Computational Complexity 4:
Phase transitions in physics and computer science

Cristopher Moore
Santa Fe Institute

Magnetism

When cold enough, iron will stay magnetized, and even magnetize spontaneously

But above a critical temperature, it suddenly ceases to be magnetic

Interactions between atoms remain the same, but global behavior changes!

Like water freezing, outbreaks becoming epidemics, opinions changing...

The Ising model

Lattice (e.g. square) with n sites

Each has a "spin" $s_i = \pm 1$, "up" or "down"

Energy is a sum over neighboring pairs:

$$E = -\sum_{ij} s_i s_j$$

Lowest energy: all up or all down

Highest energy: checkerboard

Boltzmann Distribution

At thermodynamic equilibrium, temperature T

Higher-energy states are less likely:

$$P(s) \sim e^{-E(s)/T}$$

When $T \to 0$, only lowest energies appear

When $T \to \infty$, all states are equally likely

Monte Carlo

At each step, choose a random site i

Compute the change ΔE of flipping s_i

Metropolis rule:

If $\Delta E < 0$, flip s_i

If $\Delta E > 0$, flip s_i with probability $e^{-\Delta E/T}$

Keep going until we reach equilibrium
(how long will that take?)

What Happens

Below critical temperature, the system "magnetizes": mostly up or mostly down

Small islands of the minority state; as T increases, these islands grow

Above critical temperature, islands=sea;
at large scales, equal numbers of up and down

When $T=T_c$, islands of all scales:
system is scale-invariant!

Even more symmetry

Conformal invariance: any analytic map of the complex plane

Mean Field

Ignore topology: forget lattice structure

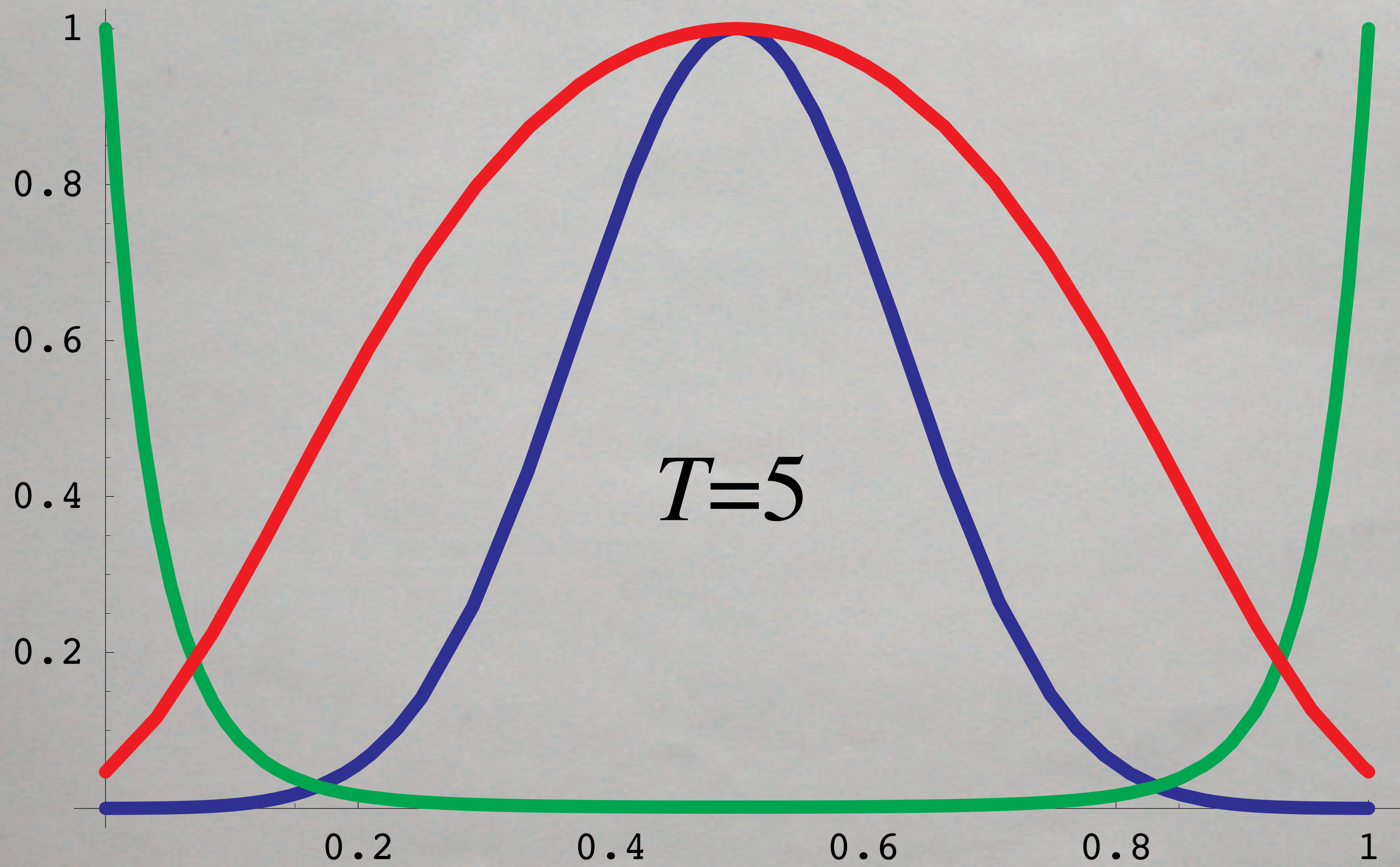
If a of the sites are up and $1–a$ are down, energy is $E = 2n^2\left(2a(1-a) - a^2 - (1-a)^2\right)$

