Generating hard and solvable satisfiability problems: A statistical mechanics approach

W. Barthel,[1] A.K. Hartmann,[2] M. Leone,[3,4] F. Ricci-Tersenghi,[4,5] M. Weigt,[1] and R. Zecchina[4,6]

[1] *Institute for Theoretical Physics, University of Göttingen, Bunsenstr. 9, 37073 Göttingen, Germany*
[2] *Laboratoire de Physique Statistique de l'ENS, 24 rue Lhomond, 75231 Paris cedex 05, France*
[3] *SISSA, via Beirut 9, 34100 Trieste, Italy*
[4] *International Centre for Theoretical Physics, Strada Costiera 11, P.O. Box 586, I-34100 Trieste, Italy*
[5] *Dipartimento di Fisica, Università di Roma "La Sapienza", Piazzale Aldo Moro 2, 00185 Roma, Italy*
[6] *Laboratoire de Physique Théorique et Modèles Statistiques, Université Paris Sud, 91405 Orsay, France*

(Dated: December 4, 2001)

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 propose random generators of hard and satisfiable instances for the 3-satisfiability problem (3-SAT). The design of the hardest problem instances is based on the existence of a first order ferromagnetic phase transition and to the glassy nature of excited states. The analytical predictions are corroborated by numerical results obtained from complete as well as stochastic local algorithms.

PACS numbers: 89.20.Ff, 75.10.Nr, 05.70.Fh, 02.70.-c

In natural sciences and in artificial systems, there exist many problems whose solution requires computational resources growing exponentially with the number of variables N needed for their encoding. Concrete examples are optimization and cryptographic problems in computer science, glassy systems and random structures in physics and chemistry, random graphs in mathematics, and scheduling problems in real-world applications.

The theory of computational complexity [1] deals with the issue of identifying equivalence classes among such problems depending on the scaling of the computational cost. Problems which can be solved in polynomial time are considered to be tractable and compose the so-called Polynomial (P) class. The harder problems are grouped in a larger class (which includes P) called NP, where NP stands for 'non-deterministic polynomial time'. These problems are such that a potential solution can be checked rapidly in polynomial time, while finding a solution may require exponential time in the worst case. In turn, the hardest problems in NP belong to a subclass called NP-complete: An efficient algorithm for solving one NP-complete problem could be easily modified to effectively solve any problem in NP. By now, a huge number of NP-complete problems has been identified, and the lack of such an algorithm corroborates the widespread conjecture P≠NP, i.e. that no such algorithm exists.

Complexity theory is based on a worst-case analysis which frequently does not describe typical, i.e. real-world applications. To deepen the understanding of typical-case complexity, computer scientists have recently focused their attention on the study of random instances of hard combinatorial problems, seeking for a link between the onset of exponential-time complexity and some intrinsic (i.e. algorithm independent) properties of the randomized NP-complete problems [2, 3]. These new developments opened the field to statistical physics methods.

In this context, the study of random 3-SAT problems has played a major role. A random 3-SAT formula F consists of M logical clauses $\{C_\mu\}_{\mu=1,\dots,M}$ over a set of N Boolean variables $\{x_i = 0,1\}_{i=1,\dots,N}$. Every clause consists of three randomly chosen Boolean variables which are connected by logical OR operations and appear negated with probability $1/2$, e.g. $C_\mu = (x_i \vee \overline{x}_j \vee x_k)$. In F the clauses are connected by logical AND operations, $F = \bigwedge_{\mu=1}^{M} C_\mu$, so that all clauses have to be satisfied simultaneously in order to satisfy the formula.

A satisfying logical assignment of the x_i is also called a solution of F. The random 3-SAT model was found to undergo a SAT/UNSAT transition [4, 5] at a critical ratio $\alpha = M/N \simeq 4.25$ (for large N): Below this threshold, almost all formulae are satisfiable, while beyond almost all formulae do not show any satisfying solution. At this phase boundary there appears a strong exponential peak in the typical (median) cost for finding solutions by the best known algorithms. Problem instances generated close to the SAT/UNSAT threshold form a natural test bed for the optimization of heuristic search algorithms which are used in many benchmark libraries, see e.g. the SATLIB [6]. However, satisfiable and unsatisfiable instances coexist in the vicinity of the phase transition. Many algorithms of practical interest are based on *incomplete* stochastic local search procedures, as e.g. simulated annealing [7] and the walk-SAT algorithm [8]. These algorithms stop once they have found a solution, but they have no way to disentangle, in finite time, if a formula is unsatisfiable or just hard to solve. It is thus very important to design generators of random problem instances which are satisfiable and for which the algorithmic proof of this satisfiability takes exponential time.

