From Cookie Monster to the IRS: Some Fruitful Interactions between Probability, Combinatorics and Number Theory

Steven J Miller
Williams College

Steven.J.Miller@williams.edu
http://www.williams.edu/Mathematics/sjmiller

UNC Charlotte, February 1, 2011

Outline

Summarize some of my interests, highlighting interplays across fields.
Joint with many faculty, grad students and undergrads.

- **Gaussian behavior in Zeckendorf decompositions:** Gene Kopp, Murat Koloğlu, Yinghui Wang.
- **More Sums Than Differences Sets:** Peter Hegarty, Brooke Orosz, Dan Scheinerman.
- **Classical Random Matrix Theory:** Eduardo Dueñez, Chris Hughes, Jon Keating, Nina Snaith, Duc Khiem Huynh, Tim Novikoff, Chris Hammond, Steven Jackson, Gene Kopp, Murat Koloğlu, Adam Massey, Thuy Pham, Anthony Sabelli, John Sinsheimer.
- **Benford's Law:** Chaouki Abdallah, Gregory Heileman, Mark Nigrini, Fernando Perez-Gonzalez, Tu-Thach Quach, Alex Kontorovich, Dennis Jang, Jung Uk Kang, Alex Kruckman, Jun Kudo.

Fibonacci Numbers

Previous Results

Fibonacci Numbers: $F_{n+1} = F_n + F_{n-1}$;
$F_1 = 1, F_2 = 2, F_3 = 3, F_4 = 5, \dots$.

Previous Results

Fibonacci Numbers: $F_{n+1} = F_n + F_{n-1}$;
$F_1 = 1, F_2 = 2, F_3 = 3, F_4 = 5, \dots$.

Zeckendorf's Theorem

Every positive integer can be written uniquely as a sum of non-consecutive Fibonacci numbers.

Previous Results

Fibonacci Numbers: $F_{n+1} = F_n + F_{n-1}$;
$F_1 = 1$, $F_2 = 2$, $F_3 = 3$, $F_4 = 5, \dots$.

Zeckendorf's Theorem

Every positive integer can be written uniquely as a sum of non-consecutive Fibonacci numbers.

Example:
$2011 = 1597 + 377 + 34 + 3 = F_{16} + F_{13} + F_8 + F_3$.

Previous Results

Fibonacci Numbers: $F_{n+1} = F_n + F_{n-1}$;
$F_1 = 1$, $F_2 = 2$, $F_3 = 3$, $F_4 = 5, \dots$.

Zeckendorf's Theorem

Every positive integer can be written uniquely as a sum of non-consecutive Fibonacci numbers.

Example:
$2011 = 1597 + 377 + 34 + 3 = F_{16} + F_{13} + F_8 + F_3$.

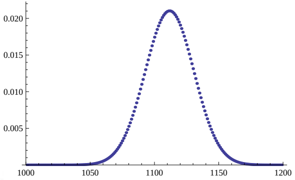
Lekkerkerker's Theorem (1952)

The average number of summands in the Zeckendorf decomposition for integers in $[F_n, F_{n+1})$ tends to $\frac{n}{\varphi^2+1} \approx .276n$, where $\varphi = \frac{1+\sqrt{5}}{2}$ is the golden mean.

Central Limit Type Theorem

Central Limit Type Theorem

As $n \to \infty$, the distribution of the number of summands, i.e., $a_1 + a_2 + \cdots + a_m$ in the generalized Zeckendorf decomposition $\sum_{i=1}^{m} a_i H_i$ for integers in $[H_n, H_{n+1})$ is Gaussian.



Far-difference Representation

Theorem (Alpert, 2009) (Analogue to Zeckendorf)

Every integer can be written uniquely as a sum of the $\pm F_n$'s, such that every two terms of the same (opposite) sign differ in index by at least 4 (3).

Example: $1900 = F_{17} - F_{14} - F_{10} + F_6 + F_2$.

K: # of positive terms, L: # of negative terms.

Generalized Lekkerkerker's Theorem

As $n \to \infty$, $E[K]$ and $E[L] \to n/10$, $E[K] - E[L] = \varphi/2 \approx .809$.

Central Limit Type Theorem

As $n \to \infty$, K and L converges to a bivariate Gaussian.

- $\text{corr}(K, L) = -(21 - 2\varphi)/(29 + 2\varphi) \approx -.551$.
- $K + L$ and $K - L$ are independent.

New Approach: Case of Fibonacci Numbers

$p_{n,k} = \#\{N \in [F_n, F_{n+1})$: the Zeckendorf decomposition of N has exactly k summands$\}$.

- Recurrence relation:
  $N \in [F_{n+1}, F_{n+2})$: $N = F_{n+1} + F_t + \cdots$, $t \le n-1$.

$$p_{n+1,k+1} \quad = \quad p_{n-1,k} + p_{n-2,k} + \cdots$$

New Approach: Case of Fibonacci Numbers

$p_{n,k} = \#\{N \in [F_n, F_{n+1})$: the Zeckendorf decomposition of N has exactly k summands$\}$.

- Recurrence relation:
  $N \in [F_{n+1}, F_{n+2})$: $N = F_{n+1} + F_t + \cdots$, $t \leq n-1$.

$$\begin{aligned} p_{n+1,k+1} &= p_{n-1,k} + p_{n-2,k} + \cdots \\ p_{n,k+1} &= p_{n-2,k} + p_{n-3,k} + \cdots \end{aligned}$$

New Approach: Case of Fibonacci Numbers

$p_{n,k} = \#\{N \in [F_n, F_{n+1})$: the Zeckendorf decomposition of N has exactly k summands$\}$.

- Recurrence relation:
  $N \in [F_{n+1}, F_{n+2})$: $N = F_{n+1} + F_t + \cdots$, $t \leq n-1$.

$$\begin{aligned} p_{n+1,k+1} &= p_{n-1,k} + p_{n-2,k} + \cdots \\ p_{n,k+1} &= p_{n-2,k} + p_{n-3,k} + \cdots \\ \Rightarrow p_{n+1,k+1} &= p_{n,k+1} + p_{n-1,k}. \end{aligned}$$

New Approach: Case of Fibonacci Numbers

$p_{n,k} = \#\{N \in [F_n, F_{n+1})$: the Zeckendorf decomposition of N has exactly k summands$\}$.

- Recurrence relation:
  $N \in [F_{n+1}, F_{n+2})$: $N = F_{n+1} + F_t + \cdots$, $t \le n-1$.
  $$\begin{aligned} p_{n+1,k+1} &= p_{n-1,k} + p_{n-2,k} + \cdots \\ p_{n,k+1} &= p_{n-2,k} + p_{n-3,k} + \cdots \\ \Rightarrow p_{n+1,k+1} &= p_{n,k+1} + p_{n-1,k}. \end{aligned}$$
- Generating function: $\sum_{n,k>0} p_{n,k} x^k y^n = \frac{y}{1-y-xy^2}$.
- Partial fraction expansion:
  $$\frac{y}{1-y-xy^2} = \frac{-y}{y_1(x)-y_2(x)}\left(\frac{1}{y-y_1(x)} - \frac{1}{y-y_2(x)}\right)$$
  where $y_1(x)$ and $y_2(x)$ are the roots of $1-y-xy^2=0$.

Coefficient of y^n: $g(x) = \sum_{n,k>0} p_{n,k} x^k$.

New Approach: Case of Fibonacci Numbers (Continued)

K_n: random variable associated with k.
$g(x) = \sum_{n,k>0} p_{n,k} x^k$.

- Differentiating identities:
  $g(1) = \sum_{n,k>0} p_{n,k} = F_{n+1} - F_n$,
  $g'(x) = \sum_{n,k>0} k p_{n,k} x^{k-1}$, $g'(1) = g(1) E[K_n]$,
  $(xg'(x))' = \sum_{n,k>0} k^2 p_{n,k} x^{k-1}$,
  $(xg'(x))' |_{x=1} = g(1) E[K_n^2]$, ...
- Method of moments (for normalized K_n'):
  $E[(K_n')^{2m}]/(SD(K_n'))^{2m} \to (2m-1)!!$,
  $E[(K_n')^{2m-1}]/(SD(K_n'))^{2m-1} \to 0$.

New Approach: General Case

Let $p_{n,k} = \#\{N \in [H_n, H_{n+1})$: the generalized Zeckendorf decomposition of N has exactly k summands$\}$.

- Recurrence relation:

  Fibonacci: $p_{n+1,k+1} = p_{n,k+1} + p_{n,k}$.

  General: $p_{n+1,k} = \sum_{m=0}^{L-1} \sum_{j=s_m}^{s_{m+1}-1} p_{n-m,k-j}$.

  where $s_0 = 0, s_m = c_1 + c_2 + \cdots + c_m$.

- Generating function:

  Fibonacci: $\frac{y}{1-y-xy^2}$.

  General:

$$\frac{\sum_{n \le L} p_{n,k} x^k y^n - \sum_{m=0}^{L-1} \sum_{j=s_m}^{s_{m+1}-1} x^j y^{m+1} \sum_{n<L-m} p_{n,k} x^k y^n}{1 - \sum_{m=0}^{L-1} \sum_{j=s_m}^{s_{m+1}-1} x^j y^{m+1}}.$$

New Approach: General Case (Continued)

- Partial fraction expansion:

  Fibonacci: $-\frac{y}{y_1(x)-y_2(x)}\left(\frac{1}{y-y_1(x)}-\frac{1}{y-y_2(x)}\right)$.

  General:

$$-\frac{1}{\sum_{j=s_{L-1}}^{s_L-1} x^j}\sum_{i=1}^{L}\frac{B(x,y)}{(y-y_i(x))\prod_{j\neq i}(y_j(x)-y_i(x))}.$$

$$B(x,y)=\sum_{n\leq L} p_{n,k}x^k y^n-\sum_{m=0}^{L-1}\sum_{j=s_m}^{s_{m+1}-1} x^j y^{m+1}\sum_{n<L-m} p_{n,k}x^k y^n,$$

$$y_i(x)\text{: root of } 1-\sum_{m=0}^{L-1}\sum_{j=s_m}^{s_{m+1}-1} x^j y^{m+1}=0.$$

  Coefficient of y^n: $g(x)=\sum_{n,k>0} p_{n,k}x^k$.

- Differentiating identities
- Method of moments: $\Rightarrow K_n \to$ Gaussian.

Random Matrix Theory

Fundamental Problem: Spacing Between Events

General Formulation: Studying system, observe values at $t_1, t_2, t_3, \dots$.

