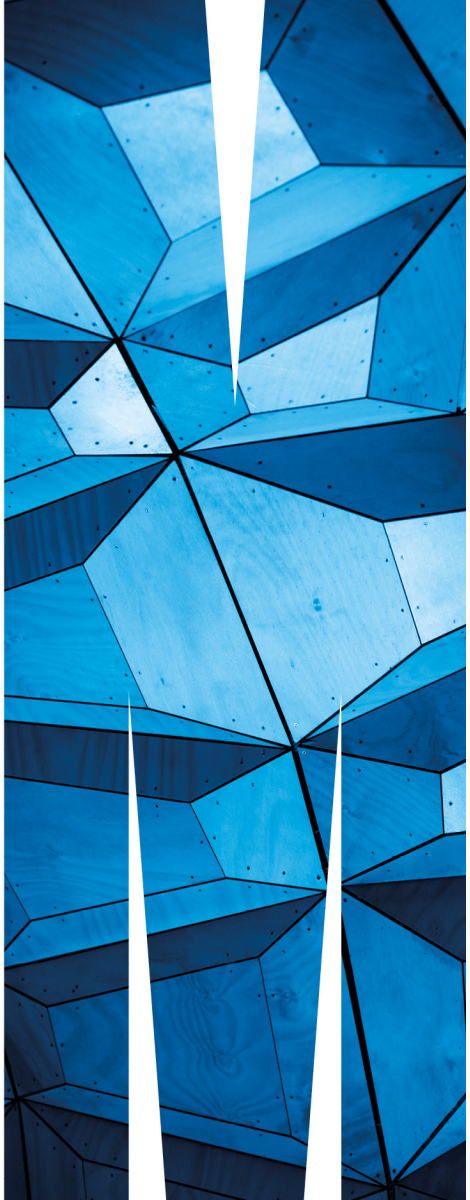
MONASH University

The satisfiability threshold and solution geometry of random linear equations over finite fields

Jane Gao (jane.gao@monash.edu)
School of Mathematical Sciences

Joint work with Peter Ayre, Amin Coja-Oghlan, and Noëla Müller

GROUP OF EIGHT AUSTRALIA



Examples

- k-SAT
- k-NAESAT
- k-XORSAT
- k-colouring of graphs
- 2-colouring of k-uniform hyper graphs
- Potts model
- Ising model (ferromagnetic, antiferromagnetic)
- graph matching (monomer-dimer model)
- independent set (hard core model)
- SK model
- mixed p-spin model

For large k...

- Kirousis, Kranakis, Krizanc, Stamatiou 1998; Franz, Leone 2003: $c_k \leq 2^k \ln 2 - (1 + \ln 2)/2 + o_k(1)$.
- Achlioptas, Peres 2004: $c_k \geq 2^k \ln 2 - (k/2) \ln 2 - (1 + \ln 2/2) + o_k(1)$.
- Mertens, Mézard, Zecchina 2006: $c_k = 2^k \ln 2 - (1 + \ln 2)/2 + o_k(1)$ (1RSB).
- Coja-Oghlan, Panagiotou 2013: $c_k \geq 2^k \ln 2 - (3/2) \ln 2 + o_k(1)$.
- Coja-Oghlan 2014: $c_k = 2^k \ln 2 - (1 + \ln 2)/2 + o_k(1)$.

K-SAT threshold

MONASH University

Let d^+, d^- be independent samples from the Pois$(\alpha k/2)$ distribution, and write $\underline{d} \equiv (d^+, d^-)$. Let $\mathscr{P}$ denote the space of probability measures on $[0,1]$, and define a recursion $\boldsymbol{R} \equiv \boldsymbol{R}^\alpha : \mathscr{P} \to \mathscr{P}$ as follows. Given $\mu \in \mathscr{P}$, generate (independently of $\underline{d}$) an array $\underline{\eta} \equiv [(\eta_j)_{j \geqslant 1}, (\eta^+_{ij}, \eta^-_{ij})_{i,j \geqslant 1}]$ of i.i.d. samples from μ. Then $\boldsymbol{R}\mu \in \mathscr{P}$ is the law of

$$R(\underline{d}, \underline{\eta}) \equiv \frac{(1 - \Pi^-)\Pi^+}{\Pi^+ + \Pi^- - \Pi^+\Pi^-}, \text{ where } \Pi^\pm \equiv \Pi^\pm(\underline{d}, \underline{\eta}) \equiv \prod_{i=1}^{d^\pm} \Big(1 - \prod_{j=1}^{k-1} \eta^\pm_{ij}\Big). \tag{7}$$

Proposition 2. *Fix k, α and write $\boldsymbol{R} \equiv \boldsymbol{R}^\alpha$. Let $\mu_\ell \equiv \mu^\alpha_\ell \in \mathscr{P}$ $(\ell \geqslant 0)$ be the sequence of probability measures defined by $\mu_0 = \delta_{1/2}$, and $\mu_\ell = \boldsymbol{R}\mu_{\ell-1}$ for all $\ell \geqslant 1$. For $k \geqslant k_0$ and $\alpha_{\rm lbd} \leqslant \alpha \leqslant \alpha_{\rm ubd}$, this sequence converges weakly as $\ell \to \infty$ to a limit $\mu = \mu_\alpha \in \mathscr{P}$, satisfying $\boldsymbol{R}\mu = \mu$.*

