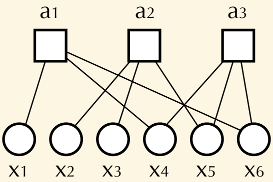
The rank of random matrices over $\mathbb{F}_q$

Amin Coja-Oghlan
Goethe University Frankfurt

joint work with Pu Gao

Linear codes

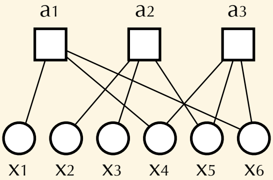
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 1 \end{pmatrix}$$



- let q be a prime power and A and $m \times n$ matrix over $\mathbb{F}_q$
- the codebook is $\ker A$
- the rate of the code is $\mathrm{nul}(A)/n$

Low-density parity check codes

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 1 \end{pmatrix}$$



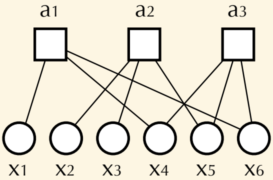
- let $\boldsymbol{d} \geq 1$, $\boldsymbol{k} \geq 3$ be random variables with $\mathrm{E}[\boldsymbol{d}^{2+\varepsilon}], \mathrm{E}[\boldsymbol{k}^{2+\varepsilon}] < \infty$
- with $d = \mathrm{E}[\boldsymbol{d}]$, $k = \mathrm{E}[\boldsymbol{k}]$ and $m \sim \mathrm{Po}(dn/k)$ and given

$$\sum_{i=1}^{n} \boldsymbol{d}_i = \sum_{i=1}^{m} \boldsymbol{k}_i$$

  generate a random bipartite graph $\mathbf{G}$ with degrees $\boldsymbol{d}_i, \boldsymbol{k}_i$
- insert entries drawn from $\boldsymbol{\chi} \in \mathbb{F}_q^*$ independently to obtain $\boldsymbol{A}$

Low-density parity check codes

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & 1 \end{pmatrix}$$

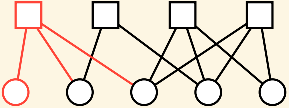


- $\boldsymbol{A}$ is a sparse random matrix over $\mathbb{F}_q$
- define the rate of the code as $1 - \lim_{n\to\infty} \mathrm{rank}(\boldsymbol{A})/n$
- *Goal:* given $\boldsymbol{d}, \boldsymbol{k}, \boldsymbol{\chi}$, find $\lim_{n\to\infty} \mathrm{rank}(\boldsymbol{A})/n$

Prior work

- classical work on dense matrices [K96]
- the case $\boldsymbol{d} = d$, $\boldsymbol{k} = k$ [MC03]
- sufficient condition for full rank [MMU08]
- full rank: $q = 2$, $\boldsymbol{d} \sim \mathrm{Po}(d)$, $\boldsymbol{k} = k$ [DM03,DGMMPR10,PS16]
- rank for $q = 2$, $\boldsymbol{d} \sim \mathrm{Po}(d)$, $\boldsymbol{k} = k$ [CFP18]
- rank for $q > 2$, $\boldsymbol{d} \sim \mathrm{Po}(d)$, $\boldsymbol{k} = k$ [ACOGM17]

A graph-theoretic bound



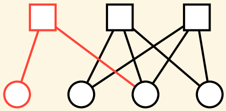
The 2-core

Keep removing

- zero columns
- columns with one non-zero entry along with that row

How many ways are there to extend $\boldsymbol{A}_* 0 = 0$ to a solution of $\boldsymbol{A}x = 0$?

A graph-theoretic bound



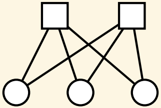
The 2-core

Keep removing

- zero columns
- columns with one non-zero entry along with that row

How many ways are there to extend $\boldsymbol{A}_* 0 = 0$ to a solution of $\boldsymbol{A}x = 0$?

A graph-theoretic bound



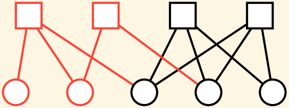
The 2-core

Keep removing

- zero columns
- columns with one non-zero entry along with that row

How many ways are there to extend $\boldsymbol{A}_* 0 = 0$ to a solution of $\boldsymbol{A} x = 0$?

