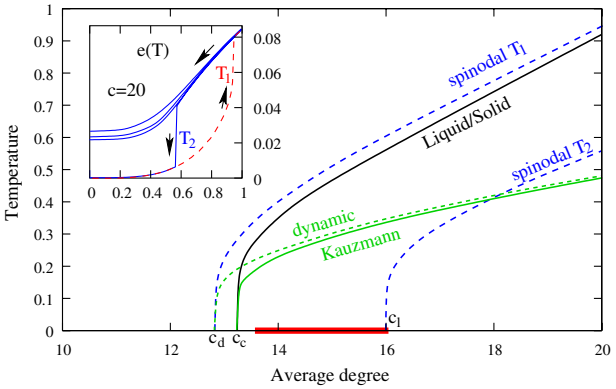

FIG. 3 (color online). Finite temperature phase diagram of the planted 5-coloring. At high temperature the liquid is the unique Gibbs state. Below the higher spinodal line T_1 a planted (solid) Gibbs state appears, and becomes thermodynamically dominant at the liquid-solid transition. The supercooled liquid state is locally stable until the lower spinodal line T_2. The liquid undergoes the usual dynamical and Kauzmann (ideal) glass transitions (data from [10]). The thick line depicts the algorithmically hard region, the left boundary being the freezing transition [10]. Inset: Energy versus temperature in Monte Carlo annealing with rate $\delta T = 10^{-2}, 10^{-3}, 10^{-4}$, and 10^{-5} per sweep for $N = 5 \times 10^5$ at $c = 20 > c_l$. Above c_l a slow enough annealing undergoes a transition towards the planted state.

phenomenology: Upon lowering the temperature, the liquid can be supercooled, the solid phase avoided, and a glass transition observed. But with slow enough annealing the system transits to the solid (planted) state at temperature T_2. In this case a simple simulated annealing is able to find the ground state. If the system is initialized in the planted solution and the temperature is increased, the solid will melt to the liquid state at temperature T_1. For connectivities $c \leq c_l$ the absence of the liquid spinodal line and the mean field nature of the model (barriers between states are extensive) makes algorithms based on local dynamics unable to find the planted cluster. This gives a physical interpretation behind the hard-easy transition at c_l.

Conclusion.—We have discussed the graph coloring problem on the planted ensemble and showed that quantitative results, explicitly checked via numerical experiments, can be readily deduced from what is known in the purely random ensemble. In particular we showed that for $c < c_c$ the planted ensemble is asymptotically equivalent to the purely random ensemble. Several papers have established the easiness of the planted ensemble at very large [8] or at very small average degree. Here we bridged the gap and showed that while the easy-hard transition in the planted ensemble is similar to the one in the usual random ensemble, the hard-easy transition coincides with a local instability of the liquid phase at $c_l = (q-1)^2$. This leaves a large region of very hard problems with a known hidden solution. We also showed how to create mean field "glass" models with a solidlike or planted state.

Let us finish by discussing the (large) class of CSPs where the quiet planting is possible and where our phenomenology readily applies. The crucial property that we used when stating that the natural planting does not change much of the structural properties was the uniformity of the BP fixed point in the purely random ensemble [e.g., in coloring $\psi = (1/q, \ldots, 1/q)$]. Many other CSPs actually share this property, e.g., all the problems without disordered interactions on random regular graphs, the hypergraph bicoloring [14], or the balanced locked problems of [4]. These last ones are particularly appealing as hard satisfiable benchmarks. The random satisfiability problem, however, is a canonical example where the fixed point of the BP equation is not uniform and where our results do not apply. It would be interesting to generalize our approach to plant quiet solutions in such cases.

[1] S. A. Cook, in *Proceedings of the 3rd STOC* (ACM, New York, 1971).
[2] P. Cheeseman, B. Kanefsky, and W. M. Taylor, in *Proceedings of the 12th IJCAI Conference* (Morgan Kaufmann, San Mateo, CA, 1991).
[3] M. Mézard and R. Zecchina, Phys. Rev. E **66**, 056126 (2002); F. Krzakala *et al.*, Proc. Natl. Acad. Sci. U.S.A. **104**, 10 318 (2007).
[4] L. Zdeborová and M. Mézard, Phys. Rev. Lett. **101**, 078702 (2008); J. Stat. Mech. (2008) P12004.
[5] W. Barthel *et al.*, Phys. Rev. Lett. **88**, 188701 (2002).
[6] H. Haanpää *et al.*, JSAT **2**, 27 (2006); D. Achlioptas *et al.*, in *Proceedings of AAAI-2000, Austin, Texas* (AAAI Press, Menlo Park, CA, 2000); D. Achlioptas, H. Jia, and C. Moore, J. Artif. Intell. Res. **24**, 623 (2005); C. Moore, H. Jia, and D. Strain, in *Proceedings of AAAI* (AAAI Press, Menlo Park, CA, 2005).
[7] K. Li, H. Ma, and H. Zhou, Phys. Rev. E **79**, 031102 (2009).
[8] R. Monasson, F. Altarelli, and F. Zamponi, J. Phys. A **40**, 867 (2007); S. Ben-Shimon and D. Vilenchik, in DMTCS Proceedings AH, 2007 Conference on Analysis of Algorithms, AofA 07, pp. 217–226; A. Coja-Oghlan, M. Krivelevich, and D. Vilenchik, in 2007 Conference on Analysis of Algorithms, AofA 07, pp. 89–102.
[9] R. Mulet *et al.*, Phys. Rev. Lett. **89**, 268701 (2002).
[10] L. Zdeborová and F. Krzakala, Phys. Rev. E **76**, 031131 (2007); F. Krzakala and L. Zdeborová, Europhys. Lett. **81**, 57005 (2008).
[11] M. Mézard and G. Parisi, Eur. Phys. J. B **20**, 217 (2001).
[12] M. Mézard, M. Palassini, and O. Rivoire, Phys. Rev. Lett. **95**, 200202 (2005).
[13] G. Semerjian, J. Stat. Phys. **130**, 251 (2008).
[14] L. Dall'Asta *et al.*, Phys. Rev. E **77**, 031118 (2008).
[15] M. Mézard and A. Montanari, J. Stat. Phys. **124**, 1317 (2006).
[16] This is the usual "local" spin glass instability [10].
[17] In fact $q!$ states, due to the color-permutation symmetry.
[18] D. Achlioptas and A. Coja-Oghlan, arXiv:0803.2122.
[19] With $c_q = 3.83(q = 3)$ and $c_q = 7.81(q = 4)$.
[20] G. Parisi, arXiv:cs.CC/0212047.
[21] S. Franz *et al.*, Europhys. Lett. **55**, 465 (2001).