In this Letter, we propose simple and fast generators for large 3-SAT problem instances, which are satisfiable and hard at the same time. The main ideas are inspired by physical requirements, and exploit the presumed hardness of randomized 3-SAT itself (see Ref. [9] for an example of a different generator based on the so-called Latin squares completion problem). One possibility [6] would be to filter the problems at the phase boundary by complete algorithms, and to keep only the satisfiable ones. This method is limited by the small values of N and M which can be handled by the filtering algorithms, thus making the generation itself exponentially long.

We choose an arbitrary assignment of our logical variables and accept with some prescribed probability only clauses which are satisfied by this assignment. Without loss of generality, we restrict ourselves to generating formulae which are forced to be satisfied by $x_i^{(0)} = 1$, $\forall i = 1,..,N$ [10]. So, only clauses containing three negated variables are excluded, all other clauses being satisfied by $\vec{x}^{(0)}$. The generation of random 3-SAT formulae is done as follows. For every clause, we draw randomly and independently three indices (i,j,k), $i,j,k \in \{1,...,N\}$. Then, we choose one of the seven allowed clauses with the following probabilities: clause $(x_i \vee x_j \vee x_k)$ – type "0" – with probability p_0; each of the clauses $(\overline{x}_i \vee x_j \vee x_k)$, $(x_i \vee \overline{x}_j \vee x_k)$ and $(x_i \vee x_j \vee \overline{x}_k)$ – type "1" – with probability p_1; and finally each of $(\overline{x}_i \vee \overline{x}_j \vee x_k)$, $(\overline{x}_i \vee x_j \vee \overline{x}_k)$ and $(x_i \vee \overline{x}_j \vee \overline{x}_k)$ – type "2" – with probability p_2. Thus, the probabilities are restricted by $p_0 + 3p_1 + 3p_2 = 1$. The formula can be written in the following symbolic way $F = \bigwedge_{\mu=1}^{\alpha N} C_\mu = F_0 \bigwedge F_1 \bigwedge F_2$, where F_0, F_1, F_2 are just the sub-formulae composed of the three types of clauses of mean length $p_0 \alpha N$, $3p_1 \alpha N$ and $3p_2 \alpha N$ respectively. As we will show in the following, typically hard instances can be generated if the parameters are chosen as follows:

$$
\begin{array}{cc}
\alpha > 4.25 \quad , & 0.077 < p_0 < 0.25 \ , \\
p_1 = (1-4p_0)/6 \ , & p_2 = (1+2p_0)/6 \ \ .
\end{array}
$$

The hardness of typical formulae increases with p_0. In order to understand the behavior of this model, and to find values for p_0, p_1 and p_2 such that the instances are as hard as possible, we have followed a statistical mechanics approach corroborated by numerical simulations based on both complete and randomized algorithms. The analysis is based on the standard representation of 3-SAT as a diluted spin-glass model [11]: The Boolean variables $x_i = 0, 1$ are mapped to Ising spins $S_i = \pm 1$, and the Hamiltonian counts the number of unsatisfied clauses,

$$
\mathcal{H} = \frac{\alpha}{8} N - \sum_{i=1}^{N} H_i S_i - \sum_{i<j} T_{ij} S_i S_j - \sum_{i<j<k} J_{ijk} S_i S_j S_k \quad (1)
$$

with $H_i = \frac{1}{8} \sum_\mu c_{\mu,i}$, $T_{ij} = -\frac{1}{8} \sum_\mu c_{\mu,i} c_{\mu,j}$, and $J_{ijk} = \frac{1}{8} \sum_\mu c_{\mu,i} c_{\mu,j} c_{\mu,k}$, where $c_{\mu,i}$ equals $+1$ if x_i appears directly in C_μ, -1 if it appears negated, and 0 otherwise. The interactions in Eq. (1) fluctuate from sample to sample, with disorder-averaged values $\overline{H_i} = \frac{\alpha}{8}(p_0 + p_1 - p_2)$, $\overline{T_{ij}} = \frac{\alpha}{4N}(-p_0 + p_1 + p_2)$, and $\overline{J_{ijk}} = \frac{3\alpha}{4N^2}(p_0 - 3p_1 + 3p_2)$.