Question: What rules govern the spacings between the t_i?

Examples:

- Spacings b/w Energy Levels of Nuclei.
- Spacings b/w Eigenvalues of Matrices.
- Spacings b/w Primes.
- Spacings b/w $n^k\alpha$ mod 1.
- Spacings b/w Zeros of L-functions.

Origins of Random Matrix Theory

Classical Mechanics: 3 Body Problem Intractable.

Heavy nuclei (Uranium: $200+$ protons / neutrons) worse!

Get some info by shooting high-energy neutrons into nucleus, see what comes out.

Fundamental Equation:

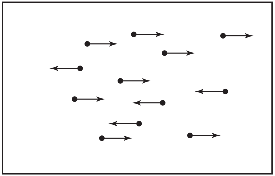
$$H\psi_n = E_n\psi_n$$

H : matrix, entries depend on system

E_n : energy levels

ψ_n : energy eigenfunctions

Origins of Random Matrix Theory



- Statistical Mechanics: for each configuration, calculate quantity (say pressure).
- Average over all configurations – most configurations close to system average.
- Nuclear physics: choose matrix at random, calculate eigenvalues, average over matrices (real Symmetric $A = A^T$, complex Hermitian $\overline{A}^T = A$).

Random Matrix Ensembles

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1N} \\ a_{12} & a_{22} & a_{23} & \cdots & a_{2N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{1N} & a_{2N} & a_{3N} & \cdots & a_{NN} \end{pmatrix} = A^T, \quad a_{ij} = a_{ji}$$

Fix p, define

$$\text{Prob}(A) = \prod_{1 \le i \le j \le N} p(a_{ij}).$$

This means

$$\text{Prob}\left(A : a_{ij} \in [\alpha_{ij}, \beta_{ij}]\right) = \prod_{1 \le i \le j \le N} \int_{x_{ij}=\alpha_{ij}}^{\beta_{ij}} p(x_{ij}) dx_{ij}.$$

Want to understand eigenvalues of A.

Eigenvalue Distribution

$\delta(x - x_0)$ is a unit point mass at x_0:
$\int f(x)\delta(x - x_0)dx = f(x_0)$.

To each A, attach a probability measure:

$$\mu_{A,N}(x) = \frac{1}{N}\sum_{i=1}^{N}\delta\left(x - \frac{\lambda_i(A)}{2\sqrt{N}}\right)$$

$$\int_a^b \mu_{A,N}(x)dx = \frac{\#\left\{\lambda_i : \frac{\lambda_i(A)}{2\sqrt{N}} \in [a,b]\right\}}{N}$$

$$\text{k}^{\text{th}}\text{ moment} = \frac{\sum_{i=1}^{N}\lambda_i(A)^k}{2^k N^{\frac{k}{2}+1}}.$$

SKETCH OF PROOF: Eigenvalue Trace Lemma

Want to understand A's eigenvalues, but it's A's elements that are chosen randomly and independently.

Eigenvalue Trace Lemma

Let A be an $N \times N$ matrix with eigenvalues $\lambda_i(A)$. Then

$$\mathrm{Trace}(A^k) \ = \ \sum_{n=1}^{N} \lambda_i(A)^k,$$

where

$$\mathrm{Trace}(A^k) \ = \ \sum_{i_1=1}^{N} \cdots \sum_{i_k=1}^{N} a_{i_1 i_2} a_{i_2 i_3} \cdots a_{i_N i_1}.$$

SKETCH OF PROOF: Correct Scale

$$\text{Trace}(A^2) = \sum_{i=1}^{N} \lambda_i(A)^2.$$

By the Central Limit Theorem:

$$\text{Trace}(A^2) = \sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij}a_{ji} = \sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij}^2 \sim N^2$$

$$\sum_{i=1}^{N} \lambda_i(A)^2 \sim N^2$$

Gives $N\,\text{Ave}(\lambda_i(A)^2) \sim N^2$ or $\text{Ave}(\lambda_i(A)) \sim \sqrt{N}$.

SKETCH OF PROOF: Averaging Formula

Recall k-th moment of $\mu_{A,N}(x)$ is $\mathrm{Trace}(A^k)/2^k N^{k/2+1}$.

Average k-th moment is

$$\int \cdots \int \frac{\mathrm{Trace}(A^k)}{2^k N^{k/2+1}} \prod_{i \le j} p(a_{ij}) da_{ij}.$$

Proof by method of moments: Two steps

- Show average of k-th moments converge to moments of semi-circle as $N \to \infty$;
- Control variance (show it tends to zero as $N \to \infty$).

SKETCH OF PROOF: Averaging Formula for Second Moment

Substituting into expansion gives

$$\frac{1}{2^2N^2}\int_{-\infty}^{\infty}\cdots\int_{-\infty}^{\infty}\sum_{i=1}^{N}\sum_{j=1}^{N}a_{ji}^2\cdot p(a_{11})da_{11}\cdots p(a_{NN})da_{NN}$$

Integration factors as

$$\int_{a_{ij}=-\infty}^{\infty}a_{ij}^2p(a_{ij})da_{ij}\quad\cdot\prod_{\substack{(k,l)\neq(i,j)\\ k<l}}\int_{a_{kl}=-\infty}^{\infty}p(a_{kl})da_{kl}\;=\;1.$$

Higher moments involve more advanced combinatorics (Catalan numbers).

SKETCH OF PROOF: Averaging Formula for Higher Moments

Higher moments involve more advanced combinatorics (Catalan numbers).

$$\frac{1}{2^k N^{k/2+1}} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \sum_{i_1=1}^{N} \cdots \sum_{i_k=1}^{N} a_{i_1 i_2} \cdots a_{i_k i_1} \cdot \prod_{i \le j} p(a_{ij}) da_{ij}.$$

Main contribution when the $a_{i_\ell i_{\ell+1}}$'s matched in pairs, not all matchings contribute equally (if did would get a Gaussian and not a semi-circle; this is seen in Real Symmetric Palindromic Toeplitz matrices).

Real Symmetric
m-Circulant Ensemble

Circulant Matrices

Study circulant matrices, period m on diagonals.

6-by-6 real symmetric period 2-circulant matrix:

$$\begin{pmatrix} c_0 & c_1 & c_2 & c_3 & c_2 & d_1 \\ c_1 & d_0 & d_1 & d_2 & c_3 & d_2 \\ c_2 & d_1 & c_0 & c_1 & c_2 & c_3 \\ c_3 & d_2 & c_1 & d_0 & d_1 & d_2 \\ c_2 & c_3 & c_2 & d_1 & c_0 & c_1 \\ d_1 & d_2 & c_3 & d_2 & c_1 & d_0 \end{pmatrix}.$$

Look at the *expected value* for the moments:

$$\begin{aligned} M_n(N) &:= \mathbb{E}(M_n(A,N)) \\ &= \frac{1}{N^{\frac{n}{2}+1}} \sum_{1 \le i_1, \dots, i_n \le N} \mathbb{E}(a_{i_1 i_2} a_{i_2 i_3} \cdots a_{i_n i_1}). \end{aligned}$$

Matchings

Rewrite:

$$M_n(N) = \frac{1}{N^{\frac{n}{2}+1}} \sum_{\sim} \eta(\sim) m_{d_1(\sim)} \cdots m_{d_l(\sim)}.$$

where the sum is over equivalence relations on $\{(1,2),(2,3),\dots,(n,1)\}$. The $d_j(\sim)$ denote the sizes of the equivalence classes, and the m_d the moments of p. Finally, the coefficient $\eta(\sim)$ is the number of solutions to the system of Diophantine equations:

Whenever $(s,s+1) \sim (t,t+1)$,

- $i_{s+1} - i_s \equiv i_{t+1} - i_t \pmod{N}$ and $i_s \equiv i_t \pmod{m}$, or
- $i_{s+1} - i_s \equiv -(i_{t+1} - i_t) \pmod{N}$ and $i_s \equiv i_{t+1} \pmod{m}$.

Matchings

- $i_{s+1} - i_s \equiv i_{t+1} - i_t \pmod{N}$ and $i_s \equiv i_t \pmod{m}$, or
- $i_{s+1} - i_s \equiv -(i_{t+1} - i_t) \pmod{N}$ and $i_s \equiv i_{t+1} \pmod{m}$.

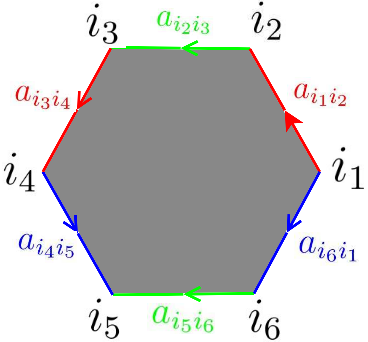
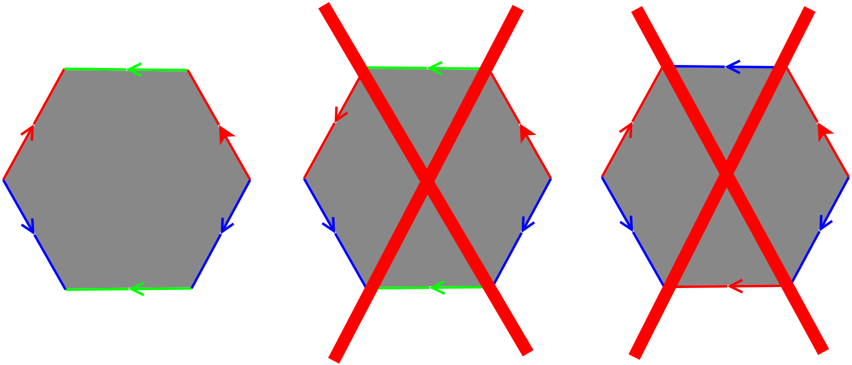


Figure: Red edges same orientation and blue, green opposite.

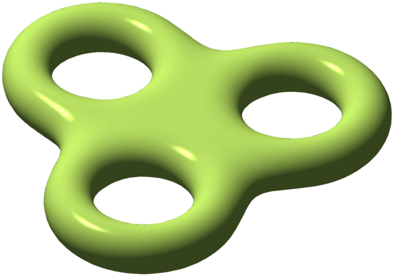
Contributing Terms

As $N \to \infty$, the only terms that contribute to this sum are those in which the entries are matched in pairs and with opposite orientation.



Contributing Terms: Algebraic Topology

Think of pairings as topological identifications, the contributing ones give rise to orientable surfaces.



