2012

A Tale of Two Sequences: A Story of Convergence, Weak and Almost Sure

Marina Skyers
Lehigh University

A Tale of Two Sequences:
A Story of Convergence, Weak and Almost Sure

by

Marina Skyers

Presented to the Graduate and Research Committee

of Lehigh University

in the Candidacy for the Degree of

Doctor of Philosophy

in

Mathematics

Lehigh University

May 2012

Approved and recommended for acceptance as a dissertation in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Marina Skyers

A Tale of Two Sequences: A Story of Convergence, Weak and Almost Sure

Date

Dissertation Advisor:

Lee J. Stanley, Ph.D.

Committee Chair

Accepted Date

Committee Members:

Vladimir Dobrić, Ph.D.

Susan Szczepanski, Ph.D.

Michael Fraboni, Ph.D.

Acknowledgments

I would first and foremost like to thank my advisor, Dr. Lee Stanley, for not only being an exceptional advisor, but an exceptional person as well. Thank you, in particular, for your guidance, honesty, and humor. I am also grateful to Dr. Vladimir Dobrić for his advice, inspiration, and dedication to research and mathematics. Further, I would like to thank the wonderful mathematics department at Lehigh University, for making me feel at home all these five years. Lastly, I would like to thank my mom, for her wish come true.

Contents

List of Figures

List of Tables

Abstract

This dissertation studies two sequences, $\left(\frac{\widetilde{S_n}}{\sqrt{n}} | n \in \mathbb{N}^+\right)$ and $\left(\frac{S_n}{\sqrt{n}} | n \in \mathbb{N}^+\right)$, of random variables on $(0,1)$ which have the same distributions, but are otherwise quite different. S_n, the random walk, is immediately intuitive, but quite disorderly. This disorder is mirrored in that $\left\{\frac{S_n}{\sqrt{n}}\right\}$ converges weakly to the standard normal on $(0,1)$, but not almost surely. We show how to effectively "rearrange" S_n to get Skorokhod's $\widetilde{S_n}$, a quite orderly step function, which has the property that $\left\{\frac{\widetilde{S_n}}{\sqrt{n}}\right\}$ converges almost surely. Our rearrangements provide explicit representations of each $\widetilde{S_n}$ as the sum of an i.i.d. family, depending only on the first n terms in the dyadic expansion of x, uniformly and effectively in n, similar to the obvious representations for the S_n. The absence of such representations was considered by some to be the main missing piece of the puzzle for the $\widetilde{S_n}$.

Chapter 2 of this dissertation presents our results on the fine structure of S_n; the Chapter begins with a number of notions from which there emerges an appealing natural structure theory. Chapter 3 develops an explicit characterization of the $\widetilde{S_n}$, and proves one of our main results on their representability. This paves the way for Chapter 4, where we provide an explicit, computationally tractable approach to obtaining "nice" sequences of rearrangements uniformly in n. Each "nice" sequence of rearrangements is encoded in a suitable sense by a primitive recursive function of two variables.

Chapter 1

Introduction

The main goal of this dissertation is to elucidate the differences and similarities between the sequences of random variables, $(X_n|n \in \mathbb{N}^+)$ and $\left(\widetilde{X_n}|n \in \mathbb{N}^+\right)$, via a very explicit construction and analysis of the latter. $X_n = \frac{S_n}{\sqrt{n}}$, where S_n is the random walk, and so, by the Central Limit Theorem, $\{X_n\}$ converges weakly to the standard normal (on $(0, 1)$).

The S_n have been the subject of intense study; their definition is immediately accessible and intuitive and each S_n is readily representable as the sum of an i.i.d. family (of size n) of irreducibly simpler random variables depending only on the first n terms in the dyadic expansion of x ("coordinates", in what follows). Nevertheless, as we will see, they are quite disorderly and this disorder is mirrored by the fact that, pointwise, $(X_n|n \in \mathbb{N}^+)$ behaves quite badly.

The tale of the two sequences begins with a theorem of Skorokhod, [9]. As a special case of his result (and by an analysis of his general construction in this special case, carried out in §3.2, below), for each $n \in \mathbb{N}^+$, $\widetilde{X_n}$ has the same distribution as X_n, and the sequence $\left(\widetilde{X_n}|n \in \mathbb{N}^+\right)$ converges almost surely to the standard normal on $(0, 1)$. We take $\widetilde{S_n} = \sqrt{n}\widetilde{X_n}$, and in what follows, we will mainly compare and contrast $\left(\widetilde{S_n}|n \in \mathbb{N}^+\right)$ and $(S_n|n \in \mathbb{N}^+)$ rather than $\left(\widetilde{X_n}|n \in \mathbb{N}^+\right)$ and $(X_n|n \in \mathbb{N}^+)$.

By analogy with the discussion of the second paragraph, the $\widetilde{S_n}$ have not received nearly as much attention as the S_n (perhaps as a consequence of their much simpler structure), and although there are other routes to the $\widetilde{S_n}$ than via Skorokhod's construction, none of their possible definitions is as accessible and intuitive as the definition of the S_n. As already mentioned parenthetically, the $\widetilde{S_n}$ are quite orderly: they are monotone non-decreasing step functions, and the almost sure convergence of $\left(\widetilde{X_n}|n \in \mathbb{N}^+\right)$ flows from this simple, orderly structure.

Thus, the $\widetilde{S_n}$ have many virtues by comparison with the S_n. The main missing piece of the puzzle was the relative indirectness of their definition, one aspect of which is the **apparent** absence of **explicit** representations as sums of i.i.d. families (of size n) of simpler random variables depending only on the first n coordinates of x.

The principal results of this dissertation directly address this issue. In particular, we will show, in Chapter 3, that each $\widetilde{S_n}$ is the sum of n independent random variables $\widetilde{R_{n,i}}$, $i = 1, \ldots, n$, such that $\widetilde{R_{n,i}}$ takes on values $-1, 1$ with equal probability. Each $\widetilde{R_{n,i}}$ depends only on the first n coordinates of x. In fact, somewhat surprisingly, there are a large number of such representations of each $\widetilde{S_n}$. In Chapter 4, we provide an explicit, highly effective construction of a "preferred" sequence of such representations, uniformly and highly effectively, in n.

1.1 Notation and Preliminaries

It is our hope that the next two paragraphs explain all notation that is not entirely standard or is not explicitly introduced later on. We will use card$x$ or card (x) to denote the cardinality of the set x, rather than the more usual $|x|$, to avoid clashes with the usual absolute value notation. We will use the symbol $\bigsqcup$ to denote a disjoint union either of two sets $(a \bigsqcup b)$ or of an indexed family of sets $(\bigsqcup_{i \in I} a_i)$.

C will denote Cantor space, which we take to be $\{0,1\}^{\mathbb{N}^+}$ rather than the somewhat more usual $\{0,1\}^{\mathbb{N}}$. We also take C' to be the set of those $x \in C$ such that $x^{-1}[\{0\}]$ is infinite, i.e., viewing x as $(x_i | i \in \mathbb{N}^+)$, such that for infinitely many i, $x_i = 0$. Thus, as usual, C' can be identified with the half-open unit interval, $[0,1)$. This is in accord with our above convention for dyadic rationals. Via this identification, even when we are regarding x as being a member of $[0,1)$, we shall not hesitate to act as though x were the corresponding member of C', and to use notations such as x_i or (more rarely) $x(i)$ accordingly. If s is a finite sequence of bits, then by N_s we mean the basic open neighborhood (relative to C') corresponding to s, ie $\{x \in C' | x \supseteq s\}$.

Definition 1.1. For $x \in C$, identify x with $\sum_{i=1}^{\infty} \frac{x_i}{2^i} \in [0,1]$. This is one-to-one except for those x which are identified with dyadic rationals. The restriction to C' is one way of remedying this, at the price of losing the right endpoint, 1. For $x \in C'$, and $n \in \mathbb{N}^+$, by $S_n(x)$ we mean $\sum_{i=1}^{n} (-1)^{1+x_i}$. Note that, obviously, S_n depends only on the first n coordinates of x. We exploit this to regard S_n as having domain $\{0,1\}^n$ when it suits our purposes to do so:

$$S_n(\boldsymbol{r}) := S_n(x) \text{ for any } x \in C' \text{ such that } x \supseteq \boldsymbol{r}.$$

For such $x \in C'$, we set $x \in \mathfrak{X}_{k,n}$ if and only if $|S_n(x)| > k\sqrt{n}$. We also take $\mathfrak{X}_k$ to be $\bigcup_{n\in\mathbb{N}^+} \mathfrak{X}_{k,n}$, and we define $\mathfrak{Y}_{k,n}$ to be $\mathfrak{X}_{k,n} \smallsetminus \bigcup_{m=1}^{n-1} \mathfrak{X}_{k,m}$.

Remark 1.2. Note that clearly $\mathfrak{X}_k = \bigsqcup_{n\in\mathbb{N}^+} \mathfrak{Y}_{k,n}$. Also note that the $\mathfrak{X}_{k,n}$, $\mathfrak{Y}_{k,n}$ are open (in fact, both are finite unions of intervals whose endpoints are dyadic rationals), and therefore, so are the $\mathfrak{X}_k$. Also, it is immediate that if $x \in C' \cap \mathfrak{X}_k$, then there is a unique $n^* = n_k^*(x)$ such that $x \in \mathfrak{Y}_{k,n^*}$, and that this n^* is the least n such that $x \in \mathfrak{X}_{k,n}$.

For finite-length binary sequences $\boldsymbol{r}$, $\text{Weight}(\boldsymbol{r})$ is the number of coordinates i such that $r_i = 1$. Observe that $S_n(\boldsymbol{r}) = -n + 2\text{Weight}(\boldsymbol{r})$.

Definition 1.3. In what follows, λ will denote Lebesgue measure on $[0,1]$ (or on one of the variants with either endpoint or both excluded; note that this includes the case of C' via the identification with $[0,1)$). As usual, a *probability space* is a triple $(\Omega, \mathscr{S}, P)$, where Ω is the set of points, $\mathscr{S}$ is the σ-algebra of Borel subsets of Ω, and $P : \mathscr{S} \to [0,1]$ is the (σ-additive) probability measure. In this dissertation we will always have $\Omega = [0,1)$, $\mathscr{S}$ will always be the σ-algebra of Borel subsets of Ω, and P will be the restriction of Lebesgue measure to the Borel sets.

1.2 Context and Motivation

The Law of the Iterated Logarithm [6], originally proved by Khintchine [8], states

$$\limsup_{n\to\infty} \frac{S_n(x)}{\sqrt{2n\log\log n}} = 1,$$

for almost all x, and

$$\liminf_{n\to\infty} \frac{S_n(x)}{\sqrt{2n\log\log n}} = -1,$$

for almost all x. An easy argument then shows that $\lambda\left(\bigcap_k \mathfrak{X}_k\right) = 1$, and that $\liminf_{n\to\infty} \frac{S_n(x)}{\sqrt{n}} = -\infty$ and $\limsup_{n\to\infty} \frac{S_n(x)}{\sqrt{n}} = \infty$ for almost all x. Since lim inf and lim sup are split on a set of measure one, for almost all x, $\left\{\frac{S_n}{\sqrt{n}}\right\}$ does not converge pointwise.

Skorokhod was able to obtain almost sure convergence for a modified sequence of random variables $\frac{\widetilde{S_n}}{\sqrt{n}}$. The $\widetilde{S_n}$ are analogues of the S_n and are explicitly constructed in Chapter 3. In recognition of his work, we will call our construction of the random variables $\frac{\widetilde{S_n}}{\sqrt{n}}$, starting from the random variables $\frac{S_n}{\sqrt{n}}$, the "Skorokhod treatment" of the $\frac{S_n}{\sqrt{n}}$.

A natural question is whether there are representations of $\widetilde{S_n}$ similar to the representation for S_n, where for $x \in [0,1)$, we represent $S_n(x)$ as the sum of $R_{n,i}(x)$, $i = 1, \ldots, n$, with $R_{n.i} = (-1)^{1+x_i}$. Once this question is answered in the affirmative, the next problem arises: we would also like to know exactly how "close to" the representation of S_n can we take the representations of $\widetilde{S_n}$.

The questions of the above paragraph will be answered in Chapters 3 and 4. In Chapter 2 we will present our results on the fine structure of S_n that lay the groundwork for further developments where k is a function of n. In this dissertation, however, we will treat k as a constant.

Remark 1.4. If k is a function of n, then $\mathfrak{X}_{k,n}$ becomes $\mathfrak{X}_{k(n),n}$, which can be naturally collapsed to $\mathfrak{X}_n^*$, at least if the function k is clear from the context. Then the union of all the $\mathfrak{X}_{k(n),n}$ becomes $\mathfrak{X}^* = \bigcup_{n\in\mathbb{N}^+} \mathfrak{X}_n^*$, an analogue of $\mathfrak{X}_k$.

Definition 1.5. For $k \in \mathbb{N}^+$, we set $U_k := \{n \in \mathbb{N}^+ | \mathfrak{Y}_{k,n} \neq \emptyset\}$. In this dissertation, we will sometimes refer to the $n \in U_k$ as "successes".

1.3 Results and Organization

A major result, Theorem 2.24, of Chapter 2 is that, surprisingly, $n+1 \in U_k$ is equivalent to a purely arithmetical condition on n, involving no overt reference to $x \in [0,1)$ or to S_n. On the way to this result, we will see that U_k is infinite and we take $(u_{k,j} | j \geq 1)$ to be its increasing enumeration. We provide a complete analysis of U_k, concentrating on the "gaps", i.e., the $u_{k,j+1} - u_{k,j}$. In §2.2, we compute the difference in measure between $\mathfrak{X}_{k,u_j}$ and $\mathfrak{X}_{k,u_{j+1}}$.

Chapter 3 begins with an explicit construction of $\widetilde{S_n}$ (the "Skorokhod treatment") extracted from Skorokhod's general method. In §3.3, we first prove Theorem 3.4 which establishes an equivalence that is fundamental for all that follows it: representations $\widetilde{S_n} = \sum_{i=1}^n \widetilde{R_{n,i}}$, as above, are canonically in one-to-one correspondence with permutations, F, of $\{0,1\}^n$ that satisfy the composition equation, $\widetilde{S_n} = S_n \circ F$. In Theorem 3.5 and Corollary 3.6 we obtain a straightforward count of the (at first sight surprisingly large) number of such permutations, and therefore of the number of such representations of $\widetilde{S_n}$.

This (initially somewhat bewildering) abundance of such permutations/representations naturally led to such questions as whether there are additional properties of such permutations which make some more natural than (and therefore preferable to) others, and whether there are "nice" sequences, $(F_n | n \in \mathbb{N}^+)$, of preferred permutations. This line of questioning led us to formulate (Definition 3.7) the notion of a suitable sequence of permutations, and to pose (Problem 3.8) the fundamental problem of proving their existence. We have little doubt that, informed as they are by the connection to representation, each of the criteria (e.g., effectiveness and uniformity in n) in the definition of suitable sequence belongs in any reasonable attempt to single out natural families of permutations/representations. We are less convinced that the list of criteria is complete.

We solve this problem in Chapter 4, more precisely in §4.3, where we construct (Lemma 4.13) our currently preferred suitable sequence $(F_n | n \in \mathbb{N}^+)$ of permutations. In Theorem 4.14, we establish its effectiveness, by showing that it is (in the appropriate sense) uniformly primitive recursive. In §4.1 we provide a bare-bones overview of the basic notions related to primitive recursion with the intent of making our work in §§4.2, 4.3 accessible to the reader with no prior acquaintance with this material.

§4.2 is a "warm-up" for our main results of §4.3. We construct (Lemma 4.6) a simpler variant, $(G_n | n \in \mathbb{N}^+)$, and prove (Theorem 4.8) that it is uniformly primitive recursive. By sacrificing one of the main properties of the F_n, we get by with a much simpler construction, allowing us to introduce many of the main ideas and techniques involved in the work of §4.3 in this simplified setting. Finally, in §4.4, we take stock of what has been accomplished and look ahead to future work.

Chapter 2

The Fine Structure of S_n

We introduce a number of notions from which there emerges an appealing natural structure theory for the $\mathfrak{Y}_{k,n}$. Notable results include Proposition 2.13, Theorem 2.24 and Lemmas 2.26, 2.27. The first of these establishes that U_k is infinite, but in a strong way: if $n \in U_k$ then for some $1 \leq j^* \leq 4$, $n + j^* \in U_k$; in Lemma 2.23 we show that, in fact, the least such j^* is at least two. This Lemma and the sequence of smaller steps that lead to it lay the groundwork for Theorem 2.24, where, as noted in §1.3, we prove that $n + 1 \in U_k$ is equivalent to a purely arithmetical condition on n. Lemmas 2.26 and 2.27 complete the structure theory. Lemma 2.26 completely characterizes the gaps in U_k in terms of the growth of the function $g(n) = [k\sqrt{n}]$. Lemma 2.27 builds on this. Part (a) improves on Proposition 2.13 by showing that far enough out the gaps of four disappear: a fairly tight lower bound is given as a function of k. Part (b) shows, in a strong way, that the gaps of two eventually predominate by showing that $\lim_{l\to\infty} \frac{u_l}{l} = 2$.

In §2.2, we give exact calculations for $\lambda(\mathfrak{X}_{k,n+1}) - \lambda(\mathfrak{X}_{k,n})$, showing that this is negative if $n+1 \notin U_k$ and positive if $n+1 \in U_k$. We use these results to obtain exact calculations of $\lambda\left(\mathfrak{X}_{k,u_{j+1}}\right) - \lambda\left(\mathfrak{X}_{k,u_j}\right)$, showing this to be slightly positive, when $u_{j+1} - u_j = 2$, and, for sufficiently large j, significantly negative when $u_{j+1} - u_j = 3$ (recall that $(u_j | j \in \mathbb{N}^+)$ is the increasing enumeration of U_k). It is worth noting that these calculations go over, with only very minor changes, to the setting where k is a function of n. The same is true for the the results of §2.1 cited in the previous paragraph.

2.1 Extreme Sequences and Structural Results

In analyzing and discussing the $\mathfrak{X}_{k,n}$, $\mathfrak{Y}_{k,n}$, it will be helpful to adopt the following terminology: we will call the inequality $|S_n(x)| > k\sqrt{n}$ the main condition on x at n, and will refer to this inequality as $I_{k,n}$. Thus (for $x \in C'$), $x \in \mathfrak{X}_{k,n}$ if and only if x satisfies $I_{k,n}$. Also, we call the inequalities $|S_t(x)| \leq k\sqrt{t}$, for $t \in [1,n) \cap \mathbb{N}$, the side conditions on x at n, and the preceding non-strict inequality is the t^{th} side condition on x at n; we refer to it as $E_{k,t}$. Thus, (for $x \in C'$), $x \in \mathfrak{Y}_{k,n}$ if and only if x satisfies $I_{k,n}$ and all of the $E_{k,t}$ for $t \in [1,n) \cap \mathbb{N}$.

Definition 2.1. For $x \in C'$, and $n \in \mathbb{N}^+$, we set $\mathrm{maj}_n(x) := 1$ if and only if $S_n(x) \geq 0$; otherwise, $\mathrm{maj}_n(x) := -1$. We set $\min_n(x) := -\mathrm{maj}_n(x)$.

Remark 2.2. $\mathrm{maj}_n(x)$, $\min_n(x)$ are the majority and minority values in $S_n(x)$, with ties (when $S_n(x) = 0$) being in favor of 1 as the majority.

Definition 2.3. For x, n as in Definition 2.1, we set $\mathrm{Maj}_n(x) := \left\{ i \in [1,n] \cap \mathbb{N} \middle| (-1)^{1+x_i} = \mathrm{maj}_n(x) \right\}$, and similarly for $\mathrm{Min}_n(x)$ and $\min_n(x)$, and we set $M_n(x) := \mathrm{card}(\mathrm{Maj}_n(x))$, $m_n(x) := \mathrm{card}(\mathrm{Min}_n(x))$.

Remark 2.4. Thus, for example, for such x and n, $\mathrm{Maj}_n(x)$ is the set of coordinates, i, with $1 \leq i \leq n$, where the majority value in $S_n(x)$ occurs. Also, note that $n = M_n(x) + m_n(x)$, $|S_n(x)| = M_n(x) - m_n(x) = n - 2m_n(x) = 2M_n(x) - n$, and so $S_n(x)$ always has the same parity as n.

Lemma 2.5. *We have the following three simple observations.*

(a) *If $n \leq k^2$ then $\mathfrak{X}_{k,n} = \emptyset$.*

(b) $\mathfrak{X}_{k,k^2+1} = \mathfrak{Y}_{k,k^2+1} = \left\{ x \middle| x \restriction \left[1, k^2+1\right] \cap \mathbb{N} \text{ is constant} \right\}$.

(c) $\lambda\left(\mathfrak{X}_{k,k^2+1}\right) = \lambda\left(\mathfrak{Y}_{k,k^2+1}\right) = 2 \cdot \frac{1}{2^{k^2+1}} = \frac{1}{2^{k^2}}$.

Proof. Immediate from the definitions. □

For $1 \leq j \leq 4$, we now present a purely arithmetical analysis of whether or not $k^2 + j \in U_k$. By Lemma 2.5 (b), we know $k^2 + 1 \in U_k$. If $x \notin \mathfrak{Y}_{k,k^2+1}$, then by (b), there is at least one minority summand somewhere at or below level $k^2 + 1$. Then $|S_{k^2+2}(x)| \leq k^2 < k\sqrt{k^2+2}$, so

$\mathfrak{Y}_{k,k^2+2} = \emptyset$. Similarly, still for $x \notin \mathfrak{Y}_{k,k^2+1}$, $|S_{k^2+3}(x)| \leq k^2+1 \leq k\sqrt{k^2+3}$ for $k \geq 3$, so $\mathfrak{Y}_{k,k^2+3} = \emptyset$. Now suppose $\mathrm{Min}_{k^2+4}(x) = \{i\}$ for some $1 \leq i \leq k^2+1$. Then $x \notin \mathfrak{X}_{k,k^2+1}$. Also, $|S_{k^2+4}(x)| = k^2+2 > k\sqrt{k^2+4}$, so $x \in X_{k,k^2+4}$. Thus $x \in \mathfrak{Y}_{k,k^2+4}$ and so $k^2+4 \in U_k$. This brief discussion forshadows the construction of Proposition 2.13.

