Evergrow: SP4

Enzo Marinari

(Roma *La Sapienza*, Italy)

What we do.

What we have done.

Greatest hits...

Goals.

(Funding: excellence, synergies, results).

The sociology of SP4 (with only some names, for situating our work):

SICS, Stockholm, Sweden: Aurell, Krishnamurthy.

HUJI, Jerusalem, Israel: Gordon, Kirkpatrick.

ISI, Turin, Italy: Leone, Pagnani, Weigt.

La Sapienza University, Rome, Italy: Marinari, Parisi, Ricci-Tersenghi.

University of Orsay, Paris, France: Martin, Mézard.

University of Magdeburg, Germany: Mertens.

ENS, Paris, France: Monasson, Montanari, Sourlas.

Aston University, UK: Opper, Saad, van Mourik.

Oxford University, UK: Sherrington.

ICTP, Trieste, Italy: Zecchina.

Starting from strong synergies. First from Statistical Mechanics of Disordered Systems, than applying ideas to optimization, error correcting codes, graphs and networks. An ideal humus for EVERGROW-th.

EVERGROW highest added value: relation with different fields (the language problem is always more severe of what one would believe). Mainly measurement experiments (DIMES, ETOMIC) and P2P. Paris meeting on this issue. So, both, “academic” and “application”.

Many simulations, and role in the “cluster”.

Relations with SP5 (among others Cavagna, Giardina, Marsili).

Many post-doc, phd students: large stress on training. Schools.

Joint work with other IP. DELIS: schools and training again. Prepare 2008 Stat. Mech. (big) conference in Rome.

Message passing in random satisfiability problems

- Combinatorial optimization.
- Error correcting codes.
- Statistical inference.

Statistical mechanics.

1. Graph.
2. “Solve equation” (or not) by “message passing” (messages can be complex, probabilistic in nature).

$$x_i = (0,1)\ .$$

There are N variables. Clauses:

$$x_{28}\ OR\ \overline{x_{318}}\ OR\ x_{1001}$$

AND of M of these clauses.

$$\alpha \equiv \frac{M}{N}$$

Interest of (very difficult) NP-complete problems.

- α small, easy.
- α larger, ..., difficult, ..., impossible.

SAT-UNSAT phase transition (use of Statistical Mechanics). α_c exists such that

- SAT almost always for $\alpha < \alpha_c$.
- UNSAT almost always for $\alpha > \alpha_c$.

How to solve the problem: first we describe the graph (see also error correcting codes). Use Message Passing.

Clauses send messages to variables telling: *I need your help: you should get a value that I find satisfactory*.

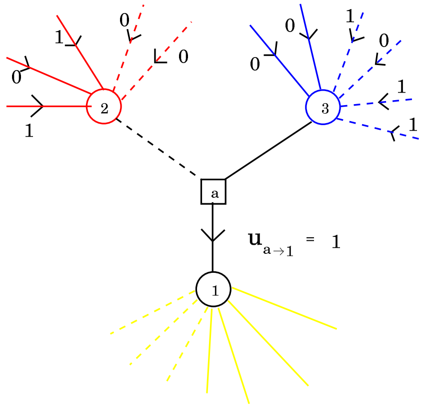
Or a message telling: *I do not need your help, since I already see, somewhere else, a value that makes me happy*.

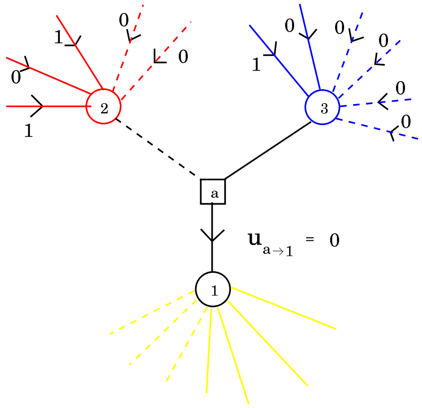
This idea is behind well celebrated Belief Propagation.

In difficult situations: "many states". Need Survey Propagation (introduced by collaboration of EVERGROW-ing research groups), where you study propagation of probability.

