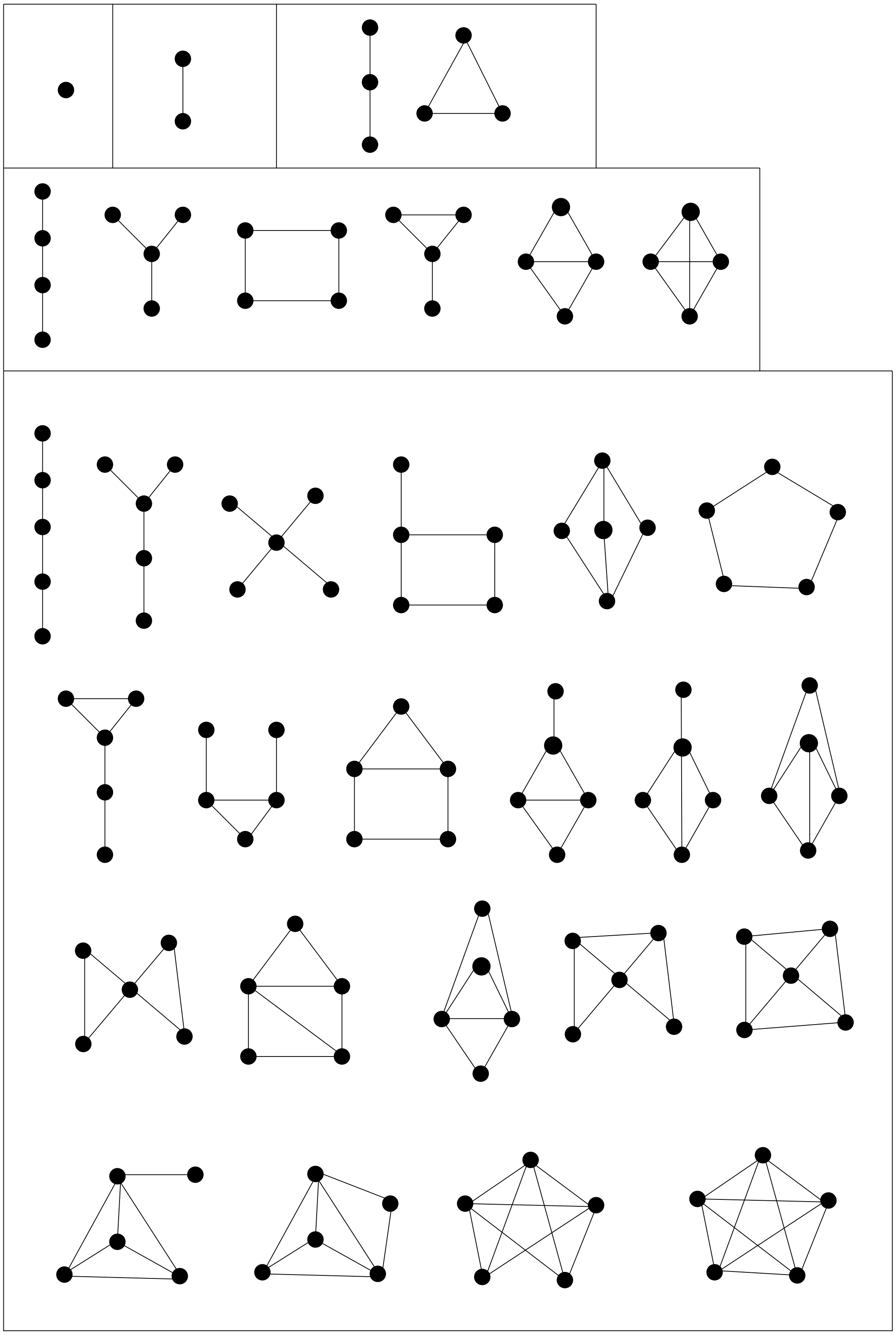
Number Theoretic Density

and Logical Limit Laws

Stanley Burris

Pure Mathematics Analysis Seminar

October 19, 2001



How to Count Graphs

Every graph is uniquely a disjoint union of connected graphs (**Unique Decomposition Property**)