Remark 2.6. Before going farther, it is worth pointing out that if $\mathfrak{Y}_{k,t} = \emptyset$, (i.e., if $t \notin U_k$), then $\bigcup_{i\in[1,t)\cap\mathbb{N}} \mathfrak{X}_{k,i} = \bigcup_{i\in[1,t]\cap\mathbb{N}} \mathfrak{X}_{k,i}$. This can be restated as: if $t \notin U_k$ and if x satisfies all the $E_{k,i}$, $1 \leq i < t$, then x (automatically) satisfies $E_{k,t}$. In other words, the only side conditions that matter occur at elements of U_k.

A key step was the formulation of the following notion.

Definition 2.7. For $k, n \in \mathbb{N}^+$, we define $\sigma_{k,n} := [k\sqrt{n}] + 2$, if $[k\sqrt{n}]$ has the same parity as n, and $\sigma_{k,n} := [k\sqrt{n}] + 1$, otherwise. We also set $m_{k,n} := \frac{1}{2}(n - \sigma_{k,n})$ and $c_{k,n} := \mathrm{card}(U_k \cap [1,n))$.

Lemma 2.8. *If $x \in \mathfrak{Y}_{k,n}$ then $|S_n(x)| = \sigma_{k,n}$.*

Proof. $\sigma_{k,n}$ is the smallest integer greater than $k\sqrt{n}$ which has the same parity as n. Also, $|S_n(x)|$ always has the same parity as n. So $|S_n(x)| > k\sqrt{n}$ if and only if $|S_n(x)| \geq \sigma_{k,n}$. Let $x \in \mathfrak{Y}_{k,n}$. Then $x \in \mathfrak{X}_{k,n}$, so $|S_n(x)| \geq \sigma_{k,n}$. Assume, towards a contradiction, that $|S_n(x)| > \sigma_{k,n}$. Then $|S_n(x)| \geq \sigma_{k,n} + 2$, since they have the same parity. Since $|S_n(x)| \leq |S_{n-1}(x)| + 1$, we have

$$|S_{n-1}(x)| \geq |S_n(x)| - 1 \geq \sigma_{k,n} + 2 - 1 = \sigma_{k,n} + 1 > k\sqrt{n} \geq k\sqrt{n-1}.$$

So $|S_{n-1}(x)| > k\sqrt{n-1}$ and $x \in \mathfrak{X}_{k,n-1}$, a contradiction, since $x \in \mathfrak{Y}_{k,n}$. This proves $|S_n(x)| = \sigma_{k,n}$. □

Remark 2.9. Lemma 2.8 implies that for $n \in U_k$, $m_{k,n} = m_n(x)$ for all $x \in \mathfrak{Y}_{k,n}$ and we can let $m_n := m_n(x)$ for any $x \in \mathfrak{Y}_{k,n}$. And so for $n \in U_k$, $m_n = m_{k,n}$.

The next Definition and Lemma are purely arithmetical:

Definition 2.10. We define the following notions.

(a) *The greatest integer jumps at* n if and only if $[k\sqrt{n+1}] = [k\sqrt{n}] + 1$.

(b) *The parity situation is the same at* n if and only if $[k\sqrt{n}] \equiv n \pmod 2$ and *the parity situation is different* otherwise.

Lemma 2.11. *The relation between Definition 2.10 (a) and (b) is as follows: if the greatest integer does not jump at n, then, in passing from n to $n+1$, the parity situation changes. If the greatest integer jumps at n, then, in passing from n to $n+1$, the parity situation does not change. Further, $\sigma_{k,n}$ depends on whether the greatest integer jumps at n as described below. In particular, $|\sigma_{k,n+1} - \sigma_{k,n}| = 1$.*

Proof. There are four possible cases. In Cases 1, 2, we assume that the greatest integer does not jump at n, and we consider the possibilities for the parity situation. In Cases 3, 4, we assume the greatest integer does jump at n and the parity situation is as in Cases 1, 2, respectively.

So first assume $\left[k\sqrt{n+1}\right] = [k\sqrt{n}]$, and, in addition:

Case 1: Suppose $[k\sqrt{n}] \equiv n \pmod 2$. Then $[k\sqrt{n}] = \left[k\sqrt{n+1}\right] \not\equiv n+1 \pmod 2$, i.e., the parity situation changes. Note also that in this case, $\sigma_{k,n} = [k\sqrt{n}]+2$, $\sigma_{k,n+1} = \left[k\sqrt{n+1}\right]+1 = [k\sqrt{n}]+1$, i.e., $\sigma_{k,n+1} = \sigma_{k,n} - 1$.

Case 2: Suppose $[k\sqrt{n}] \not\equiv n \pmod 2$. Then $[k\sqrt{n}] = \left[k\sqrt{n+1}\right] \equiv n+1 \pmod 2$, so, here too, the parity situation changes. Also, here $\sigma_{k,n} = [k\sqrt{n}]+1$, and $\sigma_{k,n+1} = \left[k\sqrt{n+1}\right]+2 = [k\sqrt{n}]+2$, i.e., $\sigma_{k,n+1} = \sigma_{k,n} + 1$.

So, when the greatest integer does not jump, the parity situation changes. Now assume that the greatest integer does jump, i.e., $\left[k\sqrt{n+1}\right] = [k\sqrt{n}] + 1$, and, in addition:

Case 3: Suppose $[k\sqrt{n}] \equiv n \pmod 2$. Then $[k\sqrt{n}] + 1 = \left[k\sqrt{n+1}\right] \equiv n+1 \pmod 2$ so the parity situation does not change. Also, here, $\sigma_{k,n} = [k\sqrt{n}]+2$ and also $\sigma_{k,n+1} = \left[k\sqrt{n+1}\right]+2 = (k\sqrt{n}+1)+2$, i.e., $\sigma_{k,n+1} = \sigma_{k,n} + 1$.

Case 4: Suppose $[k\sqrt{n}] \not\equiv n \pmod 2$. Then $[k\sqrt{n}] + 1 = \left[k\sqrt{n+1}\right] \not\equiv n+1 \pmod 2$, so, here too, the parity situation does not change. Also, here, $\sigma_{k,n} = [k\sqrt{n}] + 1$ and $\sigma_{k,n+1} = \left[k\sqrt{n+1}\right] + 1 = (k\sqrt{n}+1)+1$, i.e., $\sigma_{k,n+1} = \sigma_{k,n} + 1$. ☐

Lemma 2.12. *If $n \in U_k$ then $(-1)^{1+x_n} = maj_n(x)$.*

Proof. Suppose $x \in \mathfrak{Y}_{k,n}$ and $n \in \mathrm{Min}_n(x)$. Note that the case where $S_{n-1}(x) = 0$ and the majority value at n switches cannot arise, since $n \in U_k \Rightarrow n \geq k^2+1 \Rightarrow |S_n(x)| \geq k^2+1$. Then since $|S_n(x)| \geq 2$, $|S_n(x)| = |S_{n-1}(x)| - 1$ and so $|S_{n-1}(x)| = |S_n(x)| + 1 > k\sqrt{n}+1 \geq k\sqrt{n-1}+1 > k\sqrt{n-1}$. But then $x \in \mathfrak{X}_{k,n-1}$, a contradiction since $x \in \mathfrak{Y}_{k,n}$. So if $x \in \mathfrak{Y}_{k,n}$, then $n \in \mathrm{Maj}_n(x)$ and $|S_n(x)| = |S_{n-1}(x)| + 1$. ☐

Proposition 2.13. *Suppose $n \in U_k$. Then there is $1 \leq j^* \leq 4$ such that $n + j^* \in U_k$.*

Proof. Suppose $x \in \mathfrak{Y}_{k,n}$. We will construct a modification, x^*, of x, which is in $\mathfrak{X}_{k,n+4}$ and not in $\mathfrak{X}_{k,n}$, as follows.

Step 1: $x^*_i = x_i$ for $i < n$ or $i > n+4$.

Step 2: $x^*_n = 1 - x_n$.

Step 3: x^*_{n+j} is such that $(-1)^{1+x^*_{n+j}} = \mathrm{maj}_n(x)$, $1 \leq j \leq 4$.

Then Step 1 implies x^* satisfies all the side conditions below level n. Step 1 and Step 2 imply $|S_n(x^*)| = |S_n(x)| - 2$, so $x^* \notin \mathfrak{X}_{k,n}$. Note that, by construction, $|S_{n+4}(x^*)| = |S_n(x)| + 2$. Recall that $\mathfrak{Y}_{k,n} \neq \phi \Rightarrow n > k^2 \Rightarrow \sqrt{n} > k$. We have that

$$|S_{n+4}(x^*)|^2 = |S_n(x)|^2 + 4|S_n(x)| + 4 > k^2 n + 4k\sqrt{n} + 4 > k^2 n + 4k^2 + 4 > k^2 n + 4k^2 = k^2(n+4),$$

so $|S_{n+4}(x^*)| > k\sqrt{n+4}$, and therefore, $x^* \in \mathfrak{X}_{k,n+4}$.

We will not show $x^* \notin (\mathfrak{X}_{k,n+1} \cup \mathfrak{X}_{k,n+2} \cup \mathfrak{X}_{k,n+3})$; indeed this may be false. Rather, we have shown there is $1 \leq j \leq 4$ such that $x^* \in \mathfrak{X}_{k,n+j}$. Let j^* be the least such j. Then $x^* \in \mathfrak{Y}_{k,n+j^*}$. So there is $u \in U_k$ such that $n < u \leq n+4$. □

Corollary 2.14. *Thus, U_k is infinite.*

Remark 2.15. If we let $(u_{k,j} | j \geq 1)$ be the increasing enumeration of U_k, then Proposition 2.13 can be restated as $u_{k,j+1} - u_{k,j} \leq 4$ for all $j \in \mathbb{N}^+$. It is also worth noting that for all $j \geq 1$, $c_{k,u_j} = j - 1$.

When we are taking k to be fixed, we will lighten the notation by using u_j in place of $u_{k,j}$. Conventionally, we set $u_{k,0} = u_0 = 0$ for all $k \in \mathbb{N}^+$.

Lemma 2.16. $t \in U_k \Rightarrow \sigma_{k,t} = \left[k\sqrt{t}\right] + 1$.

Proof. Let $y \in \mathfrak{Y}_{k,t}$. Then $y \notin \mathfrak{X}_{k,t-1}$, so $|S_{t-1}(y)| \leq \left[k\sqrt{t-1}\right]$. Suppose, towards a contradiction, that $\sigma_{k,t} = \left[k\sqrt{t}\right] + 2$. Since $y \in \mathfrak{Y}_{k,t}$, $|S_t(y)| = \sigma_{k,t} = \left[k\sqrt{t}\right] + 2$. Also, Lemma 2.12 shows that $|S_{t-1}(y)| + 1 = |S_t(y)|$. Then $|S_{t-1}(y)| + 1 = \left[k\sqrt{t}\right] + 2$, and so $|S_{t-1}(y)| = \left[k\sqrt{t}\right] + 1 \geq \left[k\sqrt{t-1}\right] + 1$. Then $|S_{t-1}(y)| > k\sqrt{t-1}$, a contradiction since $y \notin \mathfrak{X}_{k,t-1}$.

□

The next few lemmas are a major step: they relate the number of side conditions (that matter, viz Remark 2.6) below n to $m_{k,n}$. It is worth noting that $m_{k,n}$ is actually negative when $n < k^2 + 1$ and becomes 0 at $k^2 + 1$. Also, the number of side conditions (that matter) below n

is 0 when $n \leq k^2+1$ and becomes 1 at k^2+2. Lemmas 2.17 through 2.21 demonstrate that this pattern persists:

$m_{k,n}$ "keeps chasing" card$\,(U_k \cap [1,n))$; it "catches up" exactly when $n \in U_k$ after which it "falls behind" again (for a bit).

Lemma 2.17. *If $n \in U_k$ then $m_n = c_{k,n}$ ($=$ card$\,(U_k \cap [1,n))$). That is, the minority count is the number of previous successes.*

Proof. Suppose $n \in U_k$, so $n = u_t$, for some t. Then, for all $x \in \mathfrak{Y}_{k,u_t}$, $|S_{u_t}(x)| = u_t - 2m_{u_t}$.

Claim: $m_{u_t} = t-1$ ($= c_{k,u_t} =$ card$\,(U_k \cap [1,u_t))$).

We prove, by induction on s, that the equation of the Claim holds, with s in place of t. The basis is $m_{u_1} = 0$, which is true since $u_1 = k^2+1$. Assume $m_{u_s} = s-1$. We will show $m_{u_{s+1}} = m_{u_s}+1$. Then $m_{u_{s+1}} = (s-1)+1 = s = (s+1)-1$. Let $x \in \mathfrak{Y}_{k,u_s}$ and construct x^*, j^* as in Proposition 2.13. Then $u_s+j^* = u_{s+1}$ and, by construction of x^*, $m_{u_s+j^*}(x^*) = m_{u_s}(x)+1$. So $m_{u_{s+1}} = m_{u_{s+1}}(x^*) = m_{u_s}(x)+1 = m_{u_s}+1$. □

The next Lemma gives the converse.

Lemma 2.18. $m_{k,t} = c_{k,t} \Rightarrow t \in U_k$.

Proof. Recall $m_{k,n} = \frac{1}{2}(n - \sigma_{k,n})$. Suppose $m_{k,t} = c_{k,t}$. We construct a $y \in \mathfrak{Y}_{k,t}$ by setting

$$y_i = \begin{cases} 1 & \text{if } i \in U_k \cap [1,t) \\ 0 & \text{otherwise.} \end{cases}$$

Then $m_t(y) =$ card$\,(U_k \cap [1,t)) = m_{k,t} = \frac{1}{2}(t - \sigma_{k,t})$. So $|S_t(y)| = t - 2m_t(y) = t - t + \sigma_{k,t} = \sigma_{k,t} > k\sqrt{t}$, so $y \in \mathfrak{X}_{k,t}$. Now we show that for all $1 \leq r < t$, $y \notin \mathfrak{X}_{k,r}$. Towards a contradiction, suppose otherwise. Consider the smallest r such that $y \in \mathfrak{X}_{k,r}$. Then also $y \in \mathfrak{Y}_{k,r}$. Then $r \in U_k$, so $c_{k,r} = m_{k,r} = m_r(y)$. By construction, $m_r(y) =$ card$\,(U_k \cap [1,r]) = c_{k,r}+1$ since $r \in U_k$. But then we have $c_{k,r} = m_r(y) = c_{k,r}+1$, a contradiction. So there is no such r. So $y \in \mathfrak{Y}_{k,t}$. □

Remark 2.19. $m_{k,t} < c_{k,t} \Rightarrow t \notin U_k$. This is since $t \in U_k \Rightarrow m_{k,t} = c_{k,t}$ by Lemma 2.17.

Lemma 2.20. $m_{k,n} \leq c_{k,n}$ *for all* $n \geq 1$.

Proof. By induction. Our induction hypothesis is that

$$m_{k,n} \leq c_{k,n}.$$

$c_{k,n}$ is non-decreasing and increases by 1 from n to $n+1$ if and only if $n \in U_k$. Also $\sigma_{k,n}$ either increases or decreases by 1. Therefore, $m_{k,n}$ is also non-decreasing, increases by 1 from n to $n+1$ if $\sigma_{k,n+1} = \sigma_{k,n} - 1$, and does not change if $\sigma_{k,n+1} = \sigma_{k,n} + 1$. We show that $m_{k,n+1} \leq c_{k,n+1}$.

Case 1: Suppose that $m_{k,n} < c_{k,n}$. Then $m_{k,n+1} \leq c_{k,n+1}$.

Case 2: Suppose that $m_{k,n} = c_{k,n}$. Then $n \in U_k$, so $c_{k,n+1} = c_{k,n} + 1$. Thus $m_{k,n+1} \leq m_{k,n} + 1 \leq c_{k,n} + 1 = c_{k,n+1}$. □

Lemma 2.21. $c_{k,n} \leq m_{k,n} + 1$ *for all* $n \geq 1$.

Proof. We prove that for all $t \geq u_1$, $m_{k,t} \leq c_{k,t} \leq m_{k,t}+1$. Lemma 2.20 gives the first inequality, so we are only concerned with the second. The proof is by induction on t; the basis is that for $t = u_1$, we have $c_{k,u_1} = 0 = m_{k,u_1}$. For the induction step, the crucial point is that the $m_{k,n}$'s are non-decreasing. So, suppose that $c_{k,t} \leq m_{k,t} + 1$. Towards a contradiction, assume that $c_{k,t+1} > m_{k,t+1} + 1$. We consider cases.

Case 1: Suppose $t \notin U_k$. Then $c_{k,t} > m_{k,t}$, and so, by the induction hypothesis, $c_{k,t} = m_{k,t} + 1$. Also, since $t \notin U_k$, $c_{k,t+1} = c_{k,t}$, so $m_{k,t} + 1 = c_{k,t+1} > m_{k,t+1} + 1$, i.e, $m_{k,t} > m_{k,t+1}$, a contradiction.

Case 2: Suppose $t \in U_k$. Then $c_{k,t} = m_{k,t}$, and $m_{k,t} + 1 = c_{k,t} + 1 = c_{k,t+1} > m_{k,t+1} + 1$, and the contradiction is as before. □

The next corollary follows immediately from Lemma 2.17.

Corollary 2.22. *For all* j, *there is exactly one* n *such that* $\mathfrak{Y}_{k,n} \neq \emptyset$ *and card*$(U_k \cap [1,n)) = j - 1 = m_n$ *(namely* $n = u_j$*).*

Lemma 2.23. *If* $n+1 \in U_k$ *then* $\mathfrak{Y}_{k,n} = \emptyset$ *(so there are never two consecutive successes).*

Proof. We first prove the following:

Claim: If $\sigma_{k,n} < \sigma_{k,n+1}$, then $n+1 \notin U_k$.

To prove the claim, suppose, towards a contradiction, that $\sigma_{k,n} < \sigma_{k,n+1}$ and $n+1 \in U_k$. Then, by Lemma 2.17, $c_{k,n+1} = \frac{n+1-\sigma_{k,n+1}}{2} = \frac{n+1-\sigma_{k,n}-1}{2} = \frac{n-\sigma_{k,n}}{2}$. Recall that $c_{k,n+1} = c_{k,n}$ if and only if $n \notin U_k$ and $c_{k,n+1} = c_{k,n} + 1$ if and only if $n \in U_k$. In the first case, apply Lemma

2.18 to n to get $n \notin U_k$ if and only if $n \in U_k$, a contradiction. In the second case, apply Lemma 2.17 to n to get $c_{k,n} + 1 = \frac{n-\sigma_{k,n}}{2} = c_{k,n}$, again, a contradiction, and the Claim is proved.

We now complete the proof of the Lemma. If $n, n+1 \in U_k$, then, applying the Claim to $n-1, n$ and then to $n, n+1$ successively, we have $\sigma_{k,n+1} = \sigma_{k,n} - 1 = \sigma_{k,n-1} - 2$. Since $\sigma_{k,n} > \sigma_{k,n+1}$, we are in the case where $[k\sqrt{n}] \equiv n \pmod 2$ and so $\sigma_{k,n} = [k\sqrt{n}] + 2$. Since $\sigma_{k,n-1} > \sigma_{k,n}$ we have $\sigma_{k,n-1} = \sigma_{k,n} + 1 = [k\sqrt{n}] + 3$. But then, by definition, $\sigma_{k,n-1} \leq \left[k\sqrt{n-1}\right] + 2 < \left[k\sqrt{n-1}\right] + 3 \leq [k\sqrt{n}] + 3 = \sigma_{k,n-1}$, a contradiction. $\square$

Theorem 2.24. *$n+1 \in U_k$ if and only if $\left(\left[k\sqrt{n+1}\right] = [k\sqrt{n}]\right.$ and $\left.n \equiv [k\sqrt{n}] \pmod 2\right)$.*

Proof. ($\Rightarrow$) By the proof of Lemma 2.11, $\left(\left[k\sqrt{n+1}\right] = [k\sqrt{n}]\right.$ and $\left.n \equiv [k\sqrt{n}] \pmod 2\right)$ if and only if $\sigma_{k,n+1} = \sigma_{k,n} - 1$, and, if $n+1 \in U_k$, then $\sigma_{k,n+1} = \sigma_{k,n} - 1$, by Lemma 2.11 and the Claim of Lemma 2.23.

($\Leftarrow$) Suppose $(\left[k\sqrt{n+1}\right] = [k\sqrt{n}]$ and $n \equiv [k\sqrt{n}] \pmod 2)$, i.e., $\sigma_{k,n+1} = \sigma_{k,n} - 1$. Then $\sigma_{k,n} = [k\sqrt{n}] + 2$, $\sigma_{k,n+1} = [k\sqrt{n}] + 1$. Since $\sigma_{k,n} \neq [k\sqrt{n}] + 1$, by Lemma 2.16, $n \notin U_k$. Note that $m_{k,n+1} = \frac{n+1-\sigma_{k,n+1}}{2} = \frac{n+1-\sigma_{k,n}+1}{2} = \frac{n-\sigma_{k,n}}{2} + 1 = m_{k,n} + 1$. Since $n \notin U_k$, $c_{k,n} = c_{k,n+1}$. Also, by Lemmas 2.18, 2.20, 2.21, $m_{k,n} + 1 = c_{k,n}$. Thus $m_{k,n+1} = m_{k,n} + 1 = c_{k,n} = c_{k,n+1}$, and so, by Lemma 2.18, again, $n+1 \in U_k$. $\square$

Remark 2.25. As already noted, Theorem 2.24 gives a purely arithmetical condition on n equivalent to $n+1 \in U_k$. As is clear from the proof, the Theorem can be reformulated as $n+1 \in U_k$ if and only if $\sigma_{k,n+1} < \sigma_{k,n}$.

