STRONG NORMALITY, MODULAR NORMALITY, AND FLAT POLYNOMIALS: APPLICATIONS OF PROBABILITY IN NUMBER THEORY AND ANALYSIS

by

Adrian Belshaw

M. Sc. (Mathematics), Simon Fraser University, 2005
M. A. (Biology), Princeton University, 1976
B. Sc. (Mathematics), University of British Columbia, 1973

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in the
Department of Mathematics
Faculty of Science

SIMON FRASER UNIVERSITY
Fall 2013

APPROVAL

Name:	**Adrian Belshaw**
Degree:	**Doctor of Philosophy (Mathematics)**
Title of Thesis:	**Strong Normality, Modular Normality, and Flat Polynomials: Applications of Probability in Number Theory and Analysis**
Examining Committee:	**Dr. Imin Chen** Chair Associate Professor
	Dr. Peter Borwein Senior Supervisor Professor
	Dr. Stephen Choi Supervisor Professor
	Dr. Richard Lockhart Internal/External Examiner Professor Department of Statistics and Actuarial Science
	Dr. David Bailey External Examiner Research Fellow Department of Computer Science University of California (Davis)
Date Approved:	**13 December, 2013**

Partial Copyright Licence

Abstract

We use probabilistic methods, along with other techniques, to address three topics in number theory and analysis.

Champernowne's number is well known to be normal, but the digits are highly patterned. The definition of normality reflects the convergence in frequency of the digits of a random number, but the behaviour of the discrepancy is better described by the law of the iterated logarithm. We use this to define "strong normality," and find that almost all numbers are strongly normal, and strongly normal numbers are normal. However, the base-2 Champernowne number is not strongly normal in the base 2. We use a method of Sierpiński to construct a number strongly normal in every base.

Next, we define normality of an integer sequence modulo an integer q; this is a refinement of the existing notion of uniform distribution modulo q. If α is normal in the base r, the sequence given by the integer part of $r^n\alpha$ is uniformly distributed modulo every integer $q > 1$; however, the sequence is normal modulo q if and only if q divides r. This particular sequence does show pseudorandom behaviour modulo every $q > r$; we define "base-r normality modulo q" to capture this behaviour.

The third topic concerns flat polynomials. A sequence of polynomials is "flat" if its values on the unit circle are bounded above and below by absolute constant multiples of $\sqrt{n}$, where n is the degree. Beck showed that there exist flat sequences of polynomials with coefficients that are lth roots of unity, for every l greater than some lower bound. Beck gave a lower bound of 400, but we correct a minor error in his proof and show that this should have been 851. Beck relied on a constant from Spencer's work on the discrepancy of linear forms. We repeat Spencer's calculation, slightly improving the value of his constant and giving a new bound of 492. An improvement of Spencer's method, due to Kai-Uwe Schmidt, allows us to lower the bound to 345.

Acknowledgements

I am indebted to Peter Borwein, for welcoming me into his home, and guiding my efforts with great wisdom and patience;
to Stephen Choi, for his keen insights and warm encouragement;
to Imin Chen, Nils Bruin, Richard Lockhart, Michael Bennett, David Muraki, Ralf Wittenberg, and both of the above, for teaching me beautiful mathematics and showing me how to teach;
to Keshav Mukunda, Idris Mercer, Alan Meichsner, Michael Coons, Himadri Ganguli, and Vishaal Kapoor, my fellow students, for being agreeable and generous companions in the road;
to Kai-Uwe Schmidt, Tamás Erdélyi, and an anonymous referee for tremendously helpful comments and suggestions;
to Diane Pogue and all the staff at Simon Fraser University, for making the life of a graduate student as pleasant as it can be;
to the Mathematics Department, for making an environment so conducive so learning and creativity;
to my colleagues and administrators at Capilano University, for their many accommodations;
and to Juniper Belshaw and Loreen Dawson for their support, understanding, and love.

Dedication

To my students in Adult Basic Education,
whose courage in returning to their studies
inspired me to follow their example;

and to my mother,
who would have been very pleased.

Contents

Chapter 1

Introduction

1.1 Probabilistic Methods

Probabilistic methods have been widely useful in combinatorics, analysis and number theory. The theorems of probability are sometimes the only known avenue to proof; in other cases, other methods can be used, but the methods of probability may be much easier to apply.

It ought not to be surprising that probability theory finds application in the study of normal numbers. The notion of normality is itself probabilistic, and Borel used the central limit theorem in his proof that almost all numbers are normal [10]. Soon after, Sierpiński gave an "elementary" proof of the same fact making direct use of measure theory [34]. By "elementary," we suggest, Sierpiński simply meant "without the tools of probability." There is no doubt that Borel's probabilistic proof is far simpler, although Sierpiński's method is of striking beauty. An even easier proof than Borel's is available, using the strong law of large numbers (see, for example, Laha and Rohatgi [23]).

It is perhaps more surprising to find probability theory applied to problems in analysis. An example relevant to our work is Kahane's proof [20] of the existence of "ultra-flat" sequences of polynomials with unimodular coefficients. Queffelec and Saffari [37] refined his work, also using the probabilistic approach; and we do not know of any other way to approach this problem.

We have used probabilistic tools, along with other techniques, to tackle three questions in number theory and analysis. The first two topics extend the notion of normality of numbers, but in different directions. The last one deals with the asymptotic behaviour of a certain class of trigonometric polynomials.

Since two of our topics concern normal numbers, in Chapter 2 we summarize the essential definitions and most relevant (to this work) results in the study of normality. We also present graphic evidence of the remarkable patterning in the digits of Champernowne's number. This motivates the work presented in Chapter 3. Here we find that the law of the iterated logarithm gives us a sharp criterion for the discrepancy of a random number. We use this to define "strong normality," and find that almost all numbers are strongly normal, but the base 2 Champernowne number is not strongly normal in the base 2. Strong normality

is a strictly more stringent condition than normality, since strongly normal numbers are normal. While a rational number may be simply normal, no rational can be simply strongly normal. We use Sierpiński's method to construct a number strongly normal in every base; unlike Sierpiński, we make use of a lemma in probability to carry out the construction. This construction would be exceedingly difficult, if not impossible, without probabilistic methods.

Next, we define normality of an integer sequence modulo an integer q. If α is normal in the base r, the integer sequence $\lfloor r^n \alpha \rfloor$ is normal modulo r. We show that this sequence is simply normal, that is, uniformly distributed, modulo every integer $q > 1$; however, the sequence is normal modulo q if and only if q divides r. We propose a notion of "base-r normality modulo q" in order to capture the pseudorandom behaviour of the sequence $\lfloor r^n \alpha \rfloor$ modulo q, when q is greater than r. The central limit theorem for Markov chains plays a key role in our argument.

The last chapter addresses a result of Beck [7]: there exist sequences of flat polynomials with coefficients that are lth roots of unity, for every integer greater than some l_0. Beck gave the value $l_0 = 400$, but we correct a minor error in his proof and show that this should have been $l_0 = 851$. However, Beck relied on a constant $K \approx 9$ from Spencer's work [35] on the discrepancy of linear forms. Spencer gave a better value, $K \approx 5.32$, and we slightly improve this to $K \approx 5.199$. Using this value of K, we are able to give a new bound of $l_0 = 492$. The Lindeberg central limit theorem is essential here, along with other more elementary tools of probability. In revisiting Spencer's method, we address various questions of convergence which were not explicitly addressed in the original work. Finally, we present a refinement of Spencer's technique, due to K.-U. Schmidt, giving a new best value of $K \approx 3.65$. Since we state Beck's theorem explicitly in terms of K, Schmidt's work immediately gives $l_0 = 345$.

1.2 Some Theorems of Probability

It seems worthwhile to gather together, for reference, the main tools of probability used in this work.

Given a probability measure $\mathbf{P}$ on a suitable set Ω, the probability of $A \subset \Omega$ is

$$\mathbf{P}[A] = \int_A \mathrm{d}\mathbf{P}.$$

The expected value of a random variable $X : \Omega \to \mathbb{R}$ is

$$\mathbf{E}[X] = \int_\Omega X \mathrm{d}\mathbf{P}.$$

If $\mu = \mathbf{E}[X]$, then the variance of X is $\mathbf{E}[(X - \mu)^2]$.

In Chapter 5, we will make repeated use of the Markov inequality (see, for example, [9], p. 65). Given a random variable X, and $\alpha, \lambda > 0$,

$$\mathbf{P}[|X| \geq \alpha] \leq \frac{\mathbf{E}[|X|^\lambda]}{\alpha^\lambda}.$$

We will ordinarily have $\lambda = 1$.

The law of the iterated logarithm (see, for example, [9], Theorem 9.5) provides the key idea in Chapter 3.

Theorem 1.2.1. *Suppose $X_1, \ldots, X_n$ are independent and identically distributed random variables with mean 0 and variance 1. If*

$$S_n = \sum_{j=1}^{n} X_j,$$

then

$$\mathbf{P}\left[\limsup_{n\to\infty} \frac{S_n}{\sqrt{2n\log\log n}} = 1\right] = 1.$$

Replacing X_i with $-X_i$ for each i gives

$$\mathbf{P}\left[\liminf_{n\to\infty} \frac{S_n}{\sqrt{2n\log\log n}} = -1\right] = 1$$

as an immediate corollary.

The central limit theorem comes in many guises, and we will need it in two forms. The Lindeberg central limit theorem is the version we need for Chapter 5; it is, for example, Theorem 27.2 in Billingsley [9].

Theorem 1.2.2. *Suppose that for each n, the random variables $X_{n1}, \ldots, X_{nr_n}$ are independent, and that*

$$\mathbf{E}[X_{nk}] = 0$$

for each nk; write

$$\sigma_{nk}^2 = \mathbf{E}[X_{nk}^2] \qquad \text{and} \qquad s_n^2 = \sum_{k=1}^{r_n} \sigma_{nk}^2.$$

Suppose, further, that, for every $\varepsilon > 0$, the Lindeberg condition holds:

$$\lim_{n\to\infty} \sum_{k=1}^{r_n} \frac{1}{s_n^2} \int_{X_{nk} \geq \varepsilon s_n} X_{nk}^2 \mathrm{d}\mathbf{P} = 0.$$

Then the distribution of $\dfrac{S_n}{s_n}$ converges weakly to the normal distribution:

$$\lim_{n\to\infty} \mathbf{P}\left[\frac{S_n}{s_n} \leq x\right] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} \mathrm{d}t$$

for every x.

A collection of random variables of this form is known as a triangular array. Note that the X_{nk} are not necessarily identically distributed. Since variance is additive for independent random variables, s_n^2 is the variance of S_n.