$p(n)$ = # of connected graphs on n vertices
$a(n)$ = # of graphs on n vertices

n	1	2	3	4	5	6	7	8	9
$p(n)$	1	1	2	6	21	112	853	11117	261080
$a(n)$	1	2	4	11	34	156	1044	12346	274668

Polya used the Frobenius-Burnside formula

$$a(n) = \frac{1}{n!} \sum_{\pi \in S_n} \mathrm{Fix}(\pi)$$

to count graphs.

In particular he showed that the proportion of graphs on n vertices that have only one automorphism (the identity map) tends to 1 as $n \to \infty$.

We prefer to use the **Fundamental Identity**:

$$\sum_{n\geq 0} a(n)x^n \;=\; \prod_{n\geq 1}(1-x^n)^{-p(n)}.$$

For graphs this is only a **formal identity** since the radius of convergence is 0.

Such identities are often referred to as **weighted partition identities**.

Hardy and **Ramanujan** analyzed this when $p(n)=1$, for all n. Then $a(n)$ is the number of partitions of n, and they proved (1918)

$$a(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}.$$

Some Asymptotic Density results in Graphs:

• Prob(*connected*) = 1.

$\star$ Prob(*2-connected*) = 1.

• **[Polya]** Prob(*rigid*) = 1.
Thus, for graphs,

$$a(n) \;\sim\; p(n) \;\sim\; \frac{2^{n(n-1)/2}}{n!}$$

• Prob(*Hamiltonian*) = 1.

$\star$ Prob(*Triangle Free*) = 0.

$\star\star$ **[Fagin; Glebskii, et al]** For φ first-order

$$\boxed{\text{Prob}(\ \varphi\ \textit{holds}) \in \{0,1\}.}$$

Finite Abelian Groups

The **indecomposables** are the cyclic groups $(Z_{q^k}, +)$, where q is a prime.

$p(n) = \#$ of indecomposables of order n
$a(n) = \#$ of order n.

$$p(n) \;=\; \begin{cases} 1 \text{ if } n = q^k \\ 0 \text{ else} \end{cases}$$

$$a(q_1^{e_1} \cdots q_k^{e_k}) \;=\; \#\text{part}(e_1) \cdots \text{part}(e_k).$$

Since finite Abelian groups have the **Unique Factorization Property** we can express the relation between the $a(n)$ and $p(n)$ by an identity.

The **Fundamental Identity** is

$$\sum_{n\geq 1} a(n)n^{-x} \;=\; \prod_{n\geq 2}(1-n^{-x})^{-p(n)}.$$

The left side is the ζ **function** for Abelian groups, the right side the **Euler product** for Abelian groups.

Euler looked at the identity

$$\sum_{n\geq 1}\frac{1}{n^x} \;=\; \prod_{q \text{ prime}}(1-q^{-x})^{-1}.$$

For multiplicative systems we prefer **global counts**

$$\begin{aligned} P(x) &= \sum_{j\leq x} p(j) \\ A(x) &= \sum_{j\leq x} a(j). \end{aligned}$$

[Erdös and Szekeres 1934]

$$A(x) \sim Cx, \qquad C = \prod_{k \geq 2} \zeta(k) \approx 2.295.$$

[Compton] For φ a first-order sentence about Abelian groups one has (using global counts):

> Prob(φ *holds*) always exists (but need not be 0 or 1).

Example: The probability that an Abelian group has odd order is given by

$$\prod_{k \geq 1} (1 - 2^{-k}) \approx 0.29.$$

The Additive and Multiplicative Cases

Additive	Multiplicative
$\|\mathbf{A} \cup \mathbf{B}\| = \|\mathbf{A}\| + \|\mathbf{B}\|$	$\|\mathbf{A} \times \mathbf{B}\| = \|\mathbf{A}\| \cdot \|\mathbf{B}\|$

One can think of $\mathcal{K}$ as a generalized number system.

