MONASH University

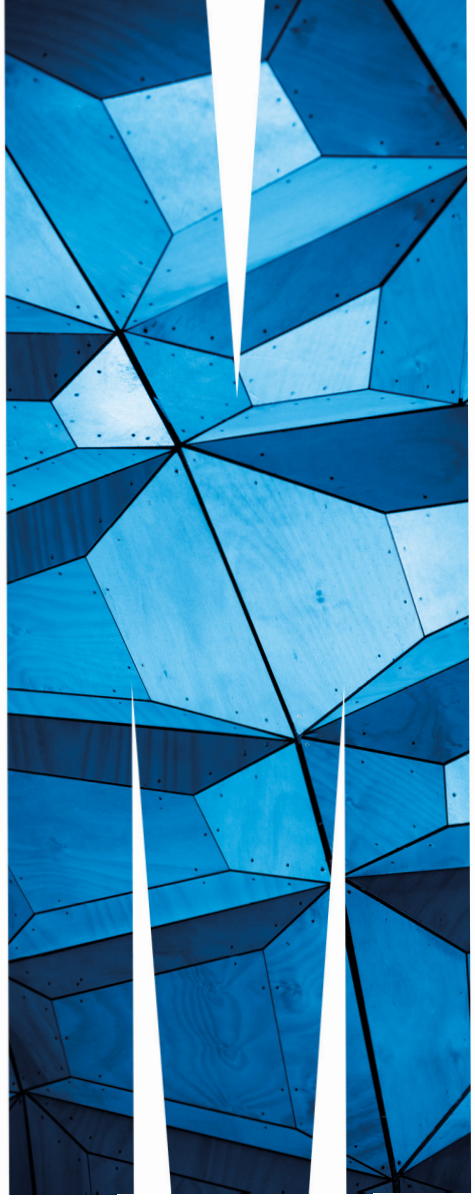
Rate of random low-density parity-check codes

Jane Gao (Monash University)

17-October 2018

Joint work with Amin Coja-Oghlan

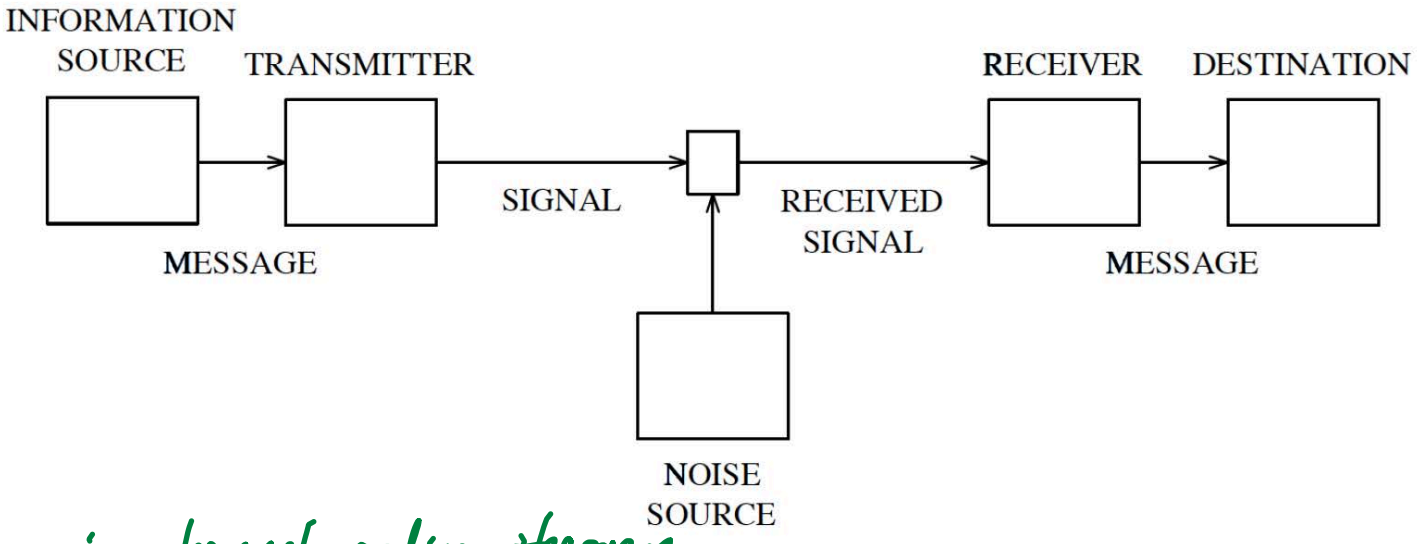
GROUP OF EIGHT AUSTRALIA



Information theory.