The weak convergence of the conclusion is uniform on $\mathbb{R}$ (although, in general, weak convergence is not necessarily uniform).

In Chapter 4, we need Doeblin's central limit theorem for Markov chains (see, for example, [15], p. 99). We give the theorem here in simplified form; the theorem applies to a more general class of Markov chains and holds for the partial sums of values of any real functional on the state space.

Consider a finite state space $\{c_1, \ldots, c_q\}$, and an irreducible Markov chain $\{x_n\}$, $n = 1, 2, \ldots$; suppose the transition probabilities are independent of n (the transition probability p_{ij} is the probability that $x_{n+1} = c_j$ if $x_n = c_i$, for any n). Fix some $i \in \{1, \ldots, q\}$, and define the random variable y_n by

$$\begin{cases} y_n = 1 & \text{if} \quad x_n = c_i, \\ y_n = 0 & \text{otherwise.} \end{cases}$$

In other words, y_n is the indicator functional for the ith state.

Let π_i be the stable frequency of the ith state. For the Markov chains we will be considering, this is non-zero, and indeed for our case $\pi_i = 1/q$.

In the more general case, we need to consider a random variable defined to be the sum of the values of a functional from $n = \tau_\nu$ to $n = \tau_{\nu+1} - 1$, where τ_ν is the νth value of n for which $x_n = c_i$ (the νth entrance time for the ith state). In our simplified case, however, this is always 1, and we can ignore it in the statement of the theorem.

With this simplification, we can define the random variables

$$z_n = y_n - \pi_i$$

and

$$Z_\nu = \sum_{n=\tau_\nu}^{\tau_{\nu+1}-1} z_n,$$

where τ_ν is, again, the νth entrance time for the ith state. Now put

$$\sigma_i^2 = \mathbf{E}[Z_\nu^2].$$

We are interested in the partial sums of y_n. If we let

$$S_n = \sum_{k=1}^{n} y_k,$$

then S_n counts the number of times the ith state c_i occurs in the first n steps of the Markov process.

Finally, we define

$$B = \pi_i \sigma_i^2.$$

In the more general version of the theorem, the conditions are that the expected return time for the ith state be finite, and that σ_i^2 be finite. In the case of interest to us, these two conditions certainly hold.

Here, then, is the central limit theorem for functionals on Markov chains, in simplified form:

Theorem 1.2.3. *With S_n, π_i and B as defined above,*

$$\lim_{n\to\infty} \mathbf{P}\left[\frac{S_n - \pi_i n}{\sqrt{Bn}} \leq x\right] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} \mathrm{d}t.$$

In the more general version, we should note, the state space can be countably infinite, but we assume the state space is not decomposable. Moreover, if we are considering a functional for which

$$\mu_i = \mathbf{E}\left[\sum_{n=\tau_\nu}^{\tau_{\nu+1}-1} y_n\right] \neq 1,$$

then we have to replace the π_i with $M_i = \pi_i \mu_i$ in the definition of z_n and in the conclusion of the theorem.

In our application of the theorem, it will be convenient that the conclusion is independent of the starting state of the Markov chain. This follows from the fact that π_i and σ_i^2, and their product B, do not depend on the distribution of the initial state x_1.

Chapter 2

Normal Numbers

This chapter and the next have appeared as [6].

2.1 Normality

We can write a real number α in any integer base $r \geq 2$ as a sum of powers of the base:

$$\alpha = \sum_{j=-d}^{\infty} a_j r^{-j},$$

with $a_j \in \{0, 1, \ldots, r-1\}$. The standard "decimal" notation is

$$\alpha = a_{-d}\ a_{-(d-1)}\ \cdots a_0\ .\ a_1\ a_2\ \cdots\ .$$

The sequence of digits $\{a_j\}$ gives the representation of α in the base r, and this representation is unique unless α is rational, in which case α may have two representations. (For example, in the base 10, $0.1 = 0.0999\cdots$.)

We call a subsequence of consecutive digits a *string*. The string may be finite or infinite; we call a finite string of t digits a *t-string*. An infinite string beginning in a specified position we call a *tail*, and we call a finite string beginning in a specified position a *block*.

A number α is *simply normal* in the base r if every 1-string in its base-r expansion occurs with an asymptotic frequency approaching $1/r$. That is, given the expansion $\{a_j\}$ of α in the base r, and letting $m_k(n)$ be the number of times that $a_j = k$ for $j \leq n$, we have

$$\lim_{n\to\infty} \frac{m_k(n)}{n} = \frac{1}{r}$$

for each $k \in \{0, 1, \ldots, r-1\}$. This is Borel's original definition [10].

A number is *normal* in the base r if every t-string in its base-r expansion occurs with a frequency approaching r^{-t}. Equivalently, a number is normal in the base r if it is simply normal in the base r^t for every positive integer t (see [10, 31, 40]).

A number is *absolutely normal* if it is normal in every base. Borel [10] showed that almost every real number is absolutely normal.

In 1933, Champernowne [14] produced the first concrete construction of a normal number. Champernowne's number is

$$\gamma_{10} = .1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ \cdots .$$

The number is written in the base 10, and its digits are obtained by concatenating the natural numbers written in the base 10. This number is likely the best-known example of a normal number.

Generally, the base-r Champernowne number is formed by concatenating the integers 1, 2, 3, ... in the base r. For example, the base-2 Champernowne number is written in the base 2 as

$$\gamma_2 = .1\ 10\ 11\ 100\ 101\ \cdots .$$

For any r, the base-r Champernowne number is normal in the base r. However, the question of its normality in any other base (not a power of r) is open. For example, it is not known whether the base-10 Champernowne number is normal in the base 2.

In 1917, Sierpiński [34] gave a construction of an absolutely normal number (in fact, one such number for each ε with $0 < \varepsilon \leq 1$). A computable version of this construction was given by Becher and Figueira in 2002 [3].

Most fundamental irrational constants, such as $\sqrt{2}$, $\log 2$, π, and e, appear to be normal, and statistical tests done to date are consistent with the hypothesis that they are normal. (See, for example, Kanada on π [20] and Beyer, Metropolis and Neergard on irrational square roots [8].) However, there is no proof of the normality of any of these constants.

There is an extensive literature on normality in the sense of Borel. Introductions to the literature may be found in [7] and [12].

2.2 Walks on the Digits of Numbers and on Chromosomes

In this section we graphically compare two walks on the digits of numbers with a walk on the values of the Liouville λ function and a walk on the nucleotides of the human X chromosome.

The walks are generated on a binary sequence of digits (Figures 2.1 and 2.2) by converting each 0 in the sequence to -1, and then using digit pairs $(\pm 1, \pm 1)$ to walk $(\pm 1, \pm 1)$ in the plane. The colour or shading in the figures gives a rough indication of the number of steps taken in the walk. The values of the Liouville λ function (Figure 2.3) are already ± 1.

There are four nucleotides in the X chromosome sequence, and each of the four is assigned one of the values $(\pm 1, \pm 1)$ to create a walk on the nucleotide sequence (Figure 2.4). The nucleotide sequence is available on the UCSC Genome Browser [39].

A random walk on a million digits is expected to stay within roughly a thousand units of the origin, and this will be seen to hold for the walks on the digits of π and on the Liouville λ function values. On the other hand, the walks on the digits of Champernowne's number and on the X chromosome travel much farther than would be expected of a random walk.

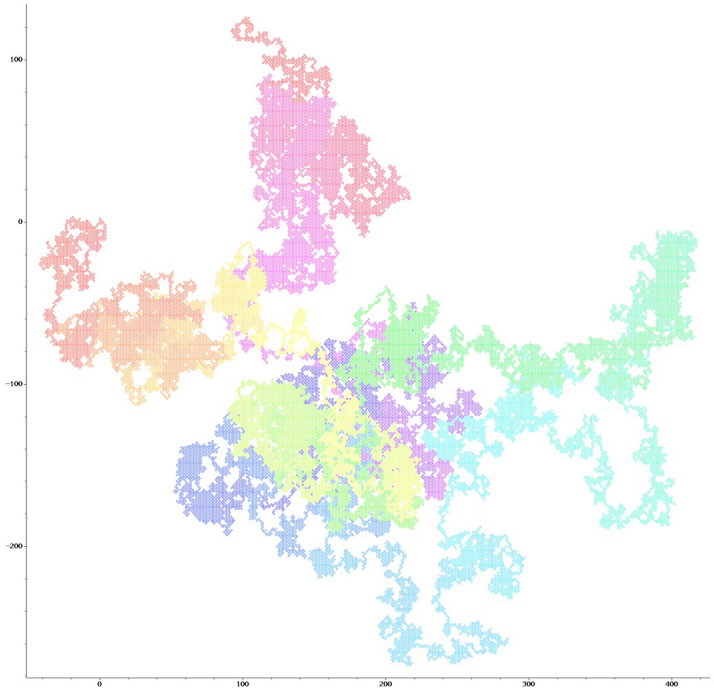

Figure 2.1: A walk on 10^6 binary digits of π

The walk on the Liouville λ function moves away from the origin like $\sqrt{n}$, but it does not seem to move randomly near the origin. In fact, the positive values of λ first outweigh the negative values when $n = 906180359$ [24], which is not at all typical of a random walk.