We are interested in the ground states of this Hamiltonian. In the case of a satisfiable formula we know that the corresponding ground state energy vanishes. In order to analytically characterize the ground states properties, we first calculate the free energy at a formal temperature T, using the functional replica trick in the replica-symmetric framework [11]. Then we send $T \to 0$, and we study the zero-temperature phase diagram of the model using the mean connectivity 3α as the control parameter, pretty much as it is usually done only in temperature.

The replica-symmetric order parameter determining the different phases of the system is the distribution of local magnetizations $P(m) = 1/N \ \sum_i \delta(m - m_i)$, where $m_i = \langle S_i \rangle_{T=0}$ is the average value of S_i over all ground states. There are mainly two different possibilities:
(i) $P(m)$ has a non-zero average and/or is broad, but all $|m_i|$ are less than 1. This corresponds, depending on the values of p_0, p_1 and p_2, to a ferromagnetic phase or to a paramagnetic phase in a field. $P(m)$ can be determined using a simple population dynamics algorithm [12] or variationally [13] and both determinations coincide.
(ii) $P(m)$ has finite weight in $m = +1$, i.e. an extensive number of variables is fixed to $x_i = 1$ in all satisfying assignments. These variables form the so-called *backbone*, which is of central interest in the discussion of random SAT, see e.g. Ref. [14]. In this case the system is ferromagnetic, and the $P(m)$ can be calculated exactly.

Going back to the class of generators proposed above, one could naively use $p_0 = p_1 = p_2 = 1/7$, choosing any of the allowed clauses with the same probability. The typically generated formulae are, however, known to be effectively solvable by local search procedures [9]. In our walk-SAT implementation, the maximal resolution-time [15] grows like $t \propto N^{1.58}$, and large systems of sizes up to $N \simeq 10^4$ can be easily handled.

The statistical mechanics approach clarifies this result: The proposed generator behaves like a paramagnet in an exterior random field, and no ferromagnetic phase transition appears. Local search algorithms may exploit the average local field $\overline{H_i} = \alpha/56$ pointing into the direction of the forced solution $\vec{x}^{(0)}$ and rapidly find a solution.

To avoid this, we can fix the average local field to zero by choosing $p_0 + p_1 - p_2 = 0$. The probabilities are thus restricted by $0 \le p_0 \le 1/4$, $p_1 = (1-4p_0)/6$, and $p_2 = (1+2p_0)/6$.

Let us start the discussion of these possibilities with the case $p_0 = 0$, and so $p_1 = p_2 = 1/6$ (*model 1/6*). In this (and only this) case, there is a second guaranteed solution: $x_i = 0$, $\forall i$. The average of all J_{ijk} vanishes. The model is paramagnetic at low α, and undergoes a second order ferromagnetic transition at $\alpha \simeq 3.74$. But also in the ferromagnetic phase the backbone is still zero as long as $\alpha \lesssim 4.91$: at this point it appears continuously from strongly magnetized spins.