Beurling (1937) — generalized prime number theorems, extending Landau's work (1903) on integral ideals of the integers of an algebraic number field.

Bateman and Diamond (1969) — article on Beurling's work for the MAA.

Knopfmacher (1975) — more conditions for prime number theorems; emphasis on algebraic systems, e.g., abelian groups.

Abstract Number Systems

Additive	Multiplicative
$(\mathsf{A}, \mathsf{P}, +, 0, \\| \ \\|)$	$(\mathsf{A}, \mathsf{P}, \cdot, 1, \\| \ \\|)$

A = the set of abstract numbers

P = the set of indecomposable numbers

$\\| \ \\|$ is additive	$\\| \ \\|$ is multiplicative
Local Density	Global Density

of a subset B of A

$$\delta(\mathsf{B}) \ = \ \lim_{n\to\infty} \frac{b(n)}{a(n)} \qquad \Delta(\mathsf{B}) \ = \ \lim_{x\to\infty} \frac{B(x)}{A(x)}$$

Goal: Find conditions to guarantee

$(\star)$ $\boxed{\textbf{partition sets } \mathsf{B} \text{ have asymptotic density.}}$

What is a Partition Set?

Let $\mathsf{P}_1, \ldots, \mathsf{P}_k$ be a partition of the set P of indecomposables into finitely may sets.

Let γ_i be in one of the forms

$$\gamma_i \;=\; m_i \qquad \gamma_i \;=\; (\leq m_i) \qquad \gamma_i \;=\; (\geq m_i).$$

Then a subset B of the form

$$\mathsf{P}_1^{\gamma_1} \cdots \mathsf{P}_k^{\gamma_k}$$

is a partition set.

In other words, B consists of all elements of A which have exactly

γ_1 indecomposables from P_1,
...
γ_k indecomposables from P_k.

Example from Graphs:

Let $\mathsf{P}_1 \;=\; \{$triangle free connected graphs$\}$.

Let P_2 be the other connected graphs.

Then $\boxed{\mathsf{B} \;=\; (\geq 0)\mathsf{P}_1 + 0\mathsf{P}_2}$

is the collection of **triangle-free graphs**.

Example from Abelian Groups:

Let $\mathsf{P}_1 \;=\; \{Z_{2^k} : k \geq 1\}$.

Let $\mathsf{P}_2 \;=\; \{Z_{q^k} : q$ is an odd prime, $k \geq 1\}$.

Then $\boxed{\mathsf{B} \;=\; \mathsf{P}_1^0 \cdot \mathsf{P}_2^{\geq 0}}$

is the collection of **Abelian groups of odd order**.

Where does Logic fit in?

Suppose we are given a class of structures satisfying the Fundamental Identity.

Theorem

The subcollection of structures satisfying a sentence φ can be expressed as a disjoint union of finitely many partition sets.

Corollary

(a) If every partition set has asymptotic density then one has a **limit law** for the class, that is, the probability that any sentence φ holds will exist.

(b) If every partition set has asymptotic density equal to 0 or 1 then one has a **zero-one law** for the class, that is, the probability that any sentence φ holds will exist and be either 0 or 1.

Ratio Test and Regular Variation at Infinity

Definition A sequence $s(n)$ is in RT_ρ if it is eventually positive and

$$\lim_{n\to\infty} \frac{s(n-1)}{s(n)} = \rho.$$

Definition A function $S(x)$ is in RV_α if it is eventually defined, eventually positive and

$$\lim_{t\to\infty} \frac{S(tx)}{S(t)} = x^\alpha$$

for $x > 0$.

A function in RV_0 is *slowly varying at infinity*.