At any T, most-likely states have a=0 or a=1

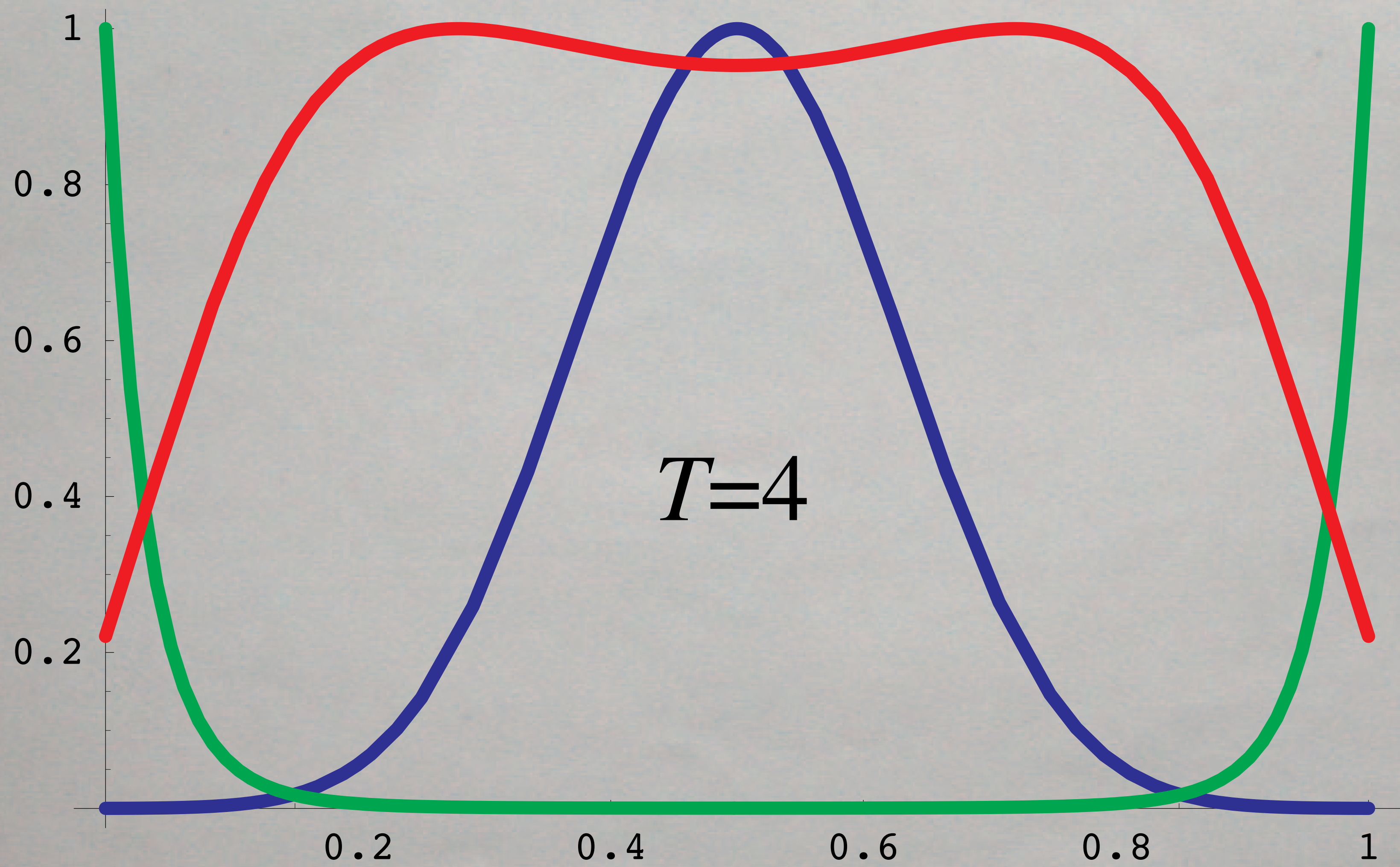
But the number of such states is $\binom{n}{an}$, which is tightly peaked around a=1/2.

Total probability(a) = #states(a) Boltzmann(a)

