Hiding solutions in random satisfiability problems: A statistical mechanics approach

W. Barthel, A.K. Hartmann, M. Leone, F. Ricci-Tersenghi, M. Weigt, and R. Zecchina

1Institute for Theoretical Physics, University of Göttingen, Bunsenstr. 9, 37073 Göttingen, Germany
2SISSA, via Beirut 9, 34100 Trieste, Italy
3International Centre for Theoretical Physics, Strada Costiera 11, P.O. Box 586, I-34100 Trieste, Italy
4Dipartimento di Fisica, Università di Roma “La Sapienza”, Piazzale Aldo Moro 2, 00185 Roma, Italy

(Dated: February 1, 2008)

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 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, 02.60.Pn, 05.70.Fh, 75.10.Nr

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.

Having fast and powerful algorithms for the resolution of these problems is of primary relevance for their theoretical study as well as for applications. The evaluation of such algorithms is based on the availability of hard benchmarks, having the following properties: They provide problem instances, with a given known solution, in a fast way (e.g. linear in \( N \)), but the resolution of an instance takes a time exponential in \( N \) for any known algorithm. So the best algorithms can be easily selected. In this letter we propose a new generator of hard and solvable test instances, having all the properties listed above. It is based on a NP-complete problem (3-SAT).

The main idea for the construction of such hard and solvable problems is very simple: to hide a known solution within a multitude of coexisting random meta-stable configurations which constitute dynamical barriers. In the physical approach based on a mapping from 3-SAT to a spin glass model, such random configurations correspond to glassy states. It is to be noted, however, that many previous attempts to implement this idea were unsuccessful, because the random structure was usually easy to remove, or knowledge that a solution has been forced can be exploited to find it. In the instances we propose, instead, the presence of a known solution does not alter the structure of the glassy state, which confuses the solver and makes the problem hard.

As an important application of these ideas to cryptography, random one-way functions are provided: A given message, e.g. a password, can be coded in a 3-SAT formula and thus verified efficiently, but decoding it is extremely time-consuming.

We use the framework of the typical-case computational complexity. There, the study of random 3-SAT problems has played a major role. A random 3-SAT formula \( F \) consists of \( M \) logical clauses \( \{C_\mu\}_{\mu=1,...,M} \) over a set of \( N \) Boolean variables \( \{x_i\}_{i=1,...,N} \) with \( 0=\text{FALSE} \) and \( 1=\text{TRUE} \). Every clause consists of three randomly chosen Boolean variables which are connected by logical OR operations (\( \lor \)) and appear negated with probability \( 1/2 \), e.g. \( C_\mu = (x_i \lor x_j \lor \bar{x}_k) \). In \( F \) the clauses are connected by logical AND operations (\( \land \)), \( F = \bigwedge_{\mu=1}^M C_\mu \), 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 phase transition at a critical ratio \( \alpha_c = M/N \approx 4.25 \) \((N \gg 1)\): Below \( \alpha_c \), almost all formulae are satisfiable, while beyond almost all formulae do not show any solution. At this threshold, a strong exponential peak in the typical (median) cost for finding solutions by the best known algorithms appears. Problem instances generated close to it form a natural test bed for the optimization of heuristic search algorithms. However, satisfiable and unsatisfiable instances coexist in this region. Many algorithms of practical interest are based on incomplete stochastic local search procedures, as e.g. simulated annealing and the walk-SAT algorithm. These algorithms stop once they have found a solution, but they have no way to disentangle, in polynomial time in \( N \), if a formula is unsatisfiable or just hard to solve. It is thus very important to generate benchmarks which are satisfiable and for which the algorithmic proof of this satisfiability takes an exponential time in \( N \).

In this Letter, we propose simple and fast generators of such benchmark problems. The main ideas are inspired by physical requirements, and exploit the presumed hard-
ness of random 3-SAT itself. One obvious possibility is 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. In addition, the hardest instances are the unsatisfiable ones. Other approaches use mappings from various hard problems to 3-SAT, including e.g. factorization graph coloring [12] and Latin square completion [13].

To avoid this, we can fix the average local field to zero $\langle \overline{H} \rangle = 3\alpha / 56$ pointing into the direction of the forced solution $\vec{x}^{(0)}$, and rapidly find a solution.

To understand 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 [2]. The Boolean variables $x_i = 0, 1$ are mapped to Ising spins $S_i = (-1)^x_i$, and the Hamiltonian counts the number of unsatisfied clauses,

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

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 $c_{\mu,i} = 1$ if $x_i$ appears directly in $C_\mu$, $-1$ if it appears negated, and 0 otherwise. The interactions in (3) fluctuate from sample to sample, with disorder-averages $\overline{H_i} = \frac{3\alpha}{8}(p_0 + p_1 - p_2)$,

$$\overline{T_{ij}} = \frac{3\alpha}{12}(p_0 + p_1 + p_2), \quad \overline{J_{ijk}} = \frac{3\alpha}{12}(p_0 - 3p_1 + 3p_2).$$

We are interested in the ground states of this Hamiltonian. For 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 formal temperature $T$,
which stays well above the asymptotic walk-SAT result.

Once we use $p_0 > 0$, the situation changes: The ferromagnetic transition becomes first order, as can be seen best by the existence of metastable solutions for $P(m)$. The transition point moves towards the random 3-SAT threshold $\alpha_c$, 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 $0.077 < p_0 < 1/4$, 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 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 model 1/4, without loosing the satisfiability of the enlarged formula [24]. The completed formula becomes a sample of random satisfiable 3-XOR-SAT (also known as hyper-SAT [23]), which can be mapped to a system of linear equations modulo 2, and solved in time of $O(N^3)$ [24].

