Lecture III:

Frobenius numbers and circulant graphs

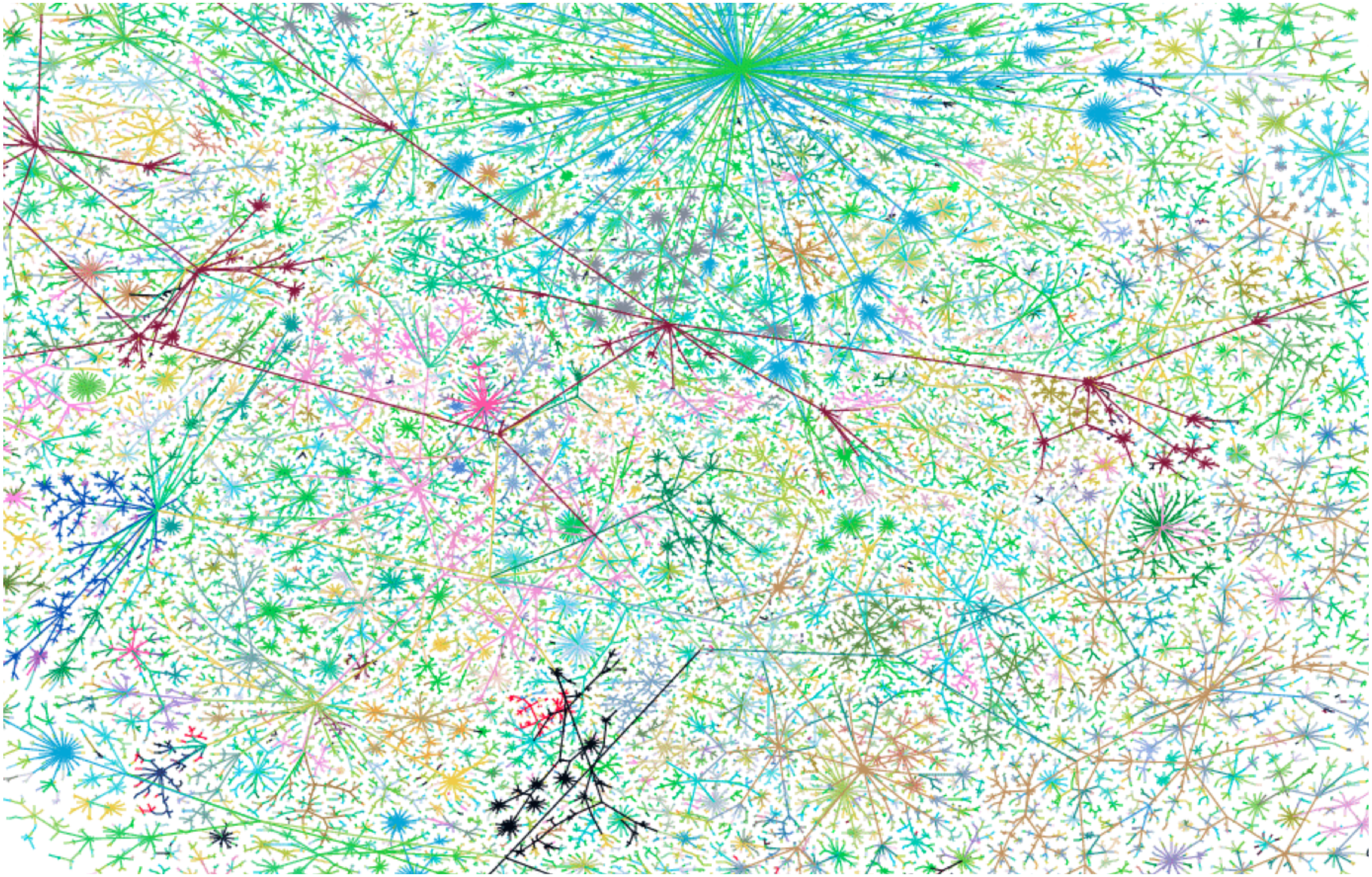
Applications of measure rigidity: from number theory to statistical mechanics
Simons Lectures, Stony Brook
October 2013

Jens Marklof

University of Bristol
http://www.maths.bristol.ac.uk

supported by Royal Society and ERC

Random graphs in the real world



The internet; from Newman, SIAM Review 2003

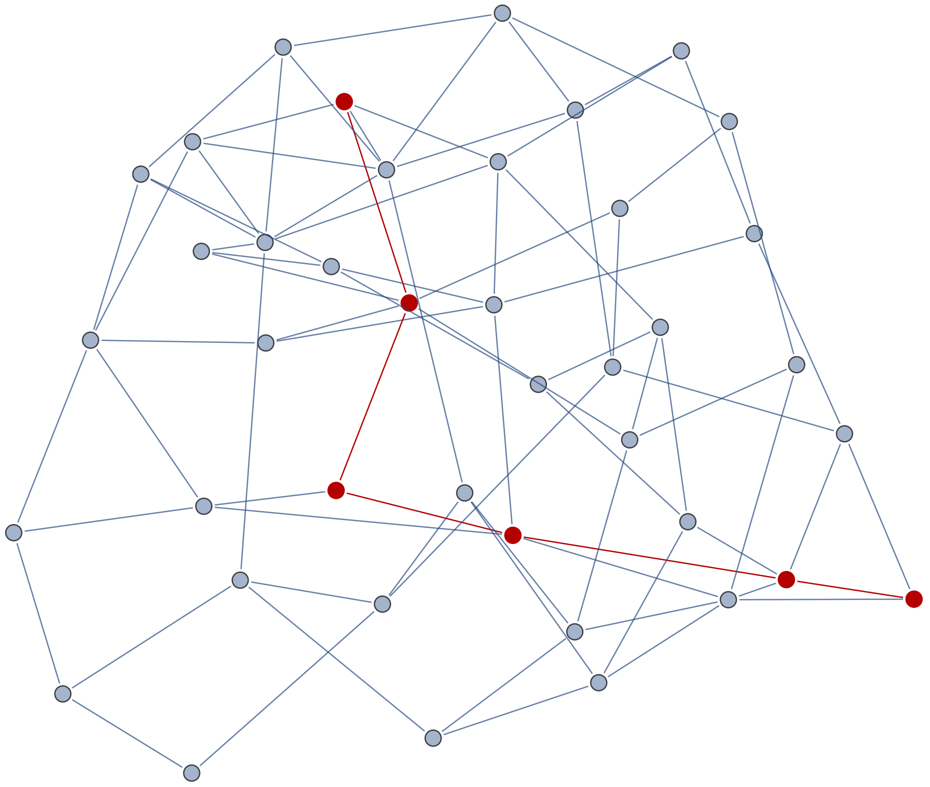
The diameter of a network

$d(i,j)$ — the distance between vertex i and j

$\mathrm{diam} = \mathrm{max}_{i,j}\, d(i,j)$ — the maximal distance or “diameter”

```
In[13]:= HighlightGraph[#, FindDiameterPath[#]] &[
          RandomGraph[WattsStrogatzGraphDistribution[41, 0.5]]]
```