$\{0,1\}^m \xrightarrow{\text{Enc}} x \in \{0,1\}^n$

$y \in \{0,1\}^n \xrightarrow{\text{Dec}} \{0,1\}^m$



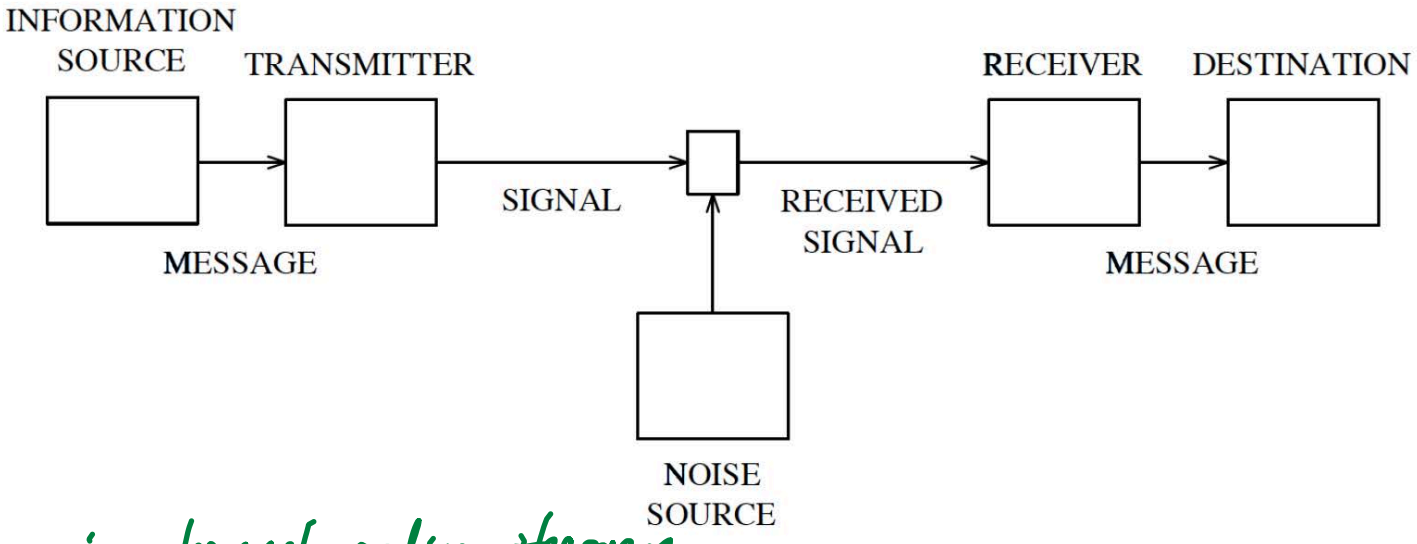
Shannon's channel coding theorem

$\Rightarrow$ random codes achieve the theoretical best performance.

Information theory.

$\{0,1\}^m \xrightarrow{\text{Enc}} x \in \{0,1\}^n$

$y \in \{0,1\}^n \xrightarrow{\text{Dec}} \{0,1\}^m$



Shannon's channel coding theorem

$\Rightarrow$ random codes achieve the theoretical best performance.

$\Rightarrow$ however, not practical !!

Linear codes

* linear subspace of $\mathbb{F}_q^n$.
* (G, H) : $\mathrm{row}(G) = \ker(H)$

generator matrix — parity check matrix

- G: $d \in \mathbb{F}_q^m \mapsto dG \in \mathbb{F}_q^n$
- If $x \in \mathbb{F}_q^n$ is a codeword then $Hx = 0$.

Random LDPC codes

- d and k are two independent random variables

  $\mathbb{E}(d^{2+r}) < \infty$, $\mathbb{E}(k^{2+r}) < \infty$, $(r > 0)$; $\mathrm{supp}(d) \subseteq \mathbb{N}_{\geq 1}$, $\mathrm{supp}(k) \subseteq \mathbb{N}_{\geq 3}$.

- $d_1, \cdots, d_n$, i.i.d. copies of d

  $k_1, \cdots, k_m$, i.i.d. copies of k.

  $\mathbb{E}(d) \cdot n \approx \mathbb{E}(k) \cdot m$, $\gcd(\mathrm{supp}(k)) \mid n$.

  $E: \left\{ \sum_{i=1}^{n} d_i = \sum_{j=1}^{m} k_j \right\}$

- A: uniformly random matrix
  - * row j has k_j non-zero entries;
  - * column i has d_i non-zero entries
  - * each non-zero entry is a random $x \in \mathbb{F}_q \setminus \{0\}$.

- rate of ldpc codes $= \frac{1}{n} \mathrm{nul}(A)$

Rank of A.

- $D(x) = \sum_{i \geq 0} x^i \, P(d = i)$, $K(x) = \sum_{j \geq 0} x^j \, P(k = j)$.
- $\Phi(\alpha) = D\left(1 - \frac{K'(\alpha)}{k}\right) + \frac{d}{k}\left(K(\alpha) + (1-\alpha)K'(\alpha) - 1\right)$; $d = \mathbb{E}(d)$, $k = \mathbb{E}(k)$.