A graph-theoretic bound



The 2-core bound

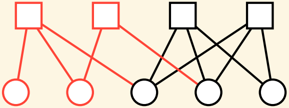
- let $\boldsymbol{n}^*$ = #columns and $\boldsymbol{m}^*$ = #rows of the 2-core
- then

$$\mathrm{nul}(\boldsymbol{A}) \geq n - \boldsymbol{n}^* - (m - \boldsymbol{m}^*) \qquad \text{and thus}$$

$$\mathrm{rank}(\boldsymbol{A}) \leq \boldsymbol{n}^* + m - \boldsymbol{m}^*$$

- also trivially $\mathrm{rank}(\boldsymbol{A}) \leq m$

A graph-theoretic bound



The 2-core bound

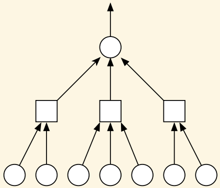
- with $D(\cdot)$, $K(\cdot)$ the p.g.f. of $\boldsymbol{d}, \boldsymbol{k}$, let

$$\Phi(z) = D(1 - K'(z)/k) + \frac{d}{k}\left(K(z) + (1-z)K'(z) - 1\right),$$
$$\varrho = \max\left\{z \in [0,1] : \Phi'(z) = 0\right\}$$

- Then

$$\limsup_{n\to\infty} \operatorname{rank}(\boldsymbol{A})/n \le 1 - (\Phi(0) \vee \Phi(\varrho))$$

The cavity method…



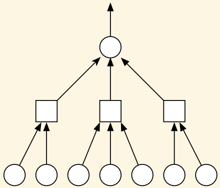
The replica symmetric ansatz [AS08]

- size-biased check degrees $\mathrm{P}[\hat{\boldsymbol{k}} = i] = i\mathrm{P}[\boldsymbol{k} = i]/k$
- fixed points of the Belief Propagation recurrence

$$\boldsymbol{\mu}(\sigma) \propto \prod_{i=1}^{\boldsymbol{d}} \sum_{\tau \in \mathbb{F}_q^{\hat{\boldsymbol{k}}_i}} \mathbf{1}\left\{\tau_1 = \sigma, \sum_{h=1}^{\hat{\boldsymbol{k}}_i} \boldsymbol{\chi}_{i,h}\tau_h = 0\right\} \prod_{h=2}^{\hat{\boldsymbol{k}}_i} \boldsymbol{\mu}_{i,h}(\tau_h)$$

via population dynamics

The cavity method…



The replica symmetric ansatz [AS08]

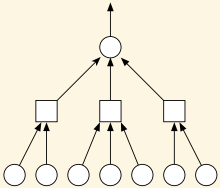
- the Bethe free entropy

$$\mathscr{B}(\boldsymbol{\mu}) = \mathrm{E}\left[\log_q \sum_{\sigma_1 \in \mathbb{F}_q} \prod_{i=1}^{\boldsymbol{d}} \sum_{\sigma_2,\ldots,\sigma_{\hat{\boldsymbol{k}}_i} \in \mathbb{F}_q} \mathbf{1}\left\{\sum_{j=1}^{\hat{\boldsymbol{k}}_i} \sigma_j \boldsymbol{\chi}_{i,j} = 0\right\} \prod_{j=2}^{\hat{\boldsymbol{k}}_i} \boldsymbol{\mu}_{i,j}(\sigma_j)\right] - \frac{d}{k}\mathrm{E}\left[(\boldsymbol{k}-1)\log_q \sum_{\sigma_1,\ldots,\sigma_{\boldsymbol{k}} \in \mathbb{F}_q} \mathbf{1}\left\{\sum_{i=1}^{\boldsymbol{k}} \sigma_i \boldsymbol{\chi}_i = 0\right\} \prod_{i=1}^{\boldsymbol{k}} \boldsymbol{\mu}_i(\sigma_i)\right]$$

should yield

$$\mathrm{rank}(\boldsymbol{A})/n \sim 1 - \mathscr{B}(\boldsymbol{\mu})$$

The cavity method…



The replica symmetric ansatz [AS08]

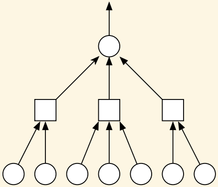
- solutions for various $\boldsymbol{d}, \boldsymbol{k}$ read

$$\boldsymbol{\mu} = \begin{cases} \delta_0 & \text{with probability } z \\ q^{-1}\mathbf{1} & \text{with probability } 1-z \end{cases} \qquad \text{for } z \in \{0, \varrho\}$$