Contribution from such a pairing is m^{-2g}, where g is the genus (number of holes) of the surface. Proof: combinatorial argument involving Euler characteristic.

Computing the Even Moments

Theorem: Even Moment Formula

$$M_{2k} = \sum_{g=0}^{\lfloor k/2 \rfloor} \varepsilon_g(k) m^{-2g} + O_k\left(\frac{1}{N}\right),$$

with $\varepsilon_g(k)$ the number of pairings of the edges of a $(2k)$-gon giving rise to a genus g surface.

J. Harer and D. Zagier (1986) gave generating functions for the $\varepsilon_g(k)$.

Computing the Even Moments

Harer and Zagier

$$\sum_{g=0}^{\lfloor k/2 \rfloor} \varepsilon_g(k) r^{k+1-2g} \ = \ (2k-1)!!\, c(k,r)$$

where

$$1 + 2\sum_{k=0}^{\infty} c(k,r) x^{k+1} \ = \ \left(\frac{1+x}{1-x}\right)^r.$$

Thus, we write

$$M_{2k} \ = \ m^{-(k+1)}(2k-1)!!\, c(k,m).$$

Computing the Even Moments

A multiplicative convolution and Cauchy's residue formula yields the *characteristic function* of the distribution (inverse Fourier transform of the density).

$$\begin{aligned}
\phi(t) &= \sum_{k=0}^{\infty} \frac{(it)^{2k} M_{2k}}{(2k)!} \\
&= \frac{1}{2\pi i m} \oint_{|z|=2} \frac{1}{2z^{-1}} \left(\left(\frac{1+z^{-1}}{1-z^{-1}} \right)^m - 1 \right) e^{-t^2 z/2m} \frac{dz}{z} \\
&= \frac{1}{m} e^{\frac{-t^2}{2m}} \sum_{l=1}^{m} \binom{m}{l} \frac{1}{(l-1)!} \left(\frac{-t^2}{m} \right)^{l-1}.
\end{aligned}$$

Results

Fourier transform and algebra yields

Theorem: Kopp, Koloğlu and M–

The limiting spectral density function $f_m(x)$ of the real symmetric m-circulant ensemble is given by the formula

$$f_m(x) = \frac{e^{-\frac{mx^2}{2}}}{\sqrt{2\pi m}} \sum_{r=0}^{m} \frac{1}{(2r)!} \sum_{s=0}^{m-r} \binom{m}{r+s+1} \frac{(2r+2s)!}{(r+s)!s!} \left(-\frac{1}{2}\right)^s (mx^2)^r.$$

As $m \to \infty$, the limiting spectral densities approach the semicircle distribution.

Results (continued)

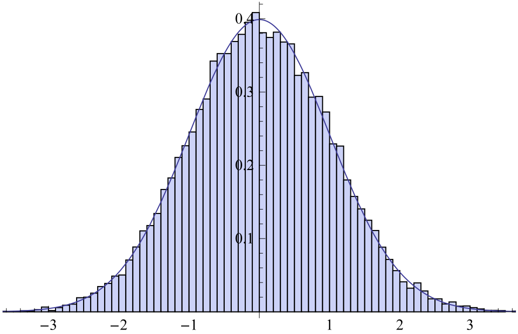


Figure: Plot for f_1 and histogram of eigenvalues of 100 circulant matrices of size 400×400.

Results (continued)

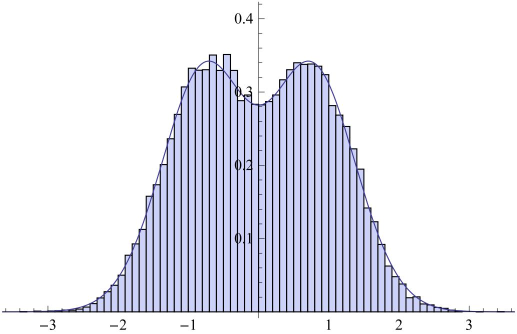


Figure: Plot for f_2 and histogram of eigenvalues of 100 2-circulant matrices of size 400×400.

Results (continued)

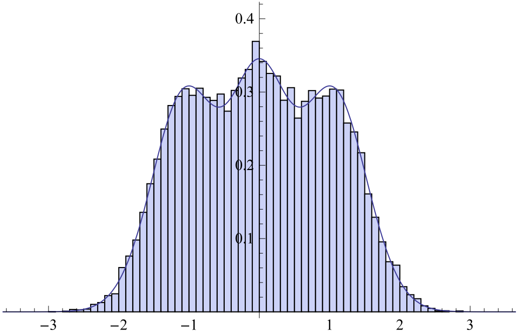


Figure: Plot for f_3 and histogram of eigenvalues of 100 3-circulant matrices of size 402×402.

Results (continued)

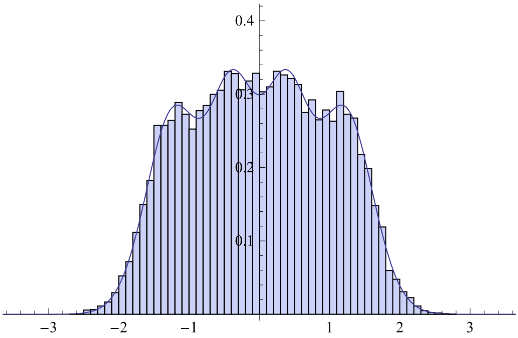


Figure: Plot for f_4 and histogram of eigenvalues of 100 4-circulant matrices of size 400×400.

Results (continued)

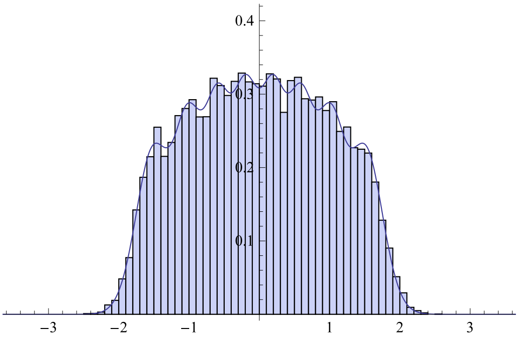


Figure: Plot for f_8 and histogram of eigenvalues of 100 8-circulant matrices of size 400×400.

Results (continued)

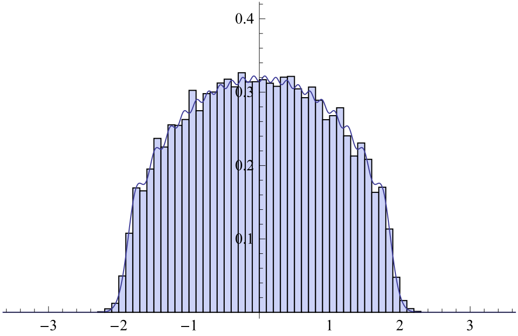


Figure: Plot for f_{20} and histogram of eigenvalues of 100 20-circulant matrices of size 400×400.

Results (continued)

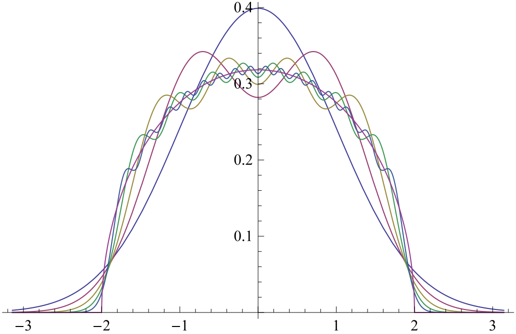


Figure: Plot of convergence to the semi-circle.

Benford History and Applications

Benford's Law: Newcomb (1881), Benford (1938)

Statement

For many data sets, probability of observing a first digit of d base B is $\log_B\left(\frac{d+1}{d}\right)$.

First 60 values of 2^n (only displaying 30)

			digit	#	Obs Prob	Benf Prob
1	1024	1048576	1	18	.300	.301
2	2048	2097152	2	12	.200	.176
4	4096	4194304	3	6	.100	.125
8	8192	8388608	4	6	.100	.097
16	16384	16777216	5	6	.100	.079
32	32768	33554432	6	4	.067	.067
64	65536	67108864	7	2	.033	.058
128	131072	134217728	8	5	.083	.051
256	262144	268435456	9	1	.017	.046
512	524288	536870912				

Examples

- recurrence relations
- special functions (such as $n!$)
- iterates of power, exponential, rational maps
- products of random variables
- L-functions, characteristic polynomials
- iterates of the $3x + 1$ map
- differences of order statistics
- hydrology and financial data

Applications

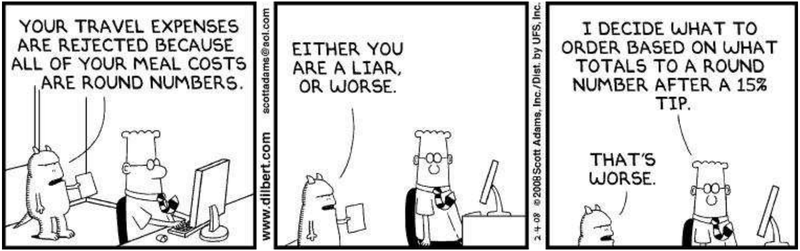
- analyzing round-off errors
- determining the optimal way to store numbers
- detecting tax fraud and data integrity

Caveats!

- A math test indicating fraud is *not* proof of fraud: unlikely events, alternate reasons.

Caveats!

- A math test indicating fraud is *not* proof of fraud: unlikely events, alternate reasons.



Detecting Fraud

Bank Fraud

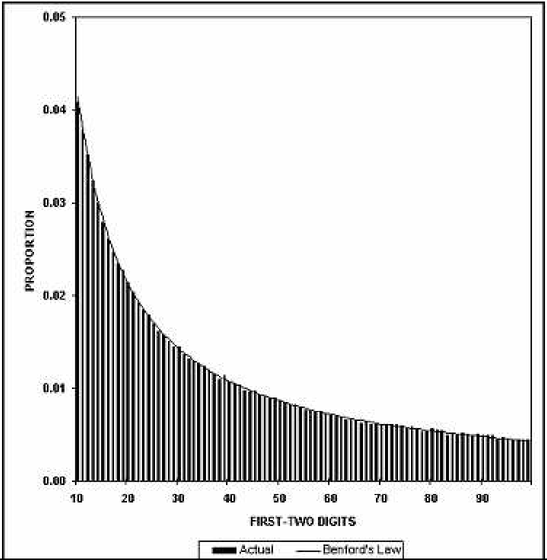
- Bank audit: huge spike of numbers starting with 48 and 49, most due to one person.