In walk-SAT experiments, we find that the generated instances are still solvable in polynomial time, with peak

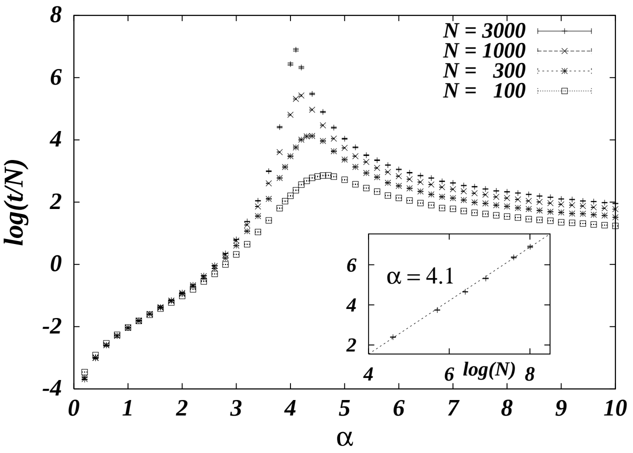

FIG. 1: Typical walk-SAT complexity for the model 1/6. We show the average value of $\log(t/N)$. We find a clear data collapse for small α in the linear regime, $t \propto N$. The complexity peak at $\alpha \simeq 4.1$ grows polynomially as shown in the inset. The slope of the straight line in the inset is 1.3.

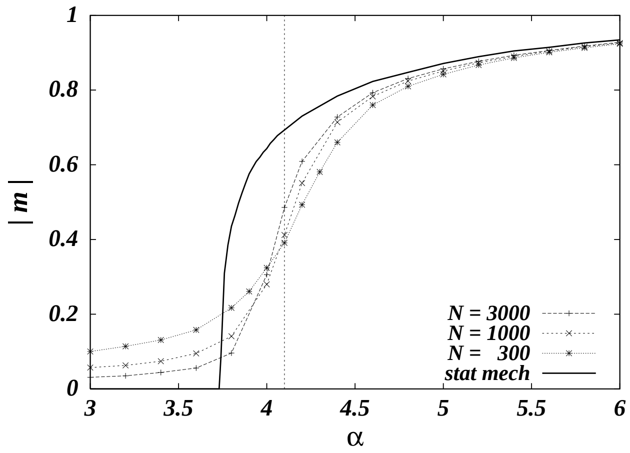

FIG. 2: Magnetization of the first solution found by walk-SAT for the model 1/6. Due to the (average) spin-flip symmetry, we plot the average of $|m|$. For large system size, the magnetization stays zero up to $\alpha \simeq 4.1$ (mark by the vertical line). The full line shows the thermodynamical average, which stays well above the asymptotic walk-SAT result.

resolution-times growing as $N^{2.3}$, see Fig. 1. However, the complexity peak is not at the phase transition, but very close to the critical point of random 3-SAT. This is due to the fact that walk-SAT does not sample solutions according to the thermodynamic equilibrium distribution: Most probably it finds solutions with small magnetization (i.e. closer to the starting point), see Fig. 2. For large N, this magnetization stays zero even after the ferromagnetic transition. Indeed, if we restrict the statistical mechanics analysis to zero magnetization, we find a sub-dominant, but non-zero solution entropy also beyond $\alpha = 3.74$. More interestingly, this entropy coincides with the solution entropy of random 3-SAT, which is positive for α values below the SAT/UNSAT transition ($\alpha_c \simeq 4.25$), and then jumps to $-\infty$ [11]. So, approaching α_c, walk-SAT is no longer able to find unmagnetized solutions for the model 1/6, and it has to go to magnetized assignments, giving rise to the resolution-time peak.

Once we use $p_0 > 0$, the situation changes: The ferromagnetic transition becomes first order, the transition point moves towards the random 3-SAT threshold α_c, and the computational complexity increases with p_0.

Still, for $p_0 \lesssim 0.077$, the ferromagnetic phase arises without backbone and solutions can be easily found.

In the region $0.077 \lesssim p_0 < 1/4$, the first order transition is more pronounced. The system jumps at $\alpha \simeq 4.25$ from a paramagnetic phase to a ferromagnetic one, with a discontinuous appearance of a backbone: For $p_0 \simeq 0.077$, the backbone size at the threshold is about $0.72N$, and goes up to $0.94N$ for $p_0 = 1/4$ (see Fig. 3). We conjecture the ferromagnetic critical point in these models to coincide with the SAT/UNSAT threshold in random 3-SAT, since the topological structures giving rise to ferromagnetism in the formers induce frustration and thus