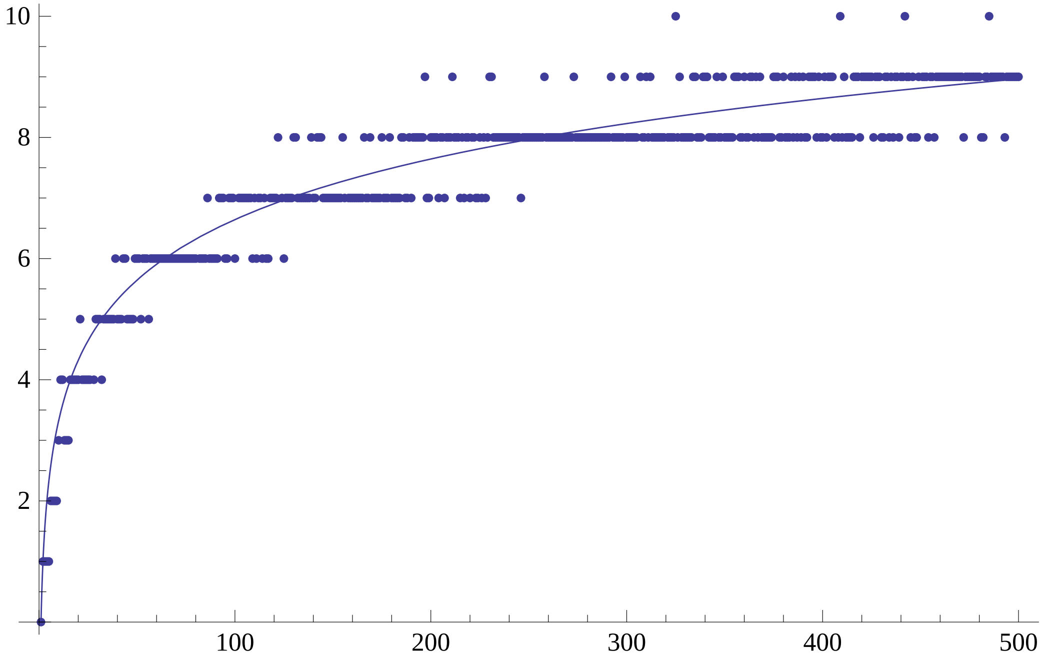
Out[13]=



The small-world phenomenon

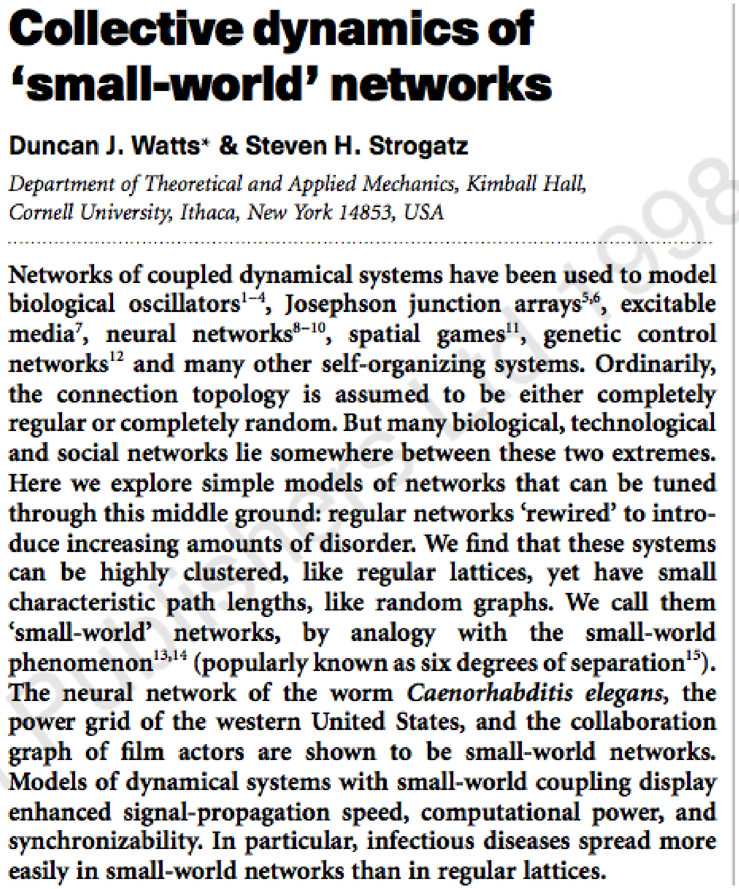
```
In[14]:= data :=
          Table[GraphDiameter[RandomGraph[WattsStrogatzGraphDistribution[n, 0.5]]], {n, 1, 500}]

In[15]:=
         Show[ListPlot[data], Plot[Log[2, x], {x, 1, 500}], Plot[Log[2, x], {x, 1, 10}]]
```

Out[15]=



The diameter grows *logarithmically* in the number of vertices: diam $\sim c \log n$ (in the above example $c = 1/\log 2$)

Small-world networks: the Watts-Strogatz model



Collective dynamics of 'small-world' networks

Duncan J. Watts* & Steven H. Strogatz

Department of Theoretical and Applied Mechanics, Kimball Hall, Cornell University, Ithaca, New York 14853, USA

Networks of coupled dynamical systems have been used to model biological oscillators[1–4], Josephson junction arrays[5,6], excitable media[7], neural networks[8–10], spatial games[11], genetic control networks[12] and many other self-organizing systems. Ordinarily, the connection topology is assumed to be either completely regular or completely random. But many biological, technological and social networks lie somewhere between these two extremes. Here we explore simple models of networks that can be tuned through this middle ground: regular networks 'rewired' to introduce increasing amounts of disorder. We find that these systems can be highly clustered, like regular lattices, yet have small characteristic path lengths, like random graphs. We call them 'small-world' networks, by analogy with the small-world phenomenon[13,14] (popularly known as six degrees of separation[15]). The neural network of the worm *Caenorhabditis elegans*, the power grid of the western United States, and the collaboration graph of film actors are shown to be small-world networks. Models of dynamical systems with small-world coupling display enhanced signal-propagation speed, computational power, and synchronizability. In particular, infectious diseases spread more easily in small-world networks than in regular lattices.