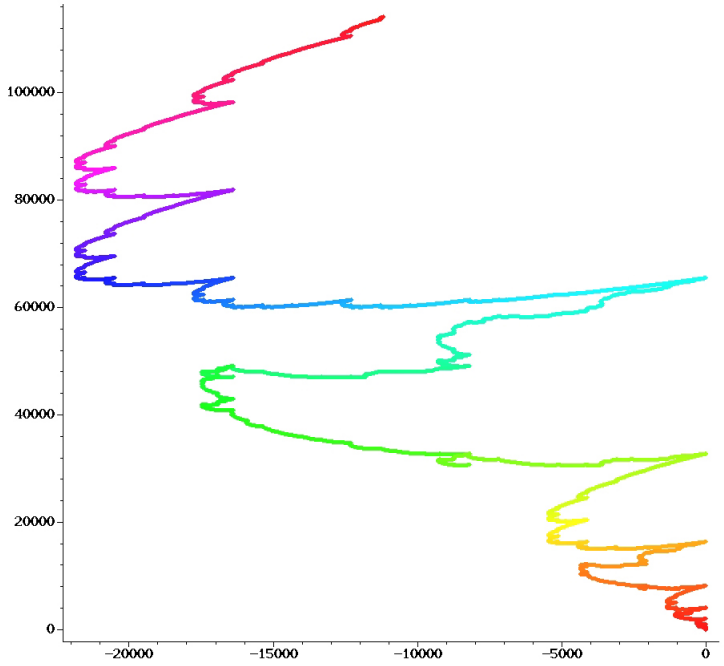

Figure 2.2: A walk on 10^6 binary digits of the base-2 Champernowne number

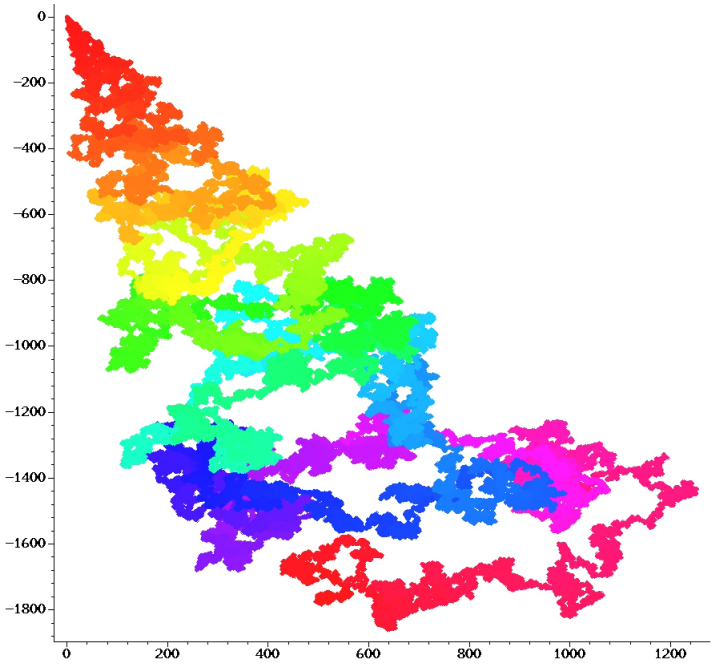

Figure 2.3: A walk on 10^6 values of the Liouville λ function

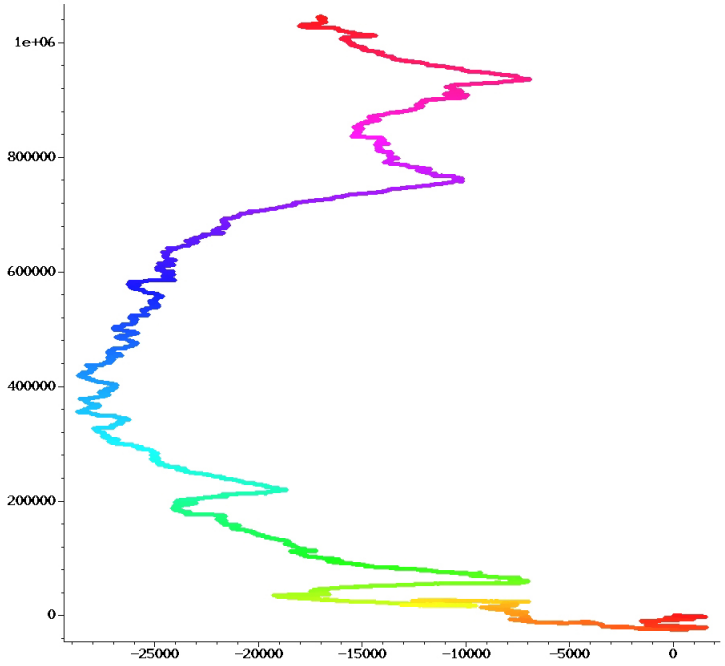

Figure 2.4: A walk on the nucleotides of the human X chromosome

Chapter 3

Strong Normality of Numbers

3.1 Definition of Strong Normality

Mauduit and Sárközy [27] have shown that the digits of the base-2 Champernowne number γ_2 fail two tests of randomness. Dodge and Melfi [16] compared values of an autocorrelation function for Champernowne's number and π, and found that π had the expected pseudorandom properties but that Champernowne's number did not.

Here we provide another test of pseudorandomness, and show that it must be passed by almost all numbers. Our test is a simple one, in the spirit of Borel's test of normality, and Champernowne's number will be seen to fail the test.

If the digits of a real number α are chosen at random in the base r, the asymptotic frequency $m_k(n)/n$ of each 1-string approaches $1/r$ with probability 1. However, the *discrepancy* $m_k(n) - n/r$ does not approach any limit, but fluctuates.

Kolmogorov's law of the iterated logarithm allows us to make a precise statement about the discrepancy of a random number. We use this to define our criterion.

Definition 3.1.1. *For real α, and $m_k(n)$ as above, α is* simply strongly normal *in the base r if for each $k \in \{0, \ldots, r-1\}$*

$$\limsup_{n\to\infty} \frac{m_k(n) - \dfrac{n}{r}}{\dfrac{\sqrt{r-1}}{r}\sqrt{2n \log\log n}} = 1$$

and

$$\liminf_{n\to\infty} \frac{m_k(n) - \dfrac{n}{r}}{\dfrac{\sqrt{r-1}}{r}\sqrt{2n \log\log n}} = -1 \ .$$

We make two further definitions analogous to the definitions of normality and absolute normality.

Definition 3.1.2. *A number is* strongly normal *in the base r if it is simply strongly normal in each of the bases r^j, $j = 1, 2, 3, \ldots$.*

Definition 3.1.3. *A number is* absolutely strongly normal *if it is strongly normal in every base.*

This definition of strong normality is sharper than the one given previously in [5].

3.2 Almost All Numbers are Strongly Normal

Theorem 3.2.1. *Almost all numbers are simply strongly normal in any base r.*

Without loss of generality, we consider numbers in the interval $[0, 1]$ and fix the integer base $r \geq 2$. We take Lebesgue measure to be our probability measure. For any k, $0 \leq k \leq r-1$, the ith digit of a randomly chosen number is k with probability r^{-1}. For $i \neq j$, the ith and jth digits are both k with probability r^{-2}, so the digits are pairwise independent.

We define the sequence of random variables X_j by

$$X_j = \sqrt{r-1}$$

if the jth digit is k, with probability $\dfrac{1}{r}$, and

$$X_j = -\frac{1}{\sqrt{r-1}}$$

otherwise, with probability $\dfrac{r-1}{r}$.

Then the X_j form a sequence of independent identically distributed random variables with mean 0 and variance 1. Put

$$S_n = \sum_{j=1}^{n} X_j \ .$$

By the law of the iterated logarithm (Theorem 1.2.1), with probability 1,

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

and

$$\liminf_{n\to\infty} \frac{S_n}{\sqrt{2n \log\log n}} = -1 \ .$$

Now we note that, if $m_k(n)$ is the number of occurrences of the digit k in the first n digits of our random number, then

$$S_n = m_k(n)\sqrt{r-1} - \frac{n - m_k(n)}{\sqrt{r-1}} \ .$$

Substituting this expression for S_n in the limits immediately above shows that the random number satisfies Definition 3.1.1 with probability 1. □

This is easily extended.

Corollary 3.2.1. *Almost all numbers are strongly normal in any base r.*

By the theorem, the set of numbers in $[0,1]$ which fail to be simply strongly normal in the base r^j is of measure zero, for each j. The countable union of these sets of measure zero is also of measure zero. Therefore the set of numbers simply strongly normal in every base r^j is of measure 1. □

The following corollary is proved in the same way as the last.

Corollary 3.2.2. *Almost all numbers are absolutely strongly normal.*

The results for $[0,1]$ are extended to $\mathbb{R}$ in the same way.

3.3 Champernowne's Number is Not Strongly Normal

We begin by examining the digits of Champernowne's number in the base 2,

$$\gamma_2 = .1\ 10\ 11\ 100\ 101\ \cdots\ .$$

Each integer q, for $2^{n-1} \leq q \leq 2^n - 1$, has an n-digit base-2 representation, and so contributes an n-block to the expansion of γ_2. In each of these n-blocks, the first digit is 1. If we consider the remaining $n-1$ digits in each of these n-blocks, we see that every possible $(n-1)$-string occurs exactly once. The n-digit integers, concatenated, together contribute a block of length $n2^{n-1}$, and in this block, if we set aside the ones corresponding to the initial digit of each integer, the zeros and ones are equal in number. In the whole block there are $(n-1)2^{n-2}$ zeros and $(n-1)2^{n-2} + 2^{n-1}$ ones. The excess of ones over zeros in the entire $\left(n2^{n-1}\right)$-block is just equal to the number of integers, 2^{n-1}, contributing to the block.

As we concatenate the integers from 1 to $2^k - 1$, we write the first

$$N - 1 = \sum_{n=1}^{k} n2^{n-1} = (k-1)2^k + 1$$

digits of γ_2. The excess of ones in the digits is

$$2^k - 1.$$

The locally greatest excess of ones occurs at the first digit contributed by the integer 2^k, since each power of 2 is written as a 1 followed by zeros. At this point the number of digits is $N = (k-1)2^k + 2$ and the excess of ones is 2^k. That is, the actual number of ones in the first N digits is

$$m_1(N) = (k-2)2^{k-1} + 1 + 2^k.$$

This gives

$$m_1(N) - \frac{N}{2} = 2^{k-1}\ .$$

Thus, we have

$$\frac{m_1(N) - \frac{N}{2}}{N^{1/2+\varepsilon}} \geq \frac{2^{k-1}}{((k-1)2^k)^{1/2+\varepsilon}}.$$

For any sufficiently small positive ε, the right-hand expression is unbounded as $k \to \infty$. We have

$$\limsup_{N\to\infty} \frac{m_1(N) - \frac{N}{2}}{\frac{1}{2}\sqrt{2N \log\log N}} \geq \limsup_{N\to\infty} \frac{m_1(N) - \frac{N}{2}}{N^{1/2+\varepsilon}} = \infty \ .$$

We thus have:

Theorem 3.3.1. *The base-2 Champernowne number is not strongly normal in the base 2.*

One can show that Champernowne's number also fails the lower limit criterion. In fact, $m_1(N) - \dfrac{N}{2} > 0$ for every N.

To see this, we suppose it true for $N \leq N_k = (k-1)2^k + 1$, and proceed by induction on k. We can arrange the digits of the integers $2^k, 2^k + 1, \ldots, 2^k + 2^{k-1} - 1$ in a 2^{k-1} by $k+1$ matrix, where the i-th row is given by the digits of the integer $2^k + i - 1$. Each row begins with $(1, 0, \ldots)$, and if we delete the first two columns we now have a matrix with the i-th row given by the digits of the integer $i-1$, possibly preceded by some zeros. If we ignore the first row and the initial zeros in each subsequent row, we get the first N_{k-1} digits of γ_2, and by our induction hypothesis $m_1(N) > m_0(N)$ for $N \leq N_{k-1}$. Therefore, if we now include all the zeros as we read the matrix in the natural order, any excess of zeros must come from the initial zeros, and there are $2^{k-1}-1$ of these. As we showed above, $m_1(N_k) - m_0(N_k) = 2^k - 1$, so $m_1(N) > m_0(N) + 2^{k-1}$ for every N with $N_k \leq N \leq N_k + (k+1)2^{k-1}$.

