Mathematical
Surveys
and
Monographs

Volume 86

# Number Theoretic Density and Logical Limit Laws

Stanley N. Burris

American Mathematical Society

# Contents

# Preface

In the late 1980s Kevin Compton published papers showing how to apply an analysis of the popular partition identities to obtain monadic second-order limit laws, including 0–1 laws, for numerous classes of graphs, posets, etc. I was fascinated by this work. When he gave a colloquium talk in the early 1990s in Waterloo on his recent work on a limit law for Abelian groups, the temptation to learn more about this subject was irresistible. This engaged a favorite area of my own research, algebraic structures.

Compton's papers can be somewhat opaque for specialists in combinatorics and number theory, as well as for specialists in logic, because of the intimate way he has woven these subjects together. After seeing the books [**29**], [**30**] of John Knopfmacher on abstract analytic number theory, it seemed worthwhile to separate Compton's treatment into two parts, one on density in number systems, and the other on the application of number theoretic density results to obtain logical limit laws. Each of these parts is of interest in its own right.

The reader will find a leisurely and detailed exposition of Compton's investigations, and closely related work of others, including recent contributions of Jason Bell, Edward Bender, Peter Cameron, Paweł Idziak, Arnold Knopfmacher, John Knopfmacher, Andrew Odlyzko, Bruce Richmond, András Sárközy, Cameron Stewart, Richard Warlimont, Alan Woods, and the author. The presentation is from the perspective of abstract number systems, in the spirit of John Knopfmacher's work in abstract analytic number theory.

This book has been used as an undergraduate special topics reading text at the University of Waterloo. Part 1, on Additive Number Systems, is completely accessible to an advanced undergraduate student. All chapters preceding Chapter 6 are devoted to number theoretic density, requiring only the usual undergraduate background in analysis, especially in power series, and an exposure to abstract mathematics. The well known ratio test plays a central role. The section on asymptotics, at the end of Chapter 5, uses basic complex analysis, including the Cauchy integral formula. Chapter 6 covers the logical aspects for Part 1. This chapter is self-contained so that one can work through it without prior exposure to logic. It features one of the most delightful tools of logic, the Ehrenfeucht-Fraissé games. (Having had a first course in logic, so that one is comfortable with first-order languages and structures, will no doubt make the chapter more rapid reading.)

Part 2, on Multiplicative Number Systems, offers the challenge and reward of becoming reasonably comfortable with Dirichlet series. The parallels with Part 1 show Dirichlet series as a natural companion of power series. Having worked through Part 1, one will be able to predict many of the results to be proved—the local density results of Part 1 seem, as if by magic, to reappear as global density results in Part 2. There is surely some deep connection between power series and Dirichlet series that we have not yet understood. The last chapter introduces the reader to the Feferman-Vaught Theorem, a favorite tool to analyze direct products, and Skolem's analysis of first-order sentences about Boolean algebras.

The reader will find all the material needed to thoroughly understand the method of Compton for proving logical limit laws. Above all, I think one will be delighted to see so many interesting tools from elementary mathematics pull together to help answer the question "What is the probability that a randomly chosen structure has a given property?"

Thanks go to Paweł Idziak for his contributions to the study of limit laws when I was first starting to work in the area, to Andrew Odlyzko for helping me understand what was going on with the Dirichlet series, to András Sárközy for helping develop the general multiplicative theory of limit laws during a visit to Waterloo, to Cameron Stewart for discussions of the ratio test, to Dejan Delic for help with proofreading an early draft of the book, to Bruce Richmond for helping me to locate and understand several relevant results from asymptotics, to John Knopfmacher for challenging me to take a harder look at what was going on with logical limit laws, to Richard Warlimont for a remarkable amount of beautifully handwritten correspondence regarding ways to improve the presentation, to Jason Bell for keeping me informed of his recent research in this area, and to Karen Yeats, a second year mathematics undergraduate at U. Waterloo who eagerly read the entire manuscript during the summer of 2000, giving me detailed feedback on how the text comes across to an undergraduate. Kevin Compton is, of course, the ultimate inspiration for this work, through his publications and his elegant lectures over the years.

Edward Dunne, Christine Thivierge and Elaine Becker of the AMS Book Program did everything possible to make the transition from manuscript to book a pleasant and trouble-free experience; and Barbara Beeton of the AMS Technical Support group was (as always!) able to solve all of my Tex related problems with the document.

Finally, I want to thank the Natural Sciences and Engineering Research Council of Canada for their long standing support of my investigations in universal algebra, logic, and computation, the support that has made it possible to write this book.

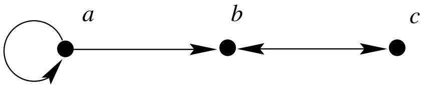
For errata and updates see www.thoralf.uwaterloo.ca.

Stanley Burris
Waterloo, 2000

# Overview

When studying a subject with a bewildering variety of specimens one hopes to discover simple structural patterns. This happened in the study of finite relational structures with the discovery of 0–1 laws in the mid 1970s.

A finite relational structure $\mathbf{S} = (S, R_1, \dots, R_n)$ is a set $S$ with a list of relations $R_1, \dots, R_n$ on $S$. The most popular relations $R$ are binary, that is, $R \subseteq S \times S$. But $R \subseteq S^k$, for any $k \geq 1$, is also permitted. For the purpose of this overview it suffices to consider relational structures $\mathbf{S} = (S, R)$ with a single binary relation. One can think of $R$ as a directed edge relation on the set of vertices $S$ and draw a picture, for example:



In this picture one sees that $aRa$, $aRb$, $bRc$, $cRb$. Such structures are *directed graphs.*

As specializations of directed graphs one has several well known classes. If the relation $R$ is irreflexive (not $aRa$, for any $a \in S$) and symmetric ($aRb \Rightarrow bRa$) one has a *graph.* If it is reflexive, symmetric and transitive, then one has an *equivalence relation.* And if it is reflexive, antisymmetric and transitive, then one has a *poset.* Finite (directed) graphs exhibit incredible diversity and have provided a rich source of examples and problems, from Euler's analysis of the Seven Bridges of Königsberg problem to the modern study of complexity in computer science. Indeed, the interest in finite structures has blossomed in tandem with the growth of theoretical computer science.