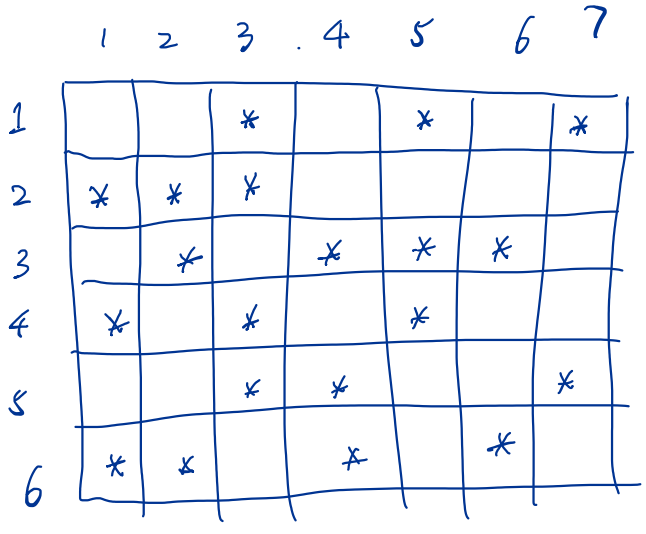
Theorem [Coja-Oghlan, G.]

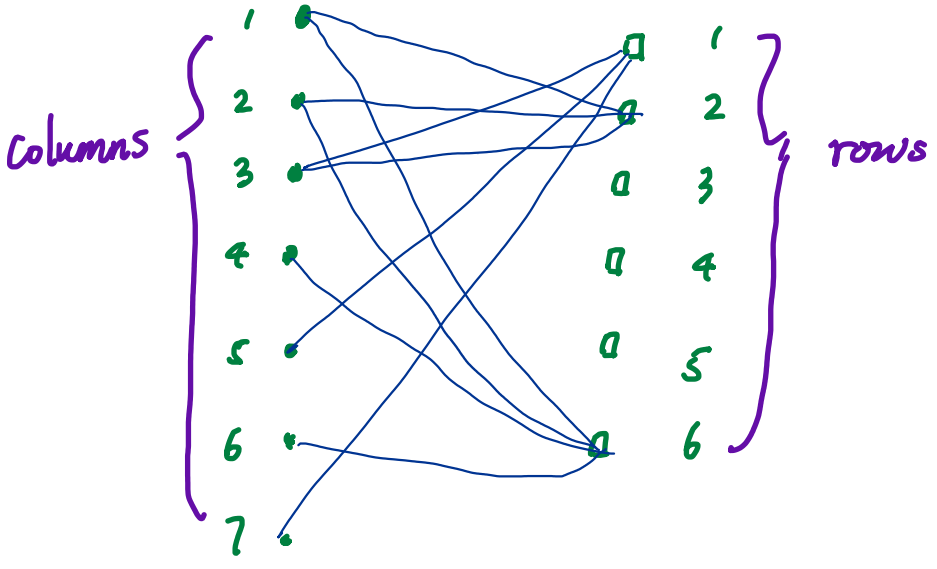
$$\lim_{n \to \infty} \frac{rk(A)}{n} = 1 - \sup_{\alpha \in [0,1]} \Phi(\alpha)$$

← conjectured by Lelarge.

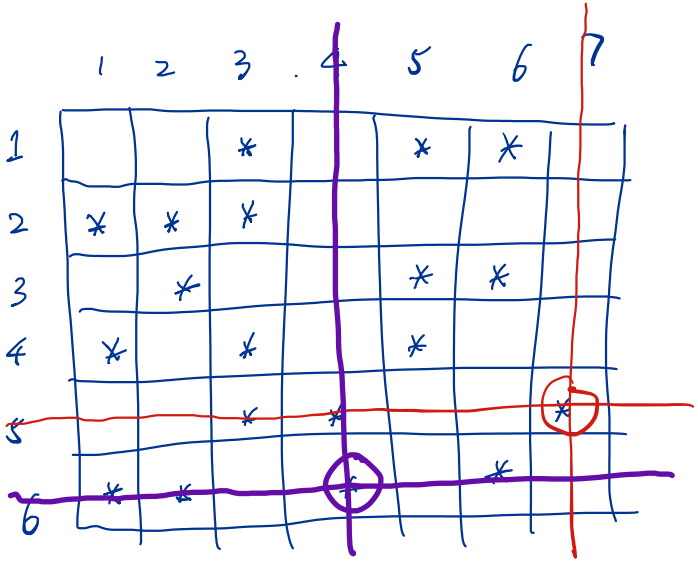
Upper bound by Lelarge ⇐ size of maximum matching in the factor graph of A.