Parisi *Replica Symmetry Breaking* physics.

On general grounds: use algorithms using all you know about a given problem. Why does annealing work? Or, as a celebrated example, Swendsen-Wang Monte Carlo cluster algorithm for Ising model (base on existence of Fortuin-Kasteleyn representation). (Next three figures are from Mézard talks and lectures)

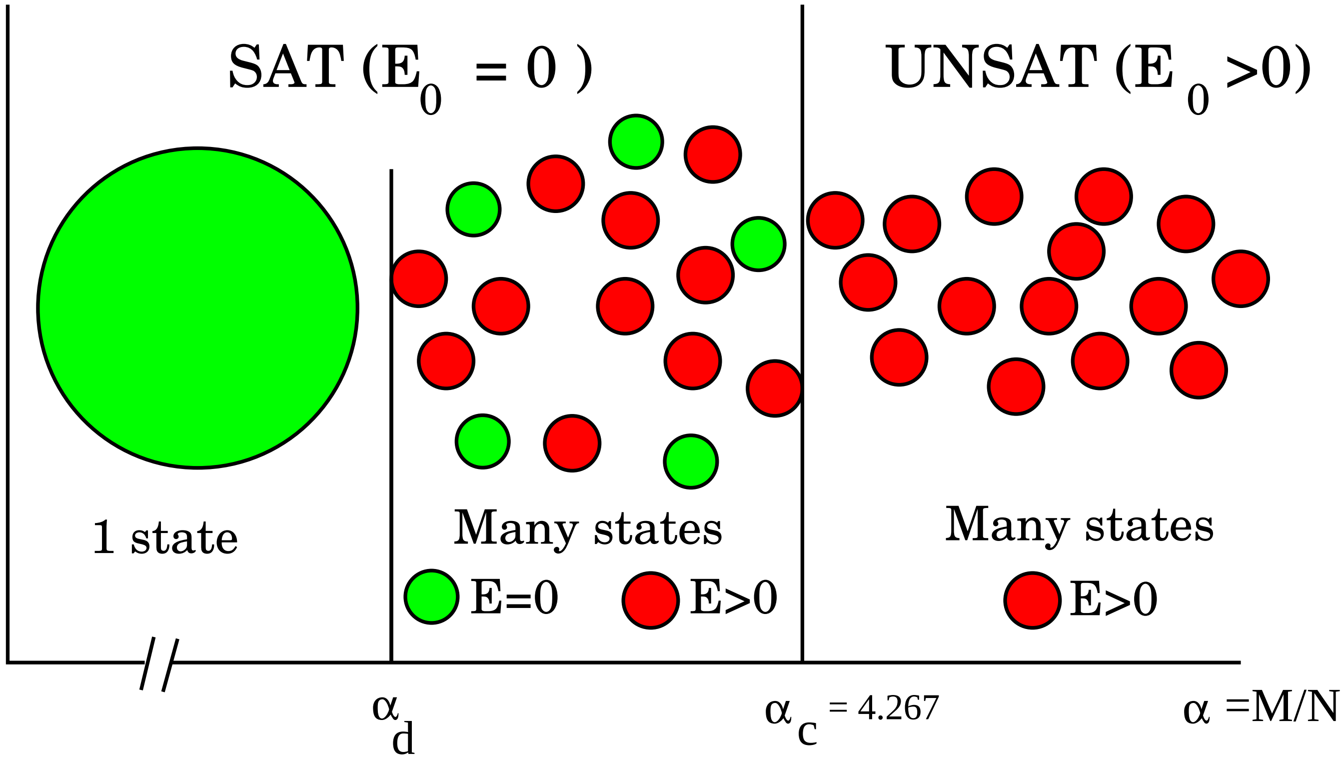




A variable is represented by a circle. A clause is represented by a square, connected with a full (resp. dashed) line to a variable when this variable appears as such (resp. negated) in the clause.