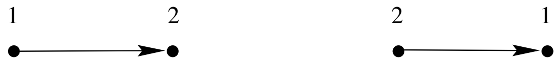
One of the fundamental questions is 'What can be said about a randomly chosen structure?' Consider a property $\mathcal{P}$ and a class $\mathcal{K}$ of finite structures. One can ask 'What is the probability that a finite structure chosen randomly from $\mathcal{K}$ satisfies $\mathcal{P}$?' The simplest and most natural definition of this probability is to let $p_n$ be the proportion of structures in $\mathcal{K}$ of size $n$ that have the property $\mathcal{P}$, and then to let the probability that $\mathcal{P}$ holds for a randomly chosen structure from $\mathcal{K}$ be the limit of $p_n$ as $n$ goes to infinity (whenever this limit exists). This probability is called *the asymptotic density* of the collection of structures in $\mathcal{K}$ that satisfy $\varphi$.

There is a problem with this definition if there are infinitely many $n$ such that $\mathcal{K}$ has no structures of size $n$, for then $p_n$ is infinitely often undefined.

This is handled by considering only those $p_n$ that are defined. With this understanding it turns out that the general theory is a minor variation of the theory where one assumes that the $p_n$ are eventually well-defined. So, for the purpose of this overview, it will be assumed that the classes $\mathcal{K}$ have structures of size $n$ for all $n$ greater than some $N$.

Glebskij, Logan, Liogonkij and Talanov (1969), and independently Fagin (1976), considered properties defined by first-order sentences. For example, the sentence $\forall x \exists y (xRy)$ says, in the case of finite graphs, that there are no isolated vertices; and the sentence $\forall x \forall y \big[(xRy) \rightarrow \exists z (xRz \wedge zRy)\big]$ says one can interpolate a vertex between adjacent vertices. For $\mathcal{K}$ the class of finite directed graphs, or the class of finite graphs, they showed, for any first-order sentence $\varphi$, that the probability of $\varphi$ holding is either 0 or 1. Hence [directed] graphs have a *first-order 0–1 law.* If the probability of a property holding in a class $\mathcal{K}$ is 1 then the property is *almost certainly true* in $\mathcal{K}$.

The method used to prove these results does not generalize readily. First the result is proved for *labeled structures*, using the set of vertices $\{1, \ldots, n\}$ for $n$-element structures. The following two directed graphs are identified when counting up to isomorphism, but are considered distinct when counting labeled structures:



When counting up to isomorphism one is said to be counting *unlabeled* structures.

To prove a 0–1 law for labeled structures, the original method is to understand the structures in $\mathcal{K}$ well enough to propose a basis $\Phi$ for the almost certainly true sentences. Then one proves that each member of $\Phi$ is indeed almost certainly true. Finally, to take a labeled 0–1 law back to the unlabeled case one needs to know that the property of being *rigid*[1] is almost certainly true in $\mathcal{K}$. Finding a basis $\Phi$, and proving that rigidity is almost certainly true, are both serious obstacles to extending the applications of this method. Compton was able to carry this out for *posets*, but there are precious few other examples.

In the 1980s an alternate approach to proving 0–1 laws was developed by Compton. By considering *adequate* classes $\mathcal{K}$ of finite structures, that is, classes closed under disjoint union and components, he was able to show that the single condition $a(n-1)/a(n) \rightarrow 1$ is sufficient for a first-order 0–1 law. Here $a(n)$ counts the total number of structures of size $n$ in $\mathcal{K}$ (counting up to isomorphism). This method does not apply to the original examples of graphs and directed graphs as these classes grow so rapidly that one has $a(n-1)/a(n) \rightarrow 0$. However, it is a beautiful technique that does apply to a truly wide range of slowly growing classes such as equivalence relations, permutations, linear forests, etc.

[1] A structure is rigid if the only automorphism is the identity map.

Furthermore, Compton's technique yields a 0–1 law for *monadic second-order logic.* This logic extends the well known first-order logic by allowing quantification over subsets—it is able to express far more properties than first-order logic. For example, in first-order logic one cannot say that a graph is *connected*, but in monadic second-order logic this is expressible by saying that 'if the domain is partitioned into two sets then it is always possible to find two vertices, one from each partition set, with an edge between them':

$$\forall U \forall V \Bigg[ \Big( \exists x (Ux) \wedge \exists y (Vy) \wedge \forall x \big( Ux \leftrightarrow \neg Vx \big) \Big) \\ \rightarrow \exists x \exists y \big( Ux \wedge Vy \wedge xRy \big) \Bigg].$$

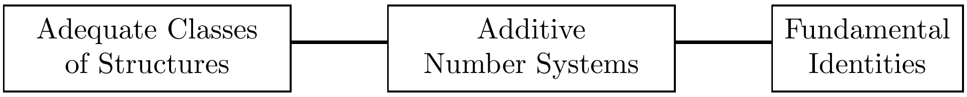
A considerable portion of the work in Compton's treatment is devoted to studying *Dirichlet density.* (This density is the limiting value of a quotient of two generating series.) He also uses the *fundamental identity*

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

that relates $a(n)$ to $p(n)$, where $p(n)$ is the number of *components* of size $n$ (counting up to isomorphism). On the surface, Dirichlet density appears to have little to do with the probability that a randomly chosen structure has a property, but under a natural hypothesis one can show that if the probability exists then so does the Dirichlet density, and they are equal. Thus Dirichlet density extends probability (defined as asymptotic density), and the main goal is to find theorems for a converse result that guarantees that if the Dirichlet density exists then it is the asymptotic density. Such converses are called Tauberian Theorems. For the development of the very large part of Compton's theory just described in this paragraph, one does not need the details of the relations involved in the individual structures, but rather just the additive number system associated with $\mathcal{K}$.