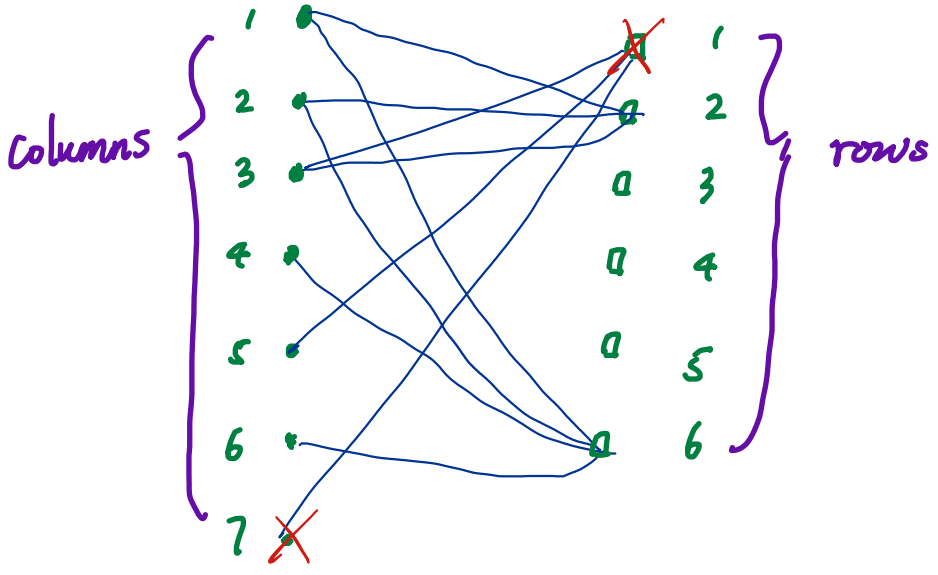
Factor graphs





2-core





Size of 2-core

$$\Phi(\alpha) = D\left(1 - \frac{K'(\alpha)}{k}\right) + \frac{d}{k}\left(K(\alpha) + (1-\alpha)K'(\alpha) - 1\right):$$

$$\Rightarrow$$

$$\Phi'(\alpha) = \frac{d}{k} K''(\alpha)\varphi(\alpha): \quad \varphi(\alpha) = 1 - \alpha - \frac{1}{d} D'\left(1 - \frac{K'(\alpha)}{k}\right).$$

Let $\rho = \max\{x \in [0,1]: \varphi(x) = 0\}$.

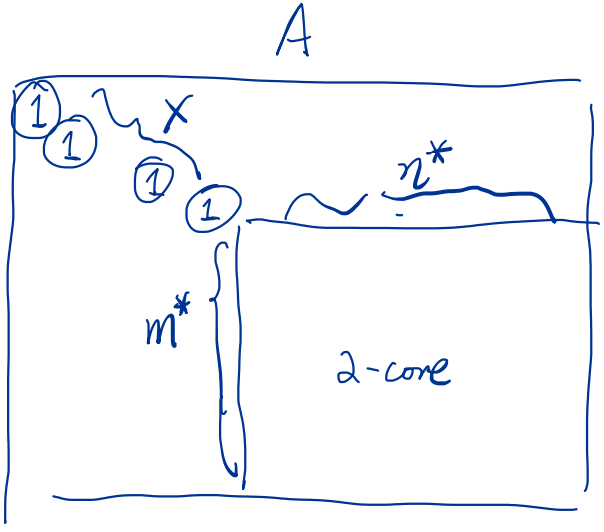
Theorem [Coja-Oghlan, G.] Assume $\varphi'(\rho) < 0$.

$$\frac{n^*}{n} \to 1 - D\left(1 - \frac{K'(\rho)}{k}\right) - \frac{K'(\rho)}{k} D'\left(1 - \frac{K'(\rho)}{k}\right)$$

$$\frac{m^*}{n} \to \frac{d}{k} K(\rho)$$

Remark: If $\rho = 0$, then $\frac{n^*}{n} \to 0$, $\frac{m^*}{n} \to 0$.

From rk(2-core(A)) to rk(A)



$$\operatorname{rank}(A) \le \min\{m^*,\ n^*\} + X$$

$$\le \min\{m^*,\ n^*\} + (m - m^*)$$

$$\Rightarrow$$

$$\lim_{n\to\infty} \frac{rk(A)}{n} \le 1 - \max\{\Phi(0),\ \Phi(\rho)\}. \qquad (*)$$

Theorem [Coja-Oghlan, G.] (*) holds with = if

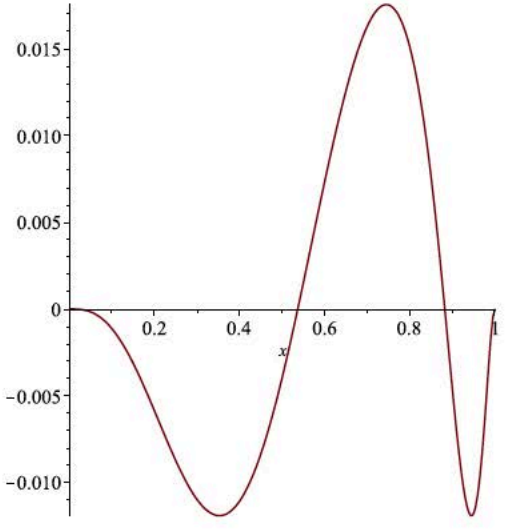
(i) $d = d$ or $d \sim Po_{\ge \ell}(\lambda)$, $\ell \ge 1$. and

(ii) $k = k$ or $k \sim Po_{\ge \ell}(\lambda)$, $\ell \ge 3$

Previously known: $d \sim Po(\lambda)$, and $k = k$.