Lemma 2.26. *Suppose $n \in U_k$.*

(a) *$n+2 \in U_k$ if and only if $[k\sqrt{n}] = \left[k\sqrt{n+2}\right]$.*

(b) *If $n+2 \notin U_k$ then*

  (i) *$n+3 \in U_k$ if and only if $\left[k\sqrt{n+3}\right] = [k\sqrt{n}] + 1$,*

  (ii) *$n+4 \in U_k$ if and only if $\left[k\sqrt{n+3}\right] = [k\sqrt{n}] + 2$.*

Proof. For (a), suppose $n \in U_k$.

($\Rightarrow$) If also $n+2 \in U_k$, then we are in the case where $\sigma_{k,n+2} = \sigma_{k,n+1} - 1$ and $\left[k\sqrt{n+2}\right] = \left[k\sqrt{n+1}\right] \not\equiv n+2 \pmod 2$. Since $n \in U_k$, we also have $\sigma_{k,n} = \sigma_{k,n-1} - 1$ and $[k\sqrt{n}] \not\equiv n \pmod 2$. If $[k\sqrt{n}] \neq \left[k\sqrt{n+1}\right]$ then we would have $\left[k\sqrt{n+1}\right] \equiv n \equiv n+2 \pmod 2$, a contradiction. So $[k\sqrt{n}] = \left[k\sqrt{n+1}\right] = \left[k\sqrt{n+2}\right]$.

($\Leftarrow$) Let $[k\sqrt{n}] = [k\sqrt{n+2}]$. Since $n \in U_k$, we are in the case where $\sigma_{k,n} = \sigma_{k,n-1} - 1$ and $[k\sqrt{n}] \not\equiv n \pmod 2$. Then $[k\sqrt{n+2}] \not\equiv n \pmod 2$ and $\sigma_{k,n+2} = [k\sqrt{n+2}] + 1 = \sigma_{k,n}$. Since there are never two consecutive successes, $\operatorname{card}(U_k \cap [1, n+2)) = \operatorname{card}(U_k \cap [1, n)) + 1 = \frac{n-\sigma_{k,n}}{2} + 1 = \frac{n+2-\sigma_{k,n+2}}{2}$, so $n+2 \in U_k$.

For (b), suppose $n \in U_k$ but $n+2 \notin U_k$. Since $n \in U_k$, $[k\sqrt{n}] \not\equiv n \bmod 2$ and $\sigma_{k,n} = [k\sqrt{n}]+1$.

For (i): ($\Rightarrow$) Suppose $n+3 \in U_k$. Then, by Theorem 2.24, $[k\sqrt{n+2}] = [k\sqrt{n+3}]$. So the greatest integer does not jump at $n+2$. Since $n+2 \notin U_k$, by (a), above, $[k\sqrt{n}] \neq [k\sqrt{n+2}]$, so there is a jump at n or $n+1$. Since there is no jump at $n+2$, thus there is a jump only at n or $n+1$, i.e., $[k\sqrt{n+3}] = [k\sqrt{n}] + 1$.

($\Leftarrow$) First suppose there is a jump only at $n+1$, i.e., $[k\sqrt{n+3}] = [k\sqrt{n+2}] = [k\sqrt{n+1}] + 1 = [k\sqrt{n}] + 1 \not\equiv n+1 \pmod 2$. Then we have $[k\sqrt{n+3}] = [k\sqrt{n+2}] \equiv n+2 \pmod 2$, so by Theorem 2.24, $n+3 \in U_k$.

Now suppose there is a jump only at n, i.e., $[k\sqrt{n+3}] = [k\sqrt{n+2}] = [k\sqrt{n+1}] = [k\sqrt{n}] + 1 \not\equiv n+1 \pmod 2$. Then, just as above, we have $[k\sqrt{n+3}] = [k\sqrt{n+2}] \equiv n+2 \pmod 2$, and so $n+3 \in U_k$.

For (ii): ($\Rightarrow$) Suppose $n+4 \in U_k$. Then, by Theorem 2.24, $[k\sqrt{n+4}] = [k\sqrt{n+3}] \equiv n+3 \pmod 2$. So the greatest integer does not jump at $n+3$. Since $n \in U_k$ and $n+2 \notin U_k$, $[k\sqrt{n+2}] \neq [k\sqrt{n}] \not\equiv n \pmod 2$, so there is a jump at n or $n+1$, and $[k\sqrt{n+2}] \equiv n \equiv n+2 \pmod 2$. Then, since $[k\sqrt{n+3}] \equiv n+3 \pmod 2$, $[k\sqrt{n+2}] \neq [k\sqrt{n+3}]$, i.e., the greatest integer jumps at $n+2$. We cannot have two consecutive jumps, so we conclude there are jumps at n and at $n+2$, i.e., $[k\sqrt{n+3}] = [k\sqrt{n}] + 2$.

($\Leftarrow$) Suppose $[k\sqrt{n+4}] = [k\sqrt{n+3}] = [k\sqrt{n+2}] + 1 = [k\sqrt{n+1}] + 1 = [k\sqrt{n}] + 2 \not\equiv n + 2 \pmod 2$. Then $[k\sqrt{n+4}] = [k\sqrt{n+3}] \equiv n+3 \pmod 2$, and, by Theorem 2.24, $n+4 \in U_k$. $\square$

Lemma 2.27. *Suppose $j, l \in \mathbb{N}^+$. Then*

(a) *for sufficiently large j, $u_{j+1} - u_j \leq 3$,*

(b) $\lim_{l\to\infty} \frac{u_l}{l} = 2$.

Proof. For (a), a fairly tight lower bound is $u_j \geq \frac{9k^2}{4}$. In order to have $u_{j+1} - u_j = 4$ (a gap of four) for some $j \in \mathbb{N}^+$, letting $n = u_j$, there must be a jump at n and $n+2$; we must have $[k\sqrt{n}] + 2 = [k\sqrt{n+3}]$. We consider the necessary conditions so that the least l such that $[k\sqrt{n+l}] \geq [k\sqrt{n}] + 2$ is greater than or equal to four.

Note that $k\sqrt{n+l} = k\sqrt{n} \cdot \sqrt{1+\frac{l}{n}}$. The series expansion at 0 of $\sqrt{1+x}$, for $|x|<1$, is $1+$ the alternating series

$$\frac{x}{2} - \frac{x^2}{8} + \frac{x^3}{16} - \frac{5x^4}{128} + \frac{7x^5}{256} + O\left(x^6\right).$$

Since it is alternating, the sum is less than $1+\frac{x}{2}$. Putting $\frac{3}{n}$ for x, we have $\sqrt{1+\frac{3}{n}} \leq 1+\frac{3}{2n}$. Then $k\sqrt{n+3} \leq k\sqrt{n}\left(1+\frac{3}{2n}\right) = k\sqrt{n} + \frac{3k}{2\sqrt{n}}$. If there is a gap of four, i.e., $[k\sqrt{n}]+2 = \left[k\sqrt{n+3}\right]$, then we will have

$$\left[k\sqrt{n}\right] + 2 \leq \left[k\sqrt{n+3}\right] \leq k\sqrt{n+3} \leq k\sqrt{n} + \frac{3k}{2\sqrt{n}}.$$

For a contradiction, it is sufficient to have $\frac{3k}{2\sqrt{n}} \leq 1$. Thus for $n \geq \frac{9}{4}k^2$ there are no more gaps of four, so for $n = u_j$ with j sufficiently large, $u_{j+1} - u_j \leq 3$.

For (b), for $\frac{9k^2}{4} < j < l$, let

$$T_2(j,l) := \{i | j < i \leq l \text{ and } u_i - u_{i-1} = 2\},$$

$$T_3(j,l) := \{i | j < i \leq l \text{ and } u_i - u_{i-1} = 3\}.$$

Then $T_2(j,l) \cup T_3(j,l) = (j,l] \cap \mathbb{N}$. Also $u_l - u_j = 2\mathrm{card}\left(T_2(j,l)\right) + 3\mathrm{card}\left(T_3(j,l)\right)$.

Claim: For any $\varepsilon > 0$ there is a j such that for all $l > j$, $\frac{\mathrm{card}(T_3(j,l))}{\mathrm{card}(T_2(j,l))} \leq \varepsilon$.

To prove the claim, fix $\varepsilon > 0$ and let $d = \frac{2}{\varepsilon} + 3$ (in fact $d \geq \frac{2}{\varepsilon} + 3$ is enough). Choose j sufficiently large so that $u_j > \frac{9k}{4}$, $u_j - u_{j-1} = 3$ and $\frac{k}{2\sqrt{u_j}} < \frac{1}{d+2}$. Let $j < l$, let $c = \mathrm{card}\left(T_3(j,l)\right)$ and let $(t_i | 1 \leq i \leq c)$ be the increasing enumeration of $T_3(j,l)$. Also, let $t_0 = j$. Note that by Lemma 2.26, for all $0 \leq i < c$, $k\sqrt{u_{t_{i+1}} - 1} - k\sqrt{u_{t_i} - 3} > 1$. Therefore, by the Mean Value Theorem, for all such i, $d + 2 < \left(u_{t_{i+1}} - 1\right) - \left(u_{t_i} - 3\right)$, i.e., $d < u_{t_{i+1}} - u_{t_i}$. But

$$\begin{aligned} 3c + 2\mathrm{card}\left(T_2(j,l)\right) &= u_l - u_j \\ &\geq \sum_{i=0}^{c-1} \left(u_{t_{i+1}} - u_{t_i}\right) \\ &> cd. \end{aligned}$$

So

$$\frac{c}{\mathrm{card}\left(T_2(j,l)\right)} < \frac{2}{d-3} \leq \varepsilon,$$

as required.

Temporarily fixing $\varepsilon > 0$, fix a j as in the Claim. For large enough $l > j$, $\mathrm{card}\left(T_2(j,l)\right)$ is large enough so that $\frac{u_j}{\mathrm{card}(T_2(j,l))} < \varepsilon$. We have

$$\begin{aligned}
u_l &= u_j + u_l - u_j \\
&= u_j + 2\mathrm{card}\left(T_2\left(j,l\right)\right) + 3\mathrm{card}\left(T_3\left(j,l\right)\right) \\
&= \frac{u_j}{\mathrm{card}\left(T_2\left(j,l\right)\right)}\mathrm{card}\left(T_2\left(j,l\right)\right) + 2\mathrm{card}\left(T_2\left(j,l\right)\right) + 3\frac{\mathrm{card}\left(T_3\left(j,l\right)\right)}{\mathrm{card}\left(T_2\left(j,l\right)\right)}\mathrm{card}\left(T_2\left(j,l\right)\right) \\
&= \left(\frac{u_j}{\mathrm{card}\left(T_2\left(j,l\right)\right)} + 2 + 3\frac{\mathrm{card}\left(T_3\left(j,l\right)\right)}{\mathrm{card}\left(T_2\left(j,l\right)\right)}\right)\mathrm{card}\left(T_2\left(j,l\right)\right) \\
&< \left(\varepsilon + 2 + 3\varepsilon\right)\mathrm{card}\left(T_2\left(j,l\right)\right)
\end{aligned}$$

So $u_l < (4\varepsilon + 2)\,\mathrm{card}\left(T_2\left(j,l\right)\right)$, and since $l > l - j > \mathrm{card}\left(T_2\left(j,l\right)\right)$, $\frac{u_l}{l} < \frac{u_l}{\mathrm{card}(T_2(j,l))} < 4\varepsilon + 2$. So for sufficiently large l, $\frac{u_l}{l} < 4\varepsilon + 2$. This is true for any ε, so $\lim_{l\to\infty}\frac{u_l}{l} = 2$. $\square$

Numerical calculation has shown that (even for $k = 3$, for example), gaps of four do occur and in fact, early on, gaps of three and four predominate, but the gaps of four disappear fairly quickly, and eventually, the gaps of two predominate.

2.2 Measure: Gain and Loss

To provide further insight into the behaviour of $\frac{S_n}{\sqrt{n}}$, we will now compute $\lambda\left(\mathfrak{X}_{k,u_{j+1}}\right) - \lambda\left(\mathfrak{X}_{k,u_j}\right)$ in a gap of two and in a gap of three. For any n,

$$\lambda\left(\mathfrak{X}_{k,n}\right) = \frac{1}{2^{n-1}}\left(\binom{n}{0} + \cdots + \binom{n}{m_{k,n}}\right);$$

note that when $n = u_j$, $m_{k,n} = j - 1$.

Suppose $n + 1 \notin U_k$. Then $\mathfrak{X}_{k,n+1} \subsetneqq \mathfrak{X}_{k,n}$, and, in fact,

$$\lambda\left(\mathfrak{X}_{k,n} \setminus \mathfrak{X}_{k,n+1}\right) = \frac{1}{2}\left(\frac{1}{2^{n-1}}\binom{n}{m_{k,n}}\right) = \frac{\binom{n}{m_{k,n}}}{2^n}:$$

half of the x's such that $|S_n(x)| = \sigma_{k,n} = n - 2m_{k,n}$ will have a "minority summand" as $(-1)^{1+x_n}$. Such x's will no longer be in $\mathfrak{X}_{k,n+1}$, but they are the only ones that will disappear.

Now suppose $n + 1 \in U_k$. Then $\mathfrak{X}_{k,n} \subseteq \mathfrak{X}_{k,n+1}$, and $x \in \mathfrak{X}_{k,n+1} \setminus \mathfrak{X}_{k,n}$ if and only if

$(|S_n(x)| = \sigma_{k,n} - 2$ and $n+1 \in \mathrm{Maj}_{n+1}(x))$. Another view of $\lambda(\mathfrak{X}_{k,n})$ is that

$$\lambda\left((\mathfrak{X}_{k,n})^C\right) = \frac{1}{2^n}\left(\binom{n}{\frac{1}{2}(n-(\sigma_{k,n}-2))} + \cdots + \binom{n}{\frac{1}{2}(n+(\sigma_{k,n}-2))}\right).$$

The first and last summands correspond to the only possible x's that enter $\mathfrak{X}_{k,n+1}$, and for each summand, half of the x's do, namely, the ones that go in the majority direction.

Thus, if $n+1 \notin U_k$, then

$$\lambda(\mathfrak{X}_{k,n+1}) = \lambda(\mathfrak{X}_{k,n}) - \frac{\binom{n}{m_{k,n}}}{2^n},$$

and, if $n+1 \in U_k$, then

$$\lambda(\mathfrak{X}_{k,n+1}) = \lambda(\mathfrak{X}_{k,n}) + \frac{\binom{n}{m_{k,n}+1}}{2^n}.$$

Suppose $u_{j+1} = u_j + 2$. Then, since $u_j \in U_k$, $u_j + 1 \notin U_k$, so

$$\lambda\left(\mathfrak{X}_{k,u_j+1}\right) = \lambda\left(\mathfrak{X}_{k,u_j}\right) - \frac{\binom{u_j}{j-1}}{2^{u_j}}.$$

Note that

$$m_{k,u_j+1} = c_{u_j+1} - 1 = c_{u_j} + 1 - 1 = c_{u_j} = j - 1,$$

and so,

$$\begin{aligned}
\lambda\left(\mathfrak{X}_{k,u_j+2}\right) &= \lambda\left(\mathfrak{X}_{k,u_j+1}\right) + \frac{\binom{u_j+1}{j}}{2^{u_j+1}} \\
&= \lambda\left(\mathfrak{X}_{k,u_j}\right) + \frac{\binom{u_j+1}{j}}{2^{u_j+1}} - \frac{2\cdot\binom{u_j}{j-1}}{2^{u_j+1}} \\
&= \lambda\left(\mathfrak{X}_{k,u_j}\right) + \frac{\binom{u_j}{j} + \binom{u_j}{j-1}}{2^{u_j+1}} - \frac{2\binom{u_j}{j-1}}{2^{u_j+1}},
\end{aligned}$$

since $\binom{u_j}{j} + \binom{u_j}{j-1} = \binom{u_j+1}{j}$. Thus

$$\lambda\left(\mathfrak{X}_{k,u_j+2}\right) = \lambda\left(\mathfrak{X}_{k,u_j}\right) + \frac{1}{2^{u_j+1}}\left(\binom{u_j}{j} - \binom{u_j}{j-1}\right).$$

Since $\binom{u_j}{j} > \binom{u_j}{j-1}$, we have $\lambda\left(\mathfrak{X}_{k,u_j+2}\right) > \lambda\left(\mathfrak{X}_{k,u_j}\right)$: measure increases in gaps of two.

Next we show measure decreases in gaps of three. Suppose $u_{j+1} = u_j + 3$. Then,

$$\begin{aligned}
\lambda\left(\mathfrak{X}_{k,u_j+3}\right) &= \lambda\left(\mathfrak{X}_{k,u_j+2}\right) + \frac{\binom{u_j+2}{m_{k,u_j+2}+1}}{2^{u_j+2}} \\
&= \lambda\left(\mathfrak{X}_{k,u_j+1}\right) + \frac{\binom{u_j+2}{m_{k,u_j+2}+1}}{2^{u_j+2}} - \frac{\binom{u_j+1}{m_{k,u_j+1}}}{2^{u_j+1}} \\
&= \lambda\left(\mathfrak{X}_{k,u_j}\right) + \frac{\binom{u_j+2}{m_{k,u_j+2}+1}}{2^{u_j+2}} - \frac{\binom{u_j+1}{m_{k,u_j+1}}}{2^{u_j+1}} - \frac{\binom{u_j}{m_{k,u_j}}}{2^{u_j}}.
\end{aligned}$$

Since $u_{j+1} = u_j + 3$, we have

$$m_{k,u_j} = j - 1 = c_{k,u_j},$$

$$m_{k,u_j+1} < c_{k,u_j+1} = c_{k,u_j} + 1 = j$$

and

$$m_{k,u_j+2} < c_{k,u_j+2} = c_{k,u_j} + 1 = j,$$

so $m_{k,u_j+1} = j - 1$ and $m_{k,u_j+2} = j - 1$. So we have

$$\lambda\left(\mathfrak{X}_{k,u_j+3}\right) = \lambda\left(\mathfrak{X}_{k,u_j}\right) + \frac{\binom{u_j+2}{j} - 2\binom{u_j+1}{j-1} - 4\binom{u_j}{j-1}}{2^{u_j+2}}.$$

Note that $\binom{u_j+2}{j} - \binom{u_j+1}{j-1} = \binom{u_j+1}{j}$ and $\binom{u_j+1}{j} - \binom{u_j}{j-1} = \binom{u_j}{j}$. Thus in a gap of three, we have

$$\begin{aligned}
\lambda\left(X_{k,u_j+3}\right) - \lambda\left(X_{k,u_j}\right) &= \frac{\binom{u_j+2}{j} - 2\binom{u_j+1}{j-1} - 4\binom{u_j}{j-1}}{2^{u_j+2}} \\
&= \frac{\binom{u_j+2}{j} - \binom{u_j+1}{j-1} - 4\binom{u_j}{j-1} - \binom{u_j+1}{j-1}}{2^{u_j+2}} \\
&= \frac{\binom{u_j+1}{j} - 4\binom{u_j}{j-1} - \binom{u_j+1}{j-1}}{2^{u_j+2}} \\
&= \frac{\binom{u_j+1}{j} - \binom{u_j}{j-1} - 3\binom{u_j}{j-1} - \binom{u_j+1}{j-1}}{2^{u_j+2}} \\
&= \frac{\binom{u_j}{j} - 3\binom{u_j}{j-1} - \binom{u_j+1}{j-1}}{2^{u_j+2}} \\
&= \frac{\binom{u_j}{j} - \binom{u_j}{j-1} - 2\binom{u_j}{j-1} - \binom{u_j+1}{j-1}}{2^{u_j+2}}. \qquad (2.1)
\end{aligned}$$

In order to compute $\binom{u_j}{j} - \binom{u_j}{j-1}$ we first compute the ratio:

$$\frac{\binom{u_j}{j}}{\binom{u_j}{j-1}} = \frac{u_j - (j-1)}{j} = \frac{u_j - m_{k,u_j}}{j} = \frac{m_{k,u_j} + \sigma_{k,u_j}}{j}.$$

Since $u_j \in U_k$, $\sigma_{k,u_j} = [k\sqrt{u_j}] + 1$, and so

$$\frac{m_{k,u_j} + \sigma_{k,u_j}}{j} = \frac{1/2\left(u_j - \left[k\sqrt{u_j}\right] - 1\right) + \left[k\sqrt{u_j}\right] + 1}{j} = \frac{1/2\left(u_j + \left[k\sqrt{u_j}\right] + 1\right)}{j}.$$

For j sufficiently large, by Lemma 2.27 (b), $u_j \approx 2j$, and so,

$$\begin{aligned}
\binom{u_j}{j} - \binom{u_j}{j-1} &= \binom{u_j}{j-1}\left(\frac{1/2\left(u_j + \left[k\sqrt{u_j}\right] + 1\right)}{j} - 1\right) \\
&\approx \binom{u_j}{j-1}\left(\frac{j + 1/2\left(\left[k\sqrt{u_j}\right] + 1\right)}{j} - 1\right) \\
&= \binom{u_j}{j-1}\left(\frac{1/2\left(\left[k\sqrt{u_j}\right] + 1\right)}{j}\right).
\end{aligned}$$

With this in mind, (2.1) becomes

$$\lambda\left(X_{k,u_j+3}\right) - \lambda\left(X_{k,u_j}\right) \approx \frac{\binom{u_j}{j-1}\left(\frac{1/2\left(\left[k\sqrt{u_j}\right]+1\right)}{j}\right) - 2\binom{u_j}{j-1} - \binom{u_j+1}{j-1}}{2^{u_j+2}}.$$

For sufficiently large j, $1/2\left(\left[k\sqrt{u_j}\right] + 1\right) < j$ and the difference $\lambda\left(X_{k,u_j+3}\right) - \lambda\left(X_{k,u_j}\right)$ is certainly negative. Thus, far enough out, measure decreases in gaps of three.

Chapter 3

$\widetilde{S_n}$: Construction/Representation

3.1 Introduction

The material of this Chapter is based on a theorem of Skorokhod, Theorem 3.1, below. In §3.2, we analyze Skorokhod's construction when it is applied to the sequence $\left(S_n \middle| n \in \mathbb{N}^+\right)$, culminating in the definitions of the $\widetilde{X_n}$ and $\widetilde{S_n}$ (Definition 3.2).