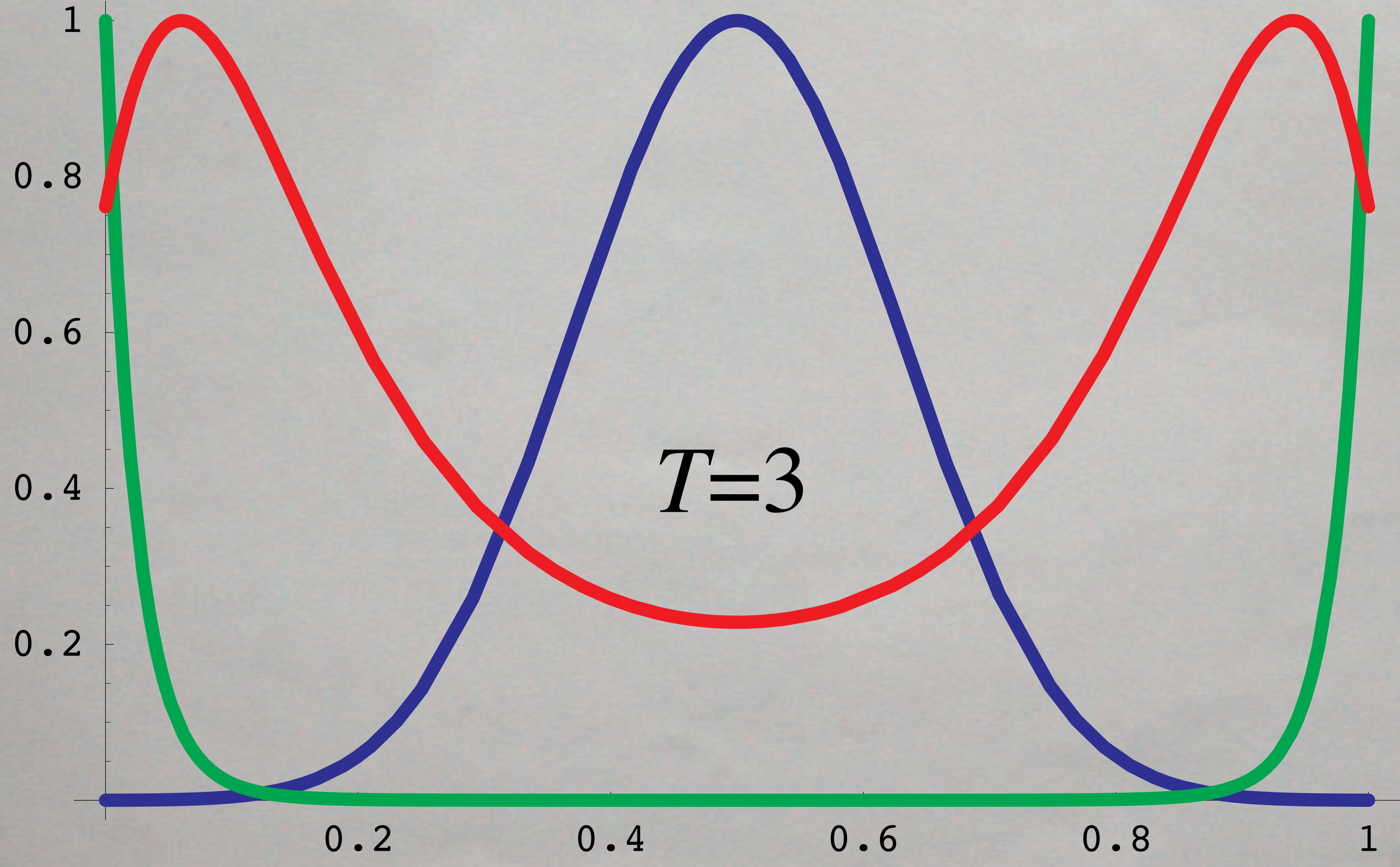
Energy vs. Entropy



Energy vs. Entropy



Energy vs. Entropy



Correlations

$C(r)$ = correlation between two sites r apart

If $T > T_c$ correlations decay exponentially:

$$C(r) \sim e^{-r/\ell}$$

Correlation length ℓ decreases as T grows

As we approach T_c correlation length diverges

At $T{=}T_c$ power-law correlations (scale-free):

$$C(r) \sim r^{-\alpha}$$

Percolation

Fill a fraction p of the sites in a lattice

When $p < p_c$, small islands, whose size is exponentially distributed:

$$P(s) \sim e^{-s/\overline{s}}$$

When $p > p_c$ a unique "giant cluster" appears

At p=p_c power-law distribution of cluster sizes:

$$P(s) \sim s^{-\alpha}$$

Phase transitions in NP-complete problems

NP-completeness is a worst-case notion

3-SAT is hard because hard instances exist...

...and we assume instances are designed by a clever adversary (cruel world!)

What if the constraints are chosen randomly instead?

As we add more constraints, more contradictions arise...

Random NP Problems

A 3-SAT formula with n variables, m clauses

Choose each clause randomly: $\binom{n}{3}$ possible triplets, negate each variable with probability 1/2

Precedents:

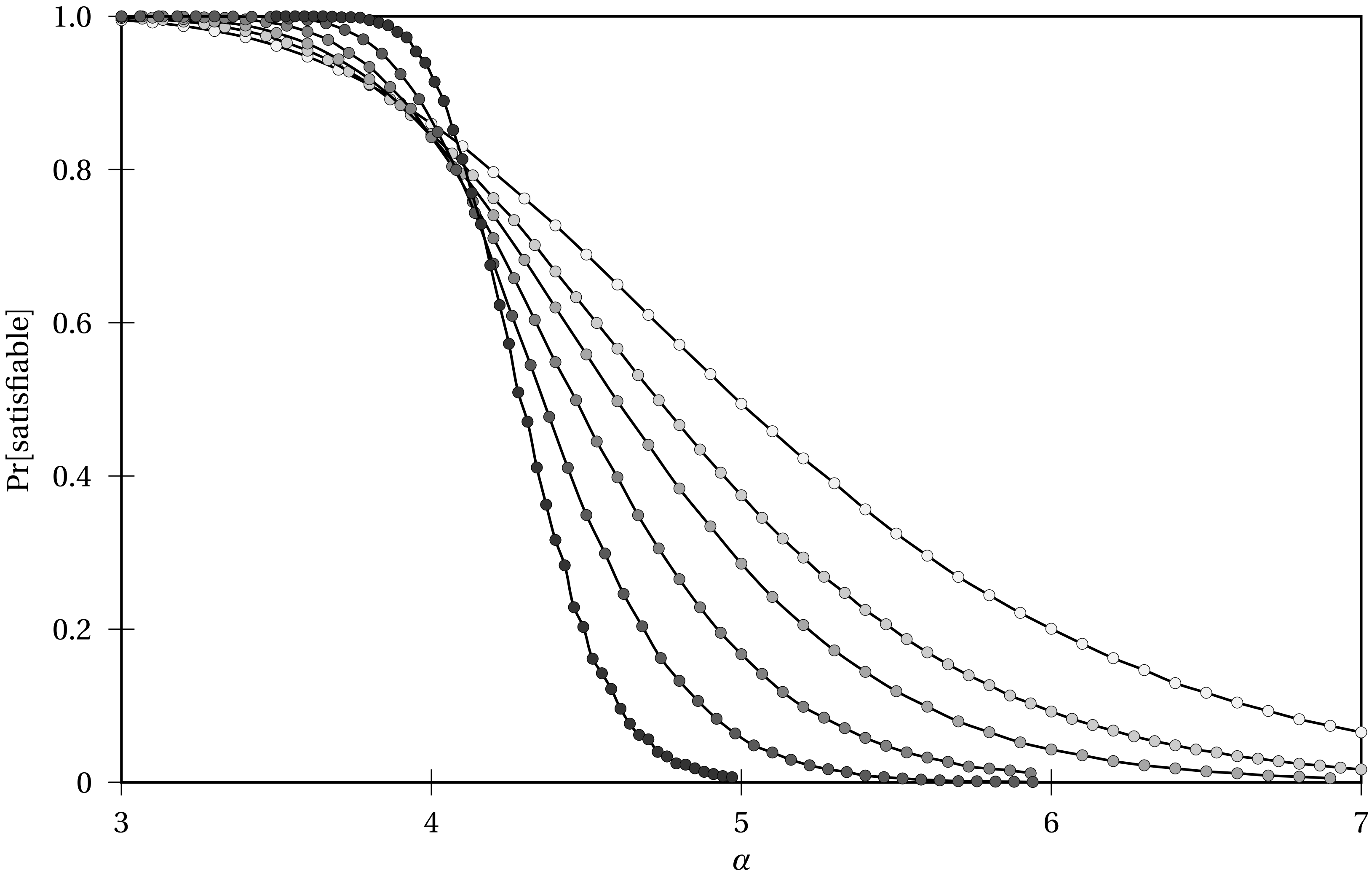
Random Graphs (Erdős-Rényi)