A similar argument on the integers from $2^k + 2^{k-1}$ to $2^{k+1} - 1$, where each row of the matrix now begins with $(1, 1, \ldots)$, gives the result that $m_1(N) > m_0(N)$ for every $N \leq N_{k+1}$. □

The theorem can be generalized to every Champernowne number, since there is a shortage of zeros in the base-r representation of the base-r Champernowne number. Each base-r Champernowne number fails to be strongly normal in the base r.

3.4 Strongly Normal Numbers are Normal

Our definition of strong normality is strictly more stringent than Borel's definition of normality:

Theorem 3.4.1. *If a number α is simply strongly normal in the base r, then α is simply normal in the base r.*

We give two proofs. The first is as in the published version [6] of this result. We have since found a much shorter proof, which we give here as a second proof.

For the first proof, we will show that if a number is not simply normal, then it cannot be simply strongly normal.

Let $m_k(n)$ be the number of occurrences of the 1-string k in the first n digits of the expansion of α in the base r, and suppose that α is not simply normal in the base r. This implies that for some k

$$\lim_{n\to\infty} \frac{rm_k(n)}{n} \neq 1.$$

Then there is some $Q > 1$ and infinitely many n_i such that either

$$rm_k(n_i) > Qn_i$$

or

$$rm_k(n_i) < \frac{n_i}{Q}.$$

If infinitely many n_i satisfy the former condition, then for these n_i,

$$m_k(n_i) - \frac{n_i}{r} > Q\frac{n_i}{r} - \frac{n_i}{r} = n_iP$$

where P is a positive constant.

Then for any $R > 0$,

$$\limsup_{n\to\infty} R\frac{m_k(n) - \frac{n}{r}}{\sqrt{2n\log\log n}} \geq \limsup_{n\to\infty} R\frac{nP}{\sqrt{2n\log\log n}} = \infty,$$

so α is not simply strongly normal.

On the other hand, if infinitely many n_i satisfy the latter condition, then for these n_i,

$$\frac{n_i}{r} - m_k(n_i) > \frac{n_i}{r} - \frac{n_i}{Qr} = n_iP,$$

and once again the constant P is positive. Now

$$\liminf_{n\to\infty} \frac{m_k(n) - \frac{n}{r}}{\sqrt{2n\log\log n}} = -\limsup_{n\to\infty} \frac{\frac{n}{r} - m_k(n)}{\sqrt{2n\log\log n}}$$

and so, in this case also, α fails to be simply strongly normal.

For the second, much shorter, proof, we suppose that α is simply strongly normal. Definition 3.1.1 implies that, for each $k \in \{0, \ldots, r-1\}$,

$$\limsup_{n\to\infty} \frac{\frac{m_k(n)}{n} - \frac{1}{r}}{\frac{\sqrt{r-1}}{r}\sqrt{\frac{2\log\log n}{n}}} = 1.$$

Since the denominator approaches 0 as $n \to \infty$, the upper limit of the numerator must be 0 as well. This, combined with a similar argument on the lower limit, gives

$$\lim_{n\to\infty} \left(\frac{m_k(n)}{n} - \frac{1}{r}\right) = 0,$$

which is exactly the definition of simple normality in the base r. □

The general result is an immediate corollary.

Corollary 3.4.1. *If α is strongly normal in the base r, then α is normal in the base r.*

3.5 No Rational Number is Simply Strongly Normal

In light of Theorem 3.4.1, it will suffice to show that no simply normal rational number can be simply strongly normal.

If α is rational and simply normal in the base r, then if we restrict ourselves to the first n digits in the repeating tail of the expansion, the frequency of any 1-string k is exactly n/r whenever n is a multiple of the length of the repeating string. The excess of occurences of k can never exceed the constant number of times k occurs in the repeating string. Therefore, with $m_k(n)$ defined as in Section 3.1,

$$\limsup_{n\to\infty}\left(m_k(n)-\frac{n}{r}\right)=Q,$$

with Q a constant due in part to the initial non-repeating block, and in part to the maximum excess in the tail.

But

$$\limsup_{n\to\infty}\frac{Q}{\sqrt{2n\log\log n}}=0\ ,$$

so α does not satisfy Definition 3.1.1.

3.6 Construction of an Absolutely Strongly Normal Number

To determine an absolutely strongly normal number, we modify Sierpiński's method of constructing an absolutely normal number [34]. We begin with an easy lemma. In what follows, the function $f(n)$ depends on both n and α, and the probability is the Lebesgue measure of the set of $\alpha\in[0,1]$ for which f satisfies the condition(s).

Lemma 3.6.1. *Let $f(n)$ be a real-valued function of the first n base r digits of a number $\alpha\in[0,1]$, and suppose*

$$\mathbf{P}\left[\limsup_{n\to\infty}f(n)=1\right]=1$$

and

$$\mathbf{P}\left[\liminf_{n\to\infty}f(n)=-1\right]=1\ .$$

Given positive numbers $\delta_1>\delta_2>\delta_3>\cdots$, and $\varepsilon_1>\varepsilon_2>\varepsilon_3>\cdots$, we can find positive integers $M_1<M_2<M_3<\cdots$ so that

$$\mathbf{P}\left[\left|\sup_{M_i\le n<M_{i+1}}f(n)-1\right|>\delta_i\quad or\quad\left|\inf_{M_i\le n<M_{i+1}}f(n)+1\right|>\delta_i\right]<\varepsilon_i\ .$$

For sufficiently large M,

$$\mathbf{P}\left[\sup_{n\ge M}f(n)>1+\delta_1\right]<\frac{\varepsilon_1}{4}\quad\text{and}$$

$$\mathbf{P}\left[\inf_{n\geq M} f(n) < -1-\delta_1\right] < \frac{\varepsilon_1}{4}\ .$$

Set M_1 to be the least such M.

Now, as $M\to\infty$,

$$\mathbf{P}\left[\sup_{M_1\leq n<M} f(n) < 1-\delta_1\right] \to 0\ ,$$

and also

$$\mathbf{P}\left[\inf_{M_1\leq n<M} f(n) > -1+\delta_1\right] \to 0\ .$$

Thus, for sufficiently large M, these four conditions are satisfied:

$$\mathbf{P}\left[\sup_{M_1\leq n<M} f(n) < 1-\delta_1\right] < \frac{\varepsilon_1}{4}\ ,$$

$$\mathbf{P}\left[\inf_{M_1\leq n<M} f(n) > -1+\delta_1\right] < \frac{\varepsilon_1}{4}\ ,$$

$$\mathbf{P}\left[\sup_{n\geq M} f(n) > 1+\delta_2\right] < \frac{\varepsilon_2}{4}\ ,$$

and

$$\mathbf{P}\left[\inf_{n\geq M} f(n) < -1-\delta_2\right] < \frac{\varepsilon_2}{4}\ .$$

We set M_2 to be the least $M > M_1$ satisfying all four conditions. Since

$$\mathbf{P}\left[\sup_{M_1\leq n<M_2} f(n) > 1+\delta_1\right] \leq \mathbf{P}\left[\sup_{n\geq M_1} f(n) > 1+\delta_1\right]\ ,$$

and

$$\mathbf{P}\left[\inf_{M_1\leq n<M_2} f(n) < -1-\delta_1\right] \leq \mathbf{P}\left[\inf_{n\geq M_1} f(n) < -1-\delta_1\right]\ ,$$

we have

$$\mathbf{P}\left[\left|\sup_{M_1\leq n<M_2} f(n)-1\right| > \delta_1 \quad \text{or} \quad \left|\inf_{M_1\leq n<M_2} f(n)+1\right| > \delta_1\right] < \varepsilon_1\ .$$

We can continue in this way, recursively choosing $M_3, M_4, M_5, \ldots$ so that each M_i is the least satisfying the required conditions. □

Now we fix an integer base $r\geq 2$ and a 1-string $k\in\{0,1,\ldots,r-1\}$. For each $\alpha\in[0,1]$, put

$$f(n) = f(\alpha,k,n) = \frac{m_k(n)-\dfrac{n}{r}}{\dfrac{\sqrt{r-1}}{r}\sqrt{2n\log\log n}}\ .$$

Here, as in Definition 3.1.1 of Section 3.1, $m_k(n)$ is the number of occurrences of k in the first n base r digits of α, and α is simply strongly normal in the base r if

$$\limsup_{n\to\infty} f(n) = 1$$

and

$$\liminf_{n\to\infty} f(n) = -1 \ .$$

By Theorem 3.2.1 , Section 3.2, these conditions hold with probability 1, so f satisfies the conditions of Lemma 3.6.1.

Now fix $0 < \varepsilon \leq 1$; set $\delta_i = \dfrac{1}{i}$ and $\varepsilon_i = \varepsilon_{r,i} = \dfrac{\varepsilon}{3 \cdot 2^i r^3}$. These δ_i and ε_i also satisfy the conditions of Lemma 3.6.1.

We will construct a set $A_\varepsilon \subset [0,1]$, of measure less than 1, in such a way that every element of A_ε^C is absolutely strongly normal.

Let $M_1 < M_2 < M_3 < \cdots$ be determined as in the proof of Lemma 3.6.1, so that the conclusion of the lemma holds. We build a set $A_{r,i}$ containing those α for which the first M_{i+1} digits are, in a loose sense, far from simply strongly normal in the base r.