Recall that we seek to express each $\widetilde{S_n}(x)$ as $\sum_{i=1}^n \widetilde{R_{n,i}}(x)$, for all $x \in (0,1)$, where for each n, $\left\{\widetilde{R_{n,i}} \middle| 1 \leq i \leq n\right\}$ are to be independent random variables on $(0,1)$, each of which depends only on the first n coordinates of x and takes on values $-1, 1$ with equal probability. For $S_n(x)$ we can simply take $R_{n,i}(x) = (-1)^{1+x_i}$.

In Theorem 3.4, we establish one of our fundamental results: representations $\widetilde{S_n} = \sum_{i=1}^n \widetilde{R_{n,i}}(x)$, as above, are in canonical one-to-one correspondence with permutations, F, of $\{0,1\}^n$ satisfying the composition equation $\widetilde{S_n} = S_n \circ F$. This, in turn, paves the way for Theorem 3.5, where we show that there are many such permutations F, and therefore (Corollary 3.6) many such representations, $\left(\widetilde{R_{n,i}} \middle| n \in \mathbb{N}^+\right)$, of each $\widetilde{S_n}$.

Theorems 3.4 and 3.5 are proved in §3.3. At the end of that section, we pose a series of questions that establish the groundwork and motivation for Chapter 4: among the continuum many sequences $\boldsymbol{f} = (f_n | n \in \mathbb{N}^+)$ of permutations, such that for each $n \in \mathbb{N}^+$, $\widetilde{S_n} = S_n \circ f_n$, are some more natural than (and therefore preferable to) others? Are any such sequences effective? This culminates in Definition 3.7, where we define the notion of a suitable sequence.

In [9], Skorokhod proved:

Theorem 3.1. *Suppose that on a probability space, we have random variables X_n, $n \in \mathbb{N}^+$,* *and X such that $\{X_n\}$ converges to X weakly. Then on $([0,1], B([0,1]), \lambda)$, there are random variables Y_n, $n \in \mathbb{N}^+$, and Y, with the same distributions as the X_n and X, respectively, and such that $\{Y_n\}$ converges to Y almost surely.*

Note that we can replace $[0,1]_{\mathbb{R}}$ in the statement of the above theorem by $(0,1)$.

A special case of the Central Limit Theorem is that $\left\{\frac{S_n}{\sqrt{n}}\right\}$ converges weakly to the standard normal on $(0,1)$, [3], for example. In the above theorem, we take our initial probability space to be $[0,1)$, and we put $X_n = \frac{S_n}{\sqrt{n}}$. Then the Y_n that result will be precisely the $\widetilde{X_n} = \frac{\widetilde{S_n}}{\sqrt{n}}$. We will explicitly carry out the construction, which we call the Skorokhod treatment, involved in the proof of this theorem in this special case, to obtain an explicit characterization of $\widetilde{X_n} = \frac{\widetilde{S_n}}{\sqrt{n}}$ (which, by Skorokhod's Theorem, will converge to the standard normal almost surely).

3.2 Skorokhod's Route to Almost Sure Convergence

Now we will look closely at Skorokhod's construction so as to obtain an explicit characterization of $\widetilde{S_n}$. Let $A_t := \{y \in (0,1) \,|\, S_n(y) \le t\sqrt{n}\}$. So $\lambda(A(t)) = P\left(\frac{S_n}{\sqrt{n}} \le t\right) = P(X_n \le t)$ (see Definition 1.3). Then $A_t = \emptyset$ for $t < -\sqrt{n}$, and $A_t = (0,1)$ for $t \ge \sqrt{n}$. More generally, A_t will be constant on these intervals of t:

$$\left(-\infty, -\sqrt{n}\right), \left[-\sqrt{n}, \frac{2-n}{\sqrt{n}}\right), \ldots, \left[\frac{-n+2k}{\sqrt{n}}, \frac{-n+2(k+1)}{\sqrt{n}}\right), \ldots, \left[\frac{n-2}{\sqrt{n}}, \sqrt{n}\right), \left[\sqrt{n}, \infty\right),$$

for $0 \le k < n$. For $x \in (0,1]$, define $\widetilde{X_n}(x) := \inf\{t \in \mathbb{R} | \lambda(A_t) \ge x\}$. A straightforward computation shows that $\widetilde{X_n}$ is a non-decreasing step function with "steps" $A_{n,i}$, $i = 0, \ldots, n$, where

$$A_{n,i} = \left(\frac{1}{2^n}\sum_{j=0}^{i-1}\binom{n}{j}, \frac{1}{2^n}\sum_{j=0}^{i}\binom{n}{j}\right].$$

Definition 3.2. For such i, and for all $x \in A_{n,i}$, letting

$$v_{n,i} = \frac{-n+2i}{\sqrt{n}},$$

we define

$$\widetilde{X_n}(x) := v_{n,i},$$

and

$$\widetilde{S_n}(x) := -n + 2i.$$

This sequence of definitions, culminating in the definition of $\widetilde{S_n}$, carries out Skorokhod's construction starting from the sequence $\left(\frac{S_n}{\sqrt{n}} \middle| n \in \mathbb{N}^+\right)$. Therefore the "Skorokhod sequence" $\left(\frac{\widetilde{S_n}}{\sqrt{n}} \middle| n \in \mathbb{N}^+\right)$ converges almost surely to the standard normal, this time on $(0,1]_{\mathbb{R}}$, but the fact that $\widetilde{S_n}(1)$ happens to be defined turns out to be more of an annoyance than a feature, so we'll view $\widetilde{S_n}$ as defined only on $(0,1)$. Note that the definition of $\widetilde{S_n}(x)$ requires only that we identify the "step", $A_{n,i}$, to which x belongs. This depends only on the first n coordinates of x, and so the same holds for $\widetilde{S_n}(x)$ (as indeed it does for $S_n(x)$). This, in turn, means that we can view $\widetilde{S_n}$ as being defined on $\{0,1\}^n$ just as we did for S_n in Definition 2.1:

$$\widetilde{S_n}(\boldsymbol{r}) := \widetilde{S_n}(x) \text{ for any } x \in C' \text{ such that } x \supseteq \boldsymbol{r}.$$

Finally, note that we have carried out all of the preceding without showing how $\widetilde{S_n}$ can be represented as the sum of the $\widetilde{R_{n,i}}$, described above. This will be done in §3.3.

For fixed $n \in \mathbb{N}^+$ and $x \in (0,1)$, let $\kappa_n = \kappa_n(x)$ be defined by:

$$\kappa_n = \sum_{i=1}^{n} x_i 2^{n-i}.$$

Then $x \in \left[\frac{\kappa_n(x)}{2^n}, \frac{\kappa_n(x)+1}{2^n}\right)$ and of course this depends only on the first n coordinates of x. We exploit this observation by viewing κ_n as a function with domain $\{0,1\}^n$: $\kappa_n(\boldsymbol{r}) = \kappa_n(x)$ for any x such that $x \supseteq \boldsymbol{r}$. From this point of view, κ_n is a bijection from $\{0,1\}^n$ to $[0,2^n) \cap \mathbb{N}$. Further, κ_n is order preserving if we take $\{0,1\}^n$ to be linearly ordered by lexicographic order. Finally, note that $\boldsymbol{r}$ is the binary representation of $\kappa_n(\boldsymbol{r})$, and that, letting $N_{\boldsymbol{r}}$ be the basic open neighborhood in Cantor space corresponding to $\boldsymbol{r}$ (so $N_{\boldsymbol{r}} = \{x \in C' | x \supseteq \boldsymbol{r}\}$), $N_{\boldsymbol{r}} = \left[\frac{\kappa_n(\boldsymbol{r})}{2^n}, \frac{\kappa_n(\boldsymbol{r})+1}{2^n}\right)$.

In view of these observations, in what follows, for fixed n, we will often identify $\boldsymbol{r} \in \{0,1\}^n$ with $\kappa_n(\boldsymbol{r})$ and dyadic intervals, $\left[\frac{\kappa}{2^n}, \frac{\kappa+1}{2^n}\right)$, of length $\frac{1}{2^n}$, with $\kappa \in [0,2^n) \cap \mathbb{N}$. From this point of view, for $x \in (0,1)$, we compute $\widetilde{S_n}(x)$ by identifying the step, $A_{n,i}$, that includes the interval $\kappa_n(x)$.

Remark 3.3. Note that, for each $n \in \mathbb{N}^+$ and for $\kappa \in [0,2^n) \cap \mathbb{N}$, $-n \leq S_n(\kappa), \widetilde{S_n}(\kappa) \leq n$ and $S_n, \widetilde{S_n}$ satisfy the dualization equations $S_n(\kappa) = -S_n(2^n - 1 - \kappa)$, $\widetilde{S_n}(\kappa) = -\widetilde{S_n}(2^n - 1 - \kappa)$.

The graphs of S_n and $\widetilde{S_n}$ through $n = 7$ are illustrated in the figures below. S_n is shown in magenta, while $\widetilde{S_n}$ is shown in green.

Figure 3.1: $S_1, \widetilde{S_1}$

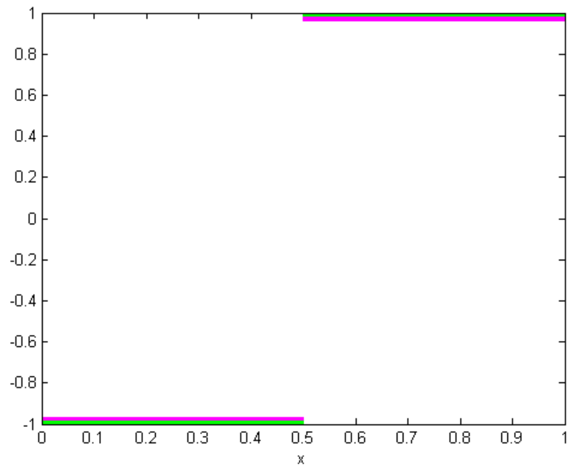


Figure 3.2: $S_2, \widetilde{S_2}$

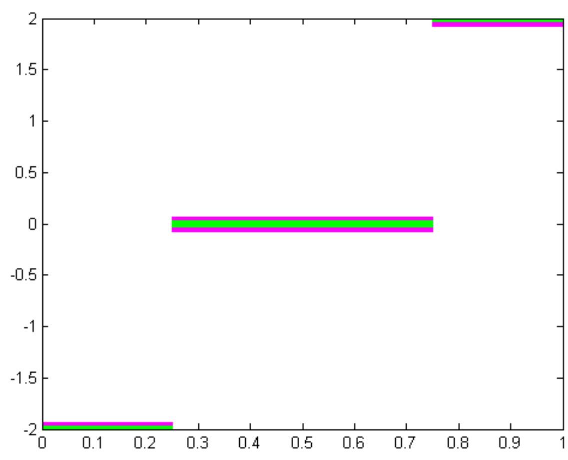


Figure 3.3: $S_3, \widetilde{S_3}$

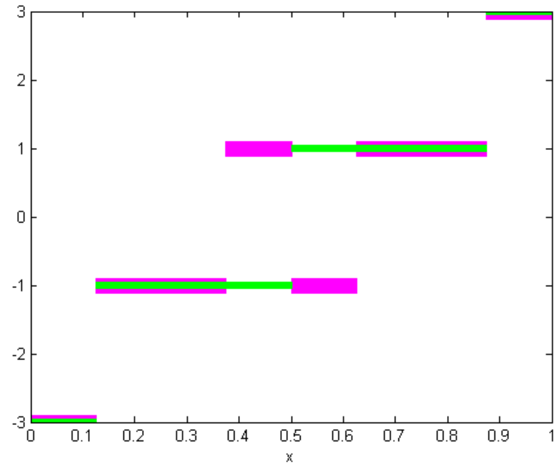


Figure 3.4: $S_4, \widetilde{S_4}$

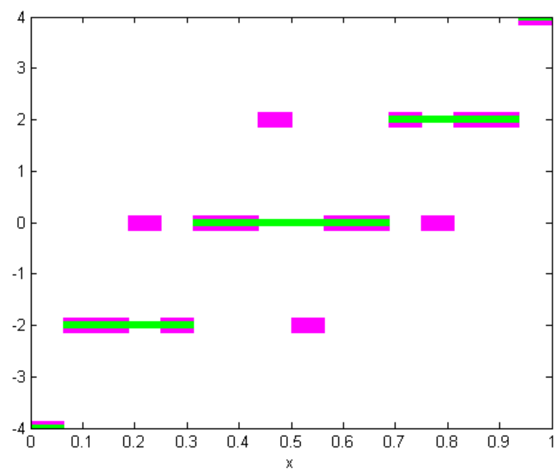


Figure 3.5: $S_5, \widetilde{S_5}$

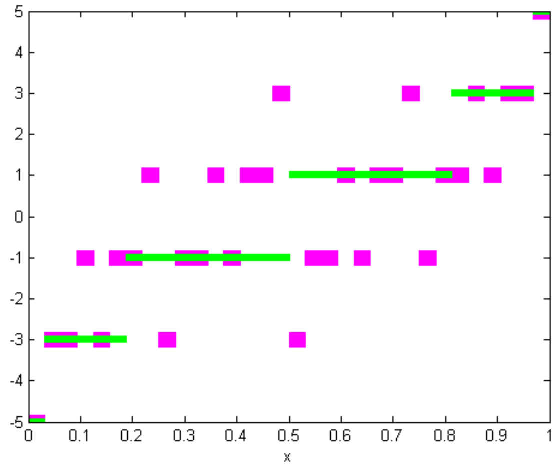


Figure 3.6: $S_6, \widetilde{S_6}$

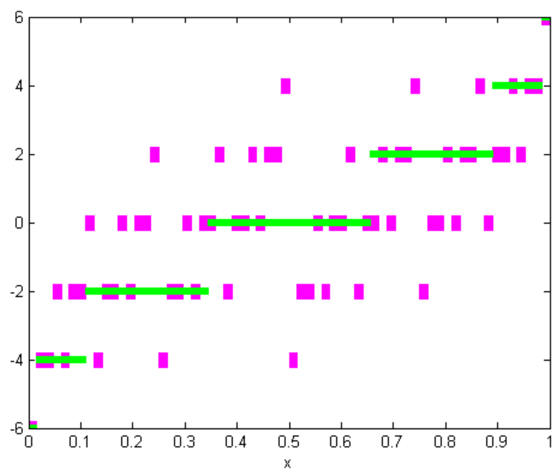
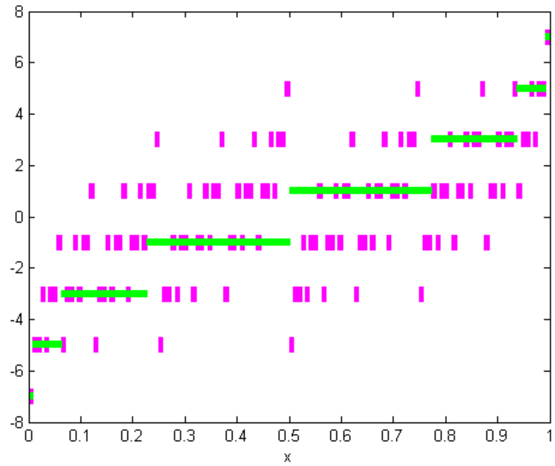


Figure 3.7: $S_7, \widetilde{S_7}$



3.3 Mapping Step to Weight (to Represent the $\widetilde{S_n}$)

In this section, we carry out the stated goal of obaining "many" representations of each $\widetilde{S_n}$.

Theorem 3.4. *For any n, there is a canonical one-to-one correspondence between permutations $F : \{0,1\}^n \to \{0,1\}^n$ such that $\widetilde{S_n} = S_n \circ F$, and representations $\widetilde{S_n} = \sum_{i=1}^n \widetilde{R_{n,i}}$, where $\left(\widetilde{R_{n,i}} | 1 \le i \le n\right)$ is an i.i.d. family of random variables on $(0,1)$ such that each $\widetilde{R_{n,i}}$ depends only on the first n coordinates of x and takes on values $-1, 1$ with equal probability.*

Proof. Temporarily, let "balanced" mean "takes on values $-1, 1$ each with probability $\frac{1}{2}$." Suppose $\widetilde{S_n} = S_n \circ F$. Define

$$\widetilde{R_{n,i}}(x) := (-1)^{1+(F(x_1,\ldots,x_n))_i}.$$

Since $S_n(x) = \sum_{i=1}^n (-1)^{1+x_i}$, $S_n(F(x)) = \sum_{i=1}^n \widetilde{R_{n,i}}(x)$. To show the $\widetilde{R_{n,i}}$ are balanced, it suffices to show for all $i = 1, \ldots, n$ and $\varepsilon \in \{0,1\}$,

$$\lambda\left(\left\{x \middle| \left(F(x_1,\ldots,x_n)\right)_i = \varepsilon\right\}\right) = \frac{1}{2}.$$

Let $A = \left\{\boldsymbol{t} \in \{0,1\}^n \middle| t_i = \varepsilon\right\}$. So $\operatorname{card}(A) = \frac{2^n}{2} = 2^{n-1}$. Since F is 1-1, $\operatorname{card}\left(F^{-1}[A]\right) = 2^{n-1}$. Now, $F^{-1}[A] = \left\{\boldsymbol{r} \in \{0,1\}^n \middle| \left(F(\boldsymbol{r})\right)_i = \varepsilon\right\}$ and $\{x | (F(x_1,\ldots,x_n))_i = \varepsilon\} = \bigsqcup_{\boldsymbol{r} \in F^{-1}[A]} N_{\boldsymbol{r}}$. So, $\lambda\left(\{x | (F(x_1,\ldots,x_n))_i = \varepsilon\}\right) = \lambda\left(\bigcup_{\boldsymbol{r} \in F^{-1}[A]} N_{\boldsymbol{r}}\right) = 2^{n-1} \cdot \frac{1}{2^n} = \frac{1}{2}$.

To show the $\widetilde{R_{n,i}}$ are independent, it suffices to show for all $\boldsymbol{s} \in \{-1,1\}^n$,

$$p(s_1,\ldots,s_n) = p_1(s_1)\cdot\ldots\cdot p_n(s_n),$$

where p is the joint pmf of the $\widetilde{R_{n,i}}$ and p_i is the pmf of $\widetilde{R_{n,i}}$ alone. We showed the right hand side is simply $\left(\frac{1}{2}\right)^n$, so it suffices to show $p(s_1,\ldots,s_n) = \frac{1}{2^n}$. Recall that $p(s_1,\ldots,s_n) = P\left(\widetilde{R_{n,1}} = s_1,\ldots,\widetilde{R_{n,n}} = s_n\right)$. Let $\boldsymbol{t} \in \{0,1\}^n$ be such that $t_i = \begin{cases} 0 & \text{if } s_i = -1 \\ 1 & \text{if } s_i = 1. \end{cases}$ F is one-to-one, so there is a unique $\boldsymbol{r} \in \{0,1\}^n$ such that $F(\boldsymbol{r}) = \boldsymbol{t}$. Then the probability of the event $E_{\boldsymbol{s}} = \left(\widetilde{R_{n,1}} = s_1,\ldots,\widetilde{R_{n,n}} = s_n\right)$ is exactly

$$\begin{aligned} \lambda\left(\{x|\,(F(x_1,\ldots,x_n))_1 = t_1,\ldots,(F(x_1,\ldots,x_n))_n = t_n\}\right) &= \lambda\left(\left\{x\middle|F(x_1,\ldots,x_n) = \boldsymbol{t}\right\}\right) \\ &= \lambda\left(\{x|\,(x_1,\ldots,x_n) = \boldsymbol{r}\}\right) \\ &= \lambda(N_{\boldsymbol{r}}) \\ &= \frac{1}{2^n}. \end{aligned}$$

Now suppose $\left(\widetilde{R_{n,i}}|1 \le i \le n\right)$ is as above. Fix $\boldsymbol{r} \in \{0,1\}^n$. $\left(\widetilde{R_{n,1}}(x),\ldots,\widetilde{R_{n,n}}(x)\right)$ is constant on $N_{\boldsymbol{r}}$. Denote that constant value by $G(\boldsymbol{r})$. So $G : \{0,1\}^n \to \{-1,1\}^n$. G is one-to-one since if $\boldsymbol{u} \in \{0,1\}^n$, $\boldsymbol{u} \neq \boldsymbol{r}$, and $G(\boldsymbol{u}) = G(\boldsymbol{r})$, then

$$P\left(\widetilde{R_{n,1}} = (G(\boldsymbol{r}))_1,\ldots,\widetilde{R_{n,n}} = (G(\boldsymbol{r}))_n\right) \ge \lambda(N_{\boldsymbol{r}}) + \lambda(N_{\boldsymbol{u}}) = \frac{1}{2^{n-1}},$$

but by our hypotheses of "balanced" and independent, $P\left(\widetilde{R_{n,1}} = (G(\boldsymbol{r}))_1,\ldots,\widetilde{R_{n,n}} = (G(\boldsymbol{r}))_n\right)$ $= \frac{1}{2^n}$. Since $G : \{0,1\}^n \to \{-1,1\}^n$, and since the domain and target of G are finite sets of the same cardinality, G is one-to-one if and only if it is onto. So we have that G is both one-to-one and onto. Define $F(\boldsymbol{r}) = \boldsymbol{t}$, where $t_i = \begin{cases} 0 & \text{if } (G(\boldsymbol{r}))_i = -1 \\ 1 & \text{if } (G(\boldsymbol{r}))_i = 1. \end{cases}$ Then $S_n(F(x)) = \sum_{i=1}^n (-1)^{1+t_i} = \sum_{i=1}^n \widetilde{R_{n,i}}(x) = \widetilde{S_n}(x)$, i.e., F is as required.