Detecting Fraud

Bank Fraud

- Bank audit: huge spike of numbers starting with 48 and 49, most due to one person.
- Write-off limit of $5,000. Officer had friends applying, run up balances just under $5,000....

Data Integrity: Stream Flow Statistics: 130 years, 457,440 records



Election Fraud: Iran 2009

Numerous protests/complaints over Iran's 2009 elections.

Lot of analysis; data moderately suspicious:

- First and second leading digits;
- Last two digits (should almost be uniform);
- Last two digits differing by at least 2.

Warning: enough tests, even if nothing wrong will find a suspicious result (but when all tests are on the boundary...).

New Test for Fraud

New Test for Fraud

Victoria Cuff, Allie Lewis, M– (2010)

Image Analysis

- Pictures aren't Benford's law, but coefficients of Discrete Cosine Transform (DCT) very close (slightly modified law).

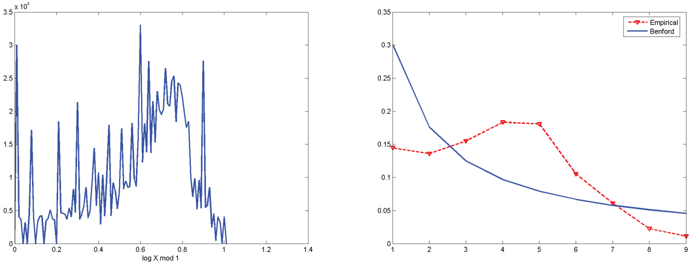
- Analysis of coefficients, from Generalized Gaussian Distributions:
  $f_X(x) = A\exp(-\|\beta x|^c)$.

- Application: detect compression, steganography (hidden message in picture by modifying least significant bit in pixels).

Image Analysis (continued)

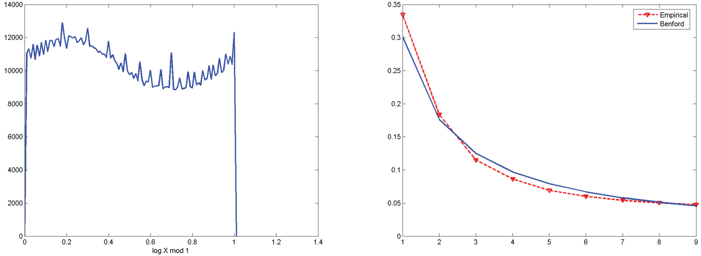
Figure 'Man' used in the experiments.

Image Analysis (continued)



(a) Histogram of the luminance values of ‘Man’ in Benford ($\log_{10} \bmod 1$) domain; (b) Distribution of first digits from ‘Man’.

Image Analysis (continued)



Histogram of the DCT values of ‘Man’ in Benford ($\log_{10}$ mod 1) domain; (b) Distribution of first digits from ‘Man’.

Logarithms and Benford's Law

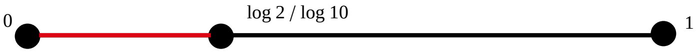
Fundamental Equivalence

Data set $\{x_i\}$ is Benford base B if $\{y_i\}$ is equidistributed mod 1, where $y_i = \log_B x_i$.

Logarithms and Benford's Law

Fundamental Equivalence

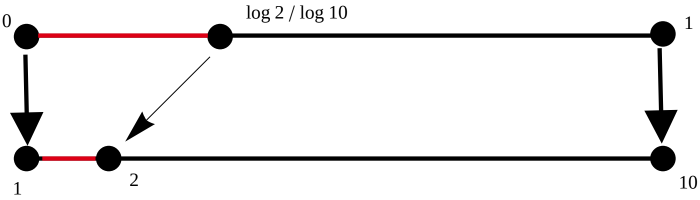
Data set $\{x_i\}$ is Benford base B if $\{y_i\}$ is equidistributed mod 1, where $y_i = \log_B x_i$.



Logarithms and Benford's Law

Fundamental Equivalence

Data set $\{x_i\}$ is Benford base B if $\{y_i\}$ is equidistributed mod 1, where $y_i = \log_B x_i$.



Logarithms and Benford's Law

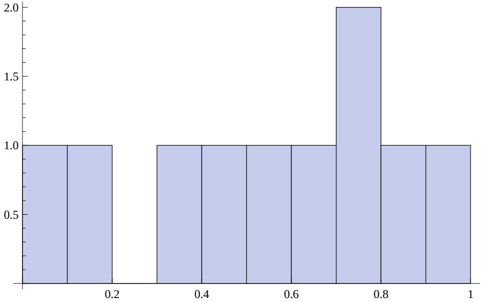
Fundamental Equivalence

Data set $\{x_i\}$ is Benford base B if $\{y_i\}$ is equidistributed mod 1, where $y_i = \log_B x_i$.

Kronecker-Weyl Theorem

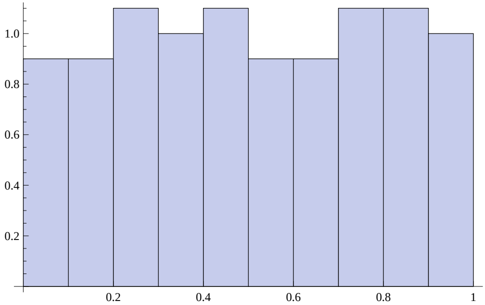
If $\beta \notin \mathbb{Q}$ then $n\beta$ mod 1 is equidistributed. (Thus if $\log_B \alpha \notin \mathbb{Q}$, then α^n is Benford.)

Example of Equidistribution: $n\sqrt{\pi}$ mod 1



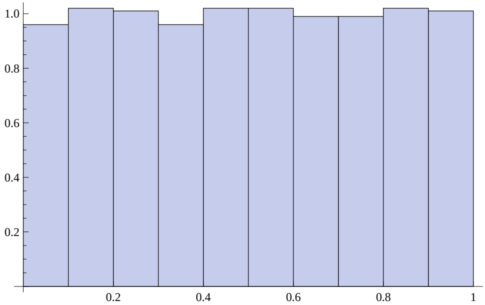
$n\sqrt{\pi}$ mod 1 for $n \le 10$

Example of Equidistribution: $n\sqrt{\pi}$ mod 1



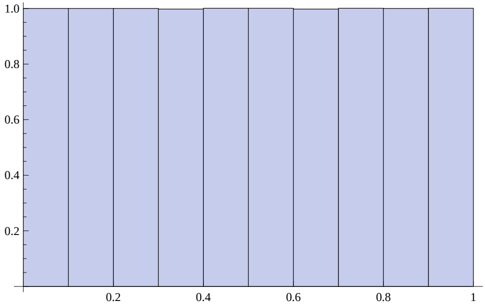
$n\sqrt{\pi}$ mod 1 for $n \leq 100$

Example of Equidistribution: $n\sqrt{\pi}$ mod 1



$n\sqrt{\pi}$ mod 1 for $n \leq 1000$

Example of Equidistribution: $n\sqrt{\pi} \bmod 1$



$n\sqrt{\pi} \bmod 1$ for $n \le 10,000$

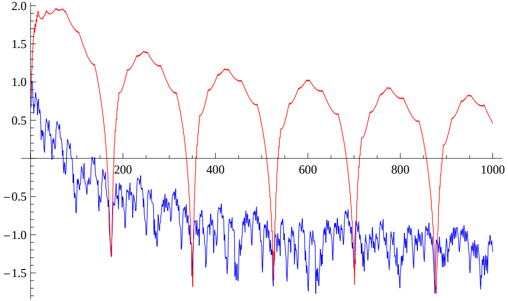
Logarithms and Benford's Law

χ^2 values for α^n, $1 \le n \le N$ (5% 15.5).

N	$\chi^2(\gamma)$	$\chi^2(e)$	$\chi^2(\pi)$
100	0.72	0.30	46.65
200	0.24	0.30	8.58
400	0.14	0.10	10.55
500	0.08	0.07	2.69
700	0.19	0.04	0.05
800	0.04	0.03	6.19
900	0.09	0.09	1.71
1000	0.02	0.06	2.90

Logarithms and Benford's Law: Base 10

$\log(\chi^2)$ vs N for π^n (red) and e^n (blue), $n \in \{1, \dots, N\}$. Note $\pi^{175} \approx 1.0028 \cdot 10^{87}$, (5%, $\log(\chi^2) \approx 2.74$).



Benford Good Processes

Poisson Summation and Benford's Law: Definitions

- Feller, Pinkham (often exact processes)

Poisson Summation and Benford's Law: Definitions

- Feller, Pinkham (often exact processes)
- data $Y_{T,B} = \log_B \overrightarrow{X}_T$ (discrete/continuous):

$$\mathbb{P}(A) \ = \ \lim_{T\to\infty} \frac{\#\{n \in A : n \leq T\}}{T}$$

Poisson Summation and Benford's Law: Definitions

- Feller, Pinkham (often exact processes)
- data $Y_{T,B} = \log_B \overrightarrow{X}_T$ (discrete/continuous):

$$\mathbb{P}(A) \ = \ \lim_{T\to\infty} \frac{\#\{n \in A : n \le T\}}{T}$$

- Poisson Summation Formula: f nice:

$$\sum_{\ell=-\infty}^{\infty} f(\ell) \ = \ \sum_{\ell=-\infty}^{\infty} \widehat{f}(\ell),$$

Fourier transform $\widehat{f}(\xi) \ = \ \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \xi} dx.$

Benford Good Process

X_T is Benford Good if there is a nice f st

$$\mathrm{CDF}_{\vec{Y}_{T,B}}(y) = \int_{-\infty}^{y} \frac{1}{T} f\left(\frac{t}{T}\right) dt + E_T(y) := G_T(y)$$

and monotonically increasing h ($h(|T|) \to \infty$):

Benford Good Process

X_T is Benford Good if there is a nice f st

$$\mathrm{CDF}_{\vec{Y}_{T,B}}(y) = \int_{-\infty}^{y} \frac{1}{T} f\left(\frac{t}{T}\right) dt + E_T(y) := G_T(y)$$

and monotonically increasing h ($h(|T|) \to \infty$):

- Small tails: $G_T(\infty) - G_T(Th(T)) = o(1)$, $G_T(-Th(T)) - G_T(-\infty) = 0(1)$.