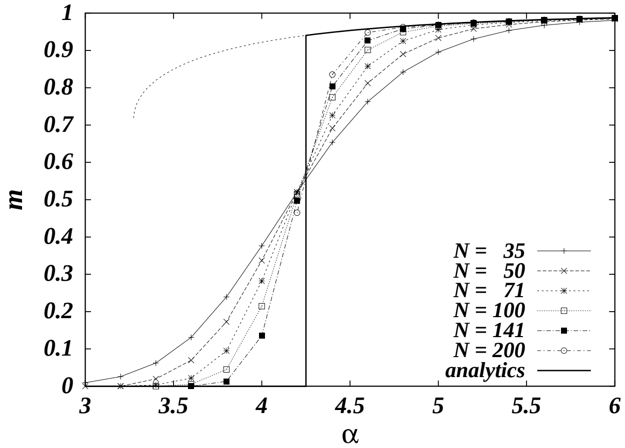

FIG. 3: Average magnetization of satisfying assignments for model 1/4, obtained with a complete algorithm. In this case, the magnetization equals the backbone size. The finite size curves cross at $\alpha \simeq 4.25$, and tend to the analytical prediction given by the full line. The dotted continuation of the analytical line gives the globally unstable ferromagnetic solution, starting at the spinodal point.

unsatisfiability in the latter.

The case $p_0 = 1/4$, and so $p_1 = 0$, $p_2 = 1/4$ (*model 1/4*), is very peculiar because it can always be solved in polynomial time using a global algorithm. Indeed one can unambiguously add three clauses to every existing one, namely the other clauses allowed in the model 1/4, without loosing the satisfiability of the enlarged formula [16]. The completed formula becomes a sample of random satisfiable 3-XOR-SAT (also known as hyper-SAT [17]), which can be mapped to a system of linear equations modulo 2, and solved in time of $\mathcal{O}(N^3)$ [18].

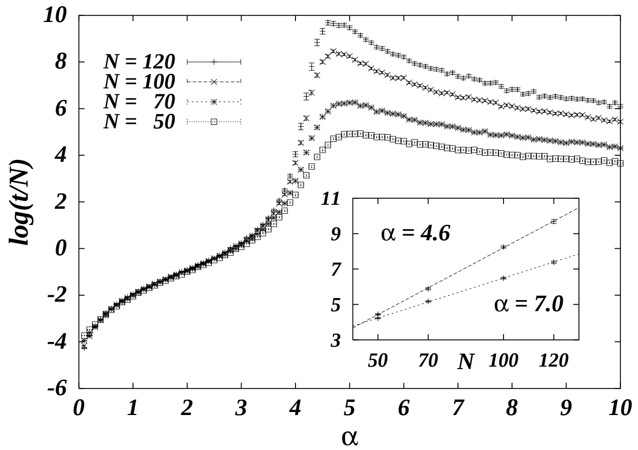

FIG. 4: Typical walk-SAT complexity for the model 1/4. Again, there is a linear regime at small α, but the complexity peak is much more pronounced than in Fig. 1 (compare e.g. the reachable system sizes). The inset shows the exponential resolution-time scaling near the peak ($\alpha = 4.6$) and deep inside the ferromagnetic phase ($\alpha = 7.0$). The slopes of the straight lines are 0.075 and 0.04 respectively.

This algorithm immediately breaks down if we choose $p_0 \neq 1/4$. Indeed, whenever one tries to map the general formula into a completed one, the presence of all three types of clauses forces it into a *frustrated* 3-XOR-SAT formula – i.e. not a satisfiable one – which undergoes a SAT/UNSAT transition at $\alpha = 0.918$ [17], well below the region of interest. So the mapping is of no use for $p_0 \neq 1/4$. In this case, any 3-SAT instance with solution $\vec{x}^{(0)}$ (and thus any solvable 3-SAT formula [10]) can be generated with non-zero probability. The worst-case is thus included in the presented generator, and there cannot be any polynomial solver if P≠NP.