Consider the example of the class $\mathcal{K}$ of finite graphs. If one defines the sum of two finite graphs to be their disjoint union then, by identifying isomorphic graphs, one ends up with an additive number system $\mathcal{A}$. The graphs are the 'numbers' in this abstract system. The graph on the empty set gives the zero element of $\mathcal{A}$. The only information that is needed for the asymptotic work with additive number systems is the addition table for the elements and the 'size' (or *norm*) of a graph (defined as the number of vertices). The indecomposable elements, the nonzero elements that cannot be written as the sum of two nonzero elements, are precisely the connected graphs. Clearly every nonzero element of $\mathcal{A}$ can be expressed uniquely as a sum of indecomposable elements since every finite graph with a nonempty set of vertices is uniquely expressible as a disjoint union of connected graphs. The essential features of an additive number system are just the addition operation and the size function. The adjective 'additive' is derived from the fact that the size function $\|\mathsf{a}\|$ is additive, that is, $\|\mathsf{a}+\mathsf{b}\| = \|\mathsf{a}\| + \|\mathsf{b}\|$.

To simplify the presentation, additive number systems are interpolated between adequate classes of structures and the fundamental identities:



This interpolation allows one to separate the logical aspects from the number-theoretic aspects. Every adequate class gives rise to a (unique) additive number system, and every additive number system can be derived from (many) adequate classes; and each additive number system gives rise to a (unique) fundamental identity that essentially defines the number system.

Given an additive number system $\mathcal{A}$, subsets called *partition sets* play a crucial role in this work. A partition set has the form $\gamma_1\mathsf{P}_1 + \cdots + \gamma_k\mathsf{P}_k$, where $\mathsf{P}_1, \ldots, \mathsf{P}_k$ is a partition of the set $\mathsf{P}$ of indecomposable elements of $\mathcal{A}$, and where each of the $\gamma_i$ is in one of the three forms $(\geq m_i)$, $m_i$, $(\leq m_i)$. The elements of such a partition set are the members of $\mathcal{A}$ which can be written as a sum of $\gamma_1$ members of $\mathsf{P}_1$ plus ... plus $\gamma_k$ members of $\mathsf{P}_k$. (Repeats are allowed when counting elements.) Thus $1\mathsf{P}$ is just $\mathsf{P}$, and $(\geq 0)\mathsf{P}$ is the entire set of 'numbers' in $\mathcal{A}$. And if $\mathsf{P}_1, \mathsf{P}_2, \mathsf{P}_3$ is a partition of the set $\mathsf{P}$ of indecomposable elements of $\mathcal{A}$ then the partition set $(\leq 5)\mathsf{P}_1 + (\geq 4)\mathsf{P}_2 + 2\mathsf{P}_3$ is the set of elements which can be expressed as the sum of at most 5 elements from $\mathsf{P}_1$ plus the sum of at least 4 elements from $\mathsf{P}_2$ plus the sum of exactly 2 elements from $\mathsf{P}_3$.

Now, if $\mathcal{K}$ is an adequate class of structures and $\mathcal{A}$ the corresponding additive number system, then the members of $\mathcal{K}$ that satisfy a given monadic second-order sentence can be described, when viewed in $\mathcal{A}$, as a disjoint union of finitely many partition sets. Thus, if one can show that every partition set of $\mathcal{A}$ has density 0 or 1 then $\mathcal{K}$ has a monadic second-order 0–1 law.

The method of Compton, to establish a 0–1 law for $\mathcal{K}$, is indeed to show that all partition sets of $\mathcal{A}$ have asymptotic density 0 or 1. The necessary and sufficient condition for this to hold is that $a(n-1)/a(n) \to 1$. To obtain interesting conditions that guarantee $a(n-1)/a(n) \to 1$, one turns to the fundamental identity. This ties in with the established work in asymptotic additive number theory, a subject often described by referring to the famous results of Hardy and Ramanujan on the number of partitions of an integer. The applications presented in Chapter 4 are based on an analysis of Bateman and Erdös of additive number systems which have at most one indecomposable of each size.

In a subsequent paper Compton turned to more general limit laws for logic, where one only requires that each sentence $\varphi$ have a probability of holding (the probability need not be 0 or 1). Again, additive number systems are used to shift to the study of conditions that guarantee that every partition set has an asymptotic density. A rather delicate analysis is needed to establish the main result of Compton. One of the striking corollaries is that if $a(n)$ is asymptotic to $C\beta^n$ then $\mathcal{K}$ has a limit law. Further applications come from the asymptotics of Knopfmacher, Knopfmacher, and Warlimont. By applying the Cauchy integral formula

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

to $\mathbf{A}(z) = \sum a(k)z^k$, they are able to find asymptotics for $a(n)$ when $p(n) = C\beta^n + \mathrm{o}(\eta^n)$, where $0 < \eta < \beta$. This gives numerous applications of Compton's theorem, for example, to two-colored linear forests.

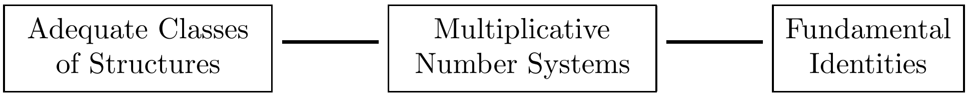
In the late 1980s Compton was considering the application of his ideas to the study of randomly chosen members of classes $\mathcal{K}$ of finite algebraic structures—the class of finite Abelian groups is an excellent example. Here the key operation is *direct product*, not disjoint union. The analog of a component (of a relational structure) is, in this setting, a (*directly*) *indecomposable* structure—that is, a structure which has at least two elements and is not isomorphic to a direct product of smaller structures. The indecomposable finite Abelian groups are precisely the $\mathbf{Z}_{p^n}$, where $\mathbf{Z}_{p^n}$ is the group of integers modulo $p^n$, for $p$ a prime number. As is well known, every nontrivial finite Abelian group can be uniquely expressed as a product of indecomposable Abelian groups. This is the *unique factorization property* for finite Abelian groups. However, unique factorization does not hold for many important classes of algebraic structures, for example, semigroups.

In the context of finite algebraic structures let us say that $\mathcal{K}$ is *adequate* if it is closed under direct product, direct factors, and it has the unique factorization property. Let $a(n)$ count the number of structures in $\mathcal{K}$ of size $n$, and let $p(n)$ count the number of indecomposables in $\mathcal{K}$ of size $n$. (All counting is done up to isomorphism.) From the fact that $\mathcal{K}$ is adequate one has the fundamental identity

$$\sum_{n\geq 1} a(n)n^{-s} \ = \ \prod_{n\geq 2}\left(1-n^{-s}\right)^{-p(n)}.$$

What is the probability that a randomly chosen structure from $\mathcal{K}$ satisfies a given property $\mathcal{P}$? If one defines $p_n$ as before, namely the proportion of structures in $\mathcal{K}$ of size $n$ that have the property $\mathcal{P}$, then very little can be said. However, if one uses the *global* count, that is, let $P_n$ be the proportion of structures in $\mathcal{K}$ of size *at most* $n$ that have the property $\mathcal{P}$, and if one lets the probability be the limit of $P_n$ as $n$ goes to infinity (provided this exists), then the results for relational structures have remarkable parallels in the algebraic setting.