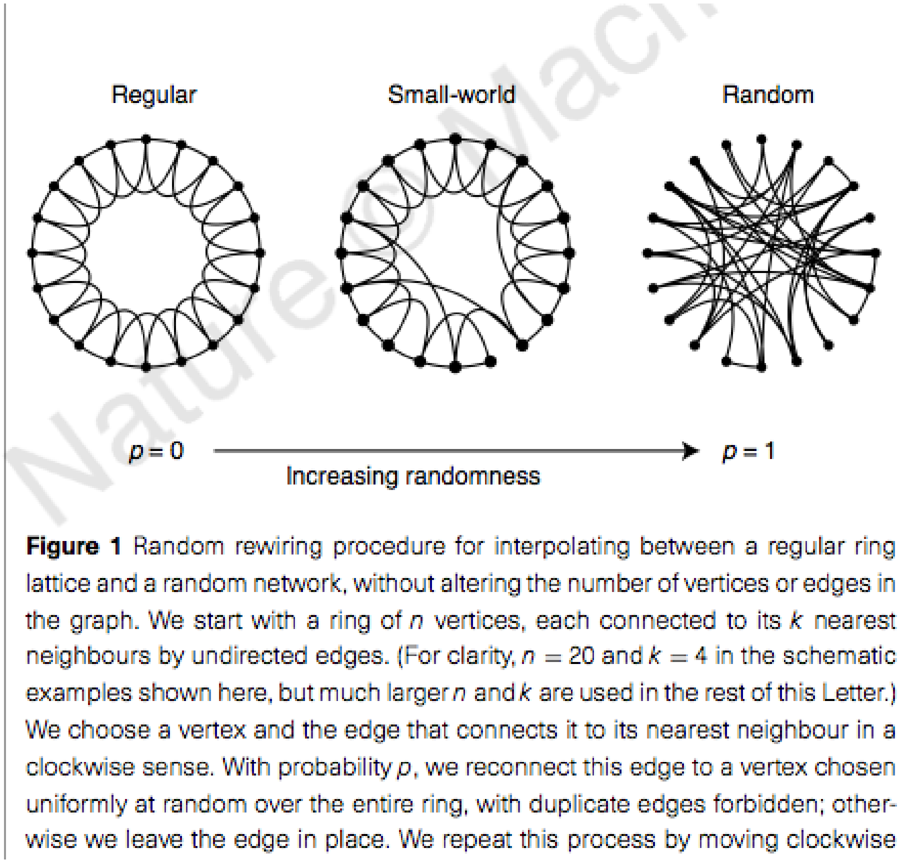


Figure 1 Random rewiring procedure for interpolating between a regular ring lattice and a random network, without altering the number of vertices or edges in the graph. We start with a ring of n vertices, each connected to its k nearest neighbours by undirected edges. (For clarity, $n = 20$ and $k = 4$ in the schematic examples shown here, but much larger n and k are used in the rest of this Letter.) We choose a vertex and the edge that connects it to its nearest neighbour in a clockwise sense. With probability p, we reconnect this edge to a vertex chosen uniformly at random over the entire ring, with duplicate edges forbidden; otherwise we leave the edge in place. We repeat this process by moving clockwise

from: Watts & Strogatz, Nature 1998

Diameters of random graph models: rigorous results

- Bollobas (TAMS 1981), random graphs à la Erdös-Rényi

- Bollobas & Fernandes de la Vega (Combinatorica 1982), k-regular random graphs

- Bollobas & Chung (SIAM Rev 1988), n-cycle plus random matching: almost surely $\log_2 n - 10 \leq \text{diam} \leq \log_2 n + \log_2 \log n + 10$

- Chung & Lu (Adv Appl Math 2001), sparse random graphs

- Bollobas & Riordan (Combinatorica 2004), scale-free random graphs (Barabasi-Albert small-world model): $(1-\epsilon) \log n / \log \log n \leq \text{diam} \leq (1+\epsilon) \log n / \log \log n$

- Fernholz & Ramachandran (Rand Struct's Algorith's 2007), sparse random graphs

- Nachmias & Peres (Ann Prob 2008), critical Erdös-Rényi graphs, $\text{diam} \approx n^{1/3}$

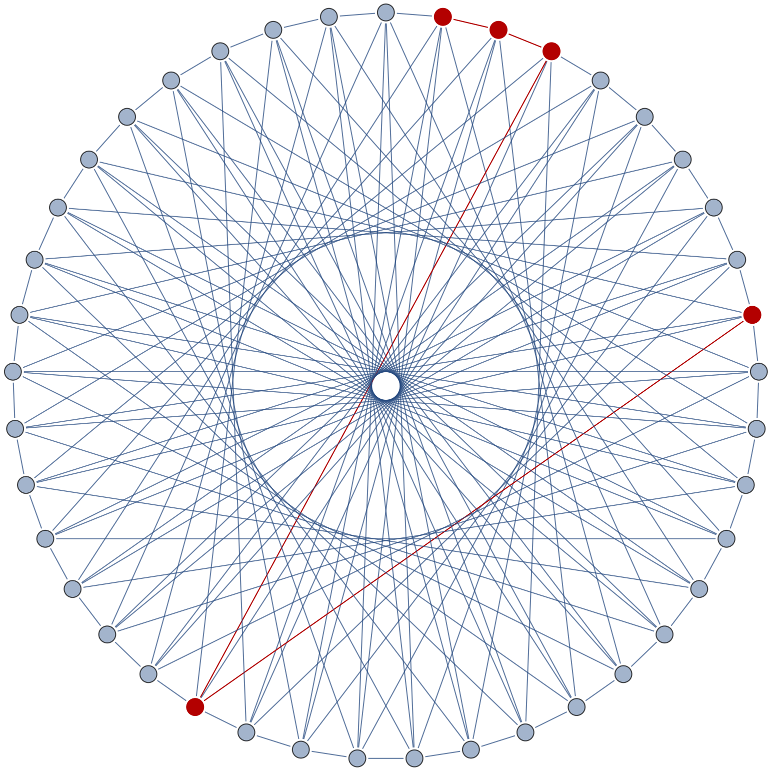
- Riordan & Wormland (Comb Prob Comp 2010), sparse random graphs

Circulant graphs

1. Fix integers $0 < a_1 < \ldots < a_k \leq n/2$ with $\gcd(a_1, \ldots, a_k, n) = 1$;
2. Connect vertex i and j, if $|i - j| \equiv a_h \bmod n$ for some a_h; assign length ℓ_h to this edge.