Behavior of Monotone Functions

Let $h : (0, \infty) \longrightarrow [0, \infty)$ be monotone nondecreasing, eventually positive. Then one of the following nonoverlapping cases must hold:

(1) $h(x)$ has regular variation at infinity with index $\alpha \geq 0$.

(2) $\lim_{t\to\infty} \dfrac{h(tx)}{h(t)}$ is defined only on a discrete subgroup of the positive reals.

(3) For some $c > 1$

$$\lim_{t\to\infty} \frac{h(tx)}{h(t)} = \begin{cases} 0 & \text{if } 0 < x < 1/c \\ \infty & \text{if } c < x. \end{cases}$$

Results

RT_1 implies 0-1 law.	RV_0 implies 0-1 law.
(*) implies RT_ρ.	(*) implies discrete or RV_α.
(*) implies $\delta(P) = 0$.	(*) implies $\Delta(P) = 0$.
[Bell] (Old Conj) $\delta(\mathsf{P}) = 0$ implies $\begin{cases} \rho > 0 \text{ and} \\ \mathbf{A}(\rho) = \infty. \end{cases}$	**[Warlimont]** (Conj I) $\Delta(\mathsf{P}) = 0$ implies $\begin{cases} \alpha < \infty \\ \mathbf{A}(\alpha) = \infty. \end{cases}$
[Bell] (Old Conj) $p(n) \in \mathsf{RT}_1$ implies $a(n) \in \mathsf{RT}_1$	**[Bell]** (Conj II) $P(x) \in \mathsf{RV}_0$ implies $A(x) \in \mathsf{RV}_0$

[Compton]

If $a(n) \in \mathsf{RT}_\rho$ and

$$\frac{a(n-m)}{a(n)} \le C\rho^m$$

for $K \le m \le n$

then $(\star)$ holds.

[Sárközy]

If $A(x) \in \mathsf{RV}_\alpha$ and

$$\frac{A(x/m)}{A(x)} \le Cm^{-\alpha}$$

for $K \le m \le n$

then $(\star)$ holds.

[Bell]

If $p(n) \in \mathsf{RT}_\rho$ and

$$\limsup_{n\to\infty} np(n)\rho^n > 1$$

then $(\star)$ holds.

[Bell] (Conj III)

If

$$P(x) \sim x^\alpha P_0(x)/\log x,$$

$P_0(x) \in \mathsf{RV}_\alpha$, eventually increasing and

$$\lim_{x\to\infty} P_0(x) \in (1/\alpha, \infty)$$

then $(\star)$ holds.

Cayley and Sylvester (1850's), Schur

Suppose there are only finitely many indecomposables in a class $\mathcal{K}$ satisfying the additive fundamental identity.

Let $r = \sum p(n)$, the number of indecomposables.

Using partial fractions in $\mathbf{C}(x)$ one can show

$$a(n) \sim Cn^{r-1}$$

From this it easily follows that $a(n) \in \mathsf{RT}_1$.

(More additive results)

Bateman and Erdös (1956)

Using elementary but clever arguments, they show that if $p(n) \leq 1$ for all n then $a(n) \in \mathsf{RT}_1$.

Jason Bell (TAMS, to appear)

If $p(n)$ is polynomially bounded then $a(n) \in \mathsf{RT}_1$.

Thus a class $\mathcal{K}$ satisfying the additive fundamental identity with a polynomially bounded number of indecomposables of each size has a 0-1 law.

Tools:

Dirichlet Density

Dirichlet density is an alternative definition of density that is much easier to work with:

$$\partial(\mathsf{B}) \;=\; \lim_{x\to\rho}\frac{\mathbf{B}(x)}{\mathbf{A}(x)} \qquad \partial(\mathsf{B}) \;=\; \lim_{x\to\alpha}\frac{\mathbf{B}(x)}{\mathbf{A}(x)}.$$

Of course we need $\rho > 0$, resp. $\alpha < \infty$.

This definition is motivated by Dirichlet's 'Dirichlet Density' of the primes in an arithmetic progression $an + b$, namely they should comprise $1/\phi(a)$ of the primes.