In Part 2 multiplicative number systems are interpolated between adequate classes and fundamental identities, giving an exact analog of the use of additive number systems in Part 1. This is used, as in Part 1, to give a separation of the number theoretic and logical aspects.


Adequate Classes of Structures

Multiplicative Number Systems

Fundamental Identities

In the case of Abelian groups one obtains the associated number system by letting the 'numbers' be the finite groups $\mathbf{G}$, and letting multiplication be direct product. These number systems are said to be multiplicative because the size function is multiplicative, that is, $\|\mathsf{a}\cdot\mathsf{b}\| = \|\mathsf{a}\|\cdot\|\mathsf{b}\|$.

The multiplicative number system analog of Compton's theorem (on general limit laws for relational structures) has, as a corollary, the fact that if $A(x)$ is asymptotic to $cx^{\alpha}$, where $A(x) = \sum_{n\leq x} a(n)$, then $\mathcal{K}$ has a first-order limit law. This applies to the example of Abelian groups, and one can show, for example, that the probability of a finite Abelian group having an element of order 2 is $1 - \prod_{n\geq 1}\left(1 - 2^{-n}\right) \approx 0.71$.

Many of the interesting examples, like Abelian groups, have limit laws, but not 0–1 laws. Further examples are again found by turning to complex analysis, using Perron's integral formula, to generalize Oppenheim's asymptotics for the number of ways to factor the numbers less than or equal to $n$. From this analysis one concludes that if $p(n) = Cn^{\alpha} + O(n^{\beta})$ with $C > 0$, $\alpha \geq 0$, and $\beta < \alpha$, then $\mathcal{K}$ has a first-order limit law. Thus the class of finite lattices that decompose into a product of chains has a first-order limit law.

Chapter 6, the last chapter of Part 1, covers the logic results for adequate classes (with respect to disjoint union) of purely relational structures; and Chapter 12, the last chapter of Part 2, covers the logic results for adequate classes (with respect to direct product) of structures.

These two chapters can be briefly summarized as follows. Given an adequate class $\mathcal{K}$ and a sentence $\varphi$, let $\mathcal{K}_{\varphi}$ be the class of members of $\mathcal{K}$ that satisfy $\varphi$. The goal is to prove that $\mathcal{K}_{\varphi}$ is a disjoint union of finitely many partition classes. Then the number theoretic results on asymptotic density of partition sets can be used.

Three tools are needed to prove these logic results: the Ehrenfeucht-Fraissé games in the additive case; and the Feferman-Vaught Theorem, with Skolem's analysis of sentences about finite Boolean algebras, in the multiplicative case. These tools are fully developed in Chapters 6 and 12.

CHAPTER 2

# Counting Functions and Fundamental Identities

Although this chapter starts off with an abstract definition of additive number systems, the reader will soon see examples of the very concrete systems that are of interest, systems that are derived from well known classes of relational structures such as equivalence relations and linear forests.

## 2.1. Defining additive number systems

Additive number systems are generalizations of the familiar system of nonnegative integers $\mathbb{N} = \{0, 1, \dots\}$ under addition. The definition of such systems requires the notion of a countable free commutative monoid.

### 2.1.1. Commutative monoids.

**Definition 2.1.** $\mathcal{M} = (M, +, 0)$ is a *commutative monoid* if $+$ is a commutative and associative operation on $M$, and $0 \in M$ is an identity element for the operation $+$, that is, the following identities hold in $\mathcal{M}$:

$$\begin{array}{rcll} x + y &=& y + x & \text{for } x, y \in M \\ x + (y + z) &=& (x + y) + z & \text{for } x, y, z \in M \\ x + 0 &=& x & \text{for } x \in M. \end{array}$$

There are many examples of commutative monoids to be found in the complex plane—just take any set $M$ of complex numbers that is closed under addition and has 0 in it. For example, $(\mathbb{C}, +, 0)$, $(\mathbb{R}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{Z}, +, 0)$, and $(\mathbb{N}, +, 0)$ are all commutative monoids. However, among these examples, only the last one is found in additive number systems because it is the only one that is countable and free.

### 2.1.2. Free commutative monoids.

**Definition 2.2.** The *indecomposable* elements of a commutative monoid $\mathcal{M}$ are the nonzero elements that cannot be written as a sum of two nonzero elements.

The set of indecomposable elements of a commutative monoid will be denoted by $P$. Here are some examples of commutative monoids and their indecomposable elements:

| commutative monoid | indecomposable elements |
|---|---|
| $(\mathbb{C}, +, 0)$ | none |
| $(\mathbb{R}, +, 0)$ | none |
| $(\mathbb{Q}, +, 0)$ | none |
| $(\mathbb{Z}, +, 0)$ | none |
| $(\mathbb{N}, +, 0)$ | 1 |
| $(\{m + in : m, n \in \mathbb{N}\}, +, 0)$ | $1, i$ |

Only the last two examples have $P \neq \varnothing$. They also have a very important property regarding $P$, namely every element of the commutative monoid can be uniquely expressed as a sum of elements from $P$.[1]

**Definition 2.3.** A commutative monoid $\mathcal{M}$ is *free* if every element of $\mathcal{M}$ can be *uniquely* expressed, up to commutativity and associativity, as a sum of indecomposable elements. If $\mathcal{M}$ is free then $P$ is called a set of *free generators* of $\mathcal{M}$, $\mathcal{M}$ is said to be *freely generated* by $P$, and $|P|$, the cardinality of $P$, is called the *rank* of $\mathcal{M}$.

Only the last two of the examples above are free commutative monoids, namely $(\mathbb{N}, +, 0)$ and $(\{m + in : m, n \in \mathbb{N}\}, +, 0)$. The first has rank 1 and the second has rank 2. (The last example is the set of Gaussian integers in the first quadrant.)