Statistical Physics: ensembles of disordered systems, e.g. spin glasses

Sparse Case: $m = \alpha n$ for some density α

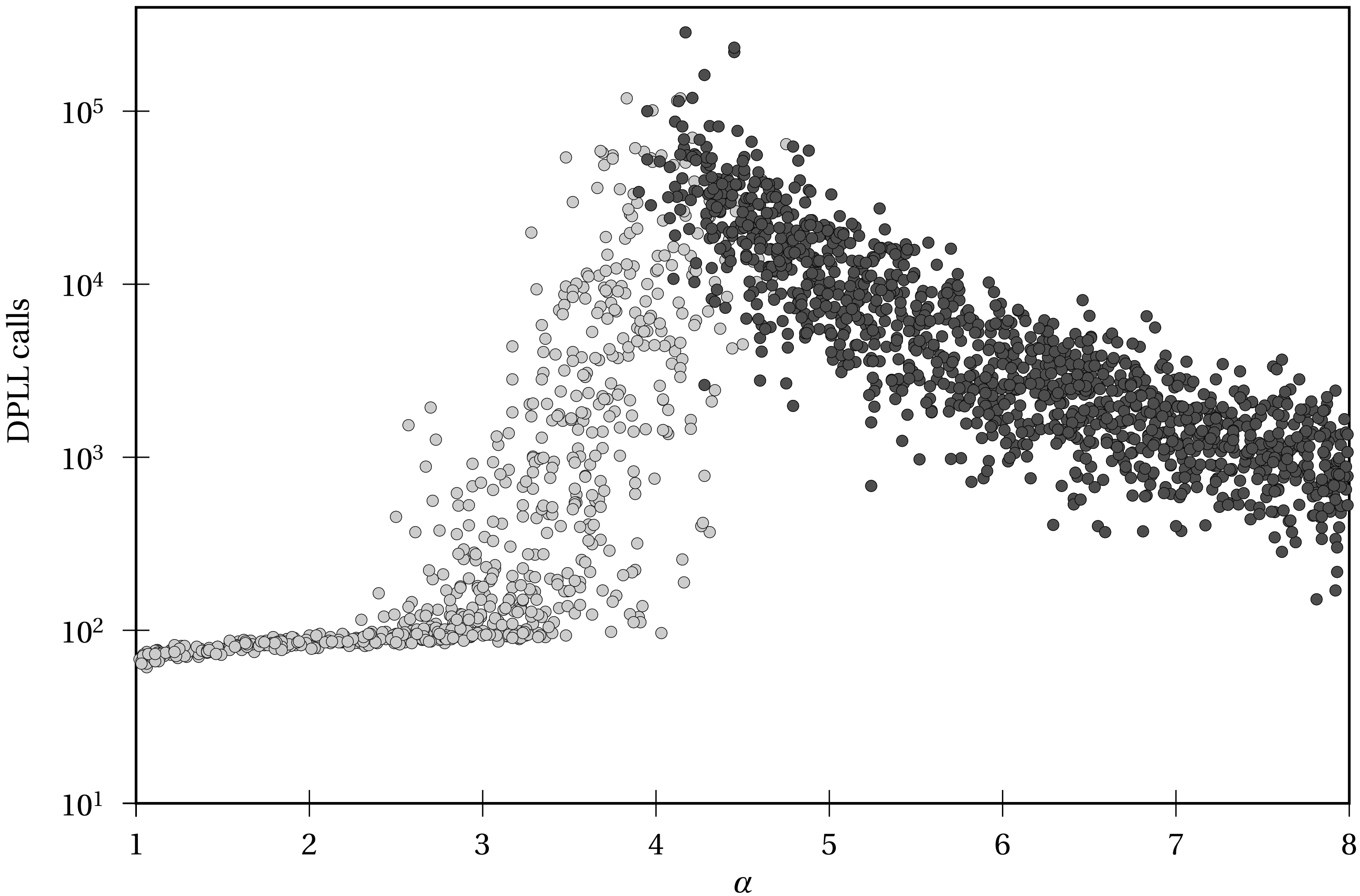
A transition from solvability to unsolvability