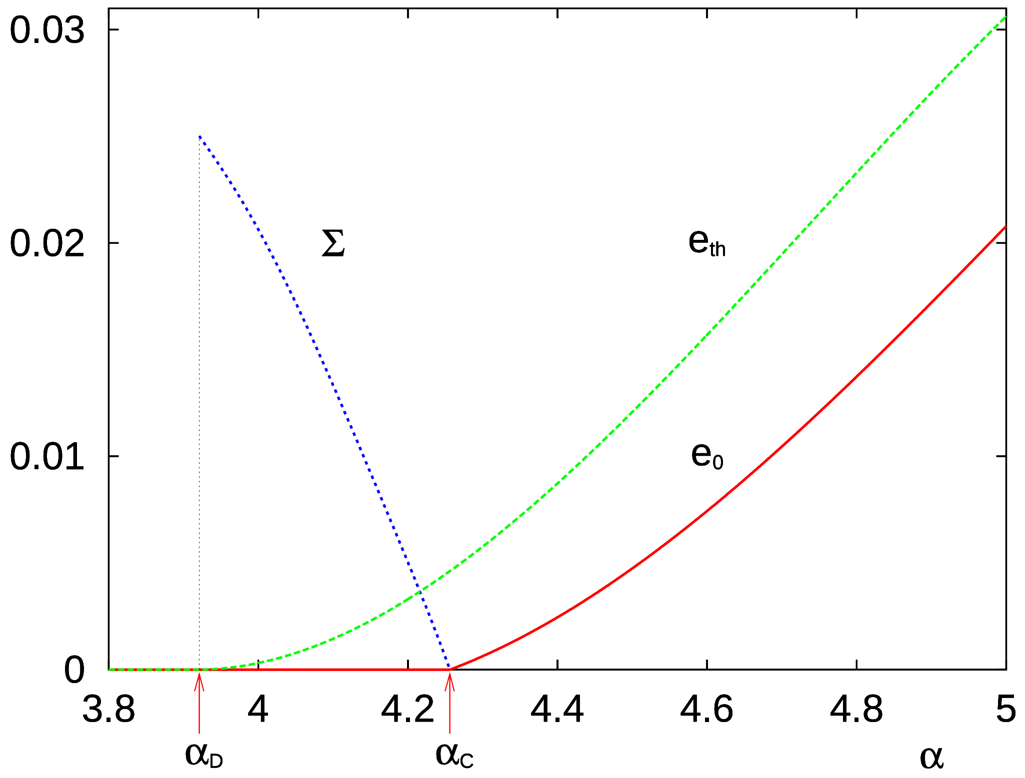
In order to determine the message which it passes to variable 1, clause a considers all the messages received by the other variables to which it is connected.

On the left, the messages received by 2 tell it to take the value $x_2 = 1$, which does not satisfy clause a, and the messages received by 3 tell it to take the value $x_3 = 0$, which also does not satisfy clause a. Therefore, in order to be satisfied, clause a must rely on variable 1. It thus sends a warning $u_{a\to 1} = 1$. Right hand side: no warning is sent.



Vary α: three distinct phases.

$\alpha < \alpha_d$ Easy- SAT, all solutions are connected.
$\alpha_d < \alpha < \alpha_c$ Hard-SAT, very different solutions.
$\alpha > \alpha_c$ UNSAT phase.



e_0 minimal number of violated clauses per variable $\Longrightarrow$ ground state energy density.

e_{th} energy density of the states where local descent algorithms get trapped.

Σ complexity of SAT states.

Error correcting codes

Transmission of data: noise causes corruption.

Information theory:

- Make data redundant before transmission (coding).
- Thanks to redundancy recover safely the data after transmission (decoding).

Turbo codes + Low Density Parity Check Codes (LPDC). They are used much and in many different contexts: heuristic.

Back to belief propagation, message passing (and statistical mechanics: TAP equations for mathematical control).

Find solutions:

- Glassy behavior.
- Slow dynamics.

Our work, only important lines, a few examples. Different groups working together.