Around each $\alpha = .a_1 a_2 \cdots a_{M_{i+1}} \cdots$ such that

$$\left| \sup_{M_i \leq n < M_{i+1}} f(n) - 1 \right| > \delta_i \tag{3.6.1}$$

or

$$\left| \inf_{M_i \leq n < M_{i+1}} f(n) + 1 \right| > \delta_i \tag{3.6.2}$$

we construct an open interval containing α:

$$\left(\frac{a_1}{r} + \frac{a_2}{r^2} + \cdots + \frac{a_{M_{i+1}}}{r^{M_{i+1}}} - \frac{1}{r^{M_{i+1}}}, \frac{a_1}{r} + \frac{a_2}{r^2} + \cdots + \frac{a_{M_{i+1}}}{r^{M_{i+1}}} + \frac{2}{r^{M_{i+1}}} \right) \ .$$

Let $A_{r,k,i}$ be the union of all the intervals constructed in this way. By our construction, the union of the closed intervals consisting of the numbers with initial digits $.a_1 a_2 \ldots a_{M_{i+1}}$ satisfying one of our two conditions (3.6.1) or (3.6.2) has measure less than ε_i, so, denoting Lebesgue measure by μ,

$$\mu\left(A_{r,k,i}\right) < 3\varepsilon_i \ = \frac{\varepsilon}{2^i r^3}.$$

In this way we construct $A_{r,k,i}$ for every base r and 1-string $k \in \{0, 1, \ldots, r-1\}$. We let

$$A_\varepsilon = \bigcup_{r=2}^{\infty} \bigcup_{k=0}^{r-1} \bigcup_{i=1}^{\infty} A_{r,k,i} \ ,$$

so

$$\begin{aligned}\mu(A_\varepsilon) &\leq \sum_{r=2}^{\infty}\sum_{k=0}^{r-1}\sum_{i=1}^{\infty}\mu\left(A_{r,k,i}\right)\\ &< \sum_{r=2}^{\infty}\sum_{k=0}^{r-1}\sum_{i=1}^{\infty}\frac{\varepsilon}{2^i r^3}\\ &= \left(\frac{\pi^2}{6}-1\right)\varepsilon\ .\end{aligned}$$

Let E_ε be the complement of A_ε in $[0,1]$. Since $\mu(A_\varepsilon) < 1$, E_ε is of positive measure. We claim that every element of E_ε is absolutely strongly normal.

For each base r and 1-string $k \in \{0, 1, \ldots, r-1\}$, we have specified a set of integers $M_1 < M_2 < M_3 < \cdots$, depending on r and k. By our construction, if $\alpha \in E_\varepsilon$, then, recalling that f depends on α, we have

$$\left|\sup_{M_i \leq n < M_{i+1}} f(n) - 1\right| < \delta_i$$

and

$$\left|\inf_{M_i \leq n < M_{i+1}} f(n) + 1\right| < \delta_i$$

for every i. Clearly for this α, since $\delta_i \to 0$,

$$\limsup_{n\to\infty} f(n) = 1$$

and

$$\liminf_{n\to\infty} f(n) = -1\ .$$

This is true for every k, so α is simply strongly normal to the base r, by Definition 3.1.1 (Section 3.1). Thus α is simply strongly normal to every base, and is therefore absolutely strongly normal by Definitions 3.1.2 and 3.1.3.

To specify an absolutely strongly normal number, we note that E_ε contains no interval, since, by Section 3.5, no rational number is simply strongly normal in any base. Since E_ε is bounded, $\inf E_\varepsilon$ is well-defined; and $\inf E_\varepsilon \in E_\varepsilon$ since otherwise $\inf E_\varepsilon$ would be interior to some open interval of A_ε.

For example, $\inf E_1$ is a well-defined absolutely strongly normal number.

3.7 Further Questions

It should be possible to construct a computable absolutely strongly normal number by the method of Becher and Figueira [3].

We conjecture that such naturally occurring constants as the irrational numbers π, e, $\sqrt{2}$, and $\log 2$ are absolutely strongly normal.

On the other hand, we speculate that the binary Liouville λ number, created in the obvious way from the λ function values, may be normal but not strongly normal.

Bailey and Crandall [2] proved normality in the base 2 for an uncountable class of "generalized Stoneham constants" of the form

$$\alpha_{2,3}(r) = \sum_{j=0}^{\infty} \frac{1}{3^j 2^{3^j + r_j}} \ ,$$

where r_j is the jth binary digit of a real number r in the unit interval.. This class of numbers may be a good place to look for examples of strong normality. However, new techniques may be required for this.

Chapter 4

Modular Normality of Integer Sequences

4.1 Uniform Distribution Modulo q and Modular Normality

For the basic definitions of the normality of numbers, we recall Section 2.1.

Niven ([29], [30]) made the following definition for sequences of integers (see also [22]).

Definition 4.1.1. *Let $\{A_j\}$ be a sequence of integers. The sequence is* uniformly distributed modulo q *if the asymptotic frequency of each residue class modulo q is $1/q$. That is, if $\mu_k(n)$ is the number of times that $A_j \equiv k \pmod{q}$ for $j \leq n$, then*

$$\lim_{n\to\infty} \frac{\mu_k(n)}{n} = \frac{1}{q} \ .$$

In this work, we will use the term *simply normal modulo q* to mean uniformly distributed modulo q. Simple normality modulo every integer $q > 1$ is known in the literature as uniform distribution modulo $\mathbb{Z}$.

The following is almost self-evident, but we state it as a theorem since it is worthy of note and we have not found it explicitly in the literature.

Theorem 4.1.1. *The number α is simply normal in the base r if and only if the sequence $\{\lfloor r^j\alpha \rfloor\}$ is simply normal modulo r.*

Here, the notation $\lfloor a \rfloor$ denotes the integer part of a for $a > 0$.

We observe that, if α has the base r representation

$$\alpha = \sum_{j=1}^{\infty} \frac{a_j}{r^j},$$

then

$$\lfloor r^j\alpha \rfloor \equiv a_j \pmod{r} \ ,$$

as long as we assume (without loss of generality) that the sequence $\{a_j\}$ does not have a tail in which every digit is $r-1$. We let $A_j = \lfloor r^j \alpha \rfloor$, and let $m_k(n)$ be the number of occurrences of the digit k in the first n base r digits of α. Then, with $\mu_k(n)$ as defined above, we have

$$\mu_k(n) = m_k(n) \ .$$

The result then follows from the definitions of simple normality of α and simple normality of the sequence $\{A_j\}$ modulo r. □

Given a sequence of integers $\{A_j\}$, we consider subsequences of length t, of the form $(A_{j+1}, \ldots, A_{j+t})$, and call them *$t$-blocks*. For each t-block we form an ordered t-tuple of residue classes modulo q, $(c_1, c_2, \ldots, c_t)$, with $c_i \equiv A_{j+i} \pmod{q}$, and call this a *$t$-string* of residues.

Definition 4.1.2. *A sequence $\{A_j\}$ of integers is* normal modulo q *if every t-string of residues modulo q has frequency approaching q^{-t} in the limit. Formally, let τ denote a t-string of residues, and let $\nu_\tau(n)$ be the number of occurrences of τ in the first n t-blocks $(A_1, \ldots, A_t), \ldots, (A_{(n-1)t+1}, \ldots, A_{nt})$. Then A_j is normal modulo q if, for every integer $t \geq 1$ and every t-string τ, we have*

$$\lim_{n\to\infty} \frac{\nu_\tau(n)}{n} = \frac{1}{q^t} \ .$$

For simplicity, the definition is based on the frequency of each t-string in the first n disjoint t-blocks. We could just as easily have taken the first n overlapping t-blocks. The proof that these definitions are equivalent is identical to the proof that the analogous definitions are equivalent for normal numbers, as in [31]. The definition we use is analogous to the definition of normality given by Pillai [33]. In our context, asymptotically uniform frequency of the t-strings of residue classes is not equivalent to simple normality modulo q^t. The non-equivalence is an evident consequence of our main theorem in this chapter, Theorem 4.3.1, which demonstrates that no sequence $\{\lfloor r^j \alpha \rfloor\}$ can be normal modulo r^t for any $t > 1$. (In fact, an examination of the proof reveals that this is true for every α, whether or not α is normal in the base r.)

On the other hand, in the context of normality of numbers, asymptotically uniform frequency of t-strings of digits in consecutive disjoint blocks in the base r is indeed equivalent to simple normality in the base r^t, since there is a one-to-one correspondence between digits in the base r^t and t-strings of digits in the base r.

Here we are considering the integer parts of the sequence $\{r^n \alpha\}$, where α is normal in the base r. We note that the fractional parts of this sequence have been well studied; they form a sequence of real numbers that is uniformly distributed modulo 1, and the Weyl criterion can be applied to establish the uniform distribution.

While we are specifically studying the sequence $\{\lfloor r^n \alpha \rfloor\}$, the concepts can of course be applied to any sequence of integers. For example, the sequence of the primes is not simply normal modulo any integer $q > 1$. On the other hand, the sequence given by $A_j = j$ is simply normal modulo every $q > 1$ (uniformly distributed modulo $\mathbb{Z}$), but it is not normal modulo any integer.

4.2 The Sequence $\lfloor 2^n\sqrt{2}\rfloor$

We illustrate the notion of modular normality by examining a simple example.

The integer part of $2\sqrt{2}$ is 2. This is 0 (mod 2), and so 0 is the first binary digit (after the "decimal" point) of $\sqrt{2}$. We have

$$\lfloor 2^2\sqrt{2}\rfloor = 5 \equiv 1 \pmod 2 ,$$

so the second binary digit of $\sqrt{2}$ is 1.

Continuing in this manner, we obtain the sequence

$$\{A_n\} = \{2, 5, 11, 22, 45, 90, 181, \ldots\}$$

giving the sequence of residue classes

$$\{a_n\} = \{0, 1, 1, 0, 1, 0, 1, \ldots\}$$

modulo 2. The sequence of residue classes, of course, exactly matches the sequence of binary digits of $\sqrt{2}$.

Note that A_{n+1} is equal to either $2A_n$ or $2A_n + 1$. This allows us to compute the residue classes of the sequence modulo any integer q, simply from the initial residue class of A_1 modulo q and the sequence $\{a_n\}$ of residue classes modulo 2. (In fact, we can use the residue class of A_n for any specified n as our initial condition.)

We have $A_1 = 2 \equiv 2 \pmod 3$. Since $a_2 = 1$, we know that $A_2 = 2A_1 + 1$ and so $A_2 \equiv 2 \cdot 2 + 1 \equiv 2 \pmod 3$. We can generate the sequence of residue classes modulo 3 referring only to the $\{a_n\}$, without any need to refer directly to the $\{A_n\}$. In this way we obtain the sequence of residues

$$\{c_n\} = \{2, 2, 2, 1, 0, 0, 1, \ldots\}$$

modulo 3.

If $a_{n+1} = 0$, then $A_{n+1} = 2A_n$, so $c_{n+1} \equiv 2c_n \pmod 3$, and we can specify the transitions by the following table:

c_n	0	1	2
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
c_{n+1}	0	2	1

.

On the other hand, if $a_{n+1} = 1$, we have $A_{n+1} = 2A_n + 1$, and $c_{n+1} \equiv 2c_n + 1 \pmod 3$, giving us these transitions:

c_n	0	1	2
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$
c_{n+1}	1	0	2

.

Thus, c_{n+1} depends jointly on a_{n+1} and c_n.