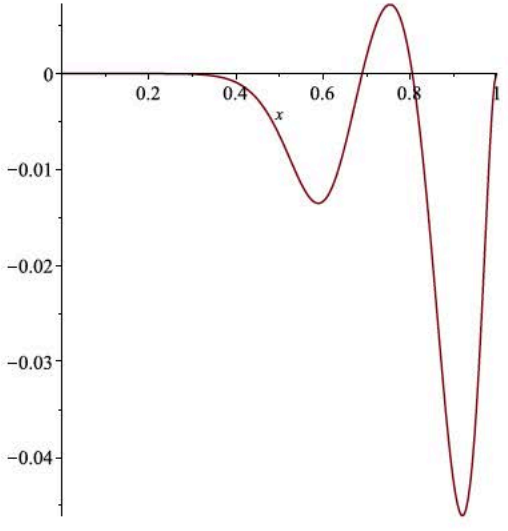
When does (*) hold with < ?

$\Phi(\alpha)$



$D(x) = k(x) = \frac{4}{5}x^3 + \frac{1}{5}x^{15}$

$\tilde{\Phi}(\alpha)$



$D(x) = \frac{190}{197}x^3 + \frac{7}{197}x^{200}$

$k(x) = x^{10}.$

From Statistical physics

Replica Symmetry $\Rightarrow$ $\lim_{n\to\infty} \frac{1}{n} \mathrm{nul}(A) = \sup_{\pi \in \mathcal{P}^2(\mathbb{F}_2)} \mathcal{B}(\pi)$.

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

$$P(\hat{k} = j) = \frac{j\,P(k=j)}{k}.$$

Literature on $\mathrm{rk}(A)$

- Dubois & Mandler (2002) $k=3$, $d \sim Po(\lambda)$, $q=2$
- Pittel & Sorkin (2016), Dietzfelbinger et al. (2010) $k=k\geq 3$, $d \sim Po(\lambda)$, $q=2$

  } $\lambda < \lambda^*$: satisfiability threshold

- Falke & Goerdt (2012) $k=k\geq 3$, $d \sim Po(\lambda)$, $q=3,4$.

- Ayre, Coja-Oghlan, G., Müller (2017+) $k=k\geq 3$, $d \sim Po(\lambda)$, $q=2$
  Cooper, Frieze, Pegden (2018+) $k=k\geq 3$, $d \sim Po(\lambda)$, q general

  } all λ.

- Lelarge (2013) general k, d, q $\Rightarrow$ upper bound on $\mathrm{rk}(A)$.

Literature on r-core

* Bollobás (1983)

  ...

* Pittel, Spencer & Wormald (1996)

  ... (2004⁻ - 2018⁺)
  - random graphs
  - random hypergraphs
  - random graphs / hypergraphs with specified degrees

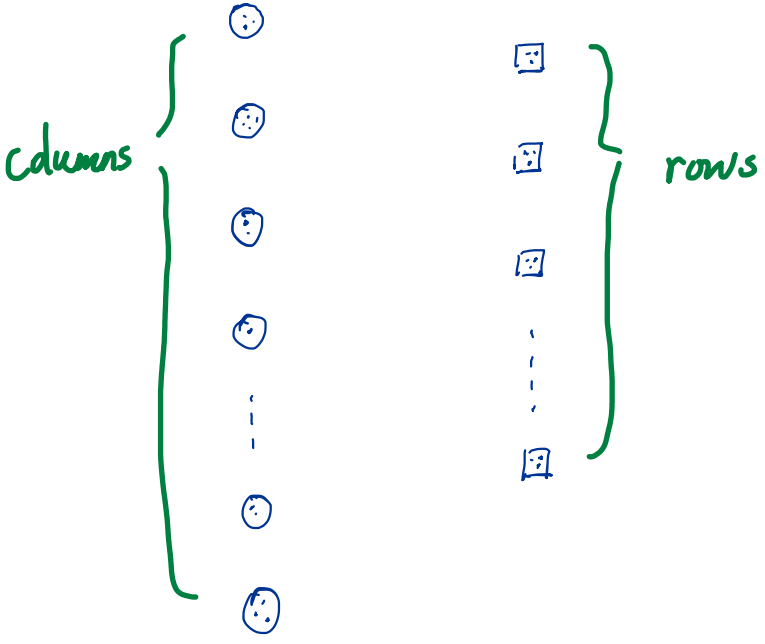
  (*) Cooper (2004)