The resulting graph $C_n(\boldsymbol{\ell}, \boldsymbol{a})$ is called a “circulant graph” (its adjacency matrix is circulant), sometimes also “multiloop network”. It is of course the undirected Cayley graph of the cyclic group of order n w.r.t. the generating set $\{\pm a_1, \ldots, \pm a_k\}$.

```
HighlightGraph[#, FindDiameterPath[#]] &[CirculantGraph[41, {1, 15, 20}]]
```



Random circulant graphs

Theorem A (JM & AS arXiv 2011). Let $k \geq 2$, $\mathcal{D} \subset \mathbb{R}^{k+1}$ bounded, non-empty and boundary of Lebesgue measure zero. Pick $(\boldsymbol{a}, n)$ at random in $T\mathcal{D}$. Then

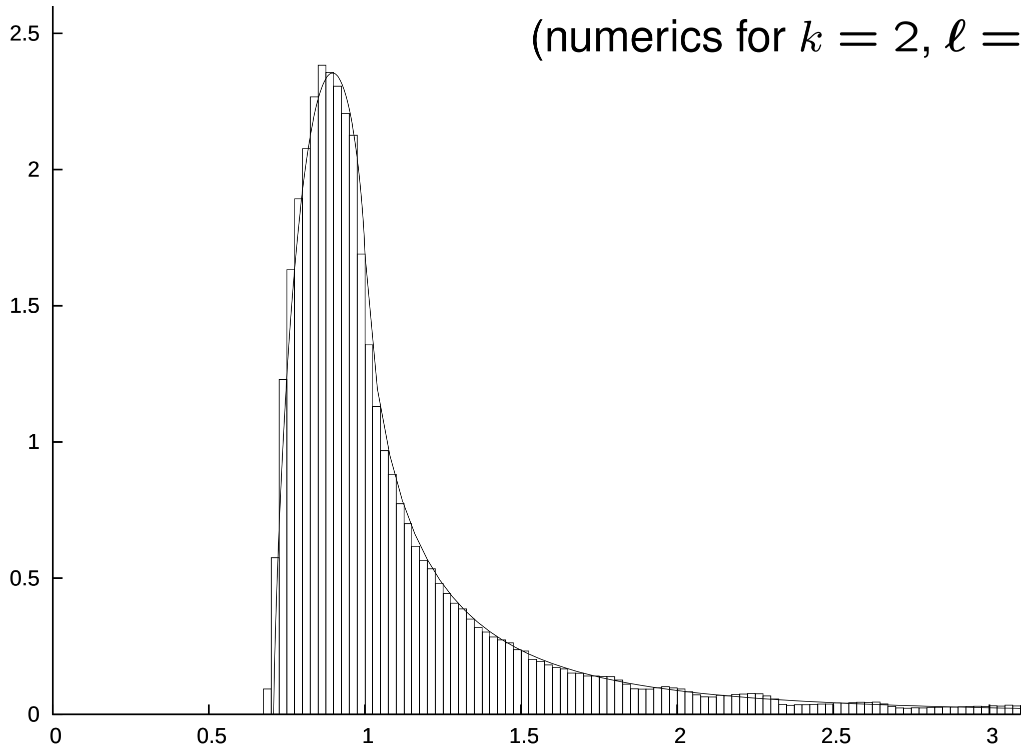
$$\frac{\mathsf{diam}\, C_n(\boldsymbol{\ell}, \boldsymbol{a})}{(n\ell_1 \cdots \ell_k)^{1/k}} \xrightarrow{\mathsf{d}} \rho(\mathfrak{P}, L) \qquad \text{as } T \to \infty,$$

where $\rho(\mathfrak{P}, L)$ is ... the covering radius of a random lattice L in $\mathbb{R}^k$ with respect to the polytope

$$\mathfrak{P} = \left\{ x \in \mathbb{R}^k : |x_1| + \ldots + |x_k| \leq 1 \right\}.$$

($\mathfrak{P}$ is a square for $k = 2$ and an octahedron for $k = 3$.)

…a random variable distributed according to the probability density



(numerics for $k = 2$, $\boldsymbol{\ell} = (1,1)$, $n = 1000$)

For $k = 2$:

$$\tilde{p}_2(R) = \begin{cases} 0 & (0 \le R \le \frac{1}{\sqrt{2}}) \\ \frac{24}{\pi^2}\left(\frac{2R^2-1}{R}\log\left(\frac{2R^2}{2R^2-1}\right) + \frac{1-R^2}{R}\log\left(\frac{R^2}{|1-R^2|}\right)\right) & (R > \frac{1}{\sqrt{2}}). \end{cases}$$

For general $k \ge 2$:

$$\tilde{p}_k(R) = 0 \ (R < \tfrac{1}{2}(k!)^{1/k}), \qquad \tilde{p}_k(R) \sim \frac{k}{2\zeta(k)} R^{-(k+1)} \ (R \to \infty)$$

Random circulant graphs

Theorem A (JM & AS arXiv 2011). Let $k \geq 2$, $\mathcal{D} \subset \mathbb{R}^{k+1}$ bounded, non-empty and boundary of Lebesgue measure zero. Pick $(\boldsymbol{a}, n)$ at random in $T\mathcal{D}$. Then

$$\frac{\mathrm{diam}\, C_n(\boldsymbol{\ell}, \boldsymbol{a})}{(n\ell_1 \cdots \ell_k)^{1/k}} \xrightarrow{\mathrm{d}} \rho(\mathfrak{P}, L) \qquad \text{as } T \to \infty,$$

where $\rho(\mathfrak{P}, L)$ is ... the covering radius of a random lattice L in $\mathbb{R}^k$ with respect to the polytope

$$\mathfrak{P} = \left\{ x \in \mathbb{R}^k : |x_1| + \ldots + |x_k| \leq 1 \right\}.$$

($\mathfrak{P}$ is a square for $k = 2$ and an octahedron for $k = 3$.)