When the density of constraints is too high, we can no longer satisfy all of them



Where the hard problems are

Search times are highest at the boundary



The Threshold Conjecture

We believe that for each $k \geq 3$ there is a critical clause density α_k such that

$$\lim_{n \to \infty} \Pr\left[F_k(n, m = \alpha n) \text{ is satisfiable}\right]$$

$$= \begin{cases} 1 & \text{if } \alpha < \alpha_k \\ 0 & \text{if } \alpha > \alpha_k \end{cases}$$

So far, only known rigorously for k=2

An Upper Bound

The *average* number of solutions is

$$2^n \left(\frac{7}{8}\right)^m = \left(2\left(\frac{7}{8}\right)^\alpha\right)^n$$

This is exponentially small whenever

$$\alpha > \log_{8/7} 2 \approx 5.19$$

But the transition is much lower, at $\alpha \approx 4.27$.
What's going on?

A Heavy Tail

In the range $4.27 < \alpha < 5.19$, the average number of solutions is exponentially large.

Occasionally, there are exponentially many...

...but most of the time there are none!

A classic “heavy-tailed” distribution

Large average doesn’t prove satisfiability!

Lower Bound #1

Idea: track the progress of a simple algorithm!

When we set variables, clauses disappear or get shorter:

$$\overline{x} \wedge (x \vee y \vee z) \Rightarrow (y \vee z)$$

Unit Clauses propagate:

$$x \wedge (\overline{x} \vee y) \Rightarrow y$$

One Path Through the Tree

If there is a unit clause, satisfy it.

Otherwise, choose a random variable and give it a random value!

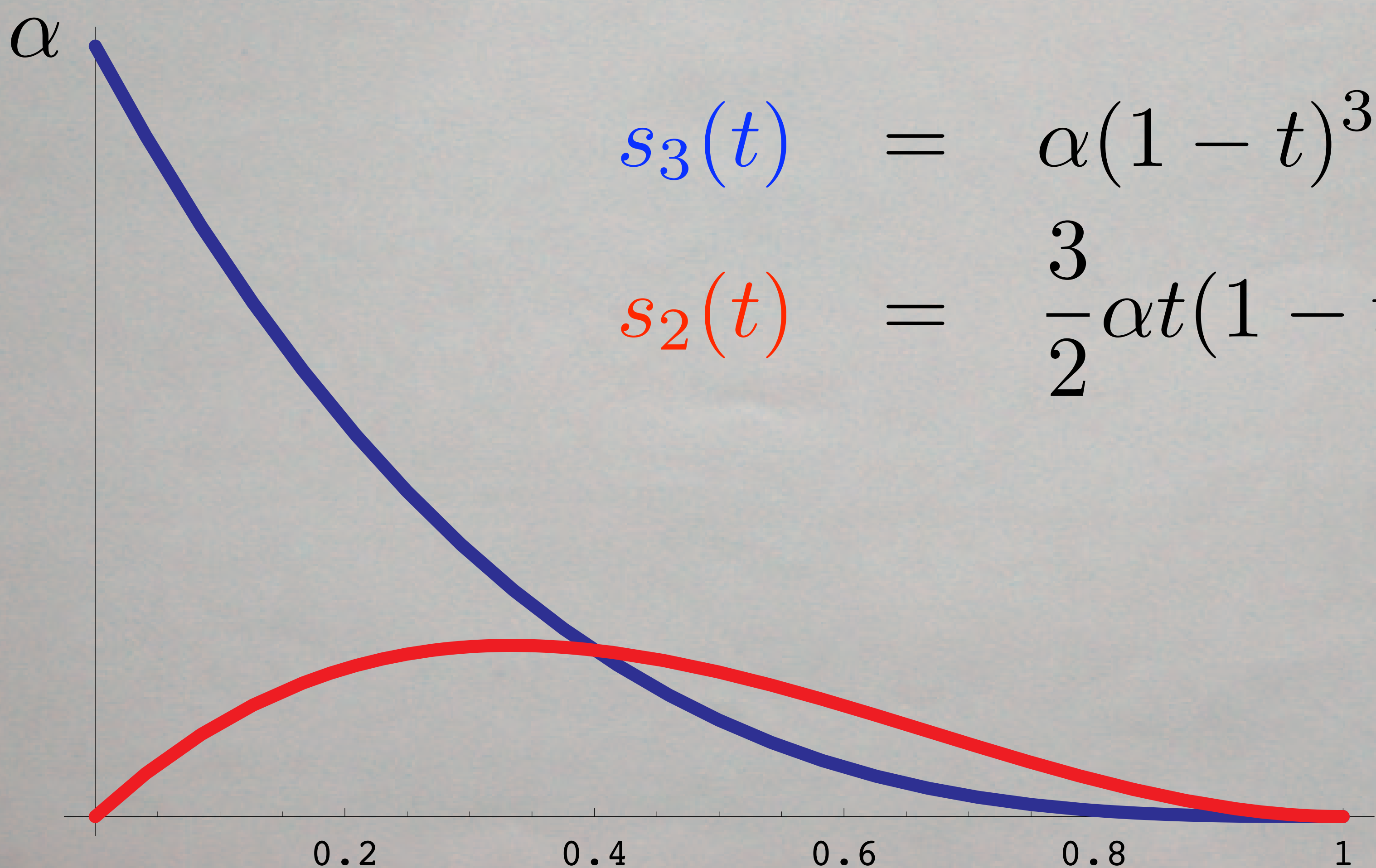
The remaining formula is random. We just need to keep track of densities of 2- and 3-clauses:

$$\frac{ds_3}{dt} = -\frac{3s_3}{1-t} \;, \qquad \frac{ds_2}{dt} = \frac{(3/2)s_3 - 2s_2}{1-t}$$