Benford Good Process

X_T is Benford Good if there is a nice f st

$$\mathrm{CDF}_{\overrightarrow{Y}_{T,B}}(y) = \int_{-\infty}^{y} \frac{1}{T} f\left(\frac{t}{T}\right) dt + E_T(y) := G_T(y)$$

and monotonically increasing h ($h(|T|) \to \infty$):

- Small tails: $G_T(\infty) - G_T(Th(T)) = o(1)$, $G_T(-Th(T)) - G_T(-\infty) = 0(1)$.
- Decay of the Fourier Transform: $\sum_{\ell \neq 0} \left|\frac{\widehat{f}(T\ell)}{\ell}\right| = o(1)$.

Benford Good Process

X_T is Benford Good if there is a nice f st

$$\mathrm{CDF}_{\vec{Y}_{T,B}}(y) = \int_{-\infty}^{y} \frac{1}{T} f\left(\frac{t}{T}\right) dt + E_T(y) := G_T(y)$$

and monotonically increasing h ($h(|T|) \to \infty$):

- Small tails: $G_T(\infty) - G_T(Th(T)) = o(1)$, $G_T(-Th(T)) - G_T(-\infty) = 0(1)$.
- Decay of the Fourier Transform: $\sum_{\ell \neq 0} \left|\frac{\widehat{f}(T\ell)}{\ell}\right| = o(1)$.
- Small translated error: $\mathcal{E}(a, b, T)) = \sum_{|\ell| \leq Th(T)} [E_T(b+\ell) - E_T(a+\ell)] = o(1)$.

Main Theorem

Theorem (Kontorovich and M–, 2005)

X_T converging to X as $T \to \infty$ (think spreading Gaussian). If X_T is Benford good, then X is Benford.

Main Theorem

Theorem (Kontorovich and M–, 2005)

X_T converging to X as $T \to \infty$ (think spreading Gaussian). If X_T is Benford good, then X is Benford.

- Examples
  - ◇ L-functions
  - ◇ characteristic polynomials (RMT)
  - ◇ $3x+1$ problem
  - ◇ geometric Brownian motion.

Sketch of the proof

- Structure Theorem:
  - ◇ main term is something nice spreading out
  - ◇ apply Poisson summation

Sketch of the proof

- Structure Theorem:
  - ◇ main term is something nice spreading out
  - ◇ apply Poisson summation
- Control translated errors:
  - ◇ hardest step
  - ◇ techniques problem specific

Sketch of the proof (continued)

$$\sum_{\ell=-\infty}^{\infty} \mathbb{P}\left(a+\ell \leq \overrightarrow{Y}_{T,B} \leq b+\ell\right)$$

Sketch of the proof (continued)

$$\sum_{\ell=-\infty}^{\infty} \mathbb{P}\left(a+\ell \leq \overrightarrow{Y}_{T,B} \leq b+\ell\right)$$

$$= \sum_{|\ell| \leq Th(T)} [G_T(b+\ell) - G_T(a+\ell)] + o(1)$$

Sketch of the proof (continued)

$$\sum_{\ell=-\infty}^{\infty} \mathbb{P}\left(a+\ell \leq \overrightarrow{Y}_{T,B} \leq b+\ell\right)$$

$$= \sum_{|\ell|\leq Th(T)} [G_T(b+\ell) - G_T(a+\ell)] + o(1)$$

$$= \int_a^b \sum_{|\ell|\leq Th(T)} \frac{1}{T} f\left(\frac{t}{T}\right) dt + \mathcal{E}(a,b,T) + o(1)$$

Sketch of the proof (continued)

$$\sum_{\ell=-\infty}^{\infty} \mathbb{P}\left(a+\ell \le \overrightarrow{Y}_{T,B} \le b+\ell\right)$$

$$= \sum_{|\ell| \le Th(T)} \left[G_T(b+\ell) - G_T(a+\ell)\right] + o(1)$$

$$= \int_a^b \sum_{|\ell| \le Th(T)} \frac{1}{T} f\left(\frac{t}{T}\right) dt + \mathcal{E}(a,b,T) + o(1)$$

$$= \widehat{f}(0)\cdot(b-a) + \sum_{\ell \ne 0} \widehat{f}(T\ell)\frac{e^{2\pi i b\ell} - e^{2\pi i a\ell}}{2\pi i\ell} + o(1).$$

Some Results

Theorem (Kontorovich and M–, 2005)

$L(s, f)$ a good L-function, as $T \to \infty$, $L(\sigma_T + it, f)$ is Benford.

Theorem (Kontorovich and M–, 2005)

As $N \to \infty$, the distribution of digits of the absolute values of the characteristic polynomials of $N \times N$ unitary matrices (with respect to Haar measure) converges to the Benford probabilities.

The $3x + 1$ Problem
and
Benford's Law

$3x + 1$ Problem

- Kakutani (conspiracy), Erdös (not ready).
- x odd, $T(x) = \frac{3x+1}{2^k}$, $2^k || 3x + 1$.

$3x + 1$ Problem

- Kakutani (conspiracy), Erdös (not ready).
- x odd, $T(x) = \frac{3x+1}{2^k}$, $2^k || 3x + 1$.
- Conjecture: for some $n = n(x)$, $T^n(x) = 1$.

$3x+1$ Problem

- Kakutani (conspiracy), Erdös (not ready).
- x odd, $T(x) = \frac{3x+1}{2^k}$, $2^k || 3x+1$.
- Conjecture: for some $n = n(x)$, $T^n(x) = 1$.
- 7

$3x + 1$ Problem

- Kakutani (conspiracy), Erdös (not ready).
- x odd, $T(x) = \frac{3x+1}{2^k}$, $2^k || 3x+1$.
- Conjecture: for some $n = n(x)$, $T^n(x) = 1$.
- $7 \to_1 11$

$3x+1$ Problem

- Kakutani (conspiracy), Erdös (not ready).
- x odd, $T(x) = \frac{3x+1}{2^k}$, $2^k || 3x+1$.
- Conjecture: for some $n = n(x)$, $T^n(x) = 1$.
- $7 \to_1 11 \to_1 17$

$3x + 1$ Problem

- Kakutani (conspiracy), Erdös (not ready).
- x odd, $T(x) = \frac{3x+1}{2^k}$, $2^k || 3x + 1$.
- Conjecture: for some $n = n(x)$, $T^n(x) = 1$.
- $7 \to_1 11 \to_1 17 \to_2 13$

$3x + 1$ Problem

- Kakutani (conspiracy), Erdös (not ready).
- x odd, $T(x) = \frac{3x+1}{2^k}$, $2^k || 3x + 1$.
- Conjecture: for some $n = n(x)$, $T^n(x) = 1$.
- $7 \to_1 11 \to_1 17 \to_2 13 \to_3 5$

$3x+1$ Problem

- Kakutani (conspiracy), Erdös (not ready).
- x odd, $T(x) = \frac{3x+1}{2^k}$, $2^k || 3x+1$.
- Conjecture: for some $n = n(x)$, $T^n(x) = 1$.
- $7 \to_1 11 \to_1 17 \to_2 13 \to_3 5 \to_4 1$

$3x+1$ Problem

- Kakutani (conspiracy), Erdös (not ready).
- x odd, $T(x) = \frac{3x+1}{2^k}$, $2^k || 3x+1$.
- Conjecture: for some $n = n(x)$, $T^n(x) = 1$.
- $7 \to_1 11 \to_1 17 \to_2 13 \to_3 5 \to_4 1 \to_2 1$,

$3x+1$ Problem

- Kakutani (conspiracy), Erdös (not ready).
- x odd, $T(x) = \frac{3x+1}{2^k}$, $2^k || 3x+1$.
- Conjecture: for some $n = n(x)$, $T^n(x) = 1$.
- $7 \to_1 11 \to_1 17 \to_2 13 \to_3 5 \to_4 1 \to_2 1$,
  2-path $(1,1)$, 5-path $(1,1,2,3,4)$.
  m-path: $(k_1, \dots, k_m)$.

Heuristic Proof of $3x + 1$ Conjecture

$$a_{n+1} = T(a_n)$$

Heuristic Proof of $3x+1$ Conjecture

$$\begin{aligned} a_{n+1} &= T(a_n) \\ \mathbb{E}[\log a_{n+1}] &\approx \sum_{k=1}^{\infty} \frac{1}{2^k} \log\left(\frac{3a_n}{2^k}\right) \end{aligned}$$

Heuristic Proof of $3x+1$ Conjecture

$$\begin{aligned} a_{n+1} &= T(a_n) \\ \mathbb{E}[\log a_{n+1}] &\approx \sum_{k=1}^{\infty} \frac{1}{2^k} \log\left(\frac{3a_n}{2^k}\right) \\ &= \log a_n + \log\left(\frac{3}{4}\right). \end{aligned}$$

Geometric Brownian Motion, drift $\log(3/4) < 1$.

Structure Theorem: Sinai, Kontorovich-Sinai

$$\mathbb{P}(A) = \lim_{N\to\infty} \frac{\#\{n \le N : n \equiv 1,5 \bmod 6, n \in A\}}{\#\{n \le N : n \equiv 1,5 \bmod 6\}}.$$

Structure Theorem: Sinai, Kontorovich-Sinai

$\mathbb{P}(A) = \lim_{N\to\infty} \frac{\#\{n\le N: n\equiv 1,5 \text{ mod } 6, n\in A\}}{\#\{n\le N: n\equiv 1,5 \text{ mod } 6\}}$.

$(k_1, \dots, k_m)$: two full arithm progressions:

$6\cdot 2^{k_1+\cdots+k_m}p+q$.

Structure Theorem: Sinai, Kontorovich-Sinai

$$\mathbb{P}(A) = \lim_{N\to\infty} \frac{\#\{n\le N: n\equiv 1,5 \bmod 6, n\in A\}}{\#\{n\le N: n\equiv 1,5 \bmod 6\}}.$$

$(k_1, \dots, k_m)$: two full arithm progressions: $6\cdot 2^{k_1+\cdots+k_m}p + q$.

Theorem (Sinai, Kontorovich-Sinai)

k_i-values are i.i.d.r.v. (geometric, $1/2$):

$$\mathbb{P}\left(\frac{\log_2\left[\frac{x_m}{\left(\frac{3}{4}\right)^m x_0}\right]}{\sqrt{2m}} \le a\right) = \mathbb{P}\left(\frac{S_m - 2m}{\sqrt{2m}} \le a\right)$$

Structure Theorem: Sinai, Kontorovich-Sinai

$$\mathbb{P}(A) = \lim_{N\to\infty} \frac{\#\{n\le N: n\equiv 1,5 \bmod 6, n\in A\}}{\#\{n\le N: n\equiv 1,5 \bmod 6\}}.$$

$(k_1, \dots, k_m)$: two full arithm progressions:

$6 \cdot 2^{k_1+\cdots+k_m} p + q$.