Random circulant graphs

Theorem A (JM & Strömbergsson, Combinatorica IP). Let $k \geq 2$, $\mathcal{D} \subset \mathbb{R}^{k+1}$ bounded, non-empty and boundary of Lebesgue measure zero. Pick $(\boldsymbol{a}, n)$ at random in $T\mathcal{D}$. Then

$$\frac{\operatorname{diam} C_n(\boldsymbol{\ell}, \boldsymbol{a})}{(n\ell_1 \cdots \ell_k)^{1/k}} \xrightarrow{\mathrm{d}} \rho(\mathfrak{P}, L) \qquad \text{as } T \to \infty,$$

where $\rho(\mathfrak{P}, L)$ is ...the covering radius of a random lattice L in $\mathbb{R}^k$ with respect to the polytope

$$\mathfrak{P} = \left\{ \boldsymbol{x} \in \mathbb{R}^k : |x_1| + \ldots + |x_k| \leq 1 \right\}.$$

($\mathfrak{P}$ is a square for $k = 2$ and an octahedron for $k = 3$.)

What is . . . a covering radius?

For a given closed bounded convex set K of nonzero volume in $\mathbb{R}^k$ and a lattice $L \subset \mathbb{R}^k$, the covering radius of K with respect to L is

$$\rho(K, L) = \mathrm{inf}\left\{r > 0 : rK + L = \mathbb{R}^k\right\}.$$

What is . . . a random lattice?

- $L \subset \mathbb{R}^k$—euclidean lattice of covolume one

- recall $L = \mathbb{Z}^k M$ for some $M \in \mathsf{SL}(k, \mathbb{R})$, therefore the homogeneous space $X_k = \mathsf{SL}(k, \mathbb{Z}) \backslash \mathsf{SL}(k, \mathbb{R})$ parametrizes the space of lattices of covolume one

- Haar measure μ_0 of $\mathsf{SL}(k, \mathbb{R})$ yields a (unique) right-$\mathsf{SL}(k, \mathbb{R})$ invariant prob measure on X_k.

To note:

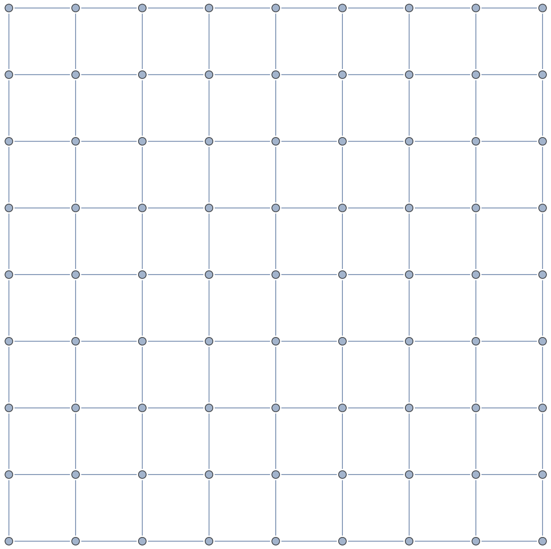
- The limit distribution is independent of the choice of $\mathcal{D}$ and $\boldsymbol{\ell}$.

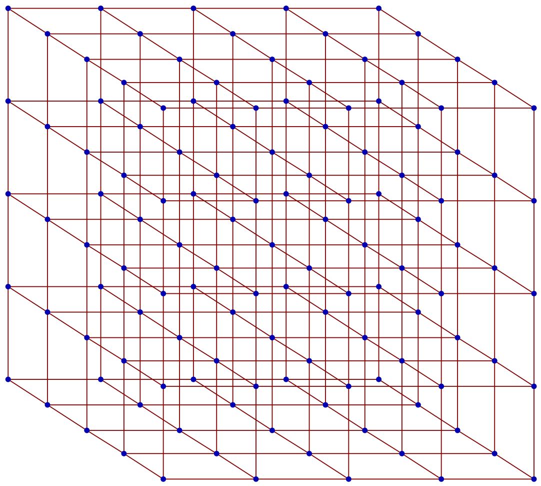
- The proof shows that the lengths $\boldsymbol{\ell}$ may even depend on $n^{-1}\boldsymbol{a}$; the limit distribution remains unchanged.

- Theorem A settles a conjecture of Amir & Gurel-Gurevich (Groups, Complexity, Cryptol 2010).

Key ideas in the proof of Theorem A:

1. Identify circulant graphs with lattice graphs on flat tori ("discrete tori")





2. Approximate discrete tori by continuous flat tori

3. Show that the tori coming from circulant graphs are uniformly distributed in the space of all tori of volume one (=the space of all lattices of covolume one)

Step 1: Discrete tori

- Define metric on $\mathbb{Z}^k$: $d(\boldsymbol{m},\boldsymbol{n}) = (\boldsymbol{n}-\boldsymbol{m})_+ \cdot \boldsymbol{\ell}$
  where $\boldsymbol{z}_+ := (|z_1|,\ldots,|z_k|)$; an "$\boldsymbol{\ell}$-weighted ℓ^1-metric"

- Denote by LG_k the corresponding lattice graph with vertex set $\mathbb{Z}^k$

- $\Lambda_n := \mathbb{Z}^k \times n\mathbb{Z}$, $\Lambda_n(\boldsymbol{a}) := \Lambda_n u(\boldsymbol{a})$, $u(\boldsymbol{a}) := \begin{pmatrix} 1_k & {}^t\boldsymbol{a} \\ \boldsymbol{0} & 1 \end{pmatrix} \in \mathrm{SL}(k+1,\mathbb{Z})$

- Note that $\Lambda_n(\boldsymbol{a})_0 := \Lambda_n(\boldsymbol{a}) \cap (\mathbb{R}^k \times \{0\})$ is a sublattice of index n in $\mathbb{Z}^k$
  ($\Lambda_n(\boldsymbol{a})_0$ is the kernel of the epimorphism $\mathbb{Z}^k \to \mathbb{Z}/n\mathbb{Z},\ \boldsymbol{m} \mapsto \boldsymbol{m}\cdot\boldsymbol{a} \bmod n$)

Lemma 1. The metric graphs $LG_k/\Lambda_n(\boldsymbol{a})_0$ and $C_n(\boldsymbol{\ell},\boldsymbol{a})$ are isomorphic.