$$s_3(0) = \alpha \;, \quad s_2(0) = 0$$

One Path Through the Tree

These differential equations give



$$s_3(t) = \alpha(1-t)^3$$

$$s_2(t) = \frac{3}{2}\alpha t(1-t)^2$$

Branching Unit Clauses

Each unit clause has on average λ children, where

$$\lambda = \frac{1}{2}\frac{2s_2}{1-t} = \frac{3}{4}\alpha t(1-t)$$

If $\lambda > 1$ an epidemic of contradictions

Maximized at *t*=1/2

If α < 8/3 then $\lambda < 1$ always, and the unit clauses stay manageable

Thus 8/3 is a lower bound on the transition

Constructive Methods Fail

Fancier algorithms, harder math: $\alpha < 3.52$

But for larger k, algorithmic methods are nowhere near the upper bound for k-SAT:

$$O\left(\frac{2^k}{k}\right) < \alpha < O(2^k)$$

We can close this gap, but the proof is nonconstructive: existence, but no algorithm

Lower Bound #2

Bound the *variance* of the number of solutions.

If X is a nonnegative random variable,

$$\Pr[X > 0] \geq \frac{\mathrm{E}[X]^2}{\mathrm{E}[X^2]}$$

$\mathrm{E}[X]$ is easy; $\mathrm{E}[X^2]$ requires us to understand *correlations* between solutions

Determining the Threshold

A series of results has narrowed the range for the transition in *k*-SAT to

$$2^k \ln 2 - O(k) < \alpha < 2^k \ln 2 - O(1)$$

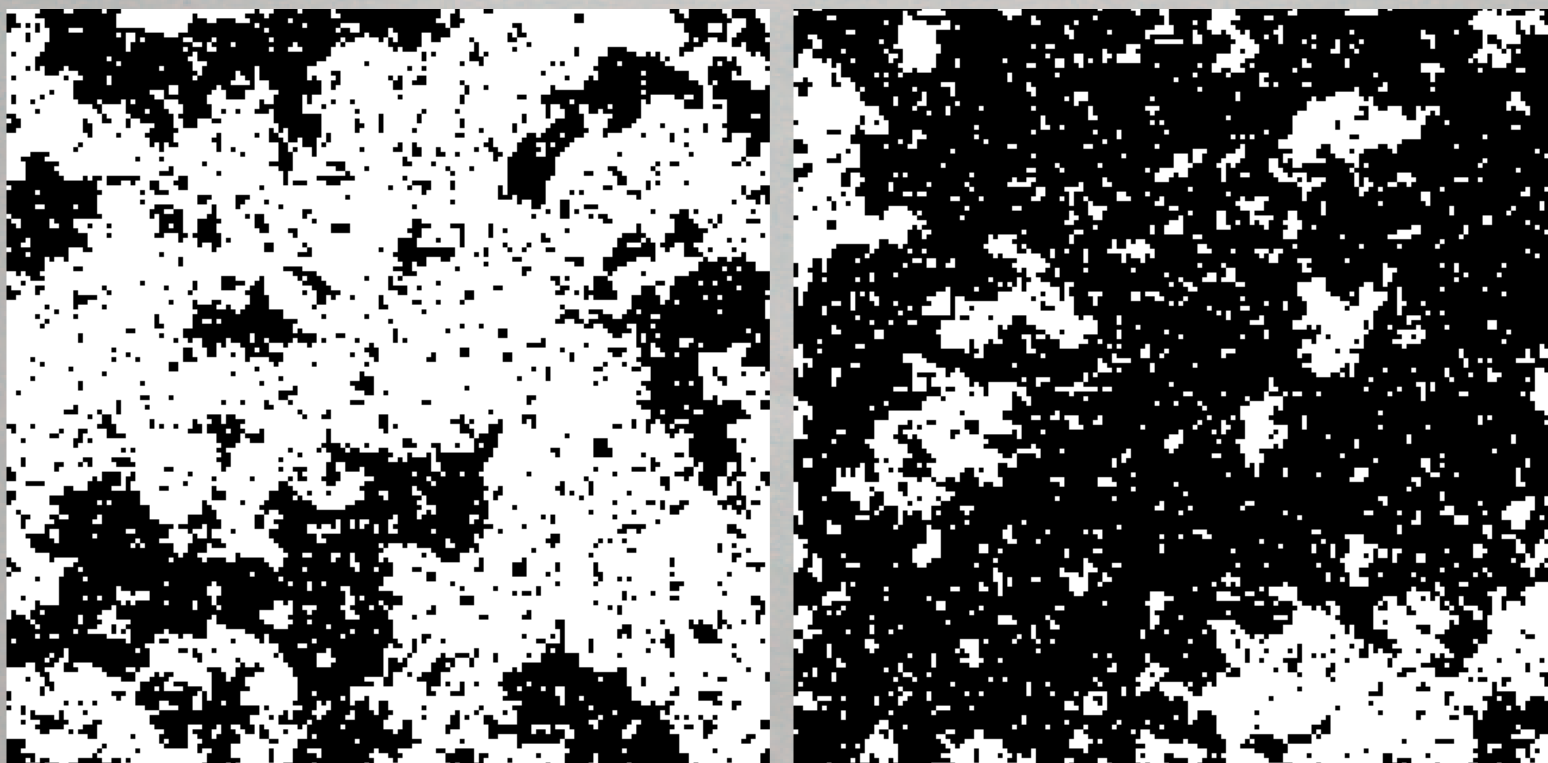
Prediction from statistical physics:

$$2^k \ln 2 - O(1)$$

Making physics rigorous can take a lot of work...