$\square$

Theorem 3.5. *For each n, there are exactly $\prod_{i=0}^n \left(\binom{n}{i}!\right)$ permutations $F : \{0,1\}^n \to \{0,1\}^n$ such that $\widetilde{S_n} = S_n \circ F$.*

Proof. Recall that

$$A_{n,i} = \left\{ \boldsymbol{s} \in \{0,1\}^n \left| \widetilde{S_n}(x) = -n + 2i \text{ for all } x \supseteq \boldsymbol{s} \right. \right\},$$

and let

$$B_{n,i} = \left\{ \boldsymbol{s} \in \{0,1\}^n \left| S_n(\boldsymbol{s}) = -n + 2i \right. \right\}.$$

Let f be a permutation of $\{0,1\}^n$. Then $\widetilde{S_n} = S_n \circ f$ if and only if for all $0 \leq i \leq n$, $f[A_{n,i}] = B_{n,i}$, i.e., if and only if $f \restriction A_{n,i}$ is a bijection from $A_{n,i}$ to $B_{n,i}$, and of course there are $\binom{n}{i}!$ such bijections. Since $f = \bigcup_{i=0}^{n} (f \restriction A_{n,i})$ and since the $A_{n,i}$ (respectively $B_{n,i}$) are pairwise disjoint, the conclusion is clear. $\square$

Corollary 3.6. *For each n, there are exactly $\prod_{i=0}^{n} \left(\binom{n}{i}!\right)$ families $\left(\widetilde{R_{n,i}} \middle| i = 1, \ldots, n\right)$ as above.*

Theorem 3.5 shows that for all n, there are many permutations, F, of $\{0,1\}^n$ satisfying $\widetilde{S_n} = S_n \circ F$. Are there some additional criteria according to which some of these permutations are more natural than (and therefore preferable to) others? Are there sequences, $(F_n | n \in \mathbb{N}^+)$, of preferred permutations, one for each n, exhibiting some uniformities in terms of n? Is there such a sequence which is also highly effective? The motivation is that by isolating suitable additional criteria and identifying such sequences, we obtain representations of the $\widetilde{S_n}$ which are rather close to those of the S_n. Moreover, the individual permutations "transfer" the computationally pleasant features of each sequence to the other while at the same time crystallizing the differences between the chaotic S_n and the orderly $\widetilde{S_n}$. A potentially important different view of what is at issue is that each permutation of $\{0,1\}^n$ amounts to a re-ordering of $\{0,1\}^n$, different from the usual lexicographical order (which is the restriction of the usual metric ordering of $(0,1)$ to the dyadic rationals).

Before turning to the next Chapter, where we establish some positive answers to the questions of the previous paragraph, we put forward our current understanding of the "right criteria". It should be noted that we view the positive answer to the second and third questions, above, as so important that we have put the "yes" answer as the first of our critera, even though this is something of a misnomer: the remaining criteria state properties of the individual F_n, whereas the first one requires the existence of a "nice" sequence all of whose terms satisfy the remaining criteria.

Definition 3.7. $(F_n | n \in \mathbb{N}^+)$ is *suitable* if and only if for all n, F_n is a permutation of $\{0,1\}^n$ satisfying $\widetilde{S_n} = S_n \circ F$ and such that:

(a) $(F_n | n \in \mathbb{N}^+)$ is explicitly and naturally definable, uniformly and highly effectively in n,

(b) if $\boldsymbol{r} \in \{0,1\}^n$ and $\widetilde{S_n}(\boldsymbol{r}) = S_n(\boldsymbol{r})$, then $F_n(\boldsymbol{r}) = \boldsymbol{r}$,

(c) F_n is "as close as possible" to being self-inverse (it is not hard to show that even for fairly small n (such as $n = 5, 6, 7$), it is impossible for F_n to literally be self-inverse).

Note that criterion (b) amounts to imposing on the bijections between the $A_{n,i}$ and $B_{n,i}$ that they should be the identity on the intersection.

For $\boldsymbol{r}, \boldsymbol{s} \in \{0,1\}^n$, if $F_n(\boldsymbol{r}) = \boldsymbol{s}$ and $F_n(\boldsymbol{s}) = \boldsymbol{r}$, then the orbit of $\boldsymbol{r}$ under F_n is just $\{r, s\}$, and, then we refer to $(\boldsymbol{r}, \boldsymbol{s})$ as a "swap"; this includes the case where $\boldsymbol{r} = \boldsymbol{s}$. If every $\boldsymbol{r} \in \{0,1\}^n$ is in a swap, then F_n is literally self-inverse. Thus, a reformulation of criterion (c) is: the number of non-identity swaps is as large as possible.

Having formulated the notion of suitable sequence, a basic issue (alluded to at the outset of the discussion leading to Definition 3.7) immediately arises:

Problem 3.8. Show that suitable sequences exist.

The next (and final) Chapter is devoted to our (positive) solution of this problem.

Chapter 4

Suitable Effective Representations

In this Chapter, we prove one of our main results, solving Problem 3.8 by answering, in the affirmative, the questions posed prior to Definition 3.7. There are (in the terminology of this definition) suitable sequences $(F_n|n \in \mathbb{N}^+)$ of permutations, and therefore, by Theorem 3.4, the corresponding sequences $\left(\left(\widetilde{R_{n,i}}|1 \leq i \leq n\right)|n \in \mathbb{N}^+\right)$ of representations of the $\widetilde{S_n}$ are also uniform and highly effective. This is the conjunction of Lemma 4.13 and Theorem 4.14, in §4.3.

In order to introduce many of the main ideas in a simpler setting, in §4.2, we prove the existence of a simpler variant, $(G_n|n \in \mathbb{N}^+)$ which satisfies the same composition equation and criteria (a), (b), but not criterion (c) of Definition 3.7. Lemma 4.6 and Theorem 4.8 are the analogues, for the sequence $(G_n|n \in \mathbb{N}^+)$, of Lemma 4.13 and Theorem 4.14. In Lemmas 4.12 and 4.23 we establish an additional desirable property of $(G_n|n \in \mathbb{N}^+)$, $(F_n|n \in \mathbb{N}^+)$, respectively: each G_n (respectively F_n) "commutes with dualization".

We establish the effectiveness of $(G_n|n \in \mathbb{N}^+)$ and $(F_n|n \in \mathbb{N}^+)$ by showing that they are uniformly primitive recursive in the sense that there are primitive recursive functions $G(n, \kappa)$, $F(n, \kappa)$ such that for all $n \in \mathbb{N}^+$ and all $0 \leq \kappa < 2^n$, $G_n(\kappa) = G(n, \kappa)$, $F_n(\kappa) = F(n, \kappa)$. While primitive recursion is a standard notion in computability theory, in §4.1 we supply an overview of what is involved with the intent of making the proofs of Theorems 4.8, 4.14 accessible to the reader with no prior knowledge of computability theory. At the end of this section, we also exploit the discussion at the end of §3.2 in order to deal with permutations of $\{0, \ldots, 2^n - 1\}$ rather than of $\{0, 1\}^n$, this allows for a "smooth" application, in §4.2, 4.3, of the primitive recursion notions introduced in §4.1.

4.1 Primitive Recursion: an Overview

A d-place relation on $\mathbb{N}$ is said to be primitive recursive if and only if its characteristic function (as a subset of $\mathbb{N}^d$) is a primitive recursive function. The primitive recursive functions and relations form very natural subcollections of the collections of computable functions and decidable relations, respectively, and they enjoy very pleasant properties. Starting from a very simple collection of (very simple) initial functions, closing under the operations of substitution and primitive recursion generates the collection of primitive recursive functions. The initial functions are the (one-place) constant zero function, the (one-place) successor function, and the projection functions, i.e., for $1 \leq i \leq n$, U_i^n, where $U_i^n(x_1, \ldots, x_n) = x_i$. We will not give a detailed presentation here of the operation of substitution; suffice it to say that it is a generalization of composition of functions appropriate for the context of functions of several variables.

We do, however, present the operation of primitive recursion; if $n \geq 0$ and f and g are total (i.e. everywhere defined) n-place, $n+2$-place functions, respectively (a zero-place function is a constant), then the (total $n+1$-place) function h whose definition follows is the function obtained from f,g by primitive recursion.

$$h(\overrightarrow{x}, 0) := f(\overrightarrow{x}) \;\; (= \text{the constant } a, \text{ if } n = 0),$$

$$h(\overrightarrow{x}, y+1) := g(\overrightarrow{x}, y, h(\overrightarrow{x}, y)).$$

The following familiar simple applications show the operations of addition and multiplication are primitive recursive. For addition,

$$x + 0 = x,$$

$$x + (y+1) = (x+y) + 1.$$

Formally, we take f to be the identity function and g to be the successor of $U_3^3(x, y, z)$. For multiplication,

$$x0 = 0,$$

$$x(y+1) = xy + x.$$

Formally, f is the constant zero function and $g(x,y,z) = z + x = U_3^3(x,y,z) + U_1^3(x,y,z)$.

Standard Computability texts, e.g. Cutland [1], develop additional closure properties of the collections of primitive recursive functions and relations, some of which we use below without comment, and also begin to build a catalogue of interesting primitive recursive functions, including the ones discussed in the next few paragraphs. Some of these interesting primitive recursive functions we single out as definitions because of the important role they play in what follows.

One important closure property is closure under the bounded minimalization operation. The closure property is that if f is primitive recursive, then so is g, the function obtained from f by bounded minimalization, i.e., if $f : \mathbb{N}^{n+1} \to \mathbb{N}$ is primitive recursive, then so is $g : \mathbb{N}^{n+1} \to \mathbb{N}$, where

$$g(\overrightarrow{x}, y) = (\mu z < y)(f(\overrightarrow{x}, z) = 0)\text{, i.e.,}$$

$$g(\overrightarrow{x}, y) = \begin{cases} \text{the least } z < y & \text{such that } f(\overrightarrow{x}, z) = 0\text{, if such a } z \text{ exists;} \\ y & \text{if there is no such } z. \end{cases}$$

Remark 4.1. Just as the class of primitive recursive functions is closed under bounded minimalization, the class of primitive recursive relations is closed under the bounded quantifiers $(\forall x < y)$, $(\exists x < y)$. The combination of these closure properties is particularly powerful when we can find (as a primitive recursive function of the remaining variables) a suitable bound for the bounded minimalization operator and the bounded quantifiers. An example of such a bound will be the notion of a "master code" introduced in §4.2.

Now we develop some machinary for the coding of finite sequences of natural numbers by natural numbers. There are various approaches to such a coding, including Godel's coding by prime powers, but we will prefer a slight variant of one developed in [1] (shifting indices down to allow 0 as an index value in various places), since the prominent role played by the binary expansion dovetails nicely with our concerns. Note that the section of [1] developing the coding only talks about computable functions, although the proofs that are provided establish primitive recursiveness, and this is important for our purposes.

The sequence coding is accomplished by a bijection $\tau : \bigcup_d \mathbb{N}^{d+1} \to \mathbb{N}$ defined by

$$\tau(a_0, \ldots, a_d) = 2^{a_0} + 2^{a_0+a_1+1} + 2^{a_0+a_1+a_2+2} + \ldots + 2^{a_0+a_1+\ldots+a_d+d} - 1.$$

For $i \leq d$, it will be helpful, in what follows, to define b_i to be the exponent of 2 in the i^{th}

term of the previous formula. If we wanted to have 0 available for coding the empty sequence, we could omit the final -1, but the approach we have taken is more natural for our purposes. While τ is clearly "effectively computable" intuitively, it would be formally incorrect to call it primitive recursive because of its domain. We take the usual way around this; we will develop primitive recursive functions $l(t)$ and $a(i,t)$ such that for all finite sequences $(a_0, \ldots, a_d)$, setting $t = \tau(a_0, \ldots, a_d)$, we will have $l(t) = d+1$ and for all $i \leq d$

$$a(i,t) = a_i.$$

Thus $\tau^{-1}(t) = (a(0,t), \ldots, a(l(t)-1, t))$.

In the discussion that follows we use $\dot{-}$ to denote the binary operation of so-called cutoff subtraction, which is defined so as to give value 0 if the second argument is greater than the first, and is thus total on $\mathbb{N}^2$. This turns out to be a primitive recursive function. We will also make use of the two-place primitive recursive function $\exp(a,b)$ defined to be the exponent of a in b, i.e., the largest c such that a^c divides b (when $a, b \geq 2$), and an appropriate default value otherwise.

The first step toward showing that l and a are primitive recursive is to define a function σ. The idea is that (with t as above)

$$\sigma(0,t) = 0,$$

and for $0 < i \leq l(t)$ it should turn out that $\sigma(i,t) = \tau(a_0, \ldots, a_{i-1})$. Of course, since σ is a stepping stone to showing that l, a are primitive recursive, we have to take another approach to obtaining the second equation. Indeed, we define σ by primitive recursion:

$$\sigma(0,t) = 0,$$

(as desired) and

$$\sigma(s+1,t) = \begin{cases} t+1 & \text{if } \sigma(s,t) \geq t+1 \\ \sigma(s,t) + 2^{\exp(2, t+1 \dot{-} \sigma(s,t))} & \text{otherwise.} \end{cases}$$

The condition in the first case will turn out to hold if $l(t) \leq s$, and the exponent of 2 in the second case will turn out to be b_{s+1}. Now we can state:

$$l(t) := (\mu s < t+1)(t+1 = \sigma(s,t)),$$

$$b(i,t) := \begin{cases} \exp(2, t+1-\sigma(i,t)) & \text{if } i \le l(t) \\ 0 & \text{if } i > l(t), \end{cases}$$

$$a(i,t) = \begin{cases} b(i,t) & \text{if } i = 0 \\ b(i,t) - b(i-1,t) - i & \text{if } 0 < i < l(t) \\ 0 & \text{if } i \ge l(t). \end{cases}$$

Remark 4.2. In view of the preceding, l, a (and b) are primitive recursive. This is because the two-place functions addition, cut-off subtraction, exponentiation, and exp are all primitive recursive, and because the collection of primitive recursive functions is closed under definition by cases, primitive recursion (of course), and bounded minimalization (which is used in the definition of l, and extensively in what follows).

The functions κ_n, defined at the end of §3.2 (just prior to Figure 3.1) allow us to transfer notions naturally associated with $\{0,1\}^n$ to $[0,2^n) \cap \mathbb{N}$. In particular, we could define Weight (κ) to be Weight $(\boldsymbol{r})$, where $\kappa = \kappa_n(\boldsymbol{r})$, i.e., Weight (κ) is the number of 1's in the binary expansion of κ. We will proceed somewhat differently so as to emphasize that Weight (κ) is independent of n and, even more importantly, is a primitive recursive function of κ. But it is important to realize that the following definition of Weight (κ) coincides with the informal definition we have just given.

Definition 4.3. For $\kappa \in \mathbb{N}$,

$$\text{Weight}(\kappa) := l(\kappa),$$

and for $n \in \mathbb{N}^+$, $\kappa \in [0,2^n) \cap \mathbb{N}$,

$$\text{Step}(n,\kappa) := (\mu i < n+1)\left(\kappa < \sum_{j=0}^{i} \binom{n}{j}\right).$$

Note that then Step (n,κ) is that i such that step $A_{n,i}$ includes the dyadic interval $\left[\frac{\kappa}{2^n}, \frac{\kappa+1}{2^n}\right)$, or, simply the level n interval κ, according to the conventions established in the final paragraphs of §3.2. Using well known properties of primitive recursive functions, the functions Step and Weight are primitive recursive. We will sometimes denote $\mathrm{Step}(n, \kappa)$ by $\mathrm{Step}_n(\kappa)$. When $\mathrm{Step}_n(\kappa) \neq \mathrm{Weight}(\kappa)$, we say κ is "out of place" at level n.

Remark 4.4. Note that, for each $n \in \mathbb{N}^+$ and for $\kappa \in [0, 2^n) \cap \mathbb{N}$, we have $0 \leq \mathrm{Weight}(\kappa), \mathrm{Step}_n(\kappa) \leq n$ and Weight, Step satisfy the dualization equations $\mathrm{Weight}(\kappa) = n - \mathrm{Weight}(2^n - 1 - \kappa)$, $\mathrm{Step}_n(\kappa) = n - \mathrm{Step}_n(2^n - 1 - \kappa)$.

Remark 4.5. An important theme in what follows will be the use of bounded minimalization and the bounded quantifiers in definitions which establish that various functions and relations are primitive recursive. In many cases, the minimalization or quantification will be over natural numbers which are to be codes of the increasing enumerations of certain finite sets of natural numbers. Thus, it will be important, as noted in Remark 4.1, to be able to find a bound (as it turns out, as a primitive recursive function of n alone) for all of the codes of interest. The "master code" function, $MC(n)$, introduced in Definition 4.9, below, and discussed more fully in Appendix I, will serve this purpose.

4.2 A Simple Variant and Some General Methods

After this brief introduction to primitive recursion, we pick up the thread of Definition 3.7. As we will see (Remark 4.22, in §4.3), there is a fairly wide range of suitable sequences $(F_n | n \in \mathbb{N}^+)$. In §4.3 we will present our current preferred one. As a "warm-up", we will first present a variant, $(G_n | n \in \mathbb{N}^+)$, satisfying only the first two criteria of Definition 3.7. $(G_n | n \in \mathbb{N}^+)$ will also have the property that each G_n will satisfy the composition equation, $\widetilde{S_n} = S_n \circ G_n$, i.e., each G_n will "map Step to Weight" (i.e., $\mathrm{Step}_n(\kappa) = \mathrm{Weight}(G_n(\kappa))$), and what is more, the mapping will be in an order-preserving fashion (except as ruled out by criterion (b) of Definition 3.7). This means that for all $0 \leq \kappa < 2^n$,

(i) If $\mathrm{Step}_n(\kappa) = \mathrm{Weight}(\kappa)$, then $G_n(\kappa) = \kappa$,

(ii) If $\mathrm{Step}_n(\kappa) \neq \mathrm{Weight}(\kappa)$, and, if further, $\kappa < m < 2^n$ and $\mathrm{Step}_n(\kappa) = \mathrm{Step}_n(m) \neq \mathrm{Weight}(m)$, then $G_n(\kappa) < G_n(m)$.

Lemma 4.6. *(i) and (ii) define a unique sequence $(G_n | n \in \mathbb{N}^+)$ such that each G_n satisfies the composition equation $S_n \circ G_n = \widetilde{S_n}$.*

Proof. Recall that in the proof of Theorem 3.5 we defined subsets $A_{n,i}$ and $B_{n,i}$ of $\{0,1\}^n$, which, via the identification provided by the function κ_n of §3.2, we now choose to view as the corresponding subsets of $[0, 2^n) \cap \mathbb{N}$. From this point of view,

$$A_{n,i} = \{\kappa | \mathrm{Step}_n(\kappa) = i\},$$

$$B_{n,i} = \{\kappa | \mathrm{Weight}(\kappa) = i\}.$$

The proof of Theorem 3.5 is essentially the simple observation that for any permutation, g, of $\{0,1\}^n$, $S_n \circ g = \widetilde{S_n}$ if and only if

$$\text{for all } 0 \le i \le n,\ g[A_{n,i}] = B_{n,i}, \tag{4.1}$$

together with the (easy) count of the number of g which do satisfy (4.1). This count depends on the fact that for all $0 \le 1 \le n$, $\mathrm{card}(A_{n,i}) = \mathrm{card}(B_{n,i})$ since if this failed for even one i, there would be no g satisfying (4.1), but since $\mathrm{card}(A_{n,i}) = \mathrm{card}(B_{n,i}) = \binom{n}{i}$, the number of such g is as in Theorem 3.5.

From the vantage point of the final remarks of §4.1, criterion (b) of Definition 3.7 is understood as imposing the additional requirement on a permutation, g, of $[0, 2^n) \cap \mathbb{N}$, that for all κ, if $\mathrm{Step}_n(\kappa) = \mathrm{Weight}(\kappa)$, then $g(\kappa) = \kappa$. Suppose that $0 \le i \le n$ and $\kappa \in A_{n,i}$. Note that $\mathrm{Step}_n(\kappa) = \mathrm{Weight}(\kappa)$ if and only if $\kappa \in A_{n,i} \cap B_{n,i}$. Thus, what is imposed by criterion (b) is:

$$\text{for all } 0 \le i \le n,\ g \restriction (A_{n,i} \cap B_{n,i}) = \mathrm{id} \restriction (A_{n,i} \cap B_{n,i}). \tag{4.2}$$

Then, putting together (4.1) and (4.2), we must have

$$\text{for all } 0 \le i \le n,\ g[A_{n,i} \setminus B_{n,i}] = B_{n,i} \setminus A_{n,i}. \tag{4.3}$$

Arguing as for Theorem 3.5, there will be some g satisfying (4.2), (4.3) if and only if

$$\text{for all } 0 \le i \le n,\ \mathrm{card}(A_{n,i} \setminus B_{n,i}) = \mathrm{card}(B_{n,i} \setminus A_{n,i}); \tag{4.4}$$

further, if (4.4) is true, then we can, for each $0 \le i \le n$, choose $g \restriction (A_{n,i} \setminus B_{n,i})$ to be the unique order-preserving map from $A_{n,i} \setminus B_{n,i}$ to $B_{n,i} \setminus A_{n,i}$, i.e., in order to complete the proof of the Lemma it suffices to verify (4.4). Happily, this is immediate since $A_{n,i} \setminus B_{n,i} =$

$A_{n,i} \smallsetminus (A_{n,i} \cap B_{n,i})$; $B_{n,i} \smallsetminus A_{n,i} = B_{n,i} \smallsetminus (A_{n,i} \cap B_{n,i})$, and so

$$\begin{aligned} \operatorname{card}(A_{n,i} \smallsetminus B_{n,i}) &= \operatorname{card} A_{n,i} - \operatorname{card}(A_{n,i} \cap B_{n,i}) \\ &= \operatorname{card} B_{n,i} - \operatorname{card}(A_{n,i} \cap B_{n,i}) \\ &= \operatorname{card}(B_{n,i} \smallsetminus A_{n,i}). \end{aligned} \tag{4.5}$$

The procedure we have just described is obviously uniform in n, and therefore we have satisfied the "uniformity part" of criterion (a) as well. The "effectiveness part" of criterion (a) will be established in Theorem 4.8. □

Remark 4.7. With an eye to upcoming developments, in the previous proof, we could have defined:

$$A_{n,i}^1 := A_{n,i} \smallsetminus B_{n,i} = A_{n,i} \smallsetminus (A_{n,i} \cap B_{n,i}),$$

$$B_{n,i}^1 := B_{n,i} \smallsetminus A_{n,i} = B_{n,i} \smallsetminus (A_{n,i} \cap B_{n,i}).$$

These are the sets of things that are out of place on the i^{th} step, or of the i^{th} weight, respectively. From this point of view, note that (4.5) is really the following equation:

$$\operatorname{card}\left(A_{n,i}^1\right) = \binom{n}{i} - \operatorname{card}(A_{n,i} \cap B_{n,i}) = \operatorname{card}\left(B_{n,i}^1\right),$$

while (4.3) becomes $g\left[A_{n,i}^1\right] = B_{n,i}^1$.