Theorem (Sinai, Kontorovich-Sinai)

k_i-values are i.i.d.r.v. (geometric, 1/2):

$$\mathbb{P}\left(\frac{\log_2\left[\frac{x_m}{\left(\frac{3}{4}\right)^m x_0}\right]}{(\log_2 B)\sqrt{2m}} \le a\right) = \mathbb{P}\left(\frac{S_m - 2m}{(\log_2 B)\sqrt{2m}} \le a\right)$$

Structure Theorem: Sinai, Kontorovich-Sinai

$$\mathbb{P}(A) = \lim_{N\to\infty} \frac{\#\{n\le N: n\equiv 1,5 \bmod 6, n\in A\}}{\#\{n\le N: n\equiv 1,5 \bmod 6\}}.$$

$(k_1,\dots,k_m)$: two full arithm progressions:
$6\cdot 2^{k_1+\cdots+k_m}p+q$.

Theorem (Sinai, Kontorovich-Sinai)

k_i-values are i.i.d.r.v. (geometric, $1/2$):

$$\mathbb{P}\left(\frac{\log_B\left[\frac{x_m}{\left(\frac{3}{4}\right)^m x_0}\right]}{\sqrt{2m}} \le a\right) = \mathbb{P}\left(\frac{\frac{(S_m-2m)}{\log_2 B}}{\sqrt{2m}} \le a\right)$$

$3x+1$ and Benford

Theorem (Kontorovich and M–, 2005)

As $m \to \infty$, $x_m/(3/4)^m x_0$ is Benford.

Theorem (Lagarias-Soundararajan 2006)

$X \geq 2^N$, for all but at most $c(B)N^{-1/36}X$ initial seeds the distribution of the first N iterates of the $3x+1$ map are within $2N^{-1/36}$ of the Benford probabilities.

Sketch of the proof

- Failed Proof: lattices, bad errors.

Sketch of the proof

- Failed Proof: lattices, bad errors.

- CLT: $(S_m - 2m)/\sqrt{2m} \to N(0,1)$:

$$\mathbb{P}\left(S_m - 2m = k\right) = \frac{\eta(k/\sqrt{m})}{\sqrt{m}} + O\left(\frac{1}{g(m)\sqrt{m}}\right).$$

Sketch of the proof

- Failed Proof: lattices, bad errors.

- CLT: $(S_m - 2m)/\sqrt{2m} \to N(0,1)$:

$$\mathbb{P}\left(S_m - 2m = k\right) = \frac{\eta(k/\sqrt{m})}{\sqrt{m}} + O\left(\frac{1}{g(m)\sqrt{m}}\right).$$

- Quantified Equidistribution: $I_\ell = \{\ell M, \dots, (\ell+1)M - 1\}$, $M = m^c$, $c < 1/2$

Sketch of the proof

- Failed Proof: lattices, bad errors.

- CLT: $(S_m - 2m)/\sqrt{2m} \to N(0,1)$:

$$\mathbb{P}\left(S_m - 2m = k\right) = \frac{\eta(k/\sqrt{m})}{\sqrt{m}} + O\left(\frac{1}{g(m)\sqrt{m}}\right).$$

- Quantified Equidistribution: $I_\ell = \{\ell M, \dots, (\ell+1)M - 1\}$, $M = m^c$, $c < 1/2$
$k_1, k_2 \in I_\ell$: $\left|\eta\left(\frac{k_1}{\sqrt{m}}\right) - \eta\left(\frac{k_2}{\sqrt{m}}\right)\right|$ small

Sketch of the proof

- Failed Proof: lattices, bad errors.

- CLT: $(S_m - 2m)/\sqrt{2m} \to N(0,1)$:

$$\mathbb{P}\left(S_m - 2m = k\right) = \frac{\eta(k/\sqrt{m})}{\sqrt{m}} + O\left(\frac{1}{g(m)\sqrt{m}}\right).$$

- Quantified Equidistribution: $I_\ell = \{\ell M, \dots, (\ell+1)M - 1\}$, $M = m^c$, $c < 1/2$
  $k_1, k_2 \in I_\ell$: $\left|\eta\left(\frac{k_1}{\sqrt{m}}\right) - \eta\left(\frac{k_2}{\sqrt{m}}\right)\right|$ small
  $C = \log_B 2$ of irrationality type $\kappa < \infty$:

$$\#\{k \in I_\ell : \overline{kC} \in [a,b]\} = M(b-a) + O(M^{1+\epsilon-1/\kappa}).$$

Irrationality Type

Irrationality type

α has irrationality type κ if κ is the supremum of all γ with

$$\underline{\lim}_{q\to\infty} q^{\gamma+1} \min_{p} \left|\alpha - \frac{p}{q}\right| = 0.$$

- Algebraic irrationals: type 1 (Roth's Thm).
- Theory of Linear Forms: $\log_B 2$ of finite type.

Linear Forms

Theorem (Baker)

$\alpha_1, \dots, \alpha_n$ algebraic numbers height $A_j \geq 4$, $\beta_1, \dots, \beta_n \in \mathbb{Q}$ with height at most $B \geq 4$,

$$\Lambda = \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n.$$

If $\Lambda \neq 0$ then $|\Lambda| > B^{-C\Omega \log \Omega'}$, with $d = [\mathbb{Q}(\alpha_i, \beta_j) : \mathbb{Q}]$, $C = (16nd)^{200n}$, $\Omega = \prod_j \log A_j$, $\Omega' = \Omega / \log A_n$.

Gives $\log_{10} 2$ of finite type, with $\kappa < 1.2 \cdot 10^{602}$:

$$|\log_{10} 2 - p/q| = |q \log 2 - p \log 10| / q \log 10.$$

Quantified Equidistribution

Theorem (Erdös-Turan)

$$D_N = \frac{\sup_{[a,b]} |N(b-a) - \#\{n \le N : x_n \in [a,b]\}|}{N}$$

There is a C such that for all m:

$$D_N \le C \cdot \left(\frac{1}{m} + \sum_{h=1}^{m} \frac{1}{h} \left| \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i h x_n} \right| \right)$$

Proof of Erdös-Turan

Consider special case $x_n = n\alpha$, $\alpha \notin \mathbb{Q}$.

- Exponential sum $\le \frac{1}{|\sin(\pi h\alpha)|} \le \frac{1}{2||h\alpha||}$.
- Must control $\sum_{h=1}^{m} \frac{1}{h||h\alpha||}$, see irrationality type enter.
- type κ, $\sum_{h=1}^{m} \frac{1}{h||h\alpha||} = O\left(m^{\kappa-1+\epsilon}\right)$, take $m = \lfloor N^{1/\kappa} \rfloor$.

$3x+1$ Data: random 10,000 digit number, $2^k || 3x+1$

80,514 iterations ($(4/3)^n = a_0$ predicts 80,319); $\chi^2 = 13.5$ (5% 15.5).

Digit	Number	Observed	Benford
1	24251	0.301	0.301
2	14156	0.176	0.176
3	10227	0.127	0.125
4	7931	0.099	0.097
5	6359	0.079	0.079
6	5372	0.067	0.067
7	4476	0.056	0.058
8	4092	0.051	0.051
9	3650	0.045	0.046

$3x + 1$ Data: random 10,000 digit number, $2|3x + 1$

241,344 iterations, $\chi^2 = 11.4$ (5% 15.5).

Digit	Number	Observed	Benford
1	72924	0.302	0.301
2	42357	0.176	0.176
3	30201	0.125	0.125
4	23507	0.097	0.097
5	18928	0.078	0.079
6	16296	0.068	0.067
7	13702	0.057	0.058
8	12356	0.051	0.051
9	11073	0.046	0.046

$5x+1$ Data: random 10,000 digit number, $2^k || 5x+1$

27,004 iterations, $\chi^2 = 1.8$ (5% 15.5).

Digit	Number	Observed	Benford
1	8154	0.302	0.301
2	4770	0.177	0.176
3	3405	0.126	0.125
4	2634	0.098	0.097
5	2105	0.078	0.079
6	1787	0.066	0.067
7	1568	0.058	0.058
8	1357	0.050	0.051
9	1224	0.045	0.046

$5x+1$ Data: random 10,000 digit number, $2|5x+1$

241,344 iterations, $\chi^2 = 3 \cdot 10^{-4}$ (5% 15.5).

Digit	Number	Observed	Benford
1	72652	0.301	0.301
2	42499	0.176	0.176
3	30153	0.125	0.125
4	23388	0.097	0.097
5	19110	0.079	0.079
6	16159	0.067	0.067
7	13995	0.058	0.058
8	12345	0.051	0.051
9	11043	0.046	0.046

Products and Chains of Random Variables

Preliminaries

- $X_1 \cdots X_n \Leftrightarrow Y_1 + \cdots + Y_n \bmod 1$, $Y_i = \log_B X_i$
- Density Y_i is g_i, density $Y_i + Y_j$ is

$$(g_i * g_j)(y) \;=\; \int_0^1 g_i(t) g_j(y-t) dt.$$

- $h_n = g_1 * \cdots * g_n$, $\widehat{g}(\xi) = \widehat{g}_1(\xi) \cdots \widehat{g}_n(\xi)$.
- Dirac delta functional: $\int \delta_\alpha(y) g(y) dy = g(\alpha)$.

Fourier input

- Fejér kernel:

$$F_N(x) = \sum_{n=-N}^{N} \left(1 - \frac{|n|}{N}\right) e^{2\pi i n x}.$$

- Fejér series: $T_N f(x) =$

$$(f * F_N)(x) = \sum_{n=-N}^{N} \left(1 - \frac{|n|}{N}\right) \widehat{f}(n) e^{2\pi i n x}.$$

- Lebesgue's Theorem: $f \in L^1([0,1])$. As $N \to \infty$, $T_N f$ converges to f in $L^1([0,1])$.
- $T_N(f * g) = (T_N f) * g$: convolution assoc.