  random hypergraph, $k = k$, given degrees, r-core, $(k, r) \neq (2, 2)$

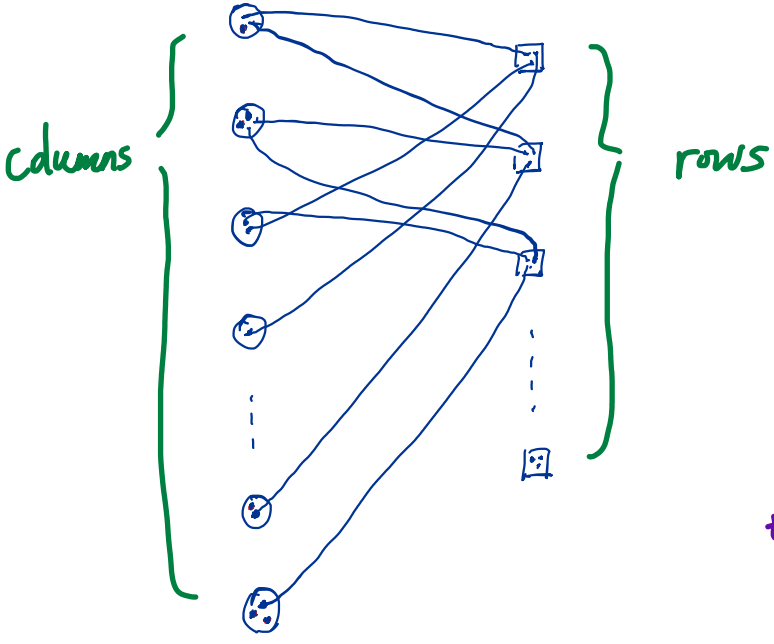
  (*) Molloy (2005)

  random hypergraph, $k = k$, r-core $(k, r) \neq (2, 2)$

Configuration model for A



Configuration model for A

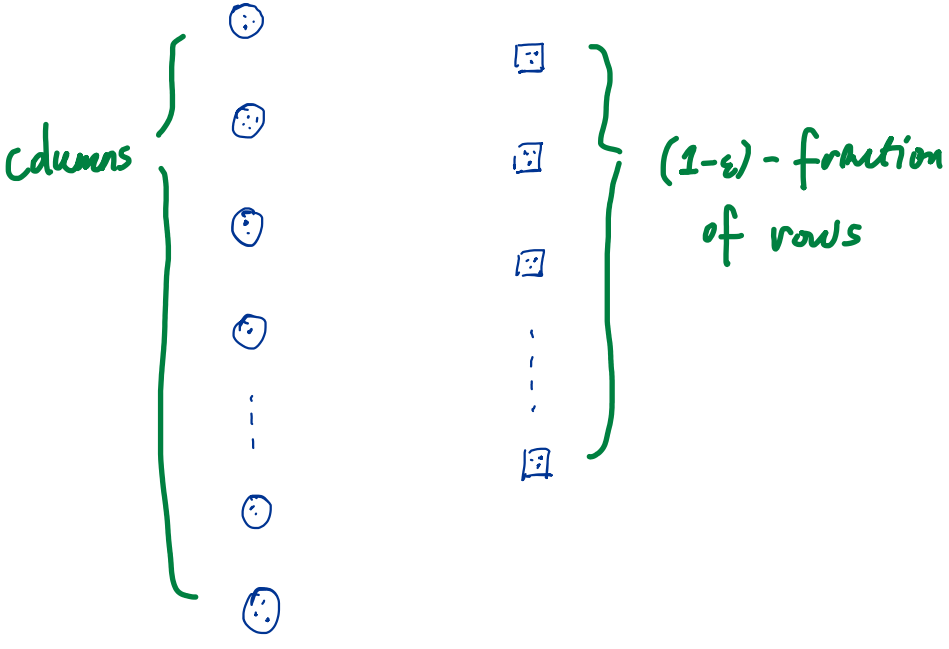


Lemma. If $\mathbb{E}(d^{2+\varepsilon}) < \infty$,
$\mathbb{E}(k^{2+\varepsilon}) < \infty$,