Now $\sqrt{2}$ is widely believed to be normal in the base 2, and indeed in every base. If this is the case, then the sequence $\{A_n\}$ is normal modulo 2, and Theorem 4.3.1 establishes that

the sequence is also simply normal modulo 3. However, it is clear that the sequence cannot be normal modulo 3, since a transition from 0 to 2 is impossible. Therefore the 2-string $\tau = (0, 2)$ cannot occur in the sequence $\{c_n\}$, and the strings $(1, 1)$ and $(2, 0)$ must likewise be missing.

Working now modulo 4, we have $A_1 = 2 \equiv 2 \pmod 4$ and $A_2 = 5 \equiv 1 \pmod 4$. We obtain the sequence of residues, modulo 4,

$$\{e_n\} = \{2, 1, 3, 2, 1, 2, 1, \ldots\}.$$

If $a_{n+1} = 0$, we get the following table of transitions:

$$\begin{array}{c|cccc} e_n & 0 & 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ e_{n+1} & 0 & 2 & 0 & 2 \end{array} .$$

When $a_{n+1} = 1$, the table looks like this:

$$\begin{array}{c|cccc} e_n & 0 & 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ e_{n+1} & 1 & 3 & 1 & 3 \end{array} .$$

Once again, although we prove in the next section that the sequence $\{A_n\}$ is simply normal modulo 4 if $\sqrt{2}$ is normal in the base 2, the sequence fails to be normal modulo 4 since the 2-string $(0, 3)$ cannot occur; there are 7 other impossible 2-strings.

We conclude these examples by considering a number β generated by choosing each of the binary digits independently and with equal probability from $\{0, 1\}$. This model of a "truly random" number gave rise to the notion of normality. Borel proved that such a number is normal in the base 2 with probability 1 [10]. We let $B_n = \lfloor 2^n \beta \rfloor$, generating a sequence of integers from the base-2 representation of β. Now we consider $\{B_n\}$ modulo 3, and as before we generate the sequence of residue classes. The three residue classes constitute the states of a Markov chain, and we obtain the matrix of transition probabilities

$$\begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} \end{bmatrix} .$$

Here the i, jth entry represents the probability of a transition from the ith to the jth residue class (for convenience we use the indices $\{i, j\} \in \{0, 1, 2\}$). For example, if $B_n \equiv 0 \pmod 3$, then $B_{n+1} \equiv 1 \pmod 3$ with probability $1/2$.

If we consider the sequence of residues of $\{B_n\}$ modulo 4, we get the following transition probability matrix:

$$\begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{2} \end{bmatrix} .$$

We will generalize this Markov chain model in the following section.

4.3 Normality of the Sequence $\lfloor r^n \alpha \rfloor$ Modulo q

For the elementary theory of Markov chains, we have relied on [9] and [18].

We assume that the number α is normal in the base r, so that the sequence given by

$$A_n = \lfloor r^n \alpha \rfloor$$

is normal modulo r.

First, consider integers $q > r$, and let c_n be the residue class of $A_n \pmod q$. We number the residue classes in the usual way from 0 to $q-1$. The possible transitions from c_n to c_{n+1} are given by

$$c_{n+1} \equiv \begin{cases} rc_n \\ rc_n + 1 \\ \cdots\cdots\cdots \\ rc_n + r - 1 \end{cases} \pmod q .$$

These possible transitions from $c_n \equiv h \pmod q$ give r distinct consecutive residue classes for any specified value of h. Furthermore, for $c_n \equiv h+1 \pmod q$, we have $rc_n \equiv rh + r \pmod q$, so the r possible transitions from $h+1$ are consecutive to the possible transitions from h.

We obtain the following transition probability matrix by setting the i,jth entry equal to $1/r$ if the transition from i to j is possible, and equal to 0 otherwise :

$$\begin{bmatrix} r^{-1} & r^{-1} & \cdots & r^{-1} & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & r^{-1} & r^{-1} & \cdots & r^{-1} & \cdots & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & \cdots & r^{-1} & r^{-1} & \cdots & r^{-1} \end{bmatrix} .$$

This is a $q \times q$ matrix with rq non-zero entries. If r divides q, then there are q/r identical blocks of r rows each. Otherwise, the consecutive residue classes "wrap around," so that some rows both begin and end with non-zero entries. In the previous section, the modulo 4 transition probability matrix is an example of the former case and the modulo 3 matrix illustrates the latter case.

Note that the transition probability matrix is not directly obtained from $\{A_n\}$. Rather, the i, jth entry gives the probability of a transition from i to j modulo q in the sequence $\{\lfloor r^n\beta \rfloor\}$, where the base r digits of β are independent random variables, each with uniform distribution on $\{0, \ldots, r-1\}$.

There are exactly r non-zero entries in each row and each column, so the rows and columns each sum to 1.

We may interpret the matrix to represent a digraph on q vertices labelled from 0 to $q-1$. Each vertex has indegree r and outdegree r. If a transition from i to j is possible in the sequence of residues c_n, then we draw an arrow from i to j. (Note that to say a transition is possible is not to say that it actually occurs in a particular sequence; we will have to show that it must occur in any sequence arising from a normal number α.)

We need to show that there is a directed path joining any pair of vertices; that is, each residue class is accessible from every other in the sequence. (Once again, this will only prove that one state can be reached from another, not that it is necessarily reached.)

First, we show that any vertex j can be reached from 0. Certainly 0 can be reached from 0 (there is a loop in the digraph at 0), so we only need consider $j > 0$. Set i to be the least index of a row with a non-zero entry in the jth column, and note that i is strictly less than j. Thus there is $i < j$ so that j can be reached from i. Now the same is true for i, so we can obtain a strictly decreasing sequence of indices such that there is a path from the vertex of least index to the jth vertex. This sequence must terminate in the first row, of index 0, so there is a path from 0 to j. Thus the digraph contains a tree rooted at 0, and is therefore connected. This, together with the fact that each vertex is of indegree equal to its outdegree, is enough to show that there is an Eulerian circuit of the digraph. Consequently, any vertex can be reached by a directed path from any other, and the Markov chain corresponding to this matrix is irreducible.

Furthermore, the loop at 0 implies that the Markov chain is aperiodic. Since the entries of the transition matrix sum to 1, there is a unique stable distribution of states, in which every state has probability $1/q$. The Markov chain converges to this distibution exponentially fast, regardless of the initial distribution (see [9], Theorem 8.7, p. 109).

If $q < r$, then the transition probability matrix has no zero entries, and there is a directed path of length 1 joining every ordered pair of vertices. We have $r = gq + h$, for unique integers $g \geq 1$ and $0 \leq h < q$. The transition matrix is of the form

$$\begin{bmatrix} (g+1)r^{-1} & \cdots & (g+1)r^{-1} & gr^{-1} & \cdots & gr^{-1} \\ gr^{-1} & \cdots & \cdots & (g+1)r^{-1} & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{bmatrix}.$$

Each row has h consecutive entries of the form $(g+1)r^{-1}$, and $q-h$ entries of the form gr^{-1}. Once again, each column and each row sums to 1, and the corresponding Markov chain is irreducible and aperiodic, and each state has stationary probability $1/q$.

Now we state and prove the main result of this chapter.

Theorem 4.3.1. *If a number α is normal in the base r, the integer sequence given by*

$$A_n = \lfloor r^n \alpha \rfloor$$

is simply normal modulo every integer greater than 1.
Furthermore, the sequence is normal modulo the integer $q > 1$ if and only if q divides r.

The first part, that $\{A_n\}$ is uniformly distributed modulo $\mathbb{Z}$, was proved by Vanden Eynden [38]. We give a new proof here, since we will use the same method to prove the second part of this theorem, and to prove Theorem 4.4.1 of the next section.

We specify an integer modulus $q > 1$, and form the integer sequence $\{A_n\}$ and the sequence of residues $\{c_n\}$ modulo q, as above. We can take the sequence $\{a_n\}$ to be the base r digits of α, or the sequence of residues of $\{A_n\}$ modulo r, as required.

We form the $q \times q$ matrix of possible transitions in the sequence $\{c_n\}$, and note, as in the first part of this section, that this matrix corresponds to an irreducible aperiodic Markov process with no transient states. The states of the process correspond to the q residue classes, and the process has a stable asymptotic distribution in which all states occur with probability approaching $1/q$.

Considering the Markov chain, we specify an arbitrary starting state k, with $0 \le k \le q-1$. Let $\mu_i(t)$ be the number of occurrences of the ith residue class in the first t steps of the Markov process. Doeblin's central limit theorem[1] (Theorem 1.2.3) guarantees that, for any $\varepsilon > 0$,

$$\mathbf{P}\left[\left|\mu_i(t) - \frac{t}{q}\right| \ge \varepsilon t\right] \to 0 \tag{4.3.1}$$

as $t \to \infty$.

Since

$$\mathbf{P}\left[\max_i \left|\mu_i(t) - \frac{t}{q}\right| \ge \varepsilon t\right] \le \sum_{i=0}^{k-1} \mathbf{P}\left[\left|\mu_i(t) - \frac{t}{q}\right| \ge \varepsilon t\right],$$

we have

$$\mathbf{P}\left[\max_i \left|\frac{\mu_i(t)}{t} - \frac{1}{q}\right| \ge \varepsilon\right] \to 0$$

as $t \to \infty$. That is, if t is large enough,

$$\mathbf{P}\left[\max_i \left|\frac{\mu_i(t)}{t} - \frac{1}{q}\right| \ge \varepsilon\right] < \varepsilon.$$

The probability measure is uniform on the set of t-strings of residue classes modulo r. Thus, there are at most εr^t strings for which $\left|\frac{\mu_i(t)}{t} - \frac{1}{q}\right| \ge \varepsilon$ for some i. Defining Ω_t to be the set of t-strings modulo r, the mean value of $\left|\frac{\mu_i(t)}{t} - \frac{1}{q}\right|$ is

$$\int_{\Omega_t} \left|\frac{\mu_i(t)}{t} - \frac{1}{q}\right| \mathrm{d}\mathbf{P} < \varepsilon + \frac{q-1}{q}\varepsilon < 2\varepsilon. \tag{4.3.2}$$

[1] In fact, a weak law of large numbers in this context would suffice. Here we take the weak law as an easy consequence of the central limit theorem.

The first term of the estimate comes from those t-strings for which no frequency $\mu_i(t)/t$ differs from $1/q$ by more than ε, of total probability at most 1, and the second comes from the other t-strings, of total probability less than ε, for which $\mu_i(t)/t$ differs from $1/q$ by at most $(q-1)/q$.