Modulo 1 Central Limit Theorem

Theorem (M– and Nigrini 2007)

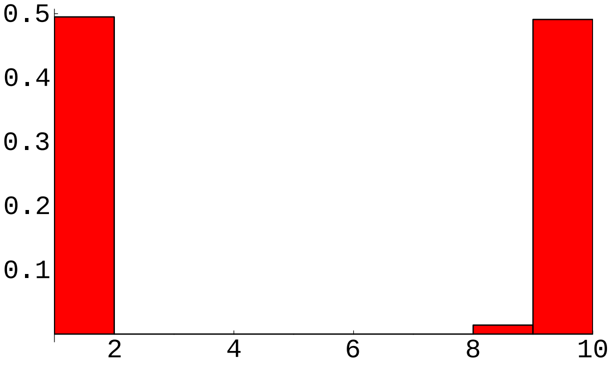
$\{Y_m\}$ independent continuous random variables on $[0,1)$ (not necc. i.i.d.), densities $\{g_m\}$. $Y_1 + \cdots + Y_M \bmod 1$ converges to the uniform distribution as $M \to \infty$ in $L^1([0,1])$ iff $\forall n \neq 0$, $\lim_{M\to\infty} \widehat{g_1}(n)\cdots\widehat{g_M}(n) = 0$.

Generalizations

- Levy proved for i.i.d.r.v. just one year after Benford's paper.
- Generalized to other compact groups, with estimates on the rate of convergence.
  ⋄ Stromberg: n-fold convolution of a regular probability measure on a compact Hausdorff group G converges to normalized Haar measure in weak-star topology iff support of the distribution not contained in a coset of a proper normal closed subgroup of G.

Non-Benford Product

Distribution of digits (base 10) of 1000 products $X_1 \cdots X_{1000}$, where $g_{10,m} = \phi_{11^m}$.
$\phi_m(x) = m$ if $|x - 1/8| \leq 1/2m$ (0 otherwise).



Proof of Modulo 1 CLT

- Density of sum is $h_\ell = g_1 * \cdots * g_\ell$.
- Suffices show $\forall\epsilon$:
$\lim_{M\to\infty}\int_0^1 |h_M(x) - 1|dx < \epsilon$.
- Lebesgue's Theorem: N large,
$||h_1 - T_N h_1||_1 =$

$$\int_0^1 |h_1(x) - T_N h_1(x)|dx < \frac{\epsilon}{2}.$$

- Claim: above holds for h_M for all M.

Proof of Modulo 1 CLT

Show $\lim_{M\to\infty} ||h_M - 1||_1 = 0$.
Triangle inequality:

$$||h_M - 1||_1 \leq ||h_M - T_N h_M||_1 + ||T_N h_M - 1||_1.$$

Choices of N and ϵ:

$$||h_M - T_N h_M||_1 < \epsilon/2.$$

Show $||T_N h_M - 1||_1 < \epsilon/2$.

Proof of Modulo 1 CLT

$$||T_N h_M - 1||_1 = \int_0^1 \left| \sum_{\substack{n=-N \\ n\neq 0}}^{N} \left(1 - \frac{|n|}{N}\right) \widehat{h_M}(n) e^{2\pi i n x} \right| dx$$

$$\leq \sum_{\substack{n=-N \\ n\neq 0}}^{N} \left(1 - \frac{|n|}{N}\right) |\widehat{h_M}(n)|$$

$\widehat{h_M}(n) = \widehat{g_1}(n) \cdots \widehat{g_M}(n) \longrightarrow_{M\to\infty} 0.$
For fixed N and ϵ, choose M large so that $|\widehat{h_M}(n)| < \epsilon/4N$ whenever $n \neq 0$ and $|n| \leq N$.

Conditions for Chains of Random Variables

Conditions

- $\{\mathcal{D}_i(\theta)\}_{i\in I}$: one-parameter distributions, densities $f_{\mathcal{D}_i(\theta)}$ on $[0,\infty)$.
- $p:\mathbb{N}\to I$, $X_1 \sim \mathcal{D}_{p(1)}(1)$, $X_m \sim \mathcal{D}_{p(m)}(X_{m-1})$.
- $m \geq 2$, $f_m(x_m) =$

$$\int_0^\infty f_{\mathcal{D}_{p(m)}(1)}\left(\frac{x_m}{x_{m-1}}\right) f_{m-1}(x_{m-1})\frac{dx_{m-1}}{x_{m-1}}$$

-

$$\lim_{n\to\infty} \sum_{\substack{\ell=-\infty \\ \ell\neq 0}}^{\infty} \prod_{m=1}^{n} (\mathcal{M}f_{\mathcal{D}_{p(m)}(1)})\left(1-\frac{2\pi i \ell}{\log B}\right) = 0$$

Behavior of Chains of Random Variables

Theorem (JKKKM)

- *If conditions hold, as $n \to \infty$ the distribution of leading digits of X_n tends to Benford's law.*
- *The error is a nice function of the Mellin transforms: if $Y_n = \log_B X_n$, then*

$$\left|\mathrm{Prob}(Y_n \bmod 1 \in [a,b]) - (b+a)\right| \le$$

$$\left|(b-a) \cdot \sum_{\substack{\ell=-\infty \\ \ell \neq 0}}^{\infty} \prod_{m=1}^{n} \left(\mathcal{M}f_{\mathcal{D}_{p(m)}}(1)\right)\left(1 - \frac{2\pi i \ell}{\log B}\right)\right|$$

Example: All $X_i \sim \mathrm{Unif}(0, k)$

- $X_i \sim \mathrm{Unif}(0, k)$: without loss of generality $k \in [1, 10)$.
- $P_n(s) = \mathrm{Prob}(M_{10}(\Xi_n) \le s)$.
- $|P_n(s) - \log_{10}(s)| \le$

$$\frac{k}{s} \frac{(\log k)^{n-1}}{\Gamma(n)} + \left(\frac{1}{2.9^n} + \frac{\zeta(n) - 1}{2.7^n}\right) 2 \log_{10} s.$$

Example: All $X_i \sim \mathrm{Exp}(1)$

- $X_i \sim \mathrm{Exp}(1)$, $Y_n = \log_B \Xi_n$.
- Needed ingredients:
  - ◇ $\int_0^\infty \exp(-x) x^{s-1} dx = \Gamma(s)$.
  - ◇ $|\Gamma(1+ix)| = \sqrt{\pi x / \sinh(\pi x)}, x \in \mathbb{R}$.
- $|P_n(s) - \log_{10}(s)| \le$

$$\log_B s \sum_{\ell=1}^{\infty} \left(\frac{2\pi^2 \ell / \log B}{\sinh(2\pi^2 \ell / \log B)} \right)^{n/2}.$$

Example: All $X_i \sim \mathrm{Exp}(1)$ (continued)

Bounds on the error

- $|P_n(s) - \log_{10} s| \le$
  - $3.3 \cdot 10^{-3} \log_B s$ if $n = 2$,
  - $1.9 \cdot 10^{-4} \log_B s$ if $n = 3$,
  - $1.1 \cdot 10^{-5} \log_B s$ if $n = 5$, and
  - $3.6 \cdot 10^{-13} \log_B s$ if $n = 10$.
- Error at most

$$\log_{10} s \sum_{\ell=1}^{\infty} \left(\frac{17.148\ell}{\exp(8.5726\ell)} \right)^{n/2} \le .057^n \log_{10} s$$

More Sums Than Difference Sets

Statement

A finite set of integers, $|A|$ its size. Form

- Sumset: $A + A = \{a_i + a_j : a_j, a_j \in A\}$.
- Difference set: $A - A = \{a_i - a_j : a_j, a_j \in A\}$.

Definition

We say A is difference dominated if $|A - A| > |A + A|$, balanced if $|A - A| = |A + A|$ and sum dominated (or an MSTD set) if $|A + A| > |A - A|$.

Questions

Expect generic set to be difference dominated:

- addition is commutative, subtraction isn't:
- Generic pair (x, y) gives 1 sum, 2 differences.

Questions

- Do there exist sum-dominated sets?
- If yes, how many?

Examples

- Conway: $\{0, 2, 3, 4, 7, 11, 12, 14\}$.
- Marica (1969): $\{0, 1, 2, 4, 7, 8, 12, 14, 15\}$.
- Freiman and Pigarev (1973): $\{0, 1, 2, 4, 5, 9, 12, 13, 14, 16, 17, 21, 24, 25, 26, 28, 29\}$.
- Computer search: random subsets of $\{1, \dots, 100\}$:
$\{2, 6, 7, 9, 13, 14, 16, 18, 19, 22, 23, 25, 30, 31, 33, 37, 39, 41, 42, 45, 46, 47, 48, 49, 51, 52, 54, 57, 58, 59, 61, 64, 65, 66, 67, 68, 72, 73, 74, 75, 81, 83, 84, 87, 88, 91, 93, 94, 95, 98, 100\}$.

Binomial model

Binomial model, parameter $p(n)$

Each $k \in \{0, \dots, n\}$ is in A with probability $p(n)$.

Consider uniform model ($p(n) = 1/2$):

- Let $A \in \{0, \dots, n\}$. Most elements in $\{0, \dots, 2n\}$ in $A + A$ and in $\{-n, \dots, n\}$ in $A - A$.
- $\mathbb{E}[|A + A|] = 2n - 11$, $\mathbb{E}[|A - A|] = 2n - 7$.

Martin and O'Bryant '06

Theorem

A from $\{0,\dots,N\}$ by binomial model with constant parameter p (so $k \in A$ with probability p). At least $k_{\mathrm{SD};p} 2^{N+1}$ subsets are sum dominated.

- $k_{\mathrm{SD};1/2} \geq 10^{-7}$, expect about 10^{-3}.

- Proof ($p = 1/2$): Generically $|A| = \frac{N}{2} + O(\sqrt{N})$.
  ⋄ about $\frac{N}{4} - \frac{|N-k|}{4}$ ways write $k \in A + A$.
  ⋄ about $\frac{N}{4} - \frac{|k|}{4}$ ways write $k \in A - A$.

Notation

- $X \sim f(N)$ means $\forall \epsilon_1, \epsilon_2 > 0$, $\exists N_{\epsilon_1,\epsilon_2}$ st $\forall N \geq N_{\epsilon_1,\epsilon_2}$

$$\text{Prob}\left(X \notin [(1-\epsilon_1)f(N), (1+\epsilon_1)f(N)]\right) \ < \ \epsilon_2.$$

- $\mathcal{S} = |A+A|$, $\mathcal{D} = |A-A|$,
  $\mathcal{S}^c = 2N+1-\mathcal{S}$, $\mathcal{D}^c = 2N+1-\mathcal{D}$.