Step 2: Discrete tori → continuous flat tori

- L any euclidean lattice in $\mathbb{R}^k$
- $\mathsf{diam}(\mathbb{R}^k/L)$:=maximal ℓ^1-distance of two points on the flat torus $\mathbb{R}^k/L$
- $D_n(\boldsymbol{\ell}) := \mathsf{diag}\big(\Pi^{-1/k}\ell_1, \ldots, \Pi^{-1/k}\ell_k\big)$, $\Pi := n\ell_1 \cdots \ell_k$.
- Then $L = \Lambda_n(\boldsymbol{a})_0 D_n(\boldsymbol{\ell}) \in X_k$, i.e., the torus $\mathbb{R}^k/L$ has volume one

Lemma 2. For $L = \Lambda_n(\boldsymbol{a})_0 D_n(\boldsymbol{\ell})$,

$$\Pi^{1/k}\,\mathsf{diam}\big(\mathbb{R}^k/L\big) - \frac{\boldsymbol{e}\cdot\boldsymbol{\ell}}{2} \leq \mathsf{diam}\big(LG_k/\Lambda_n(\boldsymbol{a})_0\big) \leq \Pi^{1/k}\,\mathsf{diam}\big(\mathbb{R}^k/L\big)$$

Lemma 3.

$$\mathsf{diam}(\mathbb{R}^k/L) = \rho(\mathfrak{P}, L)$$

Step 3: Equidistribution

Set $L_{n,\boldsymbol{a},\boldsymbol{\ell}} = \Lambda_n(\boldsymbol{a})_0 D_n(\boldsymbol{\ell})$.

Theorem B (JM, Invent Math 2010). Let $\mathcal{D} \subset \mathbb{R}^{k+1}$ be bounded with boundary of Lebesgue measure zero. Then for any bounded continuous function $f : X_k \to \mathbb{R}$,

$$\lim_{T\to\infty} \frac{1}{T^{k+1}} \sum_{(\boldsymbol{a},n)\in T\mathcal{D}} f\big(L_{n,\boldsymbol{a},\boldsymbol{\ell}}\big) = \frac{\mathrm{vol}(\mathcal{D})}{\zeta(k+1)} \int_{L\in X_k} f(L)\, d\mu_0(L).$$

That is, the random lattices $L_{n,\boldsymbol{a},\boldsymbol{\ell}}$ become equidistributed in the space of lattices X_k. This implies (modulo technicalities) that

$$\rho(\mathfrak{P}, L_{n,\boldsymbol{a},\boldsymbol{\ell}}) \xrightarrow{\mathrm{d}} \rho(\mathfrak{P}, L) \qquad \text{as } T \to \infty,$$

which proves Theorem A.

The proof of Theorem B exploits the dynamics of a certain homogeneous flow on the space of lattices. The rate of convergence has been recently estimated by H. Li (arXiv 2011) to be $O(T^{-\kappa})$ for $\mathcal{D}$ with smooth boundary.

An improvement of Theorem B

No need to average over n ...!

Theorem B' (Einsiedler, Mozes, Shah & Shapira, preprint 2013). Let $\mathcal{D} \subset \mathbb{R}^k$ be bounded with boundary of Lebesgue measure zero. Then for any bounded continuous function $f : X_k \to \mathbb{R}$,

$$\lim_{n\to\infty} \frac{1}{n^k} \sum_{\substack{\boldsymbol{a}\in n\mathcal{D} \\ \mathrm{gcd}(\boldsymbol{a},n)=1}} f\Big(L_{n,\boldsymbol{a},\boldsymbol{\ell}}\Big) = \frac{\mathrm{vol}(\mathcal{D})}{\zeta(k)} \int_{L\in X_k} f(L)\, d\mu_0(L).$$

Again, the random lattices $L_{n,\boldsymbol{a},\boldsymbol{\ell}}$ (now with n fixed) become equidistributed in the space of lattices X_k. Thus

$$\rho(\mathfrak{P}, L_{n,\boldsymbol{a},\boldsymbol{\ell}}) \xrightarrow{\mathrm{d}} \rho(\mathfrak{P}, L) \qquad \text{as } T \to \infty,$$

which proves a variant of Theorem A where n is no longer random.

The proof of Theorem B' uses ...of course... Ratner's measure classification theorem as one of the ingredients.

Frobenius numbers

- primitive lattice points:

$$\widehat{\mathbb{Z}}^d = \{\boldsymbol{a} = (a_1, \ldots, a_d) \in \mathbb{Z}^d : \mathrm{gcd}(a_1, \ldots, a_d) = 1\}$$

- given $\boldsymbol{a} \in \widehat{\mathbb{Z}}^d_{\geq 2}$, consider all positive linear combinations

$$N = \boldsymbol{m} \cdot \boldsymbol{a}, \qquad \boldsymbol{m} \in \mathbb{Z}^d_{\geq 0}$$

- Frobenius: What is the largest integer $F(\boldsymbol{a})$ that does *not* have a representation of this type?

$$F(\boldsymbol{a}) = \max \mathbb{Z} \setminus \{\boldsymbol{m} \cdot \boldsymbol{a} > 0 : \boldsymbol{m} \in \mathbb{Z}^d_{\geq 0}\}$$

- “Frobenius problem”. . . “coin exchange problem”. . . “postage stamp problem”

Frobenius numbers

- Sylvester ($d = 2$):

$$F(\boldsymbol{a}) = a_1 a_2 - a_1 - a_2$$

—no such explicit fromulas for $d \geq 3$

- Classic papers for $d \geq 3$: Brauer & Shockley 1962, Selmer 1977, Rødseth 1978, Selmer & Beyer 1978

- Numerical experiments & conjectures on the value distribution of $F(\boldsymbol{a})$ by V.I. Arnold (1999, 2007)

- Sharp lower bound: Aliev & Gruber 2007; upper bound: Fukshansky & Robins 2007

- J.L. Ramirez Alfonsin, The Diophantine Frobenius problem. Oxford University Press (2005)

Asymptotic distribution

Theorem C (JM, Invent Math 2010). Let $d \geq 3$, $\mathcal{D} \subset \mathbb{R}^d$ bounded, non-empty and boundary of Lebesgue measure zero. Pick $\boldsymbol{a} \in \widehat{\mathbb{Z}}^d_{\geq 2}$ at random in $T\mathcal{D}$. Then

$$\frac{F(\boldsymbol{a})}{(a_1 \cdots a_d)^{1/(d-1)}} \xrightarrow{\text{d}} \rho(\Delta, L) \qquad \text{as } T \to \infty,$$