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, which undergoes a SAT/UNSAT transition at $\alpha = 0.918$ [23], well below the region of our 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 one [4]) can be generated with non-zero probability. The
4.25 \times 10^{-4} \times (\alpha = 4.6) \text{ and deep inside the ferromagnetic phase } (\alpha = 7.0). \text{ The slopes of the straight lines are 0.075 and 0.04 respectively.}

The worst-case is thus included in the presented generator, and there cannot be any polynomial solver if \( P \neq NP \).

In the following table we summarize the main results for the investigated combinations of \( p_0, p_1 \) and \( p_2 \). Where only \( p_0 \) is reported, \( p_{1,2} \) are given by Eqs. \ref{eq:1}. We show the location \( \alpha_c \) and order of the ferromagnetic phase transition, together with the point \( \alpha_{ws} \) and the system-size-scaling (P/EXP) of the maximal walk-SAT complexity. For comparison, we have added the corresponding data for random 3-SAT.

| Model                  | \( \alpha_c \) (order, type) | \( \alpha_{ws} \) |
|------------------------|-------------------------------|------------------|
| \( p_{0,1,2} = 1/7 \)  | NO                            | 5.10 P            |
| \( p_0 = 0 \)               | 3.74 (2nd, ferro)              | 4.10 P            |
| \( p_0 \in [0.077, 1/4) \)| 4.25 (1st, ferro)              | 4.25 EXP          |
| \( p_0 = 1/4 \)            | 4.25 (1st, ferro)              | 4.25 P            |
| Random 3-SAT            | 4.25 (SAT/UNSAT)              | 4.25 EXP          |

Please note, that the polynomial time-complexity of model 1/4 is accidental and due to the existence of a global algorithm, whereas the walk-SAT peak grows exponentially with \( N \). To corroborate this picture, we also performed simulated annealing experiments. We easily find solutions in model 1/6, but get stuck in the vicinity of model 1/4.

As a 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. \ref{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, up to finite-size effects, with those of random 3-SAT.

The physical interpretation of the hardness in this class of models is based on the presence of glassy metastable states of zero magnetization \( 0 \) 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 dynamics of randomized search algorithms.

MW thanks the ICTP in Trieste and RZ thanks the LPTMS in Orsay for hospitality.

References:

[1] M. R. Garey and D. S. Johnson, *Computers and intractability* (Freeman, New York, 1979).
[2] R. Monasson and R. Zecchina, Phys. Rev. Lett. 76, 3881 (1996); Phys. Rev. E 56, 1357 (1997).
[3] S. Franz, M. Leone, F. Ricci-Tersenghi, and R. Zecchina, Phys. Rev. Lett. 87, 127209 (2001).
[4] D. Welsh, *Codes and Cryptography* (Clarendon Press, 1988).
[5] Artif. Intell. 81, issue 1-2 (1996).
[6] Theor. Comp. Sci. 265, issue 1-2 (2001).
[7] D. Mitchell, B. Selman, and H. Levesque, Proc. AAAI-92, 459 (1992).
[8] SATLIB, http://www.satlib.org.
[9] S. Kirkpatrick, C.D. Gelatt Jr. and M.P. Vecchi, Science 220, 671 (1983).
[10] 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).
[11] A. Horie and O. Watanabe, Lecture Notes in Computer Science 1350, 22 (1996).
[12] H. Hoos and T. Stützle, J. Autom. Reas. 24, 421 (2000).
[13] 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. Stickle, to app. in Proc. IJCAI-01 (2001).
[14] The satisfying assignment \( \bar{x}^{(i)} \) can be changed to any other one \( \bar{x}^{(i)} \) by a local gauge transformation of the generated 3-SAT formula: One has to exchange \( x_i \) and \( \bar{x}_i \) for all \( i \) with \( x_i^{(1)} = 0 \).
[15] M. Ménard and G. Parisi, Eur. Phys. J. B 20, 217 (2001).
[16] G. Birolí, R. Monasson, and M. Weigt, Eur. Phys. J. B 14, 551 (2000).
[17] R. Monasson, R. Zecchina, S. Kirkpatrick, B. Selman, and L. Troyansky, Nature 400, 133 (1999).
[18] Y. Asahiro, K. Iwama, and E. Miyano, in *Cliques, Coloring, and Satisfiability*, ed. by D.S. Johnson and M.A. Trick, DIMACS series vol. 26 (AMS, Providence, 1996).
[19] D.L. Mannen and T. Hogg, J. Art. Int. Res. 7, 47 (1997).
[20] M. Motoki and R. Uehara, Technical Report TR-C129 (Tokyo Inst. of Technology, 1999).
[21] The resolution-time \( t \) is measured by the number of single-variable flips until a satisfying solution is found.
[22] In the completed model, every clause is replaced by
groups of four in the form \((x_i \lor x_j \lor x_k) \land (x_i \lor \bar{x}_j \lor \bar{x}_k) \land (\bar{x}_i \lor x_j \lor \bar{x}_k) \land (\bar{x}_i \lor \bar{x}_j \lor x_k) = (x_i \oplus x_j \oplus x_k)\) with \(\oplus\) being the logical XOR operator. One is left with a ferromagnetic pure 3-spin model, see [23].

[23] F. Ricci-Tersenghi, M. Weigt, R. Zecchina, Phys. Rev. E 63, 026702 (2001).

[24] Note, however, that in the worst case finding a solution of zero magnetization in the model 1/4 is NP-complete (the proof will be given in a forthcoming paper).