The following is the formal characterization of the 1-RSB prediction $\alpha_\star$ for the k-SAT threshold:

Proposition 3. *Given k, α, let $\mu = \mu_\alpha$ be the fixed point of Propn. 2. Let $\underline{d} \equiv (d^+, d^-)$ as above, and let $\underline{\eta} \equiv [(\eta_j)_{j \geqslant 1}, (\eta^+_{ij}, \eta^-_{ij})_{i,j \geqslant 1}]$ be an array of i.i.d. samples from μ (independent of $\underline{d}$). Define*

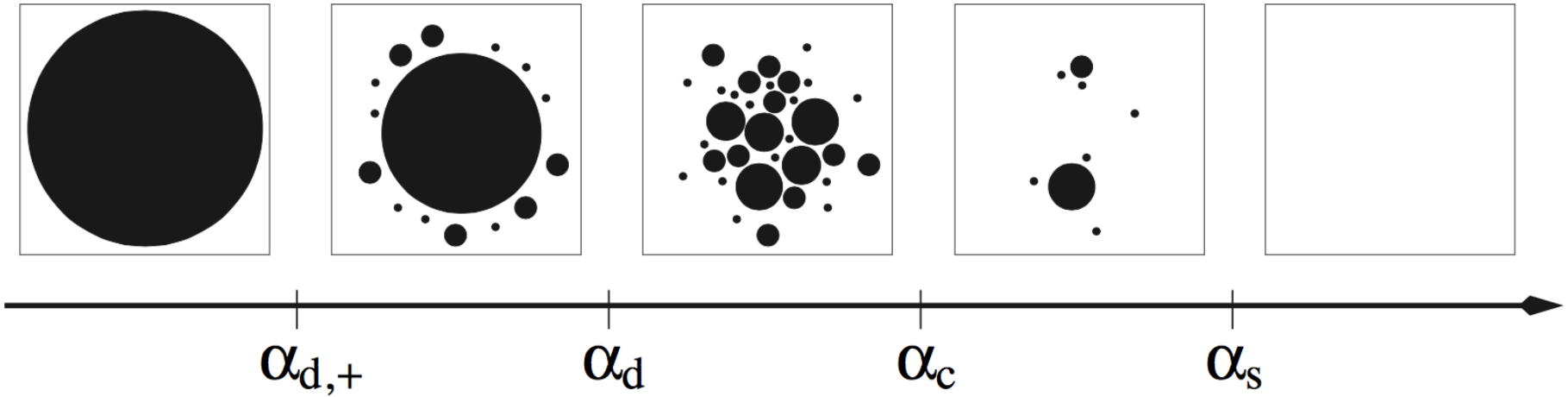
$$\Phi(\alpha) = \mathbb{E}\left[\ln \frac{\Pi^+ + \Pi^- - \Pi^+\Pi^-}{(1 - \prod_{j=1}^k \eta_j)^{\alpha(k-1)}} \right], \tag{8}$$

where $\mathbb{E}$ indicates the expectation over $(\underline{d}, \underline{\eta})$. For $k \geqslant k_0$, the function Φ is well-defined and strictly decreasing on the interval $\alpha_{\rm lbd} \leqslant \alpha \leqslant \alpha_{\rm ubd}$, with a unique zero $\alpha_\star \equiv \alpha_\star(k)$.

Main challenge: large deviation

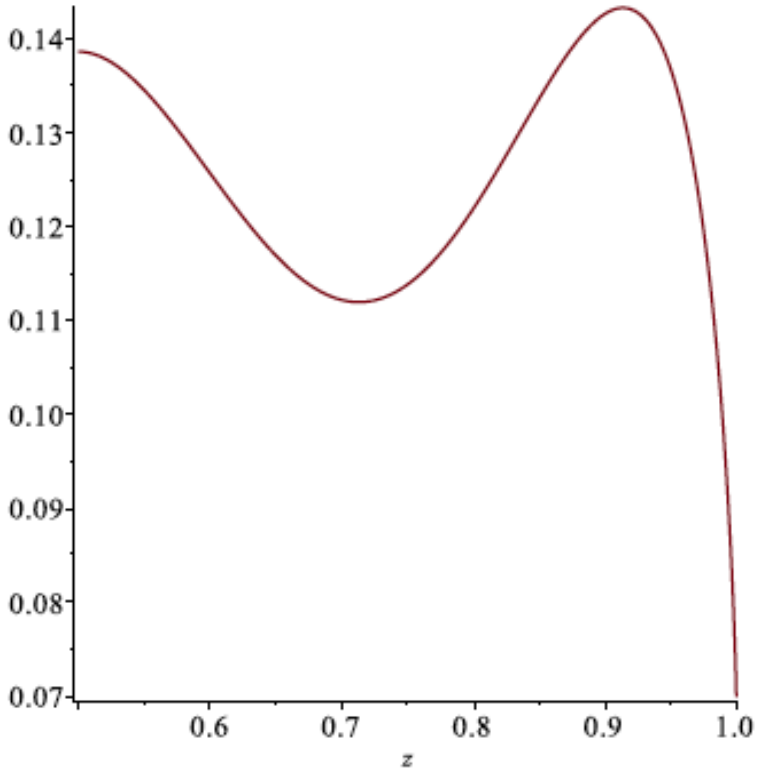
- Z: the number of k-SAT solutions;
- $\mathbf{E}Z \to \infty$;
- we need $\sqrt{\mathbf{Var}Z} = O(\mathbf{E}Z)$ to conclude $Z > 0$;
- But $\sqrt{\mathbf{Var}Z} \geq a^n \mathbf{E}Z$.