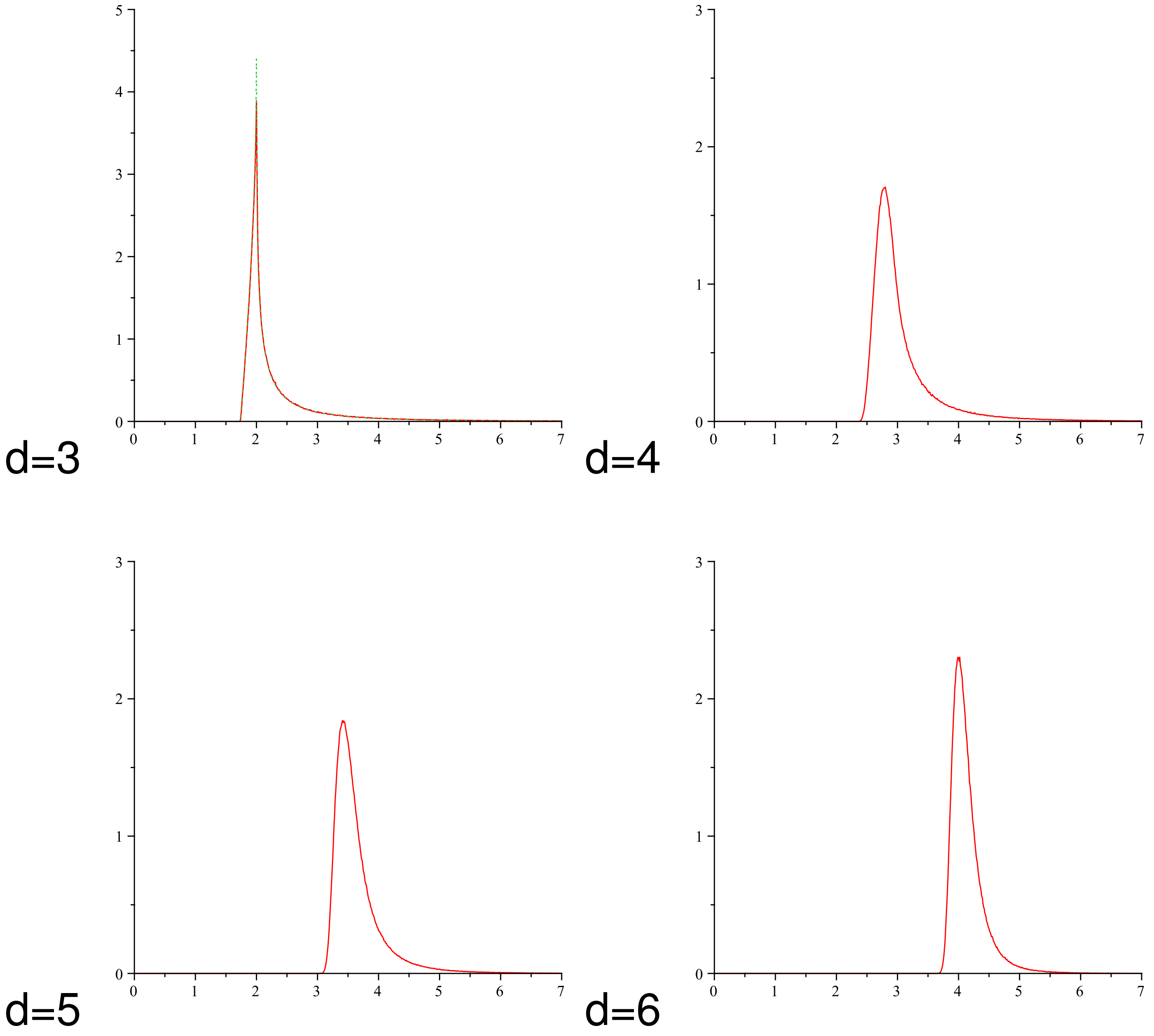
where $\rho(\Delta, L)$ is the covering radius of a random lattice L in $\mathbb{R}^k$ with respect to the simplex

$$\Delta = \left\{ \boldsymbol{x} \in \mathbb{R}^{d-1}_{\geq 0} : \boldsymbol{x} \cdot \boldsymbol{e} \leq 1 \right\}, \qquad \boldsymbol{e} := (1, 1, \ldots, 1).$$

- The normalization factor is consistent with numerics (Beihoffer et al., 2005)

- For $d = 3$ the theorem is due to Bourgain & Sinai (2007) and Shur, Sinai & Ustinov (2008)

Numerical experiments (Strömbergsson 2011)



The limit density is for $d = 3$ (Ustinov, Izv Math 2010):

$$p_2(R) = \begin{cases} 0 & (0 \le t \le \sqrt{3}) \\ \frac{12}{\pi}\Big(\frac{t}{\sqrt{3}} - \sqrt{4-t^2}\Big) & (\sqrt{3} \le t \le 2) \\ \frac{12}{\pi^2}\Big(t\sqrt{3}\,\text{arccos}\left(\frac{t+3\sqrt{t^2-4}}{4\sqrt{t^2-3}}\right) + \frac{3}{2}\sqrt{t^2-4}\,\log\left(\frac{t^2-4}{t^2-3}\right)\Big) & (2 \le t) \end{cases}$$

and for general $d = k+1 \ge 3$ (Strömbergsson, Acta Arith 2012):

$$p_k(R) = 0 \quad (R \le (k!)^{1/k})$$

$$p_k(R) \sim \frac{k(k+1)}{2\zeta(k)} R^{-(k+1)} \quad (R \to \infty)$$

H. Li (arXiv 2011) previously established an upper bound of the same order.

Reduction mod a_d (after Brauer & Shockley)

For $r \in \mathbb{Z}/a_d\mathbb{Z}$ set

$$F_r(\boldsymbol{a}) = \max(r + a_d\mathbb{Z}) \setminus \{\boldsymbol{m}\cdot\boldsymbol{a} > 0 : \boldsymbol{m} \in \mathbb{Z}^d_{\geq 0},\ \boldsymbol{m}\cdot\boldsymbol{a} \equiv r \bmod a_d\}$$

Then

$$F(\boldsymbol{a}) = \max_{r \bmod a_d} F_r(\boldsymbol{a}).$$

The smallest positive integer that has a representation in $r \bmod a_d$:

$$N_r(\boldsymbol{a}) = \min\{\boldsymbol{m}\cdot\boldsymbol{a} > 0 : \boldsymbol{m} \in \mathbb{Z}^d_{\geq 0},\ \boldsymbol{m}\cdot\boldsymbol{a} \equiv r \bmod a_d\}.$$