**Proposition 2.4.** *A free commutative monoid is determined, up to isomorphism, by its rank.*

Proof. Suppose $\mathcal{M}$ is freely generated by $P$, $\mathcal{M}'$ is freely generated by $P'$, and $|P| = |P'|$. Let $\gamma : P \to P'$ be a bijection. Then one can extend $\gamma$ to $\beta : M \to M'$ by $\beta(0) = 0$ and

$$\beta(p_1 + \cdots + p_n) \;=\; \gamma(p_1) + \cdots + \gamma(p_n).$$

This gives an isomorphism between $\mathcal{M}$ and $\mathcal{M}'$. □

For *countable* free commutative monoids, the possible ranks are the natural numbers and countably infinite, that is, $0, 1, \ldots, \aleph_0$.

Natural examples of free commutative monoids are the monoids $\sum_I \mathcal{N}$, where $\mathcal{N} = (\mathbb{N}, +, 0)$, and the elements of $\sum_I \mathcal{N}$ are the maps $f : I \to \mathbb{N}$ which have *finite support*, that is, the set $\{i \in I : f(i) \neq 0\}$ is finite. The operation $+$ is defined on $\sum_I \mathcal{N}$ coordinatewise, that is, $(f_1 + f_2)(i) = f_1(i) + f_2(i)$. The free generators of $\sum_I \mathcal{N}$ are the functions $p_i$, for $i \in I$, defined by

$$p_i(j) \;=\; \begin{cases} 1 & \text{if } j = i \\ 0 & \text{otherwise.} \end{cases}$$

Up to isomorphism, the countable free commutative monoids are as given in Figure 1.

[1] The convention used here is that 0 *is the sum of the empty set of indecomposables.*

| rank | monoid |
|---|---|
| $0$ | $(\{0\},+,0)$ |
| $1$ | $\mathcal{N}$ |
| $2$ | $\mathcal{N}+\mathcal{N}$ |
| $\vdots$ | $\vdots$ |
| $\aleph_0$ | $\sum_{\aleph_0}\mathcal{N}$ |

FIGURE 1. Countable Free Commutative Monoids

**2.1.3. A useful notation.** Let $\mathcal{M} = (M,+,0)$ be a free commutative monoid. For $a \in M$ and $n \in \mathbb{N}$ let $na$ be the sum of $n$ copies of $a$, with $0a$ the zero element of $\mathcal{M}$. Then any element of $M$ can be expressed in the form

$$\sum n_p p,$$

where $p$ runs over the members of $P$, and the $n_p$ are nonnegative integers. This convention requires that all but finitely many of the $n_p$ be 0, and that

$$\sum n_p p \;=\; \begin{cases} 0 & \text{if all } n_p = 0 \\ \displaystyle\sum_{n_p \neq 0} n_p p & \text{otherwise.} \end{cases}$$

From the unique decomposition property it follows that each element of $M$ has a unique expression in the form $\sum n_p p$. $n_p$ is called the *coefficient* of $p$ in the decomposition of the element into indecomposables.

**2.1.4. Additive number systems.** An additive number system is a countable free commutative monoid with a size function called an additive norm.

**Definition 2.5.** An *additive norm* $\|\ \|$ on a commutative monoid $\mathcal{M}$ is a mapping from $M$ to the nonnegative integers such that

- $\|a\| = 0$ iff $a = 0$
- $\|a+b\| = \|a\| + \|b\|$ .

For example, $\|n\| = 34n$ defines an additive norm on $\mathcal{N}$, and $\|m+in\| = 4m + 7n$ defines an additive norm on the Gaussian integers in the first quadrant.

**Lemma 2.6.** *If $\mathcal{M}$ is a free commutative monoid, freely generated by $P$, then any additive norm on $\mathcal{M}$ is completely determined by its restriction to the set $P$. Furthermore, any mapping $\|\ \|$ from $P$ to the set $\mathbb{P}$ of positive integers extends* (*uniquely*) *to an additive norm on $\mathcal{M}$ via*

$$\Big\|\sum n_p p\Big\| \;=\; \sum n_p\|p\|. \tag{2.6.1}$$

Proof. Given a norm $\| \ \|$ on a free commutative monoid $\mathcal{M}$, with $P$ as its set of indecomposables, for any $m \in M$ one has $m$ expressible as $\sum n_p p$. Then

$$\|m\| \ = \ \sum n_p \|p\|.$$

Thus the values of the norm are determined by its values on $P$. (This part of the proof only requires that every element be expressible as a sum of indecomposables, but not necessarily uniquely.)

Given any mapping $\| \ \|$ from $P$ to $\mathbb{P}$, it is routine to verify that the map on $M$ defined by (2.6.1) is indeed a norm for $\mathcal{M}$. (This part of the proof does require that every element be uniquely expressible as a sum of indecomposables, in order to be sure that one has indeed defined a mapping on $M$.) □

**Definition 2.7.** An *additive number system*

$$\mathcal{A} \ = \ \big(\mathsf{A}, \mathsf{P}, +, 0, \| \ \|\big)$$

consists of a countable free commutative monoid $(\mathsf{A}, +, 0)$, with $\mathsf{P}$ being the set of indecomposable elements, and with $\| \ \|$ an additive norm that satisfies, for every $n \in \mathbb{N}$,

$$\{\mathsf{a} \in \mathsf{A} : \|\mathsf{a}\| = n\} \ \text{ is finite,}$$

that is, the norm is a finite-to-one mapping. The *rank* of $\mathcal{A}$ is $|\mathsf{P}|$.

Throughout Part 1 the letter $\mathcal{A}$ will denote an additive number system whose rank is positive, that is, $\mathsf{P} \neq \varnothing$.

**Remark 2.8.** Lower case sans serif letters $\mathsf{a}$, $\mathsf{b}$, ... , $\mathsf{p}$, ... , are used for the 'numbers' of an additive number system $\mathcal{A}$, the upper case sans serif letter $\mathsf{A}$ is the set of all such 'numbers', and other upper case sans serif letters $\mathsf{B}$, $\mathsf{C}$, etc., denote subsets of $\mathsf{A}$, with $\mathsf{P}$ being the set of indecomposables. The choice of the letter $\mathsf{A}$ is motivated by the study of *abstract* number systems, both additive and multiplicative, and the letter $\mathsf{P}$ reminds one of *primes*, the indecomposables of the usual multiplicative number system.