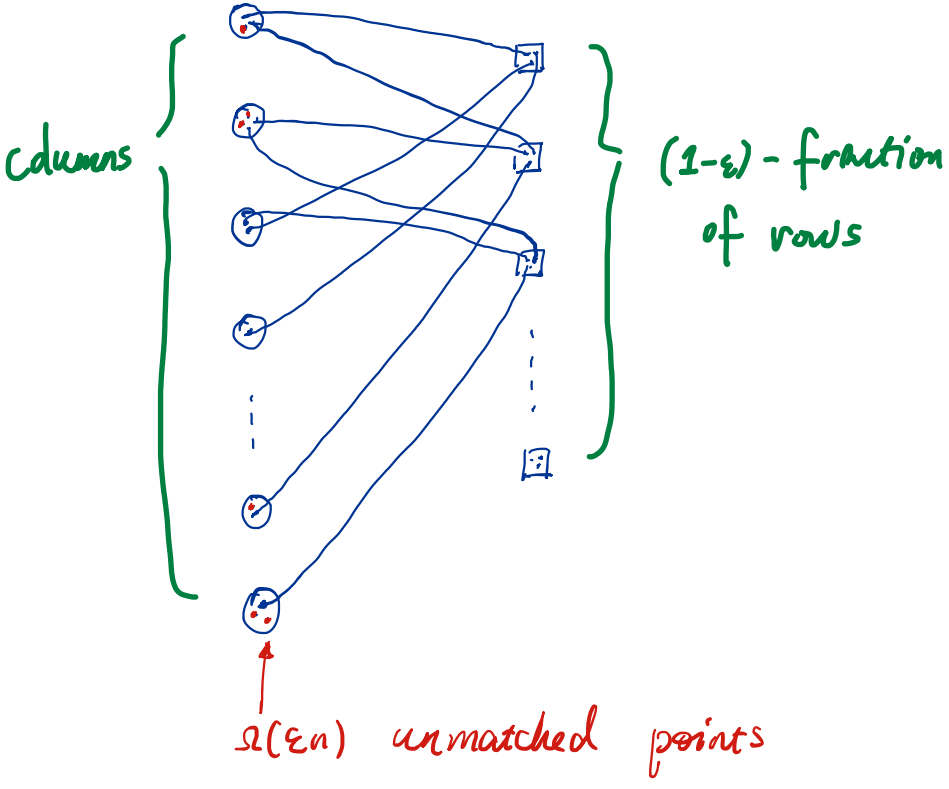
then

$P(\text{no double edges}) = \Omega(1)$.

Relaxing A to A_ε



Relaxing A to A_ε



$\mathrm{rk}(A_\varepsilon)$ approximates $\mathrm{rk}(A)$

Lemma. With probability $\geq 1-\varepsilon$,

$$|\mathrm{rk}(A_\varepsilon) - \mathrm{rk}(A)| = O(\varepsilon n)$$

Proof. Couple A_ε & A. so that they differ by $O(\varepsilon n)$ rows with probability $\geq 1-\varepsilon$. □

Concentration

Lemma. A.a.s. $\left| \mathrm{rk}(A_\varepsilon) - \mathbb{E}\,\mathrm{rk}(A_\varepsilon) \right| = O(\sqrt{n \ln n})$.

Proof. Azuma's inequality. □

$\mathbb{E}\, rk(A_\varepsilon)$

- $rk(A_\varepsilon) = n - nul(A_\varepsilon)$.

- $\mathbb{E}\, nul(A_{n,\varepsilon}) = \mathbb{E}\, nul(A_{N,\varepsilon}) + \sum_{j=N}^{n-1} \left(\mathbb{E}\, nul(A_{j+1,\varepsilon}) - \mathbb{E}\, nul(A_{j,\varepsilon}) \right)$

$$\Rightarrow \limsup_{n\to\infty} \frac{\mathbb{E}\, nul(A_{n,\varepsilon})}{n} \le \limsup_{n\to\infty} \mathbb{E}\left\{ nul(A_{n+1,\varepsilon}) - nul(A_{n,\varepsilon}) \right\}.$$

Lemma. $\mathbb{E}\left\{ nul(A_{n+1,\varepsilon}) - nul(A_{n,\varepsilon}) \right\} \le \sup_{\alpha\in[0,1]} \Phi(\alpha) + O(\varepsilon)$.

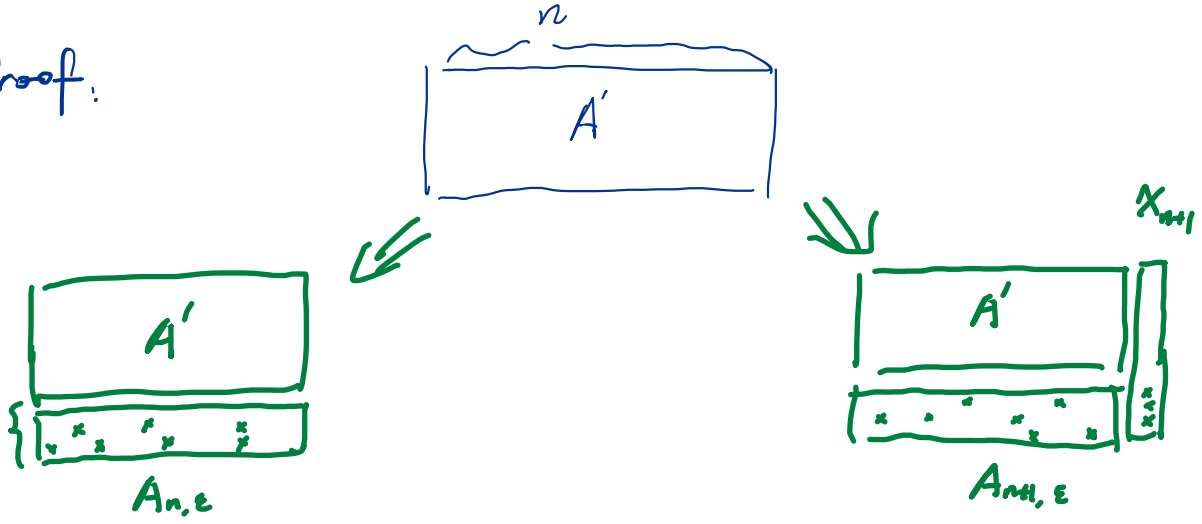
$$\Rightarrow \lim_{\varepsilon\to 0} \limsup_{n\to\infty} \frac{\mathbb{E}\, nul(A_{n,\varepsilon})}{n} \le \sup_{\alpha\in[0,1]} \Phi(\alpha)$$