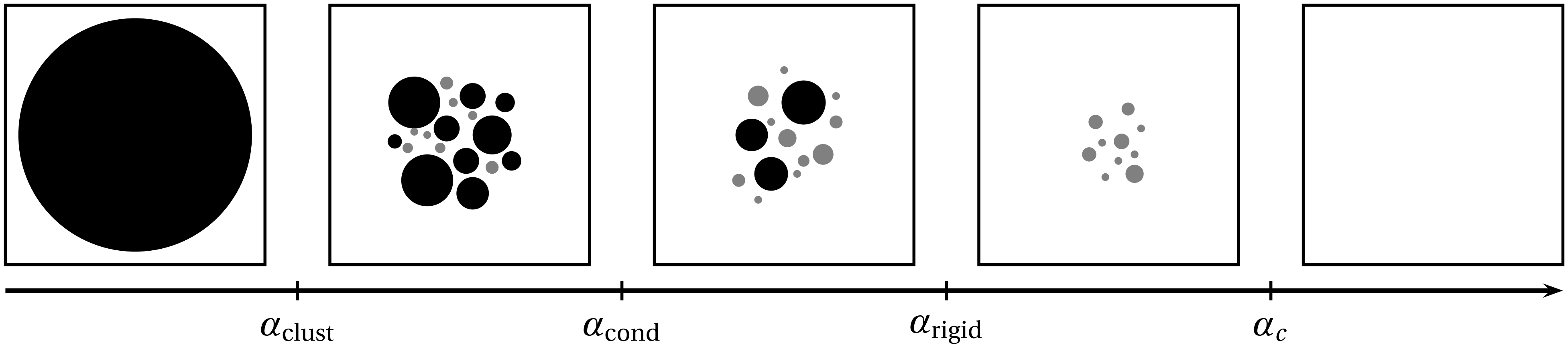
Clustering

Below the critical temperature, magnets have two *macrostates* (Gibbs measures)



Glasses, and 3-SAT, have exponentially many!

Clustering, freezing, and hardness



At a certain density, solutions break up into clusters

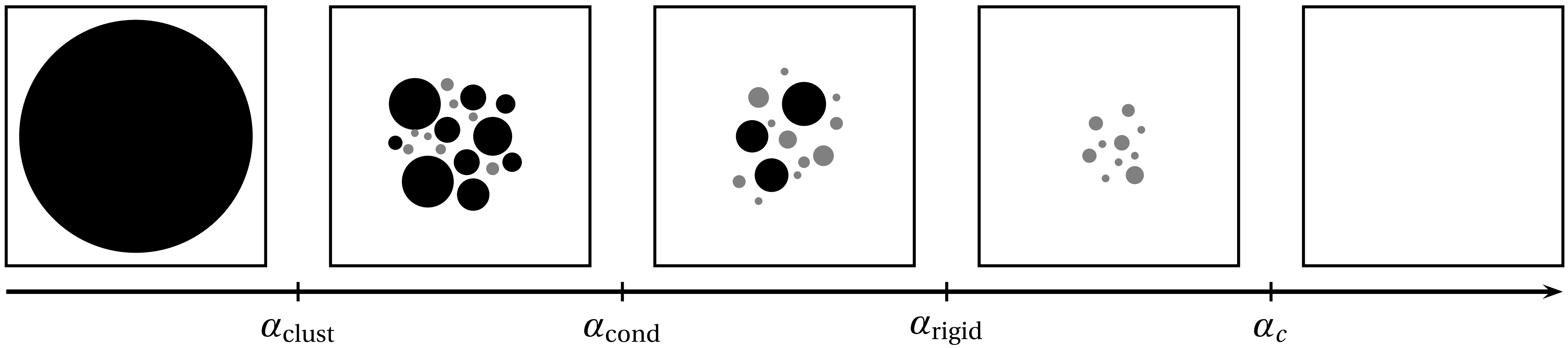
These clusters become *frozen* — many variables take a fixed value

If a search algorithm sets any of these variables wrong, it's doomed

A rugged landscape, with many local optima to get stuck in

[Achlioptas, Coja-Oghlan, Krzakala, Mezard, Molloy, Montanari, Moore, Ricci-Tersenghi, Zdeborová, Zecchina...]

Clustering, freezing, and hardness



We believe that the "freezing" transition marks where the problem becomes hard

All known algorithms for *k*-SAT stop working at or below $\alpha_{\text{rigid}} \sim 2^k \log k / k$

Hard, but satisfiable, instances up to $\alpha_c \sim 2^k \log 2$

Can this be made into a proof that P≠NP?

XORSAT

Use XOR (addition mod 2) instead of OR:

$$x_1 \oplus x_2 \oplus x_3 = 1$$
$$x_1 \oplus x_2 \oplus x_4 = 0$$
$$x_2 \oplus x_3 \oplus x_4 = 1$$

Random instances have many of the same properties as 3-SAT: clustering and freezing (at the same density) and then a transition to unsatisfiability

But XORSAT is easy! Just linear equations:

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

XORSAT

How is XORSAT like SAT, and how is it different?