In fact, our construction of $(G_n | n \in \mathbb{N}^+)$ fits into a more general framework. Certain types of procedures will always yield sequences of permutations satisfying the composition equations and the first two criteria of Definition 3.7. By (4.4), any permutation, g, of $[0, 2^n) \cap \mathbb{N}$ satisfying (4.3) will satisfy the composition equations $S_n \circ g = \widetilde{S_n}$ and criterion (b) of Definition 3.7. The procedure starts with the sets $A_{n,i}, B_{n,i}$ (stage zero), where $\operatorname{card}(A_{n,i}) = \operatorname{card}(B_{n,i})$. In stage one, we remove $A_{n,i} \cap B_{n,i}$ (on which we have a prescribed (by criterion (b)) method of defining g) from both, leaving $A_{n,i}^1, B_{n,i}^1$, and we have $\operatorname{card}\left(A_{n,i}^1\right) = \operatorname{card}\left(B_{n,i}^1\right)$. The procedure continues by determining our bijection between $A_{n,i}^1$ and $B_{n,i}^1$.

In our construction of the sequence $(G_n | n \in \mathbb{N}^+)$ above, we were only trying to satisfy $s^* = 1$ criterion: criterion (b). In a more general setting (e.g., that of the construction of $(F_n | n \in \mathbb{N}^+)$ in §4.3) we will try to satisfy $s^* > 1$ criteria, always including criterion (b). We enumerate these criteria as $c_1, \ldots, c_{s^*}$, always taking criterion (b) to be c_1. We will satisfy these criteria in stages, dealing with c_s in stage s. Thus, the passage from stage zero to stage one will always be as above. At each stage $0 \leq s \leq s^*$ we will have subsets $A^s_{n,i} \subseteq A_{n,i}$, $B^s_{n,i} \subseteq B_{n,i}$ with $\mathrm{card}\left(A^s_{n,i}\right) = \mathrm{card}\left(B^s_{n,i}\right)$. In particular, we'll have $A^0_{n,i} = A_{n,i}$, $B^0_{n,i} = B_{n,i}$ and $A^1_{n,i}, B^1_{n,i}$ as above. $A^s_{n,i}, B^s_{n,i}$ will be "what is left" of $A_{n,i}, B_{n,i}$, respectively, after satisfying $c_1, \ldots, c_{s-1}$.

The terminal stage will always be stage s^*+1, and we will always pass from stage s^* to stage s^*+1 as we passed from stage one to stage two in the construction, above, of $(G_n | n \in \mathbb{N}^+)$: we simply take the order-preserving bijections from $A^{s^*}_{n,i}$ to $B^{s^*}_{n,i}$. Before indicating how to proceed at intermediate stages s where $0 \leq s < s^*$, we should note that there is really a fixed order in which the criteria must be enumerated (beyond the mere stipulation that c_1 is to be criterion (b)). This has to do with the priority assigned to the criteria (higher priority criteria are dealt with earlier) but also with the way we must be able to satisfy them.

At an intermediate stage s, as above, we must be able to satisfy c_s by choosing non-empty subsets $a^s_{n,i}, b^s_{n,i}$ of $A^s_{n,i}, B^s_{n,i}$, with $\mathrm{card}\left(a^s_{n,i}\right) = \mathrm{card}\left(b^s_{n,i}\right)$, and, for each (n,i) choosing $h^s_{n,i}$ from a nonempty set of "admissable" bijections from $a^s_{n,i}$ to $b^s_{n,i}$, and declaring that $g \restriction a^s_{n,i} = h^s_{n,i}$. This was the situation in the above construction of $(G_n | n \in \mathbb{N}^+)$ with $s = 0$:

$$a^0_{n,i} = b^0_{n,i} = A^0_{n,i} \cap B^0_{n,i} = A_{n,i} \cap B_{n,i},$$

and the only "admissable" bijection is the identity. In the more general setting, with $s > 0$, things will be more complicated. For such s, $A^s_{n,i} \cap B^s_{n,i} = \emptyset$ (by the construction of the $A^1_{n,i}, B^1_{n,i}$), and typically (as in §4.3), for some index set $\mathrm{IND}(n)$ we will have that $a^s_{n,i} = \bigsqcup_{u \in \mathrm{IND}(n)} a^s_{n,i,u}$, $b^s_{n,i} = \bigsqcup_{u \in \mathrm{IND}(n)} b^s_{n,i,u}$, where for each (n,i,u), $\mathrm{card}\left(a^s_{n,i,u}\right) = \mathrm{card}\left(b^s_{n,i,u}\right)$. Also, typically $h^s_{n,i}$ will not be the order-preserving bijection from $a^s_{n,i}$ to $b^s_{n,i}$, but this will be true on the smaller pieces: we will typically be able to take $h^s_{n,i} \restriction a^s_{n,i,u}$ to be the order-preserving bijection from $a^s_{n,i,u}$ to $b^s_{n,i,u}$. Finally, we complete the passage from stage s to stage $s+1$ by (predictably) defining $A^{s+1}_{n,i} = A^s_{n,i} \smallsetminus a^s_{n,i}$, $B^{s+1}_{n,i} = B^s_{n,i} \smallsetminus b^s_{n,i}$. For future reference, notably looking ahead to the "out of swaps" case in the proof of Theorem 4.14, for all $s < s^*+1$, $\bigcup_i a^s_{n,i} = \bigcup_i b^s_{n,i}$, and therefore (by induction), for all $s \leq s^*+1$, $\bigcup_i A^s_{n,i} = \bigcup_i B^s_{n,i}$.

Just as in the above construction of $(G_n | n \in \mathbb{N}^+)$, the criteria, c_s, will be uniform in n, i.e., the definitions of $\mathrm{IND}(n)$ and the $\left(a^s_{n,i,u} | 0 \leq i \leq n, u \in \mathrm{IND}(n)\right)$, $\left(b^s_{n,i,u} | 0 \leq i \leq n, u \in \mathrm{IND}(n)\right)$, $\left(h^s_{n,i,u} | 0 \leq i \leq n, u \in \mathrm{IND}(n)\right)$ will be uniform in n. This being the case, just as in the construction of $(G_n | n \in \mathbb{N}^+)$ above, the procedure will specify a sequence of bijections $(g_n | n \in \mathbb{N}^+)$ whose definition is uniform in n, and so we have satisfied the uniformity part of criterion (a) of Definition 3.7.

Our next result will supply an even stronger notion of uniformity. We will prove $(G_n | n \in \mathbb{N}^+)$ is uniformly primitive recursive in the following precise sense: there exists a single primitive recursive function $G(n,\kappa)$ such that for all n, $G(n,\cdot) \upharpoonright \{0,\ldots,2^n-1\} = G_n$. In fact, if we simply take $G(n,\kappa)$ to be equal to $G_n(\kappa)$, when $0 \le \kappa < 2^n$, and supply a suitable default value (e.g., $G(n,\kappa) = 0$, or $G(n,\kappa) = \kappa$), when $\kappa \ge 2^n$ or $n = 0$, then we have defined a unique function $G : \mathbb{N}^2 \to \mathbb{N}$. The issue is whether this G is primitive recursive. We now prove that it is.

Theorem 4.8. *The function $G(n,\kappa)$ which we have just defined is primitive recursive.*

Proof. We define two primitive recursive three-place relations. Let $W(\kappa,n,i)$ be the relation "$0 \le \kappa < 2^n$ and $\text{Weight}(\kappa) = i \ne \text{Step}(n,\kappa)$". Let $S(\kappa,n,i)$ be the relation "$0 \le \kappa < 2^n$ and $\text{Step}(n,\kappa) = i \ne \text{Weight}(\kappa)$". Then the relations W and S are primitive recursive. Observe that $\{\kappa | S(\kappa,n,i)\} = A^1_{n,i}$, $\{\kappa | W(\kappa,n,i)\} = B^1_{n,i}$.

For $0 \le i \le n$ and $0 \le \kappa < 2^n$, let $w(n,i)$, $s(n,i)$ be the τ-codes (as functions of (n,i), which we will see are primitive recursive) of the increasing enumerations of $\{\kappa | W(\kappa,n,i)\}$, $\{\kappa | S(\kappa,n,i)\}$, respectively. These are typical codes for which we want to find a bound (see the discussion in Remark 4.5 above). The largest possible cardinality of each of the sets $\{\kappa | W(\kappa,n,i)\}$, $\{\kappa | S(\kappa,n,i)\}$ is $\binom{n}{\left[\frac{n}{2}\right]}$, which we will denote by $q(n)$.

In §4.3 we will need to obtain the codes of the increasing enumerations of more complicated sets, but what we do next for $S(\kappa,n,i), W(\kappa,n,i)$ presents the main ideas in a simpler setting.

Definition 4.9. MC will denote the master code function and $MC(n)$ will denote its value at level n, i.e., the master code at level n, which we take to be $MC(n) := \tau(2^n-1,\ldots,2^n-1)$ where $(2^n-1,\ldots,2^n-1)$ has length $q(n)$.

Remark 4.10. See the Appendix for a fuller discussion of what is involved in the choice of a master code.

First we require that if t is the code of the increasing enumeration of $\{\kappa | W(\kappa,n,i)\}$, then "$t$ codes an increasing sequence all of whose coordinates satisfy primitive recursive condition $W(\kappa,n,i)$":

$$(\forall s < l(t))\,(W(a(s,t),n,i) \wedge (s+1 < l(t) \to a(s,t) < a(s+1,t))). \tag{4.6}$$

Let $W_1(n,i,t)$ be the three-place relation defined by (4.6). To make sure t codes the increasing enumeration of all of $\{\kappa | W(\kappa,n,i)\}$ we need:

$$W_1(n,i,t) \wedge (\forall \kappa < 2^n)(W(\kappa,n,i) \to (\exists s < l(t))(a(s,t) = \kappa)). \tag{4.7}$$

Let $W_2(n,i,t)$ be the three-place relation defined by (4.7). Analogously, if t is the code of the increasing enumeration of $\{\kappa | S(\kappa,n,i)\}$, we require that "$t$ codes an increasing sequence all of whose coordinates satisfy primitive recursive condition $S(\kappa,n,i)$":

$$(\forall s < l(t))(S(a(s,t),n,i) \wedge (s+1 < l(t) \to a(s,t) < a(s+1,t))). \tag{4.8}$$

Let $S_1(n,i,t)$ be the three-place relation defined by (4.8). To make sure t codes the increasing enumeration of all of $\{\kappa | S(\kappa,n,i)\}$ we need:

$$S_1(n,i,t) \wedge (\forall \kappa < 2^n)(S(\kappa,n,i) \to (\exists s < l(t))(a(s,t) = \kappa)). \tag{4.9}$$

Finally, let $S_2(n,i,t)$ be the three-place relation defined by (4.9).

With our master code as defined above, we have that for all n, i as above, $w(n,i), s(n,i) < MC(n)$ and therefore $w(n,i)$ is given by

$$w(n,i) = (\mu t < MC(n))(W_2(n,i,t)),$$

and $s(n,i)$ is given by

$$s(n,i) = (\mu t < MC(n))(S_2(n,i,t)).$$

Definition 4.11. Define the least position of κ in the sequence coded by t as
$lp(\kappa,t) := (\mu s < l(t))(a(s,t) = \kappa)$.

If κ doesn't occur in the sequence coded by t, then $lp(\kappa,t)$ takes the default value associated with the bounded minimalization operator. In what follows, the default will not arise as κ will automatically occur in the relevant coded sequence, namely the sequence coded by $s(n, \mathrm{Step}(n,\kappa))$. We can now define G. For $0 \leq \kappa < 2^n$, $G(n,\kappa) = \kappa$ if $\mathrm{Weight}(\kappa) = \mathrm{Step}(n,\kappa)$. Otherwise, still for $0 \leq \kappa < 2^n$,

$$G(n,\kappa) = a(lp(\kappa, s(n, \mathrm{Step}(n,\kappa))), w(n, \mathrm{Step}(n,\kappa))).$$

Now a more substantial issue arises; we need to be sure that there is no $\kappa_0 \in [0, 2^n) \cap \mathbb{N}$ for which $G(n, \kappa_0)$ takes the default value 0 of the function a. This will follow if we have $l(s(n, \mathrm{Step}(n, \kappa_0))) = l(w(n, \mathrm{Step}(n, \kappa_0)))$, i.e., once we know that the increasing enumeration of $\{\kappa | S(\kappa, n, \mathrm{Step}(n, \kappa_0))\}$ (which is coded by $s(n, \mathrm{Step}(n, \kappa_0))$) has the same length as the increasing enumeration of $\{m | W(m, n, \mathrm{Step}(n, \kappa_0))\}$ (which is coded by $w(n, \mathrm{Step}(n, \kappa_0))$), i.e., once we know that $\{\kappa | S(\kappa, n, \mathrm{Step}(n, \kappa_0))\}$ and $\{m | W(m, n, \mathrm{Step}(n, \kappa_0))\}$ have the same cardinality. We have that $\{\kappa | S(\kappa, n, i)\} = A^1_{n,i}$, $\{\kappa | W(\kappa, n, i)\} = B^1_{n,i}$, and that the two sets have the same cardinality and so, it indeed follows that there is no $\kappa_0 \in [0, 2^n) \cap \mathbb{N}$ for which $G(n, \kappa_0)$ takes the default value 0 of the function a. So, as required, G (with a suitable default when $\kappa \geq 2^n$ or $n = 0$) is primitive recursive.

□

Since G_n satisfies criterion (b) of Definition 3.7, for fixed n, and for each $\kappa \in [0, 2^n) \cap \mathbb{N}$ such that $\mathrm{Step}(n, \kappa) = \mathrm{Weight}(\kappa)$, the orbit of κ under G_n is simply $\{\kappa\}$. For $n = 3, 4, 5, 6, 7$ and each κ such that $\mathrm{Step}(n, \kappa) \neq \mathrm{Weight}(\kappa)$ (i.e., κ is out of place at level n), the orbit of κ under G_n is presented in the table below.

Table 4.1: Some orbits under G_n

n	Orbits under G_n
3	$\{3, 4\}$
4	$\{7, 3, 8, 12\}$
5	$\{16, 7, 3, 8, 5\}, \{15, 24, 28, 23, 26\}, \{11, 17\}, \{13, 18\}, \{14, 20\}$
6	$\{32, 42, 15, 34, 49, 30, 19, 40, 56, 60, 55, 58, 47, 27, 13, 24, 11, 6\}$, $\{31, 21, 48, 29, 14, 33, 44, 23, 7, 3, 8, 5, 16, 36, 50, 39, 52, 57\}$
7	$\{64, 15, 34, 21, 48, 73, 46, 69, 39, 25, 68, 30, 11, 5, 16, 36, 22, 65, 23, 66, 27, 80, 57, 84, 99, 31, 13, 6, 32, 14, 33, 19, 40, 26, 72, 45, 67, 29, 7\}$, $\{63, 112, 93, 106, 79, 54, 81, 58, 88, 102, 59, 97, 116, 122, 111, 91, 105, 62, 104, 61, 100, 47, 70, 43, 28, 96, 114, 121, 95, 113, 94, 108, 87, 101, 55, 82, 60, 98, 120\}$, $\{3, 8\}, \{51, 74\}, \{53, 76\}, \{124, 119\}$

The next Lemma gives an additional property of G.

Lemma 4.12. *Each G_n satisfies the dualization equation $G_n(2^n - 1 - \kappa) = 2^n - 1 - G_n(\kappa)$.*

Proof. To simplify notation, we take n as fixed (but arbitrary). For $0 < i < n$, let

$$\gamma_i = \text{card}\left(A^1_{n,i}\right),$$

and so,

$$\gamma_i = \text{card}\left(B^1_{n,i}\right)$$

as well. Further, $\gamma_{n-i} = \gamma_i$, for all such i (by Remark 4.4). Let $(\alpha_{i,t}|1 \leq t \leq \gamma_i)$, $(\beta_{i,t}|1 \leq t \leq \gamma_i)$ be the increasing enumerations of $A^1_{n,i}$, $B^1_{n,i}$, respectively . Then we have that for all $0 < i < n$, $G_n(\alpha_{i,t}) = \beta_{i,t}$.

For $\kappa \in \{0, \ldots, 2^n - 1\}$, let $\widehat{\kappa}$ denote the dual of κ, i.e., define $\widehat{\kappa} := 2^n - 1 - \kappa$. We also have that for $0 < i < n$ and $1 \leq t \leq \gamma_i$,

$$\widehat{\alpha_{i,t}} = \alpha_{n-i,\gamma_i - t+1},$$

and

$$\widehat{\beta_{i,t}} = \beta_{n-i,\gamma_i - t+1}.$$

So, in particular, the set of duals of elements of $A^1_{n,i}$ (respectively $B^1_{n,i}$) is just $A^1_{n,n-i}$ (respectively $B^1_{n,n-i}$), but with the extra observation that if we enumerate the sets of duals in the order they inherit from the increasing enumerations of $A^1_{n,i}$ (respectively $B^1_{n,i}$), this gives the decreasing enumeration of the sets of duals.

Finally, let $0 < i < n$, and let $\kappa \in A^1_{n,i}$; let t be such that $\kappa = \alpha_{i,t}$. Then $\widehat{\kappa} = \alpha_{n-i,\gamma_i - t+1}$, and so

$$G_n(\widehat{\kappa}) = G_n(\alpha_{n-i,\gamma_i-t+1}) = \beta_{n-i,\gamma_i-t+1},$$

but also, $G_n(\kappa) = \beta_{i,t}$ and so

$$\widehat{G(\kappa)} = \widehat{\beta_{i,t}} = \beta_{n-i,\gamma_i-t+1} = G_n(\widehat{\kappa}).$$

□

4.3 Primitive Recursive Uniform F_n

In this section, we complete our analysis of the $\widetilde{S_n}$. The construction of our preferred suitable sequence $(F_n|n \in \mathbb{N}^+)$ of representing permutations begins in the next paragraph and culminates with the statement of Lemma 4.13, which summarizes what has been achieved. In Theorem 4.14, we show that (in the terminology developed in §4.2 and recalled just prior to the statement of the Theorem) $(F_n|n \in \mathbb{N}^+)$ is uniformly primitive recursive, and therefore highly "effective".

Our construction of $(F_n|n \in \mathbb{N}^+)$ takes place within the general framework provided by §4.2, more precisely, by the discussion between the end of the proof of Lemma 4.6 and the statement of Theorem 4.8. We adopt the notation and terminology of that framework, and draw upon its arguments without further comment, except to explicitly establish the correspondence between the notions introduced below and those of §4.2.

We now have a second criterion to satisfy, criterion (c) of Definition 3.7, which becomes c_2 (criterion (b) of Definition 3.7 remains c_1). Thus we will have $s^* = 2$, and our construction will be in $s^* + 1 = 3$ stages. Just as in §4.2, the uniformity part of criterion (a) of Definition 3.7, will be immediate, since both of our criteria are uniform in n. The effectiveness part of criterion (a) will be established in Theorem 4.14. Since the passages from stage zero to stage one, and from stage two to stage three will be exactly as in §4.2, we focus on the passage from stage one to stage two where we satisfy criterion c_2. This said, in the course of the proof of Theorem 4.14, we will have additional comments on the passage from stage two to stage three.

We define a four-place relation $Q(\kappa, n, i, j)$. Looking ahead to the proof of Theorem 4.14, in fact Q is primitive recursive, but that observation is not needed until then. Let $Q(\kappa, n, i, j)$ be the relation "$0 \leq \kappa < 2^n$ and $\mathrm{Step}(n, \kappa) = i$ and $\mathrm{Weight}(\kappa) = j$". Let $\mathrm{Pair}(n, i, j) := \{\kappa | Q(\kappa, n, i, j)\}$. We will maximize swaps by adopting the "swapping convention": exclude "the extremes" in what participates in the swaps when there is a choice about this, i.e., when the cardinalities of the sets $\mathrm{Pair}(n, i, j)$ and $\mathrm{Pair}(n, j, i)$ are unequal. It is certainly possible for these cardinalities to be unequal, and when this happens, the general approach will be to exclude the d extreme elements from the larger set, where d is the difference between the cardinality of the larger set and the cardinality of the smaller set. To illustrate what is involved in deciding what "extreme" means, an example follows.

When $n = 8$, we have:

$$\mathrm{Pair}(8, 2, 4) = \{15, 23, 27, 29, 30\},$$

while

$$\mathrm{Pair}\,(8,4,2) = \{96, 129, 130, 132, 136, 144, 160\}\,.$$

Observe that there are two extra elements in $\mathrm{Pair}\,(8,4,2)$. Our swapping convention takes the "extremes" to be those elements of the larger set that are farthest away (i.e., have the largest difference in value) from elements of the smaller set, in order that we may minimize the distance (i.e., difference) between two elements in a swap. In our example, we exclude 144 and 160 from participating in swaps, because they are the farthest away from the elements of $\mathrm{Pair}\,(8,2,4)$. We will further discuss the details of the swapping convention in the proof of Theorem 4.14. In particular, we will provide a general method for choosing the extremes.