$$\Rightarrow \liminf_{n\to\infty} \frac{rk(A)}{n} \ge 1 - \sup_{\alpha\in[0,1]} \Phi(\alpha).$$

Aizenman - Sims - Starr Scheme

Lemma. $\mathbb{E}\{\mathrm{nul}(A_{n+1,\varepsilon}) - \mathrm{nul}(A_{n,\varepsilon})\} \le \sup_{\alpha\in[0,1]} \Phi(\alpha) + O(\varepsilon)$.

Proof:



$$Z(A) = |\{x : Ax = 0\}|$$

$$\mathbb{E}\left(\mathrm{nul}(A_{n+1,\varepsilon}) - \mathrm{nul}(A_{n,\varepsilon})\right) = \mathbb{E}\left(\log_q Z(A_{n+1,\varepsilon}) - \log_q Z(A_{n,\varepsilon})\right)$$

$$= \mathbb{E}\left(\log \frac{Z(A_{n+1,\varepsilon})}{Z(A')}\right) - \mathbb{E}\left(\log \frac{Z(A_{n,\varepsilon})}{Z(A')}\right)$$

From Statistical physics

Replica Symmetry $\Rightarrow$ $\lim_{n\to\infty} \frac{1}{n} \mathrm{nul}(A) = \sup_{\pi \in \mathcal{P}^2(\mathbb{F}_2)} \mathcal{B}(\pi)$.

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

$$P(\hat{k} = j) = \frac{j\,P(k=j)}{k}.$$

For random linear equations $Ax = 0$

- Marginal:

$$\mu(\sigma_{x_i}) = \alpha \delta_{\delta_0} + (1-\alpha)\, \delta_{\frac{1}{q} \sum_{i \in \mathbb{F}_q} \delta_i}$$

for some $\alpha \in [0, 1]$.

For random linear equations $Ax = 0$

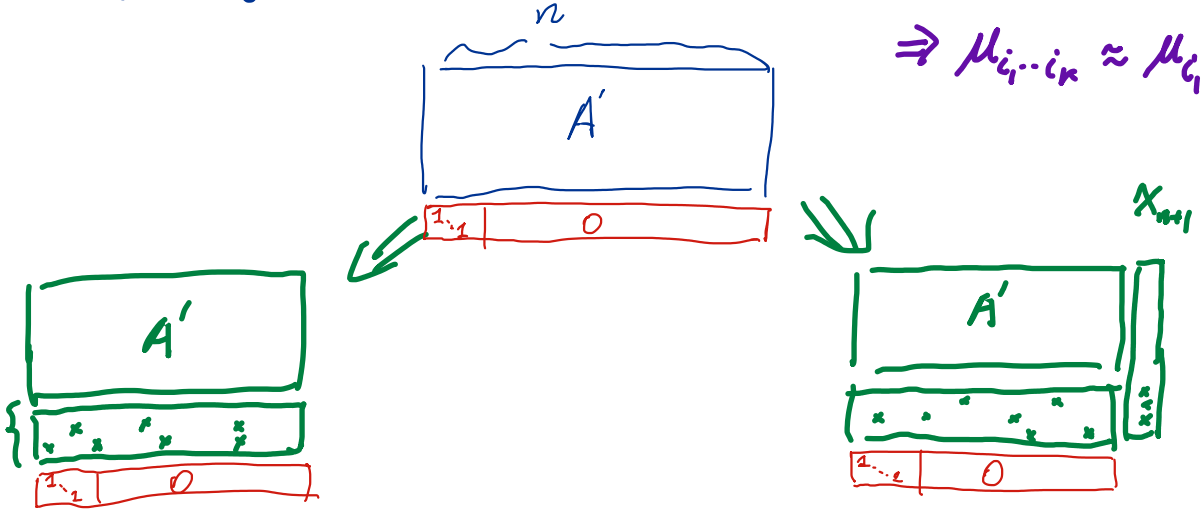
- Marginal:

$$\mu(\sigma_{x_i}) = \alpha \delta_{\delta_0} + (1-\alpha)\,\delta_{\frac{1}{q}\sum_{i \in \mathbb{F}_q} \delta_i}$$

for some $\alpha \in [0, 1]$.

- Replica Symmetry:

$$\Rightarrow \mu_{i_1 \cdots i_k} \approx \mu_{i_1} \otimes \cdots \otimes \mu_{i_k}$$



Thank you!