Returning to the sequence $\{a_n\}$, we recall that for every string length t and for every t-string τ, the frequency of τ in the first n t-blocks, $\dfrac{\nu_\tau(n)}{n}$, approaches r^{-t} as $n \to \infty$. We can choose n_t so large that, if $n \geq n_t$,

$$\left| \frac{\nu_\tau(n)}{n} - \frac{1}{r^t} \right| < \frac{\varepsilon}{r^t}$$

for every τ. (Note that n_t depends on α.) For convenience, we can assume that $n_t = mr^t$ for some integer m.

Now set $N = tn_t$, so we are considering the first N integers in the sequence $\{A_n\}$. Let $\tilde{\mu}_i(N)$ be the number of occurrences of the ith residue class modulo q if each string τ occurs exactly m times, and let $\mu_i(\tau)$ be the number of times the ith residue class occurs modulo q when the string τ occurs modulo r in the first n_t blocks of $\{a_n\}$. We continue to suppose, for now, that every t-block of the sequence $\{c_n\}$ begins with the same residue class k modulo q, so these numbers are well-defined. We have already established, by (4.3.2), that

$$\left| \frac{\tilde{\mu}_i(N)}{N} - \frac{1}{q} \right| < 2\varepsilon,$$

since

$$\left| \frac{\tilde{\mu}_i(N)}{N} - \frac{1}{q} \right| = \left| \frac{1}{r^t} \sum_\tau \frac{\mu_i(\tau)}{t} - \frac{1}{q} \right| \leq \int_{\Omega_t} \left| \frac{\mu_i(t)}{t} - \frac{1}{q} \right| \mathrm{d}\mathbf{P}.$$

We let $\mu_i(N)$ be the number of times the ith residue class occurs in the sequence $\{c_n\}$, still supposing each t-block begins with k, but now with the strings τ in their actual order determined by $\{A_n\}$. We would like to estimate

$$\left| \frac{\mu_i(N)}{N} - \frac{\tilde{\mu}_i(N)}{N} \right|.$$

Note that

$$\tilde{\mu}_i(N) = m \sum_\tau \mu_i(\tau),$$

and that

$$\mu_i(N) = \sum_\tau m_\tau \mu_i(\tau),$$

where $m_\tau = \nu_\tau(n_t)$ is the number of occurrences of τ in the first n_t t-blocks of the sequence $\{a_n\}$.

For each τ,

$$\left| \frac{m_\tau}{mr^t} - \frac{1}{r^t} \right| < \frac{\varepsilon}{r^t},$$

by assumption, and so

$$|m_\tau - m| < m\varepsilon.$$

This gives

$$\left|\frac{\mu_i(N)}{N} - \frac{\tilde{\mu}_i(N)}{N}\right| \leq \frac{1}{mtr^t}\sum_\tau |m_\tau - m|\,\mu_i(\tau) \leq \varepsilon, \tag{4.3.3}$$

since there are r^t terms in the sum, and each $\mu_i(\tau)$ is at most t.

We can conclude, then, that the actual frequency of the ith residue class differs from $1/q$ by

$$\left|\frac{\mu_i(N)}{N} - \frac{1}{q}\right| \leq \left|\frac{\mu_i(N)}{N} - \frac{\tilde{\mu}_i(N)}{N}\right| + \left|\frac{\tilde{\mu}_i(N)}{N} - \frac{1}{q}\right| < 3\varepsilon. \tag{4.3.4}$$

We need to correct our assumption that every block of $\{c_n\}$ begins with the same residue class k. In the estimate of (4.3.3), we bounded $\mu_i(\tau)$ by t, and this will not be changed by any arbitrary choice of initial states in each t-block. The estimates of (4.3.2) come from the application of the central limit theorem in (4.3.1). Since the application of the central limit theorem does not depend on the initial state (see the discussion following Theorem 1.2.3), the convergence of (4.3.1) holds regardless of the initial state of each t-block, and indeed the convergence is uniform over the set of starting states. All the estimates of (4.3.4) are valid regardless of any arbitrary assignment of residue classes at the start of each block.

We can take ε small by taking t and n_t large, so we can conclude that

$$\left|\frac{\mu_i(n)}{n} - \frac{1}{q}\right| \to 0$$

as $n \to \infty$. Thus, the sequence $\{A_n\}$ is simply normal modulo q.

Since the modulus q was arbitrary, this concludes the proof of the first part of the theorem: the sequence A_n is simply normal modulo every integer $q > 1$. That is, the sequence $\{\lfloor r^n\alpha \rfloor\}$ is equidistributed modulo $\mathbb{Z}$.

Now if $q > r$, there are $(q-r)q$ zero entries in the transition probability matrix, and each one of these corresponds to a transition that cannot occur in the sequence of residues $\{c_n\}$ modulo q. It is evident that, for every $t \geq 2$, some t-strings will not occur in the sequence $\{c_n\}$, so the sequence $\{A_n\}$ fails to be normal modulo q.

It remains to consider $q < r$. If q divides r, then all entries in the matrix of transition probabilities modulo q have the same value $1/q$. Consider strings of length s. The transition from one such string to another is itself a Markov chain, and every such transition has probability q^{-s}. We can make an argument very similar to the first part of the proof: replace the residue classes modulo q by s-strings σ of residue classes; and replace the t-strings of residue classes in our argument by st-strings (or, equivalently, t-strings of s-strings). The probability space will be Ω_{st}, again with the uniform probability measure.

To construct the matrix of transition probabilities, we arbitrarily index the s-strings σ_i, with $i = 1, \ldots, q^s$. The i, jth entry is the probability of transition from σ_i to σ_j. Again, we can initally assume that every st-string begins with some fixed s-string κ, and then correct

this assumption without affecting our estimates. In the same way as before, we can show that the frequency of each s-string in $\{c_n\}$ approaches q^{-s}. Since this is true for every s, the sequence $\{A_n\}$ is normal modulo q.

Now suppose q does not divide r, so

$$r = gq + h$$

with $g > 0$ and $0 < h < q$. Each row of the transition probability matrix modulo q has $q - h$ entries g/r, and h entries $(g+1)/r$. The frequency of any 2-string approaches one of the two distinct values $g/(qr)$ and $(g+1)/(qr)$, and neither of these is the q^{-2} required for normality. In this case, then, $\{A_n\}$ is not normal modulo q. □

4.4 A Condition Modulo q for Normality in the Base r

This work was originally motivated by the simple observation that the sequence $\{\lfloor 2^n\sqrt{2}\rfloor\}$ appeared to have random properties in moduli other than 2. This led us to wonder if the question of normality in one base could be approached via some modulus other than a power of the base. In this section we give a partial affirmative answer to the question.

We will restrict ourselves to the case $q > r$. Suppose $\alpha \in [0, 1)$, and write

$$\begin{aligned} A_n &= \lfloor r^n\alpha \rfloor, \\ a_n &\equiv A_n \pmod r, \quad a_n \in \{0, \ldots, r-1\}, \quad \text{and} \\ c_n &\equiv A_n \pmod q, \quad c_n \in \{0, \ldots, q-1\}. \end{aligned}$$

We have $A_{n+1} = rA_n + a_{n+1}$. Given any particular value of c_n, the possible values of c_{n+1} are all distinct modulo q, so for fixed c_n the value of c_{n+1} is determined by a_{n+1}, and the map $a_{n+1} \mapsto c_{n+1}$ is one-to-one. Thus, for fixed c_n, the map

$$(a_{n+1}, \ldots, a_{n+t-1}) \mapsto (c_{n+1}, \ldots, c_{n+t-1})$$

is one-to-one. For fixed a_n, the reverse map

$$(c_{n+1}, \ldots, c_{n+t-1}) \mapsto (a_{n+1}, \ldots, a_{n+t-1})$$

is also one-to-one. There are r^{t-1} possible t-strings starting with any fixed c_n; and since there are q possible values for c_n, there are qr^{t-1} possible t-strings. The set of possible t-strings is a proper subset of $\{0, \ldots, q-1\}^t$, and we will call this subset ${}_rQ_t$. As before, the set of possible t-strings in the sequence $\{a_n\}$ is $\Omega_t = \{0, \ldots, r-1\}^t$.

Now form the matrix of transition probabilities modulo q, as before, where the i, jth entry is the probability that $c_{n+1} = j$ if $c_n = i$, where $c_n \equiv \lfloor r^n\beta \rfloor \pmod q$ if the digits of β are independent and uniformly distributed in the base r. There are r entries of value r^{-1} in each row, and $q - r$ zero entries. We have uniform probability on Ω_t, so if the probability were uniform on the values c_{nt+1} at the start of each t-block, then we would have uniform

probability on ${}_rQ_t$ as well. The latter probability is not in general uniform, but it does approach uniformity as n approaches infinity.

This motivates the following definition. We continue to assume that $q > r$, so that $|{}_rQ_t| = qr^{t-1}$. The set ${}_rQ_t$ is the set of possible t-strings in the sequence $\{c_n\}$ modulo q determined by $\{\lfloor r^n\beta\rfloor\}$, where the base r digits of β are random as before. However, in the definition, we allow $\{A_n\}$ to be any integer sequence.

Definition 4.4.1. *Let $\nu_\sigma(n)$ be the number of times the s-string σ occurs in the first n s-blocks of $\{c_n\}$, where $c_n \equiv A_n \pmod q$ and $0 \le c_n \le q-1$. The integer sequence $\{A_n\}$ is* base-r normal modulo q, *or* r-normal modulo q, *if*

$$\lim_{n\to\infty}\left|\frac{\nu_\sigma(n)}{n} - \frac{1}{qr^{s-1}}\right| = 0$$

for every s-string $\sigma \in {}_rQ_s$, for every string length $s \ge 1$.

We now give a condition modulo q for normality in the base r.

Theorem 4.4.1. *Given integers $q > r > 1$, the number α is normal in the base r if and only if the sequence $\{\lfloor r^n\alpha\rfloor\}$ is r-normal modulo q.*

To prove the theorem, we repeat the argument of the last section. For the "only if" direction of proof, we replace the s-strings of residue classes modulo q with s-strings of residue classes $\sigma \in {}_rQ_s$, and otherwise proceed as before, making the argument based on the Markov chain of the s-strings.

For the "if" direction, we interchange the roles of the s-strings modulo r and the s-strings modulo q. Note that, to argue in this direction, we apply the central limit theorem for Markov chains to the process given by random s-strings modulo r, and we assume, to begin with, that every t-string of s-strings modulo r begins with some arbitrary string κ. In this direction of proof, the underlying probability space is ${}_rQ_{st}$, not Ω_{st}.