For $0 < i, j < n$, and $i \neq j$, let $\overline{\mathrm{Pair}}\,(n,i,j)$ be the set of $\kappa \in \mathrm{Pair}\,(n,i,j)$ which are chosen to participate in swaps; thus $\overline{\mathrm{Pair}}\,(n,i,j) = \mathrm{Pair}\,(n,i,j)$ if and only if $\mathrm{card}\,(\mathrm{Pair}\,(n,i,j)) \leq \mathrm{card}\,(\mathrm{Pair}\,(n,j,i))$. Once we have determined the sets $\overline{\mathrm{Pair}}\,(n,i,j)$, the swapping will be done by mapping $\overline{\mathrm{Pair}}\,(n,i,j)$ in an order-preserving fashion onto $\overline{\mathrm{Pair}}\,(n,j,i)$. In the above example, we have

$$\overline{\mathrm{Pair}}\,(8,2,4) = \mathrm{Pair}\,(8,2,4) = \{15, 23, 27, 29, 30\}$$

and

$$\overline{\mathrm{Pair}}\,(8,4,2) = \mathrm{Pair}\,(8,4,2) \smallsetminus \{144, 160\} = \{96, 129, 130, 132, 136\}\,,$$

and the resulting swaps are

$$(15, 96)\,, (23, 129)\,, (27, 130)\,, (29, 132)\,, (30, 136)\,.$$

In terms of the framework of §4.2, we let $\mathrm{IND}\,(n) = \{(i,j)\,|0 < i, j < n, i \neq j\}$, $a^2_{n,i}\,(i,j) = \overline{\mathrm{Pair}}\,(n,i,j)$, $b^2_{n,i}\,(i,j) = \overline{\mathrm{Pair}}\,(n,j,i)$, $h^2_{n,i}\,(i,j)$ be the order-preserving bijection, and then:

$$A^2_{n,i} := A^1_{n,i} \smallsetminus \bigcup_{j \neq i} \overline{\mathrm{Pair}}\,(n,i,j)\,,$$

$$B^2_{n,i} := B^1_{n,i} \smallsetminus \bigcup_{j \neq i} \overline{\mathrm{Pair}}\,(n,j,i)\,.$$

and so $a^2_{n,i} = \bigcup_{j \neq i} \overline{\mathrm{Pair}}\,(n,i,j)$ and $b^2_{n,i} = \bigcup_{j \neq i} \overline{\mathrm{Pair}}\,(n,j,i)$. According to the general framework in §4.2, since $A^1_{n,i}, B^1_{n,i}$ have the same cardinality, and we are removing sets of the same cardinality from each, $\mathrm{card}\left(A^2_{n,i}\right) = \mathrm{card}\left(B^2_{n,i}\right)$. So at stage three, the terminal stage, as specified by the general framework, we map $A^2_{n,i}$ onto $B^2_{n,i}$ in an order-preserving fashion, and mapping Step to Weight is guaranteed, since $A^2_{n,i}, B^2_{n,i}$ are subsets of $A_{n,i}, B_{n,i}$, respectively; thus we have specified a unique sequence $(F_n | n \in \mathbb{N}^+)$ satisfying all the properties of Definition 3.7, except possibly the effectiveness part of criterion (a), and such that each F_n maps Step to Weight.

This discussion proves the following Lemma.

Lemma 4.13. *The procedure we have just described defines a unique sequence $(F_n | n \in \mathbb{N}^+)$ satisfying the composition equations $S_n \circ F_n = \widetilde{S_n}$.*

Just as we did for $(G_n | n \in \mathbb{N}^+)$, we will prove this $(F_n | n \in \mathbb{N}^+)$ is uniformly primitive recursive in the following precise sense: there exists a single primitive recursive function $F(n, \kappa)$ such that for all n, $F(n, \cdot) \restriction \{0, \ldots, 2^n - 1\} = F_n$. As before, if we simply take $F(n, \kappa)$ to be equal to $F_n(\kappa)$, when $0 \leq \kappa < 2^n$, and supply a suitable default value (e.g., $F(n, \kappa) = 0$, or $F(n, \kappa) = \kappa$), when $\kappa \geq 2^n$ or $n = 0$, then we have defined a unique function $F : \mathbb{N}^2 \to \mathbb{N}$.

Theorem 4.14. *The function $F(n, \kappa)$ we have just defined is primitive recursive.*

Proof. As in the proof of Theorem 4.8, in order to satisfy criterion (b) of Definition 3.7, we will have that for $n \in \mathbb{N}^+$ and $\kappa \in [0, 2^n) \cap \mathbb{N}$, $F(n, \kappa) = \kappa$, if $\text{Weight}(\kappa) = \text{Step}(n, \kappa)$. This completes the passage from stage 0 to stage 1 in the construction of Lemma 4.13. Strictly speaking, this should be one case in a final definition by (three) cases of the function F, but we will dispense with this level of formality. However, we will note that the second case (corresponding to the second stage of the construction of Lemma 4.13) is carried out in Definition 4.19, below and the third case (corresponding to the third stage of the construction) is carried out in Definition 4.21. Also, as in the proof of Theorem 4.8, when $n = 0$ or ($n \in \mathbb{N}^+$ and $2^n \leq \kappa$) we supply an appropriate default value for $F(n, \kappa)$. Thus, in what follows, we let $n \in \mathbb{N}^+$ and we let κ vary over $[0, 2^n) \cap \mathbb{N}$, always assuming that $\text{Weight}(\kappa) \neq \text{Step}(n, \kappa)$. We proceed to formalize, in a primitive recursive fashion, the next two stages of the construction.

As should be clear from the construction of Lemma 4.13, the crucial point is to distinguish, in a primitive recursive fashion, which κ are to participate in swaps. Properly understood, this is really a decision about the triple (n, i, j), where $i = \text{Step}(n, \kappa)$, $j = \text{Weight}(\kappa)$: should all the elements of $\text{Pair}(n, i, j)$ participate in swaps? Or only a proper initial (respectively final) segment? This motivates what follows, through the next three definitions.

We will first need to get the code of the increasing enumeration of $\text{Pair}(n, i, j)$ as a primitive recursive function of (n, i, j). In addition to obtaining the code of the increasing enumeration of the whole set Pair (n,i,j), we will also need to obtain the codes of the increasing enumerations of certain subsets. We proceed exactly as in §4.2, starting with the relation Q, defined at the start of the fourth paragraph of this section, instead of the relations S and W. The passages to Q_1 and Q_2 will mirror the passages to S_1, S_2, W_1, W_2. For the increasing enumeration of Pair (n,i,j), we first require that if t is the code, then "t codes an increasing sequence all of whose coordinates satisfy primitive recursive condition $Q(\kappa,n,i,j)$":

$$(\forall s < l(t))\,(Q(a(s,t),n,i,j) \wedge (s+1 < l(t) \to a(s,t) < a(s+1,t))). \tag{4.10}$$

Let $Q_1(n,i,j,t)$ be the four-place relation defined by (4.10). To make sure t codes the increasing enumeration of $\{\kappa | Q(\kappa,n,i,j)\}$ we need:

$$Q_1(n,i,j,t) \wedge (\forall \kappa < 2^n)\,(Q(k,n,i,j) \to (\exists s < l(t))\,(a(s,t) = \kappa)). \tag{4.11}$$

Let $Q_2(n,i,j,t)$ be the four-place relation defined by (4.11). Letting $P(n,i,j)$ denote the code of the increasing enumeration of Pair (n,i,j), using the master code defined in §4.2, we have that $P(n,i,j)$ is given by

$$P(n,i,j) = (\mu t < MC(n))\,(Q_2(n,i,j,t)).$$

Definition 4.15. We define some additional notions.

- $\min^*(n,i,j) := \min(l(P(n,i,j)), l(P(n,j,i)))$.
- $\max^*(n,i,j) := \max(l(P(n,i,j)), l(P(n,j,i)))$.
- $d(n,i,j) := \max^*(n,i,j) - \min^*(n,i,j)$.

Thus, $\min^*(n,i,j) = \max^*(n,i,j)$ if and only if Pair (n,i,j) and Pair (n,j,i) are equipotent, if and only if $d(n,i,j) = 0$; otherwise, $\min^*(n,i,j)$ (respectively $\max^*(n,i,j)$) is the smaller (respectively larger) one of the cardinalities of these two sets, $d(n,i,j)$ is the (positive) difference in cardinalities and we always have $\min^*(n,i,j) = \min^*(n,j,i)$, and similarly for $\max^*$, d.

Definition 4.16. Assume that $n,i,j \in \mathbb{N}$, $0 < i,j < n$, $i \neq j$. In what follows, this will be abbreviated by saying that (n,i,j) is *relevant*.

- (n,i,j) is *simple* if $d(n,i,j) = 0$.

- (n,i,j) is *light* if $l\left(\text{Pair}\left(n,j,i\right)\right) > l\left(\text{Pair}\left(n,i,j\right)\right)$.

- (n,i,j) is *right heavy* (respectively *left heavy*) if $l\left(\text{Pair}\left(n,j,i\right)\right) < l\left(\text{Pair}\left(n,i,j\right)\right)$ and $j < i$ (respectively $i < j$).

- (n,i,j) is *heavy* if and only if it is right heavy or left heavy, i.e., if and only if $l\left(\text{Pair}\left(n,j,i\right)\right) < l\left(\text{Pair}\left(n,i,j\right)\right)$.

Note that (n,i,j) is simple if and only if (n,j,i) is simple and (n,i,j) is light if and only if (n,j,i) is heavy. Also, note that all of the notions in the last two definitions are primitive recursive. As should already by clear, if (n,i,j) is simple or light, then all elements of $\text{Pair}\left(n,i,j\right)$ will participate in swaps (i.e., we will have $\text{Pair}\left(n,i,j\right) = \overline{\text{Pair}}\left(n,i,j\right)$).

We will now indicate why the notion of right heavy (respectively left heavy) correctly formalizes when we will have that $\overline{\text{Pair}}\left(n,i,j\right)$ is the size $\min^{*}\left(n,i,j\right)$ initial (respectively final) segment of $\text{Pair}\left(n,i,j\right)$. This is simply because if $j < i$, then all of the elements of $A_{n,j}$ are smaller than all of the elements of $A_{n,i}$, and so this holds with $\text{Pair}\left(n,j,i\right)$, $\text{Pair}\left(n,i,j\right)$ in place of their respective "full steps". But then clearly it is the smallest elements of $\text{Pair}\left(n,i,j\right)$ that are closest to the elements of $\text{Pair}\left(n,j,i\right)$ with which they are to be swapped.

We are now ready to extract the τ-codes of increasing enumerations of the $\overline{\text{Pair}}\left(n,i,j\right)$.

Definition 4.17. Assume that $n,i,j \in \mathbb{N}$.

- If (n,i,j) is not relevant, set $\overline{P}\left(n,i,j\right) := 0$.

- If (n,i,j) is simple or light, set $\overline{P}\left(n,i,j\right) := P\left(n,i,j\right)$.

- If (n,i,j) is right heavy, set:

$$\overline{P}\left(n,i,j\right) := \left(\mu t < P\left(n,i,j\right)\right)\left(l\left(t\right) = \min^{*}\left(n,i,j\right)\right) \wedge \left(\forall s < l\left(t\right)\right)\left(a\left(s,t\right) = a\left(s,P\left(n,i,j\right)\right)\right).$$

- If (n,i,j) is left heavy, set:

$$\begin{aligned}\overline{P}\left(n,i,j\right) \quad := \quad & \left(\mu t < P\left(n,i,j\right)\right) \\ & \left(l\left(t\right) = \min^{*}\left(n,i,j\right)\right) \wedge \left(\forall s < l\left(t\right)\right)\left(a\left(s,t\right) = a\left(d\left(n,i,j\right)+s, P\left(n,i,j\right)\right)\right).\end{aligned}$$

We are nearly in a position to do our swapping and thereby to complete the passage from stage 1 to stage 2 in the construction. We first develop a few more useful bits of notation, and point out that we can completely characterize the κ involved. Recall that the primitive recursive function $lp(\kappa, t)$ was defined in §4.2, and in non-default situations gives the least (most often, unique) position of κ in the sequence coded by t. The use we now make of this function will not lead to any default situations.

Definition 4.18. Suppose $n, \kappa \in \mathbb{N}$. If $n = 0$ or $\text{Step}(n, \kappa) = \text{Weight}(\kappa)$ or $\kappa \geq 2^n$, set $p(n, \kappa) := 0$. Otherwise, let $i(n, \kappa) := \text{Step}(n, \kappa)$, $j(\kappa) := \text{Weight}(\kappa)$ and set

$$p(n, \kappa) := lp(\kappa, P(n, i(n, \kappa), j(\kappa)))$$

and note that κ ***will participate in swaps at level*** n if and only if $(n, i(n, \kappa), j(\kappa))$ is either simple, light, or (right heavy and $p(n, \kappa) < \min^*(n, i(n, \kappa), j(\kappa))$) or (left heavy and $p(n, \kappa) \geq d(n, i(n, \kappa), j(\kappa))$). If κ does participate in swaps at level n, then let

$$p^*(n, \kappa) := lp\left(\kappa, \overline{P}(n, i(n, \kappa), j(\kappa))\right)$$

(and $= 0$, otherwise).

As usual, these are all primitive recursive notions.

Definition 4.19. If κ participates in swaps at level n, then let

$$F(n, \kappa) := a\left(p^*(n, \kappa), \overline{P}(n, j(\kappa), i(n, \kappa))\right).$$

Thus, we have a primitive recursive implementation of our stage 2. We turn to stage 3, first showing that the sets $A^2_{n,i}$, $B^2_{n,i}$ are primitive recursive. To this end, note: $\kappa \in A^2_{n,i}$ if and only if, letting $i = i(n, \kappa), j = j(\kappa)$:

$$\left((n, i, j) \text{ is heavy} \wedge (\forall s < \min^*(n, i, j))\left(\kappa \neq a\left(s, \overline{P}(n, i, j)\right)\right)\right),$$

and similarly for $\kappa \in B^2_{n,i}$ (interchanging the roles of i and j). Also note that $A^2_{n,i} = \emptyset$ (respectively $B^2_{n,i} = \emptyset$) is a primitive recursive condition on (n, i): $A^2_{n,i} = \emptyset$ if and only if $(\forall \kappa < 2^n)\left(\kappa \notin A^2_{n,i}\right)$.

We then obtain the τ-codes of the increasing enumerations, $ST(n, i)$ and $WT(n, i)$, (taking default 0 when one is empty) of the sets $A^2_{n,i}$, $B^2_{n,i}$, respectively, in the now familiar way:

Definition 4.20. We have

$$\begin{aligned} ST(n,i) &= (\mu t < MC(n))\,(\forall s < l(t))\left(\kappa \in A^2_{n,i} \wedge (s+1 < l(t) \to a(s,t) < a(s+1,t))\right) \\ &\quad \wedge (\forall \kappa < 2^n)\left(\kappa \in A^2_{n,i} \to (\exists s < l(t))\,(\kappa = a(s,t))\right), \end{aligned}$$

$$\begin{aligned} WT(n,i) &= (\mu t < MC(n))\,(\forall s < l(t))\left(\kappa \in B^2_{n,i} \wedge (s+1 < l(t) \to a(s,t) < a(s+1,t))\right) \\ &\quad \wedge (\forall \kappa < 2^n)\left(\kappa \in B^2_{n,i} \to (\exists s < l(t))\,(\kappa = a(s,t))\right). \end{aligned}$$

Finally, we complete our definition of F with a primitive recursive implementation of our passage from stage 2 to stage 3 by:

Definition 4.21. For $\kappa \in A^2_{n,i}$, we define $F(n,\kappa) := a(lp(\kappa, ST(n,i)), WT(n,i))$.

Remark 4.22. In the second sentence of §4.2, we mentioned that there is a fairly wide range of suitable sequences. We are now in a position to back up this assertion. Examining the construction of Lemma 4.13, it is clear that if we were to relax the (crucial) conditions of uniformity and effectiveness, then, instead of taking $F_n \restriction \overline{\text{Pair}}(n,i,j)$ to be the order-preserving bijection to $\overline{\text{Pair}}(n,j,i)$, we could take it to be **any** of the $\min^*(n,i,j)!$ possible bijections from $\overline{\text{Pair}}(n,i,j)$ to $\overline{\text{Pair}}(n,j,i)$. Similarly, in the passage from stage two to stage three, instead of taking $F_n \restriction A^2_{n,i}$ to be the order-preserving bijection to $B^2_{n,i}$, we could take it to be **any** of the $\text{card}\left(A^2_{n,i}\right)!$ such bijections.

In order to recover the crucial conditions of uniformity and effectiveness, it suffices to have some uniform and effective method of making these choices. Thus, a suitable alternative, among many possible ones, to our preferred $(F_n | n \in \mathbb{N}^+)$ would come from always choosing the order-reversing bijection. Another source of variants arises from how we choose which $\min^*(n,i,j)$-many elements of $\text{Pair}(n,i,j)$ to allow into $\overline{\text{Pair}}(n,i,j)$, when $\text{card}(\text{Pair}(n,i,j)) > \text{card}(\text{Pair}(n,j,i))$.

□

As noted in §4.2, the first time there are "out of place" values of κ is when $n = 3$. Below are the graphs of F_n for $n = 3$ and $n = 4$.

Figure 4.1: Graph of F_3

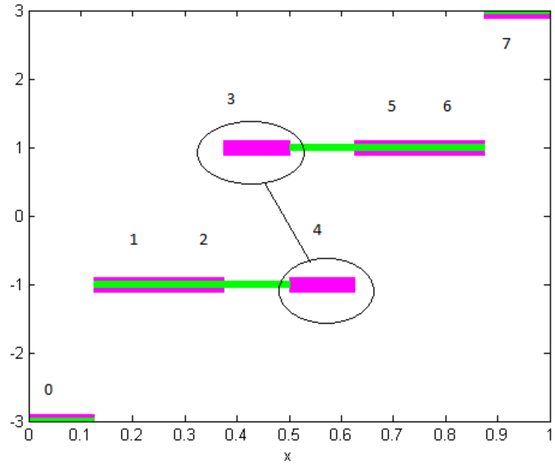
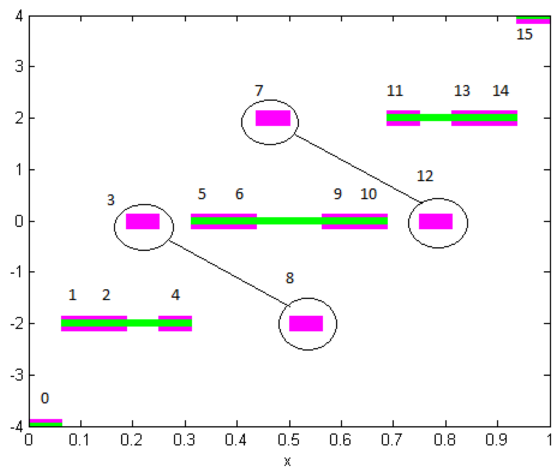


Figure 4.2: Graph of F_4



The first time there are "out of swaps" values of κ is when $n = 5$. For $n = 5, 6, 7$, in the table below we present the orbits under F_n for "out of swaps" values of κ at level n.

Table 4.2: Some orbits under F_n

n	Orbits under F_n
5	$\{16, 28, 15, 3\}$
6	$\{32, 56, 60, 31, 7, 3\}$
7	$\{64, 108, 31, 11, 3\}, \{13, 72, 113, 47\},$ $\{14, 80, 114, 55\}, \{63, 19, 96, 116, 124\}$

The resulting cycles of these “out of swaps” values of κ, corresponding to each of the rows of the table, are illustrated in the graphs below. We have a single four-cycle at $n = 5$ and a single six-cycle at $n = 6$.

Figure 4.3: Graph of F_5

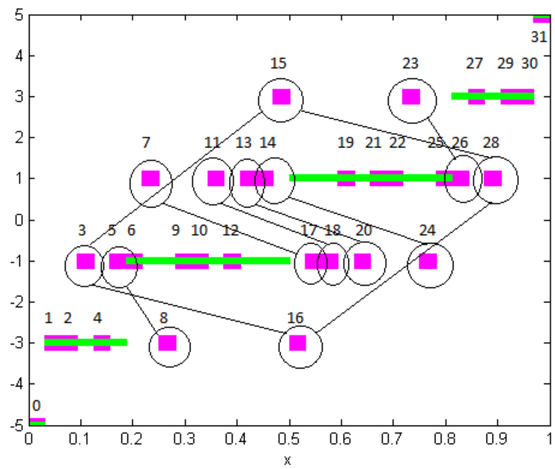
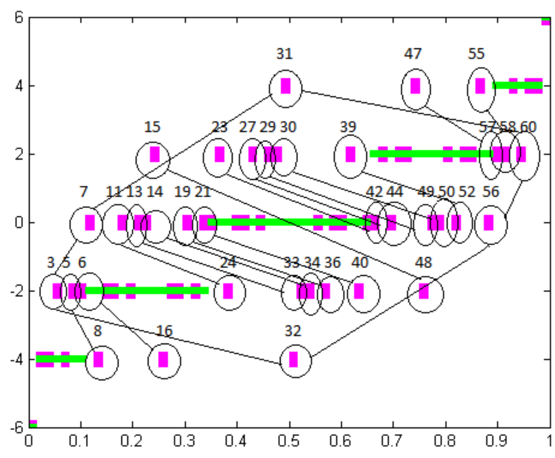
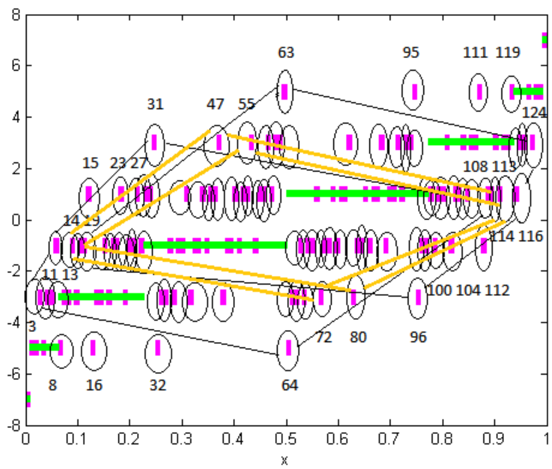


Figure 4.4: Graph of F_6



At $n = 7$ we have two four-cycles and two five-cycles. Because the graph of F_n is rather complicated by $n = 7$, we will leave out the swaps from the picture and only illustrate the cycles. The four-cycles are highlighted in orange in the figure below.