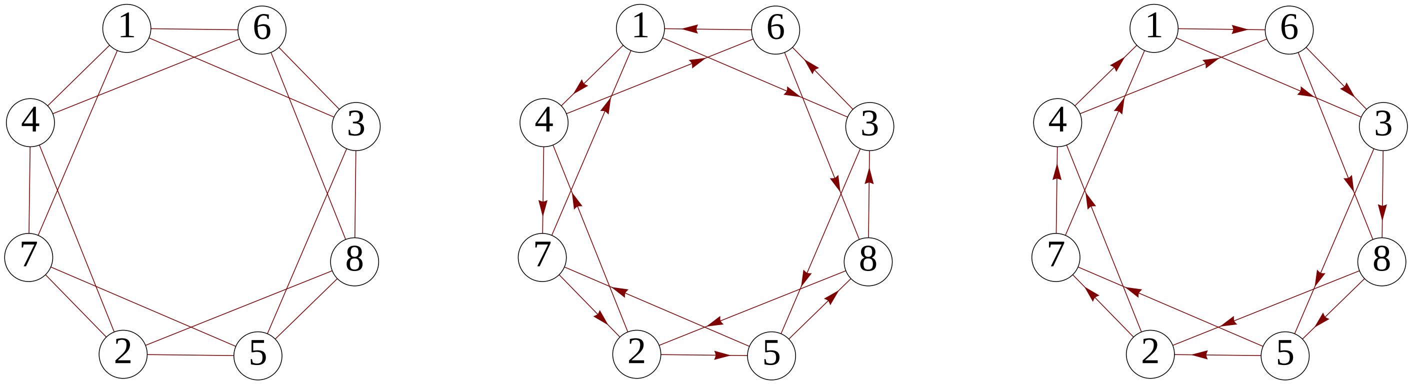
Then $F_r(\boldsymbol{a}) = N_r(\boldsymbol{a}) - a_d$ and

$$N_r(\boldsymbol{a}) = \begin{cases} a_d & (r \equiv 0 \bmod a_d) \\ \min\{\boldsymbol{m}'\cdot\boldsymbol{a}' : \boldsymbol{m}' \in \mathbb{Z}^{d-1}_{\geq 0},\ \boldsymbol{m}'\cdot\boldsymbol{a}' \equiv r \bmod a_d\} & (r \not\equiv 0 \bmod a_d) \end{cases}$$

with $\boldsymbol{a}' = (a_1, \ldots, a_{d-1})$. We conclude

$$\boxed{F(\boldsymbol{a}) = \max_{r \not\equiv 0 \bmod a_d} N_r(\boldsymbol{a}) - a_d.}$$

Frobenius numbers and circulant digraphs



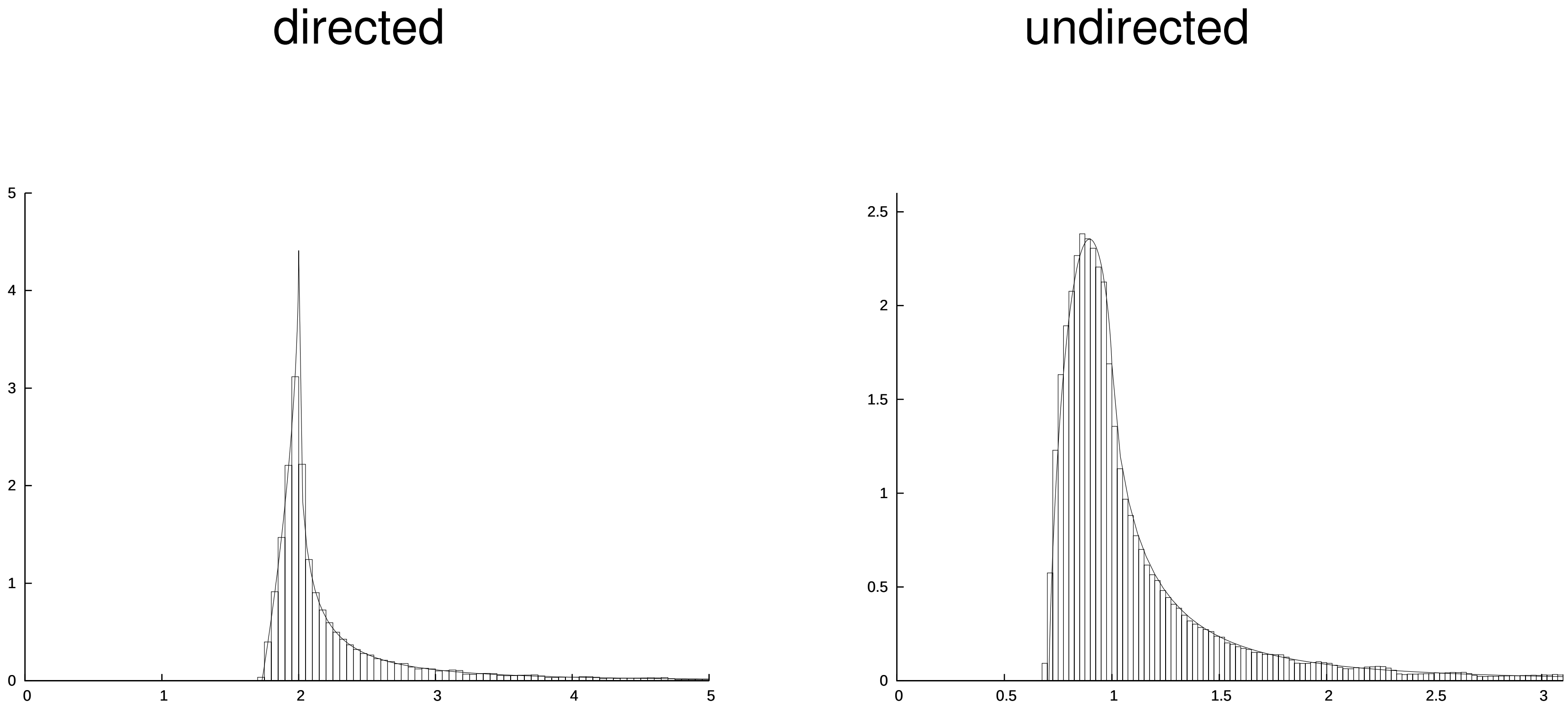
diam $= 2$ 3 4

Set $d = k + 1$, $\ell = \boldsymbol{a}' = (a_1, \ldots, a_{d-1})$, $n = a_d$. Then the above formula yields a connection between the Frobenius number and directed circulant graphs (Nijenhius, Amer Math Monthly 1979):

$$\boxed{F(\boldsymbol{a}) = \mathrm{diam}\, C_n^{+}(\boldsymbol{a}', \boldsymbol{a}') - n.}$$

The analogue of Theorem A holds for such random circulant digraphs, with the polytope $\mathfrak{P}$ replaced by Δ. This shows that the asymptotic distribution of Frobenius numbers and circulant digraphs coincide!

Diameters of random circulant graphs



directed

undirected

Numerical computation for $k = 2$, $\boldsymbol{\ell} = (1, 1)$, $n = 1000$.