- in effect, $\mathscr{B}(\boldsymbol{\mu}) = 1 - (\Phi(0) \vee \Phi(\varrho))$
- *Conjecture:* for any $\boldsymbol{d}, \boldsymbol{k}, \boldsymbol{\chi}$,

$$\lim_{n\to\infty} \operatorname{rank}(\boldsymbol{A})/n = 1 - (\Phi(0) \vee \Phi(\varrho))$$

The cavity method…



Survey Propagation and 1rsb [MM08]

- fixed points of the Survey Propagation equations [MRTZ02]
- 1rsb version of the Bethe formula
- *Prediction:* for any $\boldsymbol{d}, \boldsymbol{k}, \boldsymbol{\chi}$,

$$\lim_{n\to\infty} \mathrm{rank}(\boldsymbol{A})/n = 1 - (\Phi(0) \vee \Phi(\varrho))$$

…and its caveats

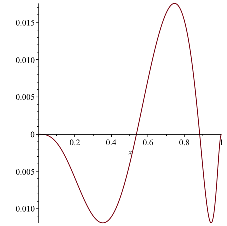
Theorem [L13]

For any $\boldsymbol{d}, \boldsymbol{k}, \boldsymbol{\chi}$,

$$\limsup_{n\to\infty} \frac{1}{n} \operatorname{rank}(\boldsymbol{A}) \leq 1 - \max_{z\in[0,1]} \Phi(z)$$

Proof via determinant and the matching number [BLS13]

…and its caveats



Example [L13]

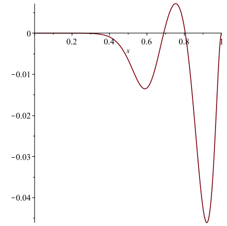
Consider $\boldsymbol{d}, \boldsymbol{k}$ with

$$D(z) = K(z) = 4z^3/5 + z^{15}/5$$

Then $\varrho = 1$ and $\Phi(0) = \Phi(\varrho) = 0$ but

$$\limsup_{n\to\infty} \frac{1}{n} \operatorname{rank}(\boldsymbol{A}) < 1.$$

…and its caveats



Example [COG18]

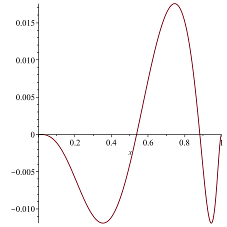
Letting $\boldsymbol{k} = 10$ and

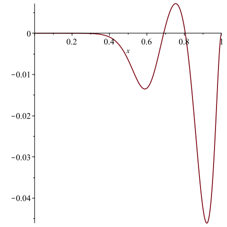
$$D(z) = (190z^3 + 7z^{200})/197,$$

we have $\varrho = 1$ and $\Phi(0) = \Phi(\varrho) = 0$ but

$$\limsup_{n\to\infty} \frac{1}{n} \operatorname{rank}(\boldsymbol{A}) < 1.$$

…and its caveats





Conjecture [L13]

For any $\boldsymbol{d}, \boldsymbol{k}, \boldsymbol{\chi}$,

$$\lim_{n\to\infty} \frac{1}{n}\mathrm{rank}(\boldsymbol{A}) = 1 - \max_{\alpha\in[0,1]} \Phi(\alpha)$$

The rank formula

Theorem [COG18]

For any $\boldsymbol{d}, \boldsymbol{k}, \boldsymbol{\chi}$,

$$\lim_{n\to\infty} \frac{1}{n} \operatorname{rank}(\boldsymbol{A}) = 1 - \max_{\alpha\in[0,1]} \Phi(\alpha)$$

The rank formula

Theorem [COG18]

If

- either $\mathrm{Var}(\boldsymbol{k}) = 0$ or $\boldsymbol{k} \sim \mathrm{Po}_{\geq \ell}(\lambda)$, and
- either $\mathrm{Var}(\boldsymbol{d}) = 0$ or $\boldsymbol{d} \sim \mathrm{Po}_{\geq \ell'}(\lambda')$,

then

$$\lim_{n\to\infty} \frac{1}{n} \mathrm{rank}(\boldsymbol{A}) = 1 - \Phi(0) \vee \Phi(\varrho)$$

This covers all examples from [AS08].