SICS + HUJI, belief, survey and random walk solvers, SP3,SP5.
ENS + Roma 1, counting circuits.
Roma1, complexity and supersimmetry.
ENS, scaling laws for solution search algorithms.
SICS, large scale behavior of P2P overlay networks, SP3,SP5.
SICS, chord under churn, SP5.
Roma1 + ISI, coloring Erdös-Renyi.
Orsay - ICTP, rigorous control of the clustered phase.
Orsay - ISI, ground states in 3-SAT.

ISI, a large combinatorial auction.
ISI, heuristic local search algorithm for coloring.
ISI, MP applied to protein networks.
Orsay, multi-index matching.
ICTP, going below threshold.
ICTP, SP with external forcing.
ENS (+ EPFL), finite length scaling for LDPC codes.
ENS (+ EPFL), codes above threshold.
ENS, bounds for LDPC codes (Guerra approach).
Aston, LPDC-coded code division multiple access systems, SP3.
Aston, SP in densely connected systems.
Orsay + ICTP, new approach to lossy data compression.

A SP4 highlight

We have used tools from the statistical mechanics of random systems to provide the first predictions of the error probabilities of the error correcting code based on message passing, when these have finite code block lengths.

Block coding is a widely adopted design principle in error correction technologies: a stream of information symbols is blocked into strings of some fixed length. Each block is encoded separately using a fixed length code, and then transmitted through the communication channel. Obviously, this implies communication delays: before a bit is transmitted, the encoder has to wait for the information source to produce enough symbols to complete the block.

EVERGROW
www.evergrow.org

Delays are inconvenient, in particular for interactive applications. This favors the choice of small block-lengths: but the performances (the error correction capabilities) of block codes rapidly deteriorate when the block-length is reduced.

We have succeeded to understand the behavior of iterative coding systems in the intermediate block-length regime (100 to 100000 bits): we believe that the potential practical uses of these findings are of large importance. We have been inspired from statistical physics, and we have been able to draw a precise mathematical picture. This block-length regime is the most interesting for innovative applications.

Goals for message passing approaches in constraint satisfaction problems

...) Proving rigorously the existence of the clusters. So far, such a proof exists only for the problem of XORSAT, where the constraints are linear in the variables. It is important to generalize it to other problems, where constraints are nonlinear.

...) Lossy data-compression methods based on SP. It has been shown recently that the clustered phase can be used for data compression: fundamentally a message is mapped to the label of the nearest cluster. In order to turn this into an efficient scheme, one must use the clustered phase for a problem where the constraints are nonlinear.

...) Analysis of the geometry of clusters: size distributions, distances... This is a first necessary step in order to be able to do some 'cluster gardening' for applications.

...) Fully distributed (i.e. parallel) version of optimization algorithms based on SP (including the decimation process).

...) Message-passing and SP algorithms over directed networks (e.g. regulatory networks and circuits).

Common work with DIMES and with ETOMIC

DIMES data: excellent (+ dynamic) map of Internet.

Kirkpatrick HUJI group and DIMES:

1. power law confirmed/established.
2. $\mathcal{K}$-shell technique. To get the $\mathcal{K}$ core:

- remove sites with number of neighbors $\leq \mathcal{K} - 1$;
- continue till no removal.

Sites in $\mathcal{K}$-core are the $\mathcal{K}$-shells: also $\mathcal{K}$ cores are power law distributed.

Circuits: Semerjian, EM, Monasson (ENS + Roma 1): circuit counting, analyzing, understanding on real, DIMES Internet.

Interaction with ETOMIC for data analysis is coming.

EVERGROW
www.evergrow.org

Goals for improving correcting codes

...) Development of the analogy of the scaling theory to describe the collective events which lead to communication errors in the threshold regime and decimation procedures in statistical mechanics.

...) Scaling laws for general memoryless channel models and their use for ensemble optimization.

...) Exploiting the know-how gathered so far in order to construct improved algorithms. Implement the scaling theory as an optimization software for code construction.

...) Dealing with correlations arising in loopy graphical structures, and constructing performances guarantees for the existing algorithms (which today have only probabilistic guarantees).

...) Integrating such systems within multi-user schemes, with, as a special concern, peer-to-peer architectures.

...) Use of iterative techniques in multi-user communications.