Clustering: local search algorithms can't move through the space, and hill-climbing algorithms get stuck in local optima

Freezing: backtracking algorithms (Davis-Putnam) take exponential time, repeatedly setting frozen variables the wrong way

But Gaussian elimination is a global rearrangement of variables and constraints, letting us turn a hard-looking problem into an easy one

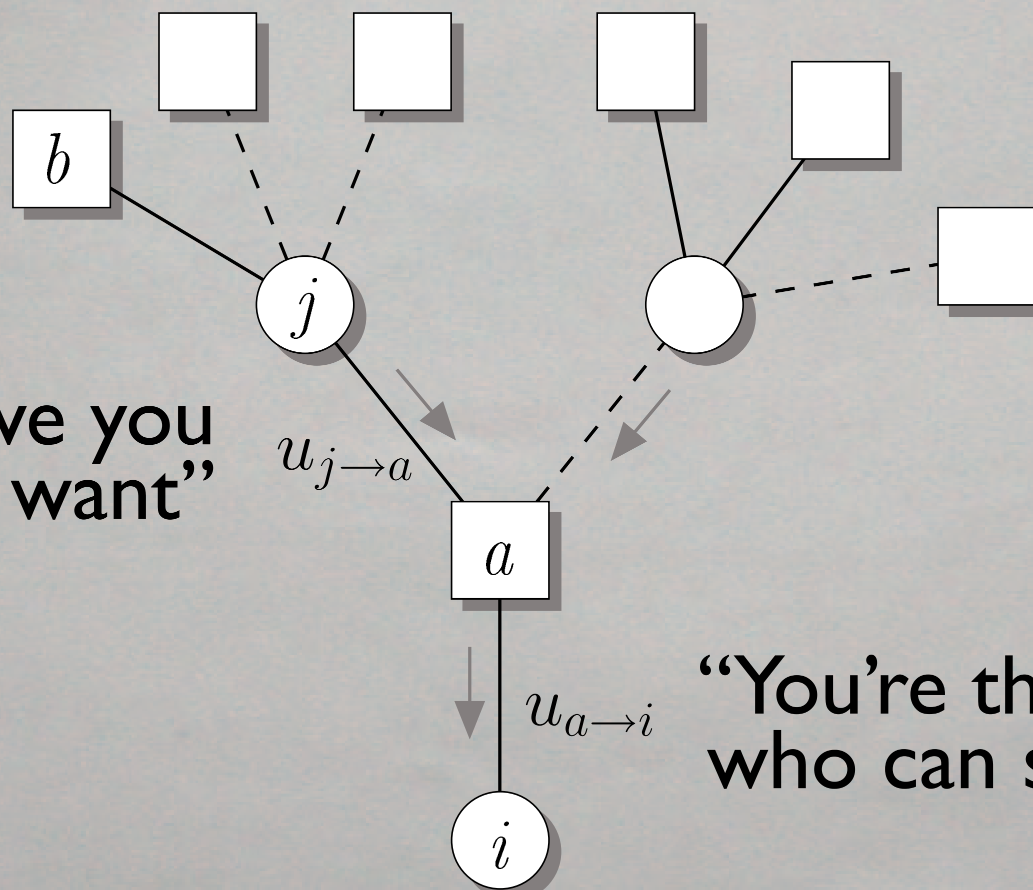
If SAT has a similar kind of rearrangement — something totally different from backtracking or local search — then P=NP

Proving that it doesn't is hard!

The Physicists' Algorithm

A "message-passing" algorithm:

"I can't give you what you want"

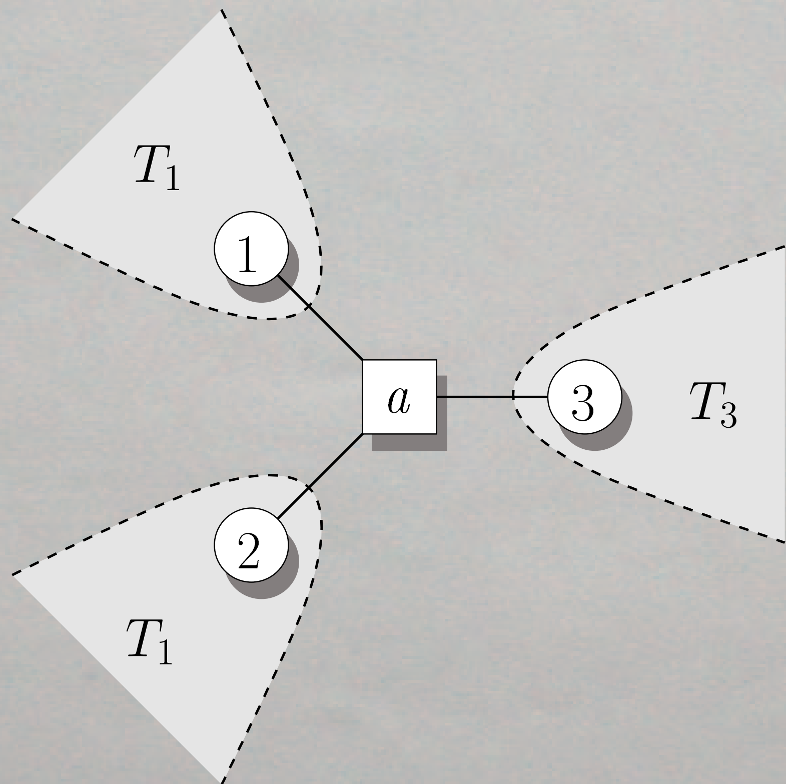


"You're the only one who can satisfy me"

Why Does It Work?

Random formulas are locally treelike.

Assume the neighbors are independent:



Proving that this works will take some deep work.

Building bridges between disciplines

A rich collaboration is growing up between physicists and computer scientists

- Techniques from physics inspire mathematical conjectures and proof techniques, leading to new computer science
- Algorithms inspired by physics can solve large real-world problems, such as analyzing the structure of social networks
- Computer scientists view physical systems, e.g. quantum, in terms of their computational power, leading to new physics

Shameless Plug

This book rocks! You somehow manage to combine the fun of a popular book with the intellectual heft of a textbook.

— Scott Aaronson

A treasure trove of information on algorithms and complexity, presented in the most delightful way.

— Vijay Vazirani

A creative, insightful, and accessible introduction to the theory of computing, written with a keen eye toward the frontiers of the field and a vivid enthusiasm for the subject matter.

— Jon Kleinberg

Oxford University Press, 2011