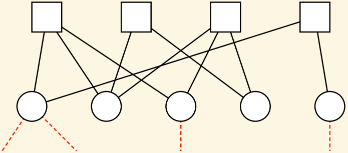
Aizenman-Sims-Starr

$$\limsup_{n\to\infty} \frac{1}{n} \mathrm{E}\left[\mathrm{nul}(\boldsymbol{A})\right] \leq \limsup_{n\to\infty} \mathrm{E}\left[\mathrm{nul}(\boldsymbol{A}_{n+1})\right] - \mathrm{E}\left[\mathrm{nul}(\boldsymbol{A}_n)\right]$$

Aizenman-Sims-Starr

$$\mathrm{E}\left[\mathrm{nul}(\boldsymbol{A}_{n+1})\right] - \mathrm{E}\left[\mathrm{nul}(\boldsymbol{A}_n)\right] \leq \max_{\alpha \in [0,1]} \Phi(\alpha) + o(1)$$

Cavities redux

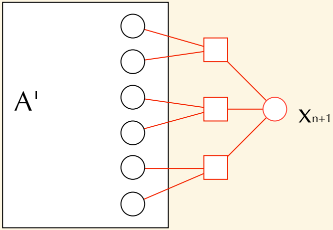


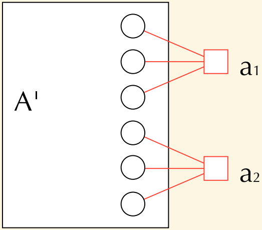
- let $\boldsymbol{A}_{\varepsilon,n}$ be a random $m_\varepsilon \times n$-matrix with

$$m_\varepsilon \sim \mathrm{Po}((1-\varepsilon)dn/k)$$

- cavities are variables that undershoot their target degrees

Cavities redux





- $\boldsymbol{A}_{\varepsilon,n+1}$ and $\boldsymbol{A}_{\varepsilon,n}$ can be coupled (relatively) easily
- we aim to show

$$\limsup_{\varepsilon\to 0}\limsup_{n\to\infty} \mathrm{E}\left[\mathrm{nul}(\boldsymbol{A}_{\varepsilon,n+1}) - \mathrm{nul}(\boldsymbol{A}_{\varepsilon,n})\right] \leq \max_{\alpha\in[0,1]} \Phi(\alpha)$$

The Boltzmann distribution

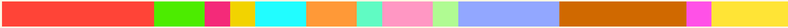
- for an $m \times n$ matrix A define $\mu_A \in \mathscr{P}(\mathbb{F}_q^n)$ by

$$\mu_A(\sigma) = \mathbf{1}\{\sigma \in \ker A\} / q^{\mathrm{nul}(A)}$$

- μ_A is (δ, ℓ)-extremal if

$$\sum_{i_1,\dots,i_\ell=1}^{n} \left\| \mu_{A,i_1,\dots,i_\ell} - \mu_{A,i_1} \otimes \cdots \otimes \mu_{A,i_\ell} \right\|_{\mathrm{TV}} < \delta n^\ell$$

The Boltzmann distribution



Lemma [ACOGM17]

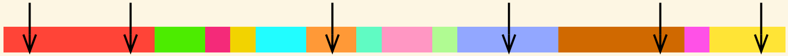
For any $m \times n$ matrix A there is a partition $I_0, \ldots, I_t$ of $\{1, \ldots, n\}$ s.t.

$$\mu_{A,i} = \begin{cases} \delta_0 & \text{if } i \in I_0 \\ q^{-1}\mathbf{1} & \text{otherwise} \end{cases}$$

$$H(\mu_{A,i,j}) = 2\log q \qquad \text{if } i \in I_s,\ j \in I_{s'},\ 1 \le s < s'$$

$$H(\mu_{A,i,j}) = \ln q \qquad \text{if } i, j \in I_s,\ 1 \le s$$

The Boltzmann distribution



Corollary [ACOGM17]