**Definition 2.9.** An additive number system $\mathcal{B} = (\mathsf{B}, \mathsf{Q}, +, 0, \| \ \|)$ is a *subsystem* of $\mathcal{A} = (\mathsf{A}, \mathsf{P}, +, 0, \| \ \|)$ if $\mathsf{Q} \subseteq \mathsf{P}$, and if the operation $+$, the constant $0$, and the norm $\| \ \|$ of $\mathcal{B}$ agree with the corresponding items of $\mathcal{A}$. This is expressed by $\mathcal{B} \leq \mathcal{A}$, and $\mathcal{B}$ is the *subsystem generated by* $\mathsf{Q}$. To indicate that $\mathcal{B}$ is a *proper* subsystem, that is, $\mathsf{B} \neq \mathsf{A}$, the expression $\mathcal{B} < \mathcal{A}$ is used. A subsystem $\mathcal{B}$ is *trivial* if $\mathsf{Q} = \varnothing$.

The concept of two additive number systems being 'essentially the same' is captured in the next definition. (Some readers might prefer the phrase 'norm preserving isomorphism' instead of the single word 'isomorphism'.)

**Definition 2.10.** Let $\mathcal{A}_i = \big(\mathsf{A}_i, \mathsf{P}_i, +_i, 0_i, \| \ \|_i\big)$, where $i = 1, 2$, be two additive number systems. $\mathcal{A}_1$ is *isomorphic to* $\mathcal{A}_2$, written $\mathcal{A}_1 \cong \mathcal{A}_2$, if there is a bijection $\mu : \mathsf{A}_1 \to \mathsf{A}_2$ that preserves addition, zero, and norm, that is,

$$\begin{array}{rcll} \mu(\mathsf{a} +_1 \mathsf{b}) & = & \mu(\mathsf{a}) +_2 \mu(\mathsf{b}) & \text{for } \mathsf{a}, \mathsf{b} \in \mathsf{A}_1 \\ \mu(\mathsf{0}_1) & = & \mathsf{0}_2 & \\ \|\mu(\mathsf{a})\|_2 & = & \|\mathsf{a}\|_1 \quad \text{for } \mathsf{a} \in \mathsf{A}_1. & \end{array}$$

Such a mapping $\mu$ is called an *isomorphism.*

Some of the detailed notational distinction between two additive number systems used in the above definition is, as is common practice in algebra, sacrificed for the clarity that comes with ambiguous notation. The $+_i$, $\mathsf{0}_i$, and $\|\ \|_i$ are replaced by $+$, $\mathsf{0}$, and $\|\ \|$.

As is usual with the study of isomorphism, inverses of isomorphisms are isomorphisms, and compositions of isomorphisms are isomorphisms. Thus, since every additive number system is isomorphic to itself, isomorphism is an equivalence relation on the class of additive number systems. Note that the indecomposables were not mentioned in the definition of isomorphism. This is because the above definition of isomorphism ensures that indecomposables map to indecomposables.

**Lemma 2.11.** *If $\mu : \mathcal{A}_1 \to \mathcal{A}_2$ is an isomorphism then $\mu(\mathsf{P}_1) = \mathsf{P}_2$.*

Proof. An element $\mathsf{a} \in \mathsf{A}_1 \smallsetminus \{\mathsf{0}\}$ is indecomposable iff $\mathsf{a} = \mathsf{b} + \mathsf{c}$ implies either $\mathsf{b} = \mathsf{0}$ or $\mathsf{c} = \mathsf{0}$. Now $\mathsf{a} = \mathsf{b} + \mathsf{c}$ iff $\mu(\mathsf{a}) = \mu(\mathsf{b}) + \mu(\mathsf{c})$, $\mathsf{b} = \mathsf{0}$ iff $\mu(\mathsf{b}) = \mathsf{0}$, and $\mathsf{c} = \mathsf{0}$ iff $\mu(\mathsf{c}) = \mathsf{0}$. Thus $\mathsf{a}$ is indecomposable iff $\mu(\mathsf{a})$ is indecomposable. □

## 2.2. Examples of additive number systems

One has the familiar additive number system of nonnegative integers $\mathbb{N}$ with the usual $+$ and 0, and with the norm being the identity map, that is, $\|n\| = n$. This is a system of rank 1. The set of Gaussian integers in the first quadrant with the usual 'norm' from number theory, namely $\|m + in\| = m^2 + n^2$, is not an additive number system because this is not an additive norm. However one can easily create additive norms, such as $\|m + in\| = 4m + 7n$, to form an additive number system of rank 2.

Although there are plenty of such 'ordinary' additive number systems, this study is concerned with additive number systems derived from classes of structures (as studied in logic)—they provide the connection with logical limit laws. Several examples are introduced in this section, to be used throughout Part 1. The idea behind derived number systems is simply to consider structures up to isomorphism, with addition being disjoint union and the norm being the number of elements in the underlying set of the structure. The structure on the empty set gives the zero element of the derived additive number system.

**2.2.1. Equivalence relations.** By an *equivalence relation* on a finite set $S$ is meant a relational structure[2] $(S, \equiv)$, where $\equiv$ satisfies the reflexive, symmetric and transitive laws:

$$\begin{array}{llll} x \equiv x & & & \text{for all } x \in S \\ x \equiv y & \text{implies} & y \equiv x & \text{for all } x, y \in S \\ x \equiv y \text{ and } y \equiv z & \text{imply} & x \equiv z & \text{for all } x, y, z \in S. \end{array}$$

Such a structure can be pictured as a graph. Figure 2 gives one on 12 elements.[3] The edge relation is the equivalence relation. The maximal connected pieces, called *components* in graph theory, are the *equivalence classes.* (The components in the graph of an equivalence relation are *cliques.*)

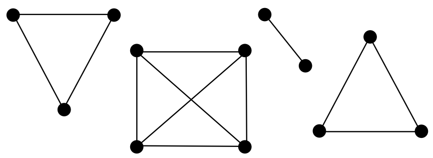


FIGURE 2. An Equivalence Relation

Clearly every finite equivalence relation on a nonempty set can be viewed as a disjoint union of cliques. By considering the structures up to isomorphism one has the additive number system of equivalence relations, where addition is disjoint union. The norm of an equivalence relation $(S, \equiv)$ is just the number of elements in $S$. The indecomposables are the equivalence relations on nonempty sets with a single equivalence class, that is, their graph is a single clique. Thus, for each $n \in \mathbb{P}$, there is exactly one indecomposable (a clique) of norm $n$.