Figure 4.5: Cycles of F_7



As the work of this section demonstrates, the existence of "out of swaps" values of κ at level n, starting at $n = 5$, is the last phenomenon (illustrated in figures 4.3-4.5) to create complications in the definition of the function F. It is conceivable that further interesting phenomena (which do not create additional complications for the definition of F) first occur for some n larger than 5, and it is far from certain whether there are finitely many such n.

The next Lemma proves the dualization property for F.

Lemma 4.23. *Each F_n satisfies the dualization equation $F_n(2^n - 1 - \kappa) = 2^n - 1 - F_n(\kappa)$.*

Proof. To simplify notation, we take n as fixed (but arbitrary). Recall that we denote the dual of κ by $\widehat{\kappa} = 2^n - 1 - \kappa$. We will first show $F_n(\widehat{\kappa}) = \widehat{F_n(\kappa)}$ for κ that is in a swap. For $0 < i < n$, observe that $\mathrm{Pair}(n, n-i, n-j) = \{\widehat{\kappa} | \kappa \in \mathrm{Pair}(n, i, j)\}$. Thus

$$\mathrm{card}(\mathrm{Pair}(n, i, j)) = \mathrm{card}(\mathrm{Pair}(n, n-i, n-j))$$

and

$$\mathrm{card}(\mathrm{Pair}(n, j, i)) = \mathrm{card}(\mathrm{Pair}(n, n-j, n-i)).$$

Thus, $\min^*(n, n-i, n-j) = \min^*(n, i, j)$ for all such i, j. Let $(\delta_{i,j,t} | 1 \le t \le \min^*(n, i, j))$, $(\eta_{i,j,t} | 1 \le t \le \min^*(n, i, j))$ be the increasing enumerations of $\overline{\mathrm{Pair}}(n, i, j)$, $\overline{\mathrm{Pair}}(n, j, i)$, respectively . Then we have that for all $0 < i, j < n$, $F_n(\delta_{i,j,t}) = \eta_{i,j,t}$.

We also have that for $0 < i, j < n$ and $1 \le t \le \min^*(n, i, j)$,

$$\widehat{\delta_{i,j,t}} = \delta_{n-i,n-j,\min^*(n,i,j)-t+1},$$

and

$$\widehat{\eta_{i,j,t}} = \eta_{n-i,n-j,\min^*(n,i,j)-t+1}:$$

just as in the proof of Lemma 4.12, it is obvious that dualization reverses the order of enumeration.

Let $0 < i, j < n$, $\kappa \in \mathrm{Pair}(n, i, j)$ and let t be such that $\kappa = \delta_{i,j,t}$. Then $\widehat{\kappa} = \delta_{n-i,n-j,\min^*(n,i,j)-t+1}$, and so

$$F_n(\widehat{\kappa}) = F_n\left(\delta_{n-i,n-j,\min^*(n,i,j)-t+1}\right) = \eta_{n-i,n-j,\min^*(n,i,j)-t+1},$$

but also, $F_n(\kappa) = \eta_{i,j,t}$ and so

$$\widehat{F(\kappa)} = \widehat{\eta_{i,j,t}} = \eta_{n-i,n-j,\min^*(n,i,j)-t+1} = F_n(\widehat{\kappa}).$$

Now we will show $F_n(\widehat{\kappa}) = \widehat{F_n(\kappa)}$ for "out of swaps" values of κ. For $0 < i < n$, let

$$\xi_i = \mathrm{card}\left(A^2_{n,i}\right),$$

and so,

$$\xi_i = \mathrm{card}\left(B^2_{n,i}\right)$$

as well. Further, we have shown in the discussion preceding Lemma 4.13 that $\xi_{n-i} = \xi_i$, for all such i. Let $(\theta_{i,t} | 1 \le t \le \xi_i)$, $(\psi_{i,t} | 1 \le t \le \xi_i)$ be the increasing enumerations of $A^2_{n,i}$, $B^2_{n,i}$, respectively . Then we have that for all $0 < i < n$, $F_n(\theta_{i,t}) = \psi_{i,t}$.

Now,

$$B^2_{n,i} = \bigcup_{j \neq i} \left(\mathrm{Pair}(n, j, i) \smallsetminus \overline{\mathrm{Pair}}(n, j, i)\right).$$

Suppose for some $0 < i < n$, $1 \le t_1, t_2 \le \xi_i$, $0 < j_1, j_2 < n$ with $j_1, j_2 \neq i$, we have κ_1, κ_2 such that $\kappa_1 = \psi_{i,t_1} \in \mathrm{Pair}(n, j_1, i) \smallsetminus \overline{\mathrm{Pair}}(n, j_1, i)$ and $\kappa_2 = \psi_{i,t_2} \in \mathrm{Pair}(n, j_2, i) \smallsetminus \overline{\mathrm{Pair}}(n, j_2, i)$. If $j_1 < j_2$, then we have

$$\mathrm{Step}_n(\kappa_1) = j_1 < j_2 = \mathrm{Step}_n(\kappa_2),$$

and so, since Step is a non-decreasing function, $\kappa_1 < \kappa_2$. Thus, the natural ordering of elements, $\psi_{i,t} \in B^2_{n,i}$, coincides with the lexicographic ordering of (j,p), where j is such that $\psi_{i,t} \in \mathrm{Pair}(n,j,i) \setminus \overline{\mathrm{Pair}}(n,j,i)$ and p is the position of $\psi_{i,t}$ in $\mathrm{Pair}(n,j,i) \setminus \overline{\mathrm{Pair}}(n,j,i)$. It then follows, much as in §4.2, that for $0 < i < n$ and $1 \le t \le \xi_i$,

$$\widehat{\psi_{i,t}} = \psi_{n-i,\xi_i-t+1}.$$

Finally, let $0 < i < n$, and let $i = \mathrm{Step}_n(\kappa)$; let t be such that $\kappa = \theta_{i,t}$. Then $\widehat{\kappa} = \theta_{n-i,\xi_i-t+1}$. Since $F_n(\theta_{i,t}) = \psi_{i,t}$, we have

$$\widehat{F_n(\kappa)} = \widehat{F_n(\theta_{i,t})} = \widehat{\psi_{i,t}} = \psi_{n-i,\xi_i-t+1} = F_n(\theta_{n-i,\xi_i-t+1}) = F_n(\widehat{\kappa}).$$

□

4.4 Epilogue and Directions for Future Work

The results of Chapters 3, 4 do indeed narrow the distance between the S_n and the $\widetilde{S_n}$ with respect to the important issue of representation. The form of the composition equation that we have given in Chapter 3, $\widetilde{S_n} = S_n \circ F_n$, emphasizes the point of view of providing suitable representations of the $\widetilde{S_n}$. But this equation could just as well have been written in the form $S_n = \widetilde{S_n} \circ F_n^{-1}$, which would emphasize the point of view of seeking to "tame the disorder" of the S_n. This is related to the rearrangement idea that is illustrated in figures 4.1-4.4: we rearrange S_n to get $\widetilde{S_n}$, and thus achieve almost sure convergence. The question remains how much rearranging of the S_n is optimal.

One possible direction of our work involves attempting to minimize the graph-theoretic complexity of the function F. As described in detail in §4.3, F maximizes the number of swaps (with the proper choice of swapping convention), but then will act just as the function G on the remaining "out of swaps" κ's. Of course we know by Theorem 3.5 that there are many other possible variants for the function F.

One might attempt to add some additional stages to the construction of F. In stage three (which might no longer be the terminal stage), one might seek to maximize the number of three-cycles just as we maximized the number of swaps (two-cycles) in stage two, and fixed all the κ's which were "in place" (thereby maximizing the number of one-cycles) in stage one. If some κ

remain outside the domain, proceed to stage four and continue. The goal would be to minimize lengths of cycles which could be viewed as one way of seeking to minimize the graph-theoretic complexity of the permutations.

Another current direction of our work involves picking up the thread of Chapter 2, and determining a precise count or good estimate of the number of gaps of two in between each gap of three. This analysis, combined with the results of §2.2, may provide an approach to an alternate proof of the Law of the Iterated Logarithm, when we replace our fixed integer k of §§2.1, 2.2 by suitable functions, $k(n)$, of n.

The discussion immediately preceding Lemma 4.17 raises an interesting possibility, namely looking into the question of whether "interesting" phenomena keep appearing arbitrarily far out. However, intriguing as this question may be, it seems difficult to attack it, if only because of the vagueness of the notion of "interesting phenomena".

Bibliography

[1] Nigel Cutland. *Computability.* Cambridge University Press (1980).

[2] L. Debnath and P. Mikusinski. *Introduction to Hilbert Spaces with Applications.* Academic Press, 2nd edition (1999) 112-114.

[3] Richard M. Dudley. *Real Analysis and Probability.* Wadsworth & Brooks/Cole Mathematics Series (1989).

[4] Herbert B. Enderton. *Computability Theory.* Academic Press (2010).

[5] P. Erdos. *On the Law of the Iterated Logarithm.* Annals of Mathematics, **43** (1942) 419-436.

[6] W. Feller. *The General Form of the So-Called Law of the Iterated Logarithm.* Transactions of the American Mathematical Society, **54** (1943) 373-402.

[7] Su Gao. *Invariant Descriptive Set Theory.* Chapman & Hall/CRC, Taylor & Francis Group (2009).

[8] A. Khintchine. *Über dyadische Brüche.* Math. Zeit., **18** (1923) 109-116.

[9] A. V. Skorokhod. *Limit Theorems for Stochastic Processes.* Theory of Probability and its Applications, **1** (1956) 261-290.

[10] Robert I. Soare. *Recursively Enumerable Sets and Degrees.* Springer-Verlag Berlin Heidelberg (1987).

Appendix

The master code function is one measure of the complexity of the functions G of §4.2 and F of §4.3 (of course complexity in terms of bound is just one possible complexity measure among many). We adopt the notation and terminology of these sections. Since the largest possible cardinality of a set $\mathrm{Pair}(n,i,j)$ is $\binom{n}{\left[\frac{n}{2}\right]}$, which we denote by $q(n)$, two obvious choices for the master code are $MC_1(n) := \tau(0,\ldots,2^n-1)$ and $MC_2(n) := \tau(2^n-1,\ldots,2^n-1)$, where $(2^n-1,\ldots,2^n-1)$ has length $q(n)$. There are possibly more refined choices for $MC(n)$, but of these two obvious choices, we choose the smaller one to minimize the complexity of G and F. In the course of determining which one is smaller, we obtain an upper bound for the (bound) complexity, and show that each is a primitive recursive function of n.

Claim. For all n, $MC_2(n) < MC_1(n)$.

Proof. Recall that $\tau(a_0,\ldots,a_d) = 2^{a_0} + 2^{a_0+a_1+1} + 2^{a_0+a_1+a_2+2} + \ldots + 2^{a_0+a_1+\ldots+a_d+d} - 1$. We have

$$\begin{aligned} MC_1(n) &:= \tau(0,\ldots,2^n-1) \\ &= -1 + 2^0 + \sum_{i=1}^{2^n-1} 2^{i+\sum_{j=0}^{i} j} \\ &= \sum_{i=1}^{2^n-1} 2^{\frac{i^2+3i}{2}}, \end{aligned}$$

while

$$\begin{aligned} MC_2(n) &:= \tau\left(2^n-1,\ldots,2^n-1\right) \\ &= -1+\sum_{i=0}^{q(n)-1} 2^{i+\sum_{j=0}^{i}(2^n-1)} \\ &= -1+\sum_{i=0}^{q(n)-1} 2^{2^n(i+1)-1}, \end{aligned}$$

where $(2^n-1,\ldots,2^n-1)$ has length $q(n) := \binom{n}{\left[\frac{n}{2}\right]}$. Thus, both MC_1, MC_2 are primitive recursive functions of n alone.

For $i>0$, the exponent of 2 in the i^{th} term of the sum for $MC_1(n)$ is $\frac{i^2}{2}+\frac{3i}{2}$. For $i=\frac{15}{16}2^n$, the exponent of 2 is $\frac{\left(\frac{15}{16}2^n\right)^2}{2}+\frac{3\left(\frac{15}{16}2^n\right)}{2} > \frac{\left(\frac{15}{16}2^n\right)^2}{2} = \frac{225}{512}2^{2n}$. Let $a_1 := \frac{225}{512}2^{2n}$. There are $2^n-\frac{15}{16}2^n = 2^{n-4}$ terms after the $i=\frac{15}{16}2^n$ term in $MC_1(n)$. Each of these 2^{n-4} terms has exponent of 2 greater than a_1, so each term is greater than 2^{a_1}, and the sum of these terms is greater than $2^{n-4}\cdot 2^{a_1} = 2^{n-4+a_1}$. Letting $s_1 := 2^{n-4+a_1}$, we have $MC_1(n) > s_1$.

On the other hand, the exponent of 2 in the largest term of the sum for $MC_2(n)$ is $2^n q(n)-1$. We consider the case when n is even and the case when n is odd separately.

First suppose n is even. Putting $k=\frac{n}{2}$,

$$\begin{aligned} q(n) &= \binom{2k}{k} \\ &= \frac{(2k)!}{k!k!} \\ &= \frac{2^k\prod_{i=1}^{k}(2i-1)}{k!} \\ &= 2^k\left(\prod_{i=4}^{k}\frac{2i-1}{i}\right)\cdot\frac{5}{3}\cdot\frac{3}{2}\cdot 1 \\ &< 2^k\cdot 2^{k-3}\cdot\frac{5}{2} \\ &= \frac{5}{16}2^{2k} \\ &= \frac{5}{16}2^n. \end{aligned}$$

Thus the exponent of 2 in the largest term of the sum for $MC_2(n)$ is $2^n q(n)-1 < 2^n q(n) < \frac{5}{16}2^{2n}$. Letting $a_2 := \frac{5}{16}2^{2n} = \frac{160}{512}2^{2n}$, the largest term of the sum for $MC_2(n)$ is 2^{a_2}. There are $q(n)$ terms in the sum for $MC_2(n)$, so $MC_2(n) < 2^{a_2}q(n) < 2^{a_2}\cdot\frac{5}{16}2^n$. Letting $s_2 := \frac{5}{16}2^{n+a_2}$, we have $MC_2(n) < s_2$. Then $\frac{s_1}{s_2} = \frac{2^{n+a_1-4}}{\frac{5}{16}2^{n+a_2}} = \frac{1}{5}2^{\frac{65}{512}2^{2n}}$ so $s_1 > s_2$. Since $MC_1(n) > s_1$ while

$MC_2(n) < s_2$, $MC_1(n)$ is greater than $MC_2(n)$.

Now suppose n is odd. Putting $k = \frac{n-1}{2}$,

$$
\begin{aligned}
q(n) &= \binom{2k+1}{k} \\
&= \frac{(2k+1)!}{k!\,(k+1)!} \\
&= \frac{2^k \prod_{i=1}^{k+1}(2i-1)}{k!} \\
&= 2^k \left(\prod_{i=4}^{k} \frac{2i-1}{i+1}\right) \cdot \frac{5}{4} \cdot \frac{3}{3} \cdot \frac{1}{2} \cdot 1 \\
&< 2^k \cdot 2^{k-2} \cdot \frac{5}{8} \\
&= \frac{5}{64} 2^{2k+1} \\
&= \frac{5}{64} 2^n.
\end{aligned}
$$

Thus the exponent of 2 in the largest term of the sum for $MC_2(n)$ is $2^n q(n) - 1 < 2^n q(n) < \frac{5}{64} 2^{2n}$. Letting $b_2 := \frac{5}{64} 2^{2n} = \frac{40}{512} 2^{2n}$, the largest term of the sum for $MC_2(n)$ is 2^{b_2}. There are $q(n)$ terms in $MC_2(n)$, so $MC2_2(n) < 2^{b_2} q(n) < 2^{b_2} \cdot \frac{5}{64} 2^n$. Letting $t_2 := \frac{5}{64} 2^{n+b_2}$, we have $MC_2(n) < t_2$. Then $\frac{s_1}{t_2} = \frac{2^{n+a_1-4}}{\frac{5}{64} 2^{n+b_2}} = \frac{4}{5} 2^{\frac{182}{512} 2^{2n}}$ so $s_1 > t_2$. Since $MC_1(n) > s_1$ while $MC_2(n) < t_2$, $MC_1(n)$ is greater than $MC_2(n)$.

$\square$

Vita

Marina Skyers

Department of Mathematics — marinaskyers@gmail.com

Lehigh University — 610.758.3757

14 East Packer Avenue

Bethlehem, PA 18015-3174

EDUCATION:

Lehigh University, Bethlehem, PA — September 2007-Present

- Ph.D. in Mathematics, May 2012.
  Dissertation: A Tale of Two Sequences: A Story of Convergence, Weak and Almost Sure
  Dissertation Director: Dr. Lee Stanley
- M.S. in Mathematics, May 2009.
- Mathematics Coursework: Probability Theory, Spectral Sequences, Cryptography, K-Theory, Set Theory, Fields and Modules, Differential Geometry, Mathematical Logic, Algebraic Topology, Computability Theory, Complex Analysis, Real Analysis, Groups and Rings, General Topology.

Barnard College, Columbia University, New York, NY — September 2003-May 2007

- B.A. in Mathematics, May 2007.
- Mathematics Coursework: Modern Analysis, Topology, p-adic Number Theory Seminar, Statistics, Cryptography, Complex Variables, Elliptic Curves and Modular Forms Seminar, Modern Algebra, Number Theory, Symbolic Logic, Linear Algebra, Ordinary Differential Equations, Calculus I-IV, Surfaces and Knots.

- Dean's List 2003-2007

Stuyvesant High School, New York, NY September 1999-June 2003

TEACHING EXPERIENCE:

- Teaching Assistant at Lehigh University for Statistics, Spring 2012, Instructor for Basic Statistics, Summer 2012, anticipated.

- Summer Program for Women in Mathematics, Summer 2011.
  -Teaching Assistant for a three week course entitled *Good Things Come to Those who Wait: An Introduction to Delay Differential Equations*.
  -Teaching Assistant for a two week course entitled *An Introduction to Groebner Bases*.

- Teaching Assistant at Lehigh University for Calculus I, II, III, September 2007-Present.
  -Teach four recitation sessions per week each semester.
  -Grade exams and homework, prepare and grade quizzes.
  -Hold office hours and attend three lectures a week.
  -Offer review sessions before exams.
  -Organized "Integration Bees" in each recitation during Calculus II, culminating in a "Grand Championship" in lecture.

- Academic Fellow for Calculus at Columbia University, September 2005-May 2006.
  -Provided academic assistance to students enrolled in Calculus.

- Teaching Assistant for College Algebra and Analytic Geometry during Columbia summer session, Summer 2005.

- Barnard Math Help Room, September 2004-May 2007.
  -Teaching Assistant for Single and Multivariable Calculus.

PRESENTATIONS:

- *Primitive Recursive Representations of "Skorokhod Sequences" for the Standard Normal*, Joint Mathematics Meetings, Boston, MA, January 4, 2012.

- *An unsolved question in Algebra solved by Algebraic Topology*, Graduate Student Seminar, Rutgers University, April 9, 2010. (First speaker in the new Seminar Exchange Program with Rutgers University.)

- *An unsolved question in Algebra solved by Algebraic Topology*, Lehigh University Graduate Student Colloquium, February 3, 2010.

PUBLICATIONS:

- *A Tale of Two Sequences: A Story of Convergence, Weak and Almost Sure*, Submitted April 2012.

- *Primitive Recursive Representations of "Skorokhod Sequences" for the Standard Normal*, Abstracts of Papers Presented to the American Mathematical Society, **33** No. 1 (2012).

- *SPWM 2011 Proceedings*, Summer Program for Women in Mathematics, The George Washington University, Internal Publication.

- *SPWM 2006 Proceedings*, Summer Program for Women in Mathematics, The George Washington University, Internal Publication.

SERVICE AND OTHER ACTIVITIES:

- Teacher Development Program, Lehigh University, Fall 2011.
  -Program included "Presentations and Communications" workshop and "Engaging Students" workshop.

- Lehigh University Graduate Student Senate, Treasurer, April 2010-August 2011.

- Mathematics Department Unit Representative to the Graduate Student Senate, September 2009-August 2011.

- Member of GSIMS (Graduate Student Intercollegiate Mathematics Seminar), Lehigh University, June 2009-Present.

- Tutor in the Lehigh University Math Help Center, September 2007-Present.

- Park City Mathematics Institute, Summer 2007.
  -Studied Discrete Probability and Brownian Motion.

- Summer Program for Women in Mathematics, Summer 2006.
  -Studied Computability Theory, Groebner Bases, Mathematical Modeling in Biology, Discrete Financial Mathematics.

- Member of Columbia University Undergraduate Math Society, September 2003-August 2007.

CONFERENCES ATTENDED:

- Presented at the Joint Mathematics Meetings, Boston, MA, January 4-7, 2012.
- C.-C. Hsiung International Symposium on Geometry and Topology, Lehigh University, May 28-30, 2010.
- Moravian College Student Mathematics Conference, Moravian College, Bethlehem, PA, February 20, 2010.
- Participated in workshop on Unstable Homotopy Theory held at the CUNY Graduate Center, New York, NY, June 26-27, 2009.
- Geometry and Topology Conference, Lehigh University, June 4-6, 2009.
- Moravian College Student Mathematics Conference, Moravian College, Bethlehem, PA, February 21, 2009.
- Joint Mathematics Meetings, Washington, DC, January 5-8, 2009.
- Everett Pitcher Lecture Series, Lehigh University:
  -Manjul Bhargava, *Quadratic and Higher Degree Forms in Arithmetic*, Spring 2011.
  -Rick Durrett, *Three Faces of Probability*, Spring 2010.
  -Maria Chudnovsky, *The Perfect Graphs - Structure and Recognition*, Spring 2009.
  -Persi Diaconis, *The Search for Randomness*, Spring 2008.

PROFESSIONAL MEMBERSHIPS:

- American Math Society (AMS)
- Mathematical Association of America (MAA)
- Association for Symbolic Logic (ASL)
- Society for Industrial and Applied Mathematics (SIAM)

COMPUTER SKILLS: Mathematica, Matlab, CoCoA, LaTex, Adobe Web Premium Creative Suite, Microsoft Office Suite.

REFERENCES: Available upon Request.