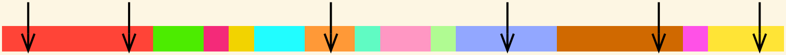
For any $\delta, \ell > 0$ there is $\boldsymbol{\theta} = \boldsymbol{\theta}(\delta, \ell) > 0$ such that for any $m \times n$ matrix A for a random column permutation $\boldsymbol{\pi}$,

$$\hat{A} = \begin{pmatrix} & A^{\boldsymbol{\pi}} & \\ \mathrm{id}_{\boldsymbol{\theta} \times \boldsymbol{\theta}} & & 0 \end{pmatrix}$$

satisfies

$$\mathrm{P}\left[\mu_{\hat{A}} \text{ is } (\delta, \ell)\text{-extrmal}\right] > 1 - \delta.$$

The Boltzmann distribution

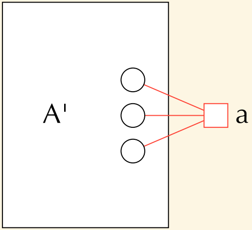


Corollary [ACOGM17]

For any $\delta, \ell > 0$ there is $\boldsymbol{\theta} = \boldsymbol{\theta}(\delta, \ell) > 0$ such that

$$\mathrm{P}\left[\mu_{\boldsymbol{A}_{\varepsilon,n,\boldsymbol{\theta}}} \text{ is } (\delta, \ell)\text{-extrmal}\right] > 1 - \delta.$$

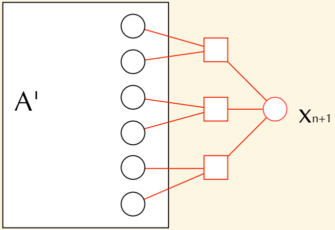
Adding a check



- let $\boldsymbol{\alpha}$ be the (weighted) fraction of frozen cavities
- adding a check a of degree κ entails

$$\mathrm{E}[\mathrm{nul}(\boldsymbol{A}' + a) \mid \boldsymbol{\alpha}] = \boldsymbol{\alpha}^{\kappa} - 1 + o(1)$$

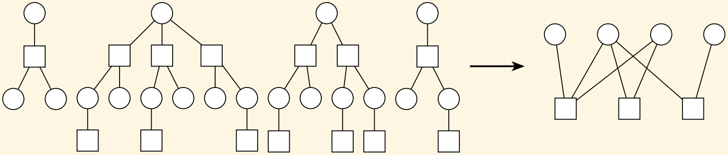
Adding a variable



- let $\boldsymbol{\alpha}$ be the (weighted) fraction of frozen cavities
- adding x_{n+1} along with checks of degrees $\kappa_1, \ldots, \kappa_{\boldsymbol{\gamma}}$ yields

$$\begin{aligned} &\mathrm{E}[\mathrm{nul}(\boldsymbol{A}' + x_{n+1} + a_1 + \cdots + a_{\boldsymbol{\gamma}}) \mid \boldsymbol{\alpha}] \\ &\quad = \boldsymbol{\gamma} \prod_{i=1}^{\boldsymbol{\gamma}} \left(1 - \boldsymbol{\alpha}^{\kappa_i - 1}\right) + \sum_{i=1}^{\boldsymbol{\gamma}} \left(\boldsymbol{\alpha}^{\kappa_i - 1} - 1\right) + (1 - \boldsymbol{\gamma}) \prod_{i=1}^{\boldsymbol{\gamma}} \left(1 - \boldsymbol{\alpha}^{\kappa_i - 1}\right) \\ &\quad = \prod_{i=1}^{\boldsymbol{\gamma}} \left(1 - \boldsymbol{\alpha}^{\kappa_i - 1}\right) + \sum_{i=1}^{\boldsymbol{\gamma}} \left(\boldsymbol{\alpha}^{\kappa_i - 1} - 1\right) \end{aligned}$$

Lower bound via interpolation



- set up an interpolation with

$$m_\varepsilon(t) = \mathrm{Po}((1-\varepsilon)\, t\, d\, n / k) \qquad \text{‘real’ checks,}$$

$$m_\varepsilon(t) = \mathrm{Po}((1-\varepsilon)(1-t)\, d\, n \mathrm{E}[\boldsymbol{k}^2]/k) \qquad \text{unary checks}$$

- actual matrices throughout the interpolation

Summary

- proof of Lelarge's rank conjecture

$$\lim_{n\to\infty} \frac{1}{n}\mathrm{rank}(\boldsymbol{A}) = 1 - \max_{\alpha\in[0,1]} \Phi(\alpha)$$

- proof strategy inspired by inference problems [COKPZ18]
- *Open problem:* random equations over finite groups?