Theorem

All partition sets have Dirichlet density.

Dirichlet density extends the asymptotic density — provided the generating series of the number system diverges at the endpoint of the region of convergence.

Theorem

If $\mathbf{A}(\rho) = \infty$ then	If $\mathbf{A}(\alpha) = \infty$ then
$\delta \subseteq \partial.$	$\mathbf{\Delta} \subseteq \partial.$

So we want **Tauberian Theorems** to go from Dirichlet density to asymptotic density.

Schur's Theorem

[Schur 1918]

If

- $\mathbf{R}(x) = \mathbf{S}(x)\mathbf{T}(x)$
- $t(n) \in \mathsf{RT}_\rho$
- $\rho_s > \rho$

then

$$\lim_{n\to\infty} \frac{r(n)}{t(n)} \;=\; \lim_{x\to\rho} \frac{\mathbf{R}(x)}{\mathbf{T}(x)}.$$

[Burris/Yeats 2001]

If

- $\mathbf{R}(x) = \mathbf{S}(x)\mathbf{T}(x)$
- $T(x) \in \mathsf{RV}_\alpha$
- $\alpha_s < \alpha$

then

$$\lim_{x\to\infty} \frac{R(x)}{T(x)} \;=\; \lim_{x\to\alpha} \frac{\mathbf{R}(x)}{\mathbf{T}(x)}.$$

For example these can be used on

$$\mathbf{A}(x) \;=\; e^{\sum_{m\ge 1} \mathbf{P}(x^m)/m}$$

$$\mathbf{A}(x) \;=\; e^{\sum_{m\ge 1} \mathbf{P}(mx)/m}$$

to focus attention on the asymptotics of

$$e^{\mathbf{P}(x)}.$$

Problem

Does $\mathsf{RT}_\rho + \mathbf{A}(\rho) = \infty$ imply $(\star)$?

Problem

Does $\mathsf{RV}_\alpha + \mathbf{A}(\alpha) = \infty$ imply $(\star)$?

Cauchy Formula

$$a(n) = \frac{1}{2\pi i}\int_{\mathcal{C}} \frac{\mathbf{A}(z)}{z^{n+1}}dz$$

Perron Formula

$$A(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \mathbf{A}(z)\frac{x^z}{z}dz$$

2*Knopfmacher+ Warlimont

$$p(n) = a\beta^n + \mathrm{O}(\eta^n), \quad \eta < \beta$$

implies

$$a(n) \sim C\beta^n \frac{e^{2\sqrt{an}}}{n^{3/4}}$$

Oppenheim +

$$p(n) = an^\beta + \mathrm{O}(n^\eta), \quad \eta < \beta$$

implies

$$A(x) \sim Cx^{\beta+1}\frac{e^{2\sqrt{a\log x}}}{(\log x)^{3/4}}$$

Using Schur:

$$\begin{aligned}\mathbf{A}(x) &= e^{\sum_{m\geq 1}\mathbf{P}(x^m)/m}\\ &= e^{\mathbf{P}(x)}\cdot e^{\sum_{m\geq 2}\mathbf{P}(x^m)/m}\end{aligned}$$

to get

$$a(n) \sim C[x^n]e^{\mathbf{P}(x)}$$

where

$$C = e^{\sum_{m\geq 2}\mathbf{P}(\rho^m)/m}$$

Using Schur Analog:

$$\begin{aligned}\mathbf{A}(x) &= e^{\sum_{m\geq 1}\mathbf{P}(mx)/m}\\ &= e^{\mathbf{P}(x)}\cdot e^{\sum_{m\geq 2}\mathbf{P}(mx)/m}\end{aligned}$$

to get

$$A(x) \sim C(\sum_{n\leq x}[n^{-u}]e^{\mathbf{P}(u)}$$

where

$$C = e^{\sum_{m\geq 2}\mathbf{P}(m\alpha)/m}$$