**2.2.2. Permutations.** By a *permutation* on a finite set $S$ is meant a relational structure $(S, R)$ where $R$ is the directed graph of a bijection from $S$ to itself. This means:

- for every $x \in S$, there is a unique $y \in S$ such that $xRy$;
- for every $y \in S$, there is a unique $x \in S$ such that $xRy$.

Such a structure can be pictured as a directed graph, as in Figure 3. The components are called *cycles*, and each permutation is a disjoint union of cycles.

By considering the structures up to isomorphism one has the additive number system of permutations, with addition and norm defined as in the

[2] The phrase *equivalence relation* is used to denote both the structure $(S, \equiv)$ as well as the binary relation $\equiv$. This should not cause any confusion. A similar comment applies to the next example on permutations.

[3] To be more precise it is a *reflexive* graph $[\forall x\, (x \equiv x)]$, as graphs are considered (at least by logicians) to be *irreflexive* $[\forall x\, (x \not\equiv x)]$. In the graph picture the loops at each vertex, to indicate that the relation is reflexive, have been omitted.

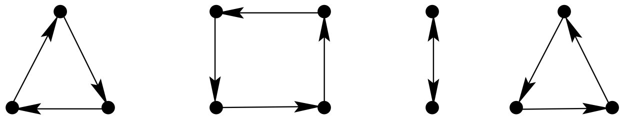


Figure 3. A Permutation

previous example. The indecomposables are the cycles, and there is exactly one indecomposable (a cycle) of norm $n$, for each $n \in \mathbb{P}$.

**2.2.3. Linear forests (as posets).** By a *linear forest* (as a *poset*) on a finite set $S$ is meant a poset $(S, \leq)$ that is a disjoint union of linearly ordered posets (called *chains*). This class is defined by the properties:

$$\begin{array}{llll} x \leq x & & & \text{for all } x \in S \\ x \leq y \text{ and } y \leq x & \text{imply} & x = y & \text{for all } x, y \in S \\ x \leq y \text{ and } y \leq z & \text{imply} & x \leq z & \text{for all } x, y, z \in S \\ x \leq z \text{ and } y \leq z & \text{imply} & x \leq y \text{ or } y \leq x & \text{for all } x, y, z \in S \\ z \leq x \text{ and } z \leq y & \text{imply} & x \leq y \text{ or } y \leq x & \text{for all } x, y, z \in S. \end{array}$$

Such a structure can be pictured using a Hasse diagram, as in Figure 4. The additive number system of linear forests has exactly one indecomposable (a chain) of norm $n$, for each $n \in \mathbb{P}$.

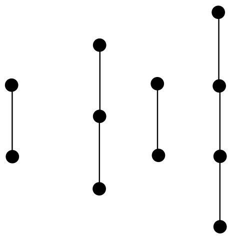


Figure 4. A Linear (Poset) Forest

**2.2.4. Linear forests (as graphs).** By a *linear forest* (as a *graph*) on a finite set $S$ is meant a graph $(S, R)$ whose components are chains, that is, each vertex of the graph is adjacent to at most two other vertices, and there are no cycles. Figure 5 shows an example. The additive number system of linear forests has exactly one indecomposable (a chain) of norm $n$, for each $n \in \mathbb{P}$.

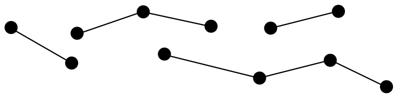


Figure 5. A Linear (Graph) Forest

**2.2.5. Two-colored linear forests (as posets).** By a *two-colored linear forest* (as a poset) on a finite set $S$ is meant a structure $(S, \leq, B, G)$ such that $(S, \leq)$ is a linear forest, and $B$ and $G$ denote two colors (blue and gold) such that each vertex has exactly one of the two colors. The latter can be expressed by: $Bx \leftrightarrow \neg\, Gx$, for $x \in S$. See Figure 6 for an example. The additive number system of two-colored linear forests has exactly $2^n$ indecomposables (two-colored chains) of norm $n$, for each $n \in \mathbb{P}$.

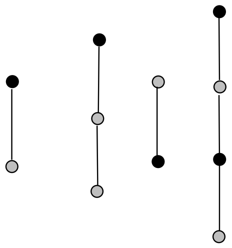


FIGURE 6. A Two-colored Linear (Poset) Forest

**2.2.6. Two-colored linear forests (as graphs).** By a *two-colored linear forest* (as a graph) on a finite set $S$ is meant a structure $(S, R, B, G)$ such that $(S, R)$ is a linear forest, and $B$ and $G$ denote two colors such that each vertex has exactly one of the two colors. See Figure 7 for an example.

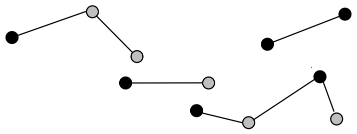


FIGURE 7. A Two-colored Linear (Graph) Forest

The additive number system of two-colored linear forests (as graphs) has a more complicated formula giving the number of indecomposables (two-colored chains) of norm $n$ due to the possibility of symmetry. Indeed, a two-colored chain is either rigid, having only the identity automorphism, or it is symmetric and has one nonidentity automorphism. Some examples are in Figure 8. There are $2^{(n+1)/2}$ symmetric chains of size $n$ (up to isomorphism) when $n$ is odd, and $2^{n/2}$ when $n$ is even, so the total number of chains of size $n$ is

$$\begin{array}{lcll} \frac{1}{2}\left(2^n - 2^{(n+1)/2}\right) + 2^{(n+1)/2} & = & 2^{n-1} - 2^{(n-1)/2} + 2^{(n+1)/2}, & \text{for } n \text{ odd} \\ \frac{1}{2}\left(2^n - 2^{n/2}\right) + 2^{n/2} & = & 2^{n-1} - 2^{(n-2)/2} + 2^{n/2}, & \text{for } n \text{ even.} \end{array}$$

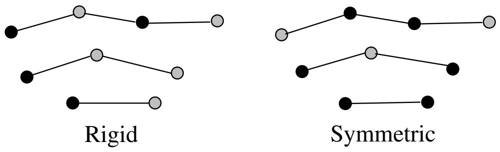


FIGURE 8. Examples of Rigid and Symmetric Chains

**2.2.7. Finite Abelian *p*-groups.** One can also obtain additive number systems from certain classes of algebraic structures, provided the sizes of the structures are always a power of some integer. The idea is again to work up to isomorphism, but with addition being direct product, and the norm being the logarithm of the size.