Phase transitions of the solution geometry



[Krzakala, Montanari, Ricci-Tersenghi, Semerjian, Zdeborova 2007]

Lottery effect kills the second moment method



Theorem 1.1. *Let $k \geq 3$, let $q > 1$ be a prime power and let P be a permutation-invariant distribution on $\mathbb{F}_q^{*k}$. Set*

$$\rho_{k,d} = \sup\left\{x \in [0,1] : x = 1 - \exp(-d x^{k-1})\right\} \qquad \text{for } d > 0, \text{ and define} \tag{1.1}$$

$$d_k = \inf\left\{d > 0 : \rho_{k,d} - d\rho_{k,d}^{k-1} + (1 - 1/k) d \rho_{k,d}^{k} < 0\right\}. \tag{1.2}$$

Then

$$\lim_{n\to\infty} \mathbb{P}\left[\exists x \in \mathbb{F}_q^n : \boldsymbol{A}x = \boldsymbol{y}\right] = \begin{cases} 1 & \text{if } d < d_k, \\ 0 & \text{if } d > d_k \end{cases}$$

and thus for $d < d_k$ we have

$$\lim_{n\to\infty} \mathbb{P}\left[\mathrm{rk}(\boldsymbol{A}) = \boldsymbol{m}\right] = 1. \tag{1.3}$$

Replica symmetry (correlation decay)

$$\omega_{\sigma,\tau}(x,x') = \frac{1}{n}\sum_{i=1}^{n} \mathbf{1}\{x_i = \sigma, x'_i = \tau\}.$$

Theorem 1.2. *Let $k \geq 3$, let $q > 1$ be a prime power, let P be a permutation-invariant distribution on $\mathbb{F}_q^{*k}$ and assume that $d < d_k$. Then*

$$\lim_{n\to\infty} \mathbb{E}\left[\left\langle \|\omega(\boldsymbol{x},\boldsymbol{x}') - \bar{\omega}\|_{\mathrm{TV}}\right\rangle_{\boldsymbol{A},\boldsymbol{y}} \,\middle|\, \exists x \in \mathbb{F}_q^n : \boldsymbol{A}x = \boldsymbol{y}\right] = 0.$$

Solution clusters

Theorem 1.3. *Let $k \geq 3$, let $q > 1$ be a prime power and let P be a permutation-invariant distribution on $\mathbb{F}_q^{*k}$. Further, with $\rho_{k,d}$ from (1.1) let*

$$d_k^\star = \inf\{d > 0 : \rho_{k,d} > 0\}. \tag{1.4}$$

(i) If $d < d_k^\star$, then the solutions to the linear system $\boldsymbol{A}x = \boldsymbol{y}$ form a single cluster w.h.p.

(ii) If $d_k^\star < d < d_k$, then the minimum distance between distinct solutions clusters is $\Omega(n)$ w.h.p.

$$\frac{1}{n}\ln|\Sigma(\boldsymbol{A},\boldsymbol{y})| \xrightarrow{n\to\infty} \left(\rho_{k,d} - d\rho_{k,d}^{k-1} + d(1-1/k)\rho_{k,d}^{k}\right)\ln q > 0 \qquad \text{in probability.}$$

Bethe free entropy

Define $\mathscr{B} : \mathscr{P}^2(\mathbb{F}_q) \to [0,\infty)$ by letting

$$\mathscr{B}_d(\pi) = \mathbb{E}\left[\ln\left(\sum_{\sigma_1\in\mathbb{F}_q}\prod_{i=1}^{r}\sum_{\sigma_2,\ldots,\sigma_k\in\mathbb{F}_q}\mathbf{1}\left\{\sum_{j=1}^{k}a_{ij}\sigma_j=0\right\}\prod_{j=2}^{k}\nu_{ij}(\sigma_j)\right)\right]$$
$$-\frac{d(k-1)}{k}\mathbb{E}\left[\ln\left(\sum_{\sigma_1,\ldots,\sigma_k\in\mathbb{F}_q}\mathbf{1}\left\{\sum_{j=1}^{k}a_{1j}\sigma_j=0\right\}\prod_{j=1}^{k}\nu_{1j}(\sigma_j)\right)\right],$$

$$\pi = \alpha\delta_{\delta_0} + (1-\alpha)\delta_{\frac{1}{q}\sum_{i=0}^{q-1}\delta_i}$$