In conclusion, we conjecture the hardest instances to be generated with p_0 values close to 1/4. The computational times for their solution are similar to those in Fig. 4, which have been obtained for $p_0 = 1/4$ without exploiting the global algorithm. Resolution-times are clearly exponential in all the ferromagnetic phase ($\alpha > 4.25$). Moreover we checked that resolution-times in the paramagnetic phase ($\alpha < 4.25$) coincide with those for random 3-SAT, finite size effects making the peak higher in the 1/4 model. Note, however, that our method relies on the hardness of random 3-SAT, which is still to be proven (even if very plausible).

To corroborate our conjecture, we also performed simulated annealing experiments. We easily find solutions in model 1/6, but get stuck in the vicinity of model 1/4.

The physical interpretation of the hardness in this class of models is based on the presence of glassy metastable states of zero magnetization [19] for $\alpha > 4.25$. These states are dynamically favored and trap the system for very long times during a stochastic local search.

We believe that the statistical mechanics approach can have a general valence in the formulation of hard and solvable problems, allowing for a systematic way of producing random one-way functions, and can help in the study of the out-of-equilibrium behavior of randomized search algorithms.

MW thanks the ICTP in Trieste for its hospitality.

[1] M. R. Garey and D. S. Johnson, *Computers and intractability* (Freeman, New York, 1979).
[2] Artif. Intell. **81**, issue 1-2 (1996).
[3] Theor. Comp. Sci. **265**, issue 1-2 (2001).
[4] D. Mitchell, B. Selman, and H. Levesque, Proc. AAAI-92, 459 (1992).
[5] S. Kirkpatrick and B. Selman, Science **264**, 1297 (1994).
[6] The SATLIB is located at http://www.satlib.org.
[7] S. Kirkpatrick, C.D. Gelatt Jr. and M.P. Vecchi, Science **220**, 671 (1983).
[8] B. Selman, H. Kautz, and B. Cohen, in *Cliques, Coloring, and Satisfiability*, ed. by D.S. Johnson and M.A. Trick, DIMACS series vol. 26 (AMS, Providence, 1996).
[9] D. Achlioptas, C. Gomes, H. Kautz, and B. Selman, Proc. AAAI-00 (2000); H. Kautz, Y. Ruan, D. Achlioptas, C. Gomes, B. Selman, and M. Stickel, to app. in Proc. IJCAI-01 (2001).
[10] The satisfying assignment $\vec{x}^{(0)}$ can be changed to any other one $\vec{x}^{(1)}$ by a local gauge transformation of the generated 3-SAT formula: One has to exchange x_i and $\overline{x}_i$ for all i with $x_i^{(1)} = 0$.
[11] R. Monasson and R. Zecchina, Phys. Rev. Lett. **76**, 3881 (1996); Phys. Rev. E **56**, 1357 (1997).
[12] M. Mézard and G. Parisi, Eur. Phys. J. B **20**, 217 (2001).
[13] G. Biroli, R. Monasson, and M. Weigt, Eur. Phys. J. B **14**, 551 (2000).
[14] R. Monasson, R. Zecchina, S. Kirkpatrick, B. Selman, and L. Troyansky, Nature **400**, 133 (1999).
[15] The resolution-time t is measured by the number of single-variable flips until a satisfying solution is found.
[16] In the completed model the single clauses will be replaced with groups of four in the form $(x_i \vee x_j \vee x_k) \wedge (x_i \vee \bar{x}_j \vee \bar{x}_k) \wedge (\bar{x}_i \vee x_j \vee \bar{x}_k) \wedge (\bar{x}_i \vee \bar{x}_j \vee x_k) = (x_i \oplus x_j \oplus x_k)$ with $\oplus$ being the XOR operator. One is left out with a ferromagnetic pure 3-spin model, since all H_i and T_{ij} vanish. The connectivity of the completed model does not change, provided that now one considers αN as the number of four clauses clusters. The ferromagnetic transition occurs at $\alpha = 0.918$ [17].
[17] F. Ricci-Tersenghi, M. Weigt, R. Zecchina, Phys. Rev. E **63**, 026702 (2001).
[18] Note, however, that finding a solution of zero magnetization in the model 1/4 is NP-complete (the proof will be given in a forthcoming paper).
[19] S. Franz, M. Leone, F. Ricci-Tersenghi, and R. Zecchina, Phys. Rev. Lett. **87**, 127209 (2001).