New model: Binomial with parameter $p(N)$:

- $1/N = o(p(N))$ and $p(N) = o(1)$;
- $\text{Prob}(k \in A) = p(N)$.

Conjecture (Martin-O'Bryant)

As $N \to \infty$, A is a.s. difference dominated.

Main Result

Theorem (Hegarty-Miller)

$p(N)$ as above, $g(x) = 2\frac{e^{-x}-(1-x)}{x}$.

- $p(N) = o(N^{-1/2})$: $\mathcal{D} \sim 2\mathcal{S} \sim (Np(N))^2$;
- $p(N) = cN^{-1/2}$: $\mathcal{D} \sim g(c^2)N$, $\mathcal{S} \sim g\left(\frac{c^2}{2}\right)N$ ($c \to 0$, $\mathcal{D}/\mathcal{S} \to 2$; $c \to \infty$, $\mathcal{D}/\mathcal{S} \to 1$);
- $N^{-1/2} = o(p(N))$: $\mathcal{S}^c \sim 2\mathcal{D}^c \sim 4/p(N)^2$.

Can generalize to binary linear forms, still have critical threshold.

Inputs

Key input: recent strong concentration results of Kim and Vu (Applications: combinatorial number theory, random graphs, ...).

Example (Chernoff): t_i iid binary random variables, $Y = \sum_{i=1}^{n} t_i$, then

$$\forall \lambda > 0 : \ \text{Prob}\left(|Y - \mathbb{E}[Y]| \geq \sqrt{\lambda n}\right) \ \leq \ 2e^{-\lambda/2}.$$

Need to allow dependent random variables.
Sketch of proofs: $\mathcal{X} \in \{\mathcal{S}, \mathcal{D}, \mathcal{S}^c, \mathcal{D}^c\}$.

1. Prove $\mathbb{E}[\mathcal{X}]$ behaves asymptotically as claimed;
2. Prove $\mathcal{X}$ is strongly concentrated about mean.

Setup for Proofs

Note: only need strong concentration for $N^{-1/2} = o(p(N))$.

Setup for Proofs

Note: only need strong concentration for $N^{-1/2} = o(p(N))$.

Will assume $p(N) = o(N^{-1/2})$ as proofs are elementary (i.e., Chebyshev: $\text{Prob}(|Y - \mathbb{E}[Y]| \geq k\sigma_Y) \leq 1/k^2$)).

Setup for Proofs

Note: only need strong concentration for $N^{-1/2} = o(p(N))$.

Will assume $p(N) = o(N^{-1/2})$ as proofs are elementary (i.e., Chebyshev: $\text{Prob}(|Y - \mathbb{E}[Y]| \geq k\sigma_Y) \leq 1/k^2$)).

For convenience let $p(N) = N^{-\delta}$, $\delta \in (1/2, 1)$.

IID binary indicator variables:

$$X_{n;N} = \begin{cases} 1 & \text{with probability } N^{-\delta} \\ 0 & \text{with probability } 1 - N^{-\delta}. \end{cases}$$

$X = \sum_{i=1}^{N} X_{n;N}$, $\mathbb{E}[X] = N^{1-\delta}$.

Proof

Lemma

$P_1(N) = 4N^{-(1-\delta)}$, $\mathcal{O} = \#\{(m,n) : m < n \in \{1, \dots, N\} \bigcap A\}$.
With probability at least $1 - P_1(N)$ *have*

1. $X \in \left[\frac{1}{2}N^{1-\delta}, \frac{3}{2}N^{1-\delta}\right]$.
2. $\frac{\frac{1}{2}N^{1-\delta}(\frac{1}{2}N^{1-\delta}-1)}{2} \le \mathcal{O} \le \frac{\frac{3}{2}N^{1-\delta}(\frac{3}{2}N^{1-\delta}-1)}{2}$.

Proof

Lemma

$P_1(N) = 4N^{-(1-\delta)}$, $\mathcal{O} = \#\{(m,n) : m < n \in \{1,\dots,N\} \bigcap A\}$. With probability at least $1 - P_1(N)$ have

1. $X \in \left[\frac{1}{2}N^{1-\delta}, \frac{3}{2}N^{1-\delta}\right]$.
2. $\frac{\frac{1}{2}N^{1-\delta}(\frac{1}{2}N^{1-\delta}-1)}{2} \le \mathcal{O} \le \frac{\frac{3}{2}N^{1-\delta}(\frac{3}{2}N^{1-\delta}-1)}{2}$.

Proof:

- (1) is Chebyshev: $\mathrm{Var}(X) = N\mathrm{Var}(X_{n;N}) \le N^{1-\delta}$.
- (2) follows from (1) and $\binom{r}{2}$ ways to choose 2 from r.

Concentration

Lemma

- $f(\delta) = \min\left(\frac{1}{2}, \frac{3\delta-1}{2}\right)$, $g(\delta)$ *any function st* $0 < g(\delta) < f(\delta)$.
- $p(N) = N^{-\delta}$, $\delta \in (1/2, 1)$, $P_1(N) = 4N^{-(1-\delta)}$, $P_2(N) = CN^{-(f(\delta)-g(\delta))}$.

With probability at least $1 - P_1(N) - P_2(N)$ *have* $\mathcal{D}/\mathcal{S} = 2 + O(N^{-g(\delta)})$.

Concentration

Lemma

- $f(\delta) = \min\left(\frac{1}{2}, \frac{3\delta-1}{2}\right)$, $g(\delta)$ *any function st* $0 < g(\delta) < f(\delta)$.
- $p(N) = N^{-\delta}$, $\delta \in (1/2, 1)$, $P_1(N) = 4N^{-(1-\delta)}$, $P_2(N) = CN^{-(f(\delta)-g(\delta))}$.

With probability at least $1 - P_1(N) - P_2(N)$ *have* $\mathcal{D}/\mathcal{S} = 2 + O(N^{-g(\delta)})$.

Proof: Show $\mathcal{D} \sim 2\mathcal{O} + O(N^{3-4\delta})$, $\mathcal{S} \sim \mathcal{O} + O(N^{3-4\delta})$.

As $\mathcal{O}$ is of size $N^{2-2\delta}$ with high probability, need $2 - 2\delta > 3 - 4\delta$ or $\delta > 1/2$.

Analysis of $\mathcal{D}$

Contribution from ‘diagonal’ terms lower order, ignore.

Analysis of $\mathcal{D}$

Contribution from ‘diagonal’ terms lower order, ignore.

Difficulty: (m, n) and (m', n') could yield same differences.

Analysis of $\mathcal{D}$

Contribution from ‘diagonal’ terms lower order, ignore.

Difficulty: (m, n) and (m', n') could yield same differences.

Notation: $m < n$, $m' < n'$, $m \le m'$,

$$Y_{m,n,m',n'} = \begin{cases} 1 & \text{if } n - m = n' - m' \\ 0 & \text{otherwise.} \end{cases}$$

Analysis of $\mathcal{D}$

Contribution from ‘diagonal’ terms lower order, ignore.

Difficulty: (m, n) and (m', n') could yield same differences.

Notation: $m < n$, $m' < n'$, $m \leq m'$,

$$Y_{m,n,m',n'} = \begin{cases} 1 & \text{if } n - m = n' - m' \\ 0 & \text{otherwise.} \end{cases}$$

$\mathbb{E}[Y] \leq N^3 \cdot N^{-4\delta} + N^2 \cdot N^{-3\delta} \leq 2N^{3-4\delta}$. As $\delta > 1/2$,
Expected number bad pairs $\lll |\mathcal{O}|$.

Analysis of $\mathcal{D}$

Contribution from 'diagonal' terms lower order, ignore.

Difficulty: (m,n) and (m',n') could yield same differences.

Notation: $m < n$, $m' < n'$, $m \le m'$,

$$Y_{m,n,m',n'} \;=\; \begin{cases} 1 & \text{if } n-m = n'-m' \\ 0 & \text{otherwise.} \end{cases}$$

$\mathbb{E}[Y] \le N^3 \cdot N^{-4\delta} + N^2 \cdot N^{-3\delta} \le 2N^{3-4\delta}$. As $\delta > 1/2$,
Expected number bad pairs $\lll |\mathcal{O}|$.

Claim: $\sigma_Y \le N^{r(\delta)}$with $r(\delta) = \frac{1}{2}\max(3-4\delta, 5-7\delta)$. This and Chebyshev conclude proof of theorem.

Proof of claim

Cannot use CLT as $Y_{m,n,m',n'}$ are not independent.

Proof of claim

Cannot use CLT as $Y_{m,n,m',n'}$ are not independent.

Use $\mathrm{Var}(U+V) \le 2\mathrm{Var}(U) + 2\mathrm{Var}(V)$.

Proof of claim

Cannot use CLT as $Y_{m,n,m',n'}$ are not independent.

Use $\mathrm{Var}(U+V) \le 2\mathrm{Var}(U) + 2\mathrm{Var}(V)$.

Write

$$\sum Y_{m,n,m',n'} \;=\; \sum U_{m,n,m',n'} + \sum V_{m,n,n'}$$

with all indices distinct (at most one in common, if so must be $n = m'$).

$$\mathrm{Var}(U) = \sum \mathrm{Var}(U_{m,n,m',n'}) + 2 \sum_{\substack{(m,n,m',n') \neq \\ (\widetilde{m},\widetilde{n},\widetilde{m}',\widetilde{n}')}} \mathrm{CoVar}(U_{m,n,m',n'}, U_{\widetilde{m},\widetilde{n},\widetilde{m}',\widetilde{n}'}).$$

Analyzing $\mathrm{Var}(U_{m,n,m',n'})$

At most N^3 tuples.

Each has variance $N^{-4\delta} - N^{-8\delta} \le N^{-4\delta}$.

Thus $\sum \mathrm{Var}(U_{m,n,m',n'}) \le N^{3-4\delta}$.

Analyzing $\mathrm{CoVar}(U_{m,n,m',n'}, U_{\widetilde{m},\widetilde{n},\widetilde{m}',\widetilde{n}'})$

- All 8 indices distinct: independent, covariance of 0.
- 7 indices distinct: At most N^3 choices for first tuple, at most N^2 for second, get

$$\mathbb{E}[U_{(1)}U_{(2)}] - \mathbb{E}[U_{(1)}]\mathbb{E}[U_{(2)}] = N^{-7\delta} - N^{-4\delta}N^{-4\delta} \leq N^{-7\delta}.$$

- Argue similarly for rest, get $\ll N^{5-7\delta} + N^{3-4\delta}$.