For $\mathbf{G}$ a finite Abelian $p$-group, define $\|\mathbf{G}\| = n$ if the number of elements in $\mathbf{G}$ is $p^n$. With addition being direct product, there is a unique indecomposable of norm $n$, for each $n \in \mathbb{P}$, namely the cyclic $p$-group $\mathbf{Z}_{p^n}$.

In reviewing the above examples, all but the two-colored examples give rise to essentially the same additive number system, namely one in which there is one indecomposable of each size. Having such a derived additive number system leads to a 0–1 law for these classes. Weaker logical limit laws hold for the two-colored classes.

## 2.3. Counting functions, fundamental identities

**Definition 2.12.** Given an additive number system $\mathcal{A} = \big(\mathsf{A}, \mathsf{P}, +, 0, \|\ \|\big)$ define, for each set $\mathsf{B} \subseteq \mathsf{A}$, the (*local*) *counting function*

$$b(n) \quad = \quad \big|\{\mathsf{b} \in \mathsf{B} : \|\mathsf{b}\| = n\}\big|,$$

that is, $b(n)$ gives the number of elements in $\mathsf{B}$ with norm $n$. In some situations, particularly when the set $\mathsf{B}$ has a more complicated name than just a single letter, the notation $|\mathsf{B}|_n$ is used to denote $b(n)$. The corresponding power series $\mathbf{B}(x)$, called the (*ordinary*) *generating series* of $\mathsf{B}$, is defined by:[4]

$$\mathbf{B}(x) \quad = \quad \sum_{n\geq 0} b(n)x^n.$$

$\mathbf{B}(x)$ can also be expressed by

$$\mathbf{B}(x) \quad = \quad \sum_{\mathsf{b}\in\mathsf{B}} x^{\|\mathsf{b}\|}.$$

The two most significant counting functions are $a(n)$ and $p(n)$, associated with $\mathsf{A}$ and $\mathsf{P}$, called the (*local*) *counting functions of* $\mathcal{A}$. Note that $a(0) = 1$ and $p(0) = 0$. So the generating series of $\mathsf{A}$ and $\mathsf{P}$ are:

$$\mathbf{A}(x) \quad = \quad \sum_{n\geq 0} a(n)x^n$$

[4] Notations similar to $Z_{\mathsf{B}}(x)$, instead of our $\mathbf{B}(x)$, are preferred by some authors.

$$\mathbf{P}(x) \;=\; \sum_{n\geq 1} p(n)x^n.$$

An additive number system is completely determined, up to isomorphism, by either of its counting functions $a(n)$ or $p(n)$.

**Proposition 2.13.** *Let $\mathcal{A}_i$, where $i = 1, 2$, be two additive number systems, and let $a_i(n), p_i(n)$ be their counting functions. Then*

$$\mathcal{A}_1 \cong \mathcal{A}_2 \quad \textit{iff} \quad p_1 = p_2 \quad \textit{iff} \quad a_1 = a_2.$$

Proof. If $\mu : \mathcal{A}_1 \to \mathcal{A}_2$ is an isomorphism then, by Lemma 2.11, $\mathsf{a} \in \mathsf{A}_1$ is an indecomposable iff $\mu(\mathsf{a})$ is an indecomposable in $\mathsf{A}_2$. As $\|\mathsf{a}\| = \|\mu(\mathsf{a})\|$, it follows that $\mathsf{a}$ is an indecomposable of norm $n$ iff $\mu(\mathsf{a})$ is an indecomposable of norm $n$. Thus $p_1(n) = p_2(n)$.

If $p_1 = p_2$ then let $\mu : \mathsf{P}_1 \to \mathsf{P}_2$ be a bijection that preserves the norm. Now extend this to $\mathsf{A}_1$ by

$$\mu\Big(\sum n_{\mathsf{p}}\mathsf{p}\Big) \;=\; \sum n_{\mathsf{p}}\mu(\mathsf{p}).$$

It is easily seen that this defines an isomorphism, so $\mathcal{A}_1 \cong \mathcal{A}_2$.

In any additive number system $\mathcal{A}$ with counting functions $a(n), p(n)$, one can determine $a(n)$ from $p(n)$ since the elements of norm $n$ are uniquely expressible as sums of indecomposables of size at most $n$. Also, one can recursively find $p(n)$ from $a(n)$ by noting that $p(1) = a(1)$, and, having determined $p(m)$ for $m < n$, compute the number $b(n)$ of elements of norm $n$ that can be expressed as sums of indecomposables of size less than $n$. Then $p(n) = a(n) - b(n)$. □

**Definition 2.14.** The *fundamental identity*[5] of $\mathcal{A}$ is

$$\sum_{n\geq 0} a(n)x^n \;=\; \prod_{n\geq 1}(1 - x^n)^{-p(n)}. \tag{2.14.1}$$

A detailed discussion of how to understand this, as describing a method to compute the values of $a(n)$ from $p(n)$, is given in §2.3.4, as well as a proof that it holds as an identity between two functions, for $0 \leq x < 1$.

[5] These identities are often referred to as *partition identities* since the original identity studied by Hardy and Ramanujan,

$$\sum_n a(n)x^n \;=\; \prod_n (1 - x^n)^{-1},$$

is such that $a(n)$ counts the number of ways to (additively) *partition* a positive integer $n$, that is, to express $n$ as a sum of positive numbers (up to commutativity and associativity). The name *fundamental identity* is preferred in this study as the word 'partition' is heavily used in the context of partition sets. The corresponding identities in Part 2 are also called 'fundamental identities'.