The transition probability matrix in this direction of proof is constructed by considering a randomly generated sequence $\{\gamma_n\}$ modulo q. The first element γ_1 is uniformly distributed on $\{0, 1, \ldots, q-1\}$. The distribution of γ_{n+1} is dependent on γ_n: given $\gamma_n = i$, we have

$$\mathbf{P}\left[\gamma_{n+1} = j\right] = \frac{1}{r}$$

if $(i, j) \in {}_rQ_2$. Now the i, jth entry of the matrix gives the probability of a transition from the ith to the jth residue class modulo r, and every entry has the value r^{-1}. □

The theorem says that, if α is normal in the base r, the sequence $\{\lfloor r^n\alpha\rfloor\}$ is as close as it can be to normality modulo every $q > r$, given the constraints imposed by the transition probabilities. Conversely, r-normality modulo q of $\{\lfloor r^n\alpha\rfloor\}$ for any integer $q > r$ implies that α is normal in the base r.

One could extend the definition of r-normality modulo q to cover the case $q < r$. However, since in this case the map from Ω_t to ${}_rQ_t$ is not one-to-one (even if we fix the first

element of each t-string), we would not expect to be able to prove both directions of the last theorem.

We are led to wonder whether there is a converse to part of Theorem 4.3.1. If $\{\lfloor r^n\alpha\rfloor\}$ is simply normal modulo every integer $q > 1$, does this guarantee normality of α in the base r? We conjecture not.

Simple normality modulo 2 of $\{\lfloor 2^n\alpha\rfloor\}$ neither implies nor precludes simple normality modulo some other q. For example, the base 2 expansion of $1/3$ is

$$.010101\ldots,$$

and this is simply normal in the base 2. The sequence $\{A_n\} = \{\lfloor 2^n/3\rfloor\}$ is

$$0, 1, 2, 5, 10, 21, \ldots,$$

and modulo 3 this is the repeating sequence

$$0, 1, 2, 2, 1, 0, 0, 1, 2, 2, 1, 0, \ldots.$$

Thus, $\{A_n\}$ is simply normal modulo 3. On the other hand, modulo 5 this is the repeating sequence

$$0, 1, 2, 0, 0, 1, 2, 0, \ldots,$$

which is not uniformly distributed modulo 5.

Now consider the sequence $\{\lfloor 2^n/5\rfloor\}$. It is easily verified that this sequence is simply normal modulo 2 and 5, but not modulo 3. The sequence modulo 5 is a repeating 20-string.

Finally, we suppose that it is feasible to construct a sequence of integers normal modulo every integer $q > 1$; we would call such a sequence "normal modulo $\mathbb{Z}$." Furthermore, we conjecture that almost every sequence of integers is normal modulo $\mathbb{Z}$, as long as we define "almost every" in the suitable asymptotic sense.

Chapter 5

Flat Sequences of Polynomials with Cyclotomic Coefficients

5.1 Littlewood's Problem and Flat Polynomials

The context of this work is the Littlewood problem in L_∞: do there exist constants A and B, and a sequence of polynomials

$$p_n = \sum_{j=0}^{n} a_{nj} z^j$$

with coefficients ± 1, such that

$$A\sqrt{n+1} \leq |p_n(z)| \leq B\sqrt{n+1}$$

for z on the unit circle? Such a sequence of polynomials is called "flat," and we loosely call an element of such a sequence a "flat polynomial." If the constants A and B can be replaced by $1-\varepsilon_n$ and $1+\varepsilon_n$, where $\varepsilon_n \to 0$ as $n \to \infty$, then the sequence is called "ultra-flat."

This problem was discussed by Littlewood [26], and related results have been reviewed by Borwein [13] and Erdélyi [17]. We note that the problem is still open.

Of interest to us here is the line followed by Kahane [19], who proved that, if the coefficients are complex with $|a_{nj}| = 1$, then ultra-flat polynomials do indeed exist. Since we will use his result, we state it now:

Theorem 5.1.1 (Kahane)**.** *There is a sequence q_n of degree n polynomials with unimodular coefficients, and a sequence $\varepsilon_n > 0$ with $\varepsilon_n \to 0$, such that*

$$(1-\varepsilon_n)\sqrt{n} \leq |q_n(z)| \leq (1+\varepsilon_n)\sqrt{n}$$

for $|z| = 1$.

It should be noted that there was an error in Kahane's proof. This was pointed out, and corrected, by Queffelec and Saffari [37]; the theorem itself is correct as originally stated by Kahane.

Beck [4] built on this result to show that sequences of flat polynomials exist of which the coefficients are lth roots of unity, if l is sufficiently large. His result, the main topic of this paper, is the following:

Theorem 5.1.2 (Beck)**.** *If l is a sufficiently large integer, then there are constants A and B and a sequence p_n of polynomials*

$$p_n(z) = \sum_{j=0}^{n} a_{nj} z^j$$

with $a_{nj} = e^{2\pi ik/l}$, $k \in \{0, \ldots, l-1\}$ for $j = 0, \ldots, n$, such that

$$A\sqrt{n+1} < |p_n(z)| < B\sqrt{n+1}$$

for $|z| = 1$ and n sufficiently large.

Beck stated and proved the theorem with $l = 400$. There was a minor error in the proof, however; with the error corrected, l should be 851. We will give the corrected proof below. It should be noted that the error only affected the numerical bound; the method of proof itself, and the qualitative result, are entirely correct.

We will need Spencer's result on the discrepancy of linear forms [35]:

Theorem 5.1.3 (Spencer)**.** *Let*

$$L_i(x_1, \ldots, x_n) = a_{i1}x_1 + \cdots + a_{in}x_n, \qquad 1 \le i \le n$$

be n linear forms in n variables with real coefficients $|a_{ij}| \le 1$. Then there is an absolute constant K, and a choice of $u_j = \pm 1$ for $j = 1, \ldots, n$, so that

$$|L_i(u_1, \ldots, u_n)| \le K\sqrt{n}, \qquad 1 \le i \le n,$$

if n is sufficiently large.

The value of K in Spencer's theorem ultimately determines the least value of l for which Beck's theorem holds. Beck used Spencer's estimate $K \approx 9$, but Spencer also gave a lower estimate of $K \approx 5.32$. Here we will obtain a slightly lower estimate, $K \approx 5.199$, and using this, we will lower the value of l to 492. A refinement of Spencer's method, due to K.-U. Schmidt (personal communication), improves this significantly, to $K \approx 3.65$. This, in turn, lowers the value of l to 345. We will outline Schmidt's result in Section 5.6.

5.2 Proof of Beck's Theorem

In this section we closely follow Beck's method of proof [4]. However, his proof was driven by a particular value of the constant K in Spencer's theorem (Theorem 5.1.3). Here we make the argument without assuming any particular value for K. In Sections 5.5 and 5.6 we will use the available values of K to draw our numerical conclusions. We believe there is still room to improve on the value of K; if this is done, the general form of Beck's theorem we give here can be applied immediately.

To be precise, the form of the theorem we will prove is as follows:

Theorem 5.2.1 (Beck)**.** *Suppose that K is such that, for sufficiently large n, for every set of n linear forms in n variables*

$$L_i(x_1, \dots, x_n) = a_{i1}x_1 + \cdots + a_{in}x_n, \qquad 1 \le i \le n,$$

with real coefficients $|a_{ij}| \le 1$ for $i, j \in \{1, \dots, n\}$, there exist $u_j = \pm 1$ for $j = 1, \dots, n$ so that

$$|L_i(u_1, \dots, u_n)| \le K\sqrt{n}, \qquad 1 \le i \le n.$$

Then there is an integer l_0 and constants A and B, such that for any integer $l \ge l_0$ there is a sequence p_n of polynomials

$$p_n(z) = \sum_{j=0}^{n} a_{nj} z^j,$$

of which each coefficient is an lth root of unity, with

$$A\sqrt{n+1} < p_n(z) < B\sqrt{n+1}$$

for $|z| = 1$ and n sufficiently large. Furthermore,

$$l_0 \le \min\left\{ l \in \mathbb{Z} : \ l \ge 3, \ \cos\frac{\pi}{l} - \frac{12K\pi\sqrt{2\pi}}{l} > 0 \right\}. \tag{5.2.1}$$

First, let

$$L_i(\mathbf{x}) = a_{i1}x_1 + \cdots + a_{in}x_n, \qquad 1 \le i \le n,$$

be a set of n linear forms in n variables with complex coefficients a_{ij}, $|a_{ij}| \le 1$. From these we form $2n$ linear forms with real coefficients in $2n$ variables:

$$M_i(x_1, \dots, x_{2n}) = \mathfrak{Re}(a_{i1})x_1 + \cdots + \mathfrak{Re}(a_{in})x_n + 0x_{n+1} + \cdots + 0x_{2n}, \qquad 1 \le i \le n,$$

$$M_{n+i}(x_1, \dots, x_{2n}) = \mathfrak{Im}(a_{i1})x_1 + \cdots + \mathfrak{Im}(a_{in})x_n + 0x_{n+1} + \cdots + 0x_{2n}, \qquad 1 \le i \le n.$$

By our assumption, we can find $u_j \in \{\pm 1\}$, $j = 1, \dots, 2n$, so that

$$|M_i(u_1, \dots, u_{2n})| \le K\sqrt{2n}, \qquad 1 \le i \le 2n.$$

In turn, this means that

$$|L_i(u_1, \dots, u_n)| \le 2K\sqrt{n}, \qquad 1 \le i \le n. \tag{5.2.2}$$

We make use of this to prove the following lemma:

Lemma 5.2.1 (Beck)**.** *Given $n+1$ complex numbers $b_0, b_1, \dots, b_n$, all of modulus at most d, there exist $u_0, u_1, \dots, u_n \in \{\pm 1\}$ such that, for any $R > K$,*

$$\max_{|z|=1} \left| \sum_{k=0}^{n} u_k b_k z^k \right| \le 4Rd\sqrt{2\pi}\sqrt{n+1} \tag{5.2.3}$$

when n is sufficiently large.

Here, as throughout this paper, K is the constant in Theorem 5.2.1, guaranteed to exist by Theorem 5.1.3.

We note that this lemma is where a slight error occurred in Beck's proof. The error was kindly pointed out to us by Tamás Erdélyi: Beck ([4], p. 274) left out a constant in the application of Bernstein's inequality to (5.2.4) below. The constant was required since Beck parametrized the unit circle by $e^{2\pi i\theta}$ rather than by $e^{i\theta}$ as we have done here. As a result, he omitted the factor $\sqrt{2\pi}$ in (5.2.3).

We have changed some details to correct the error, but apart from these minor details the proof we give is the same as the original. The substance of Beck's proof is certainly correct.

Paterson and Tarokh ([32], Lemma 6) have also given a corrected version of Beck's proof. However, they did not point out where the error lay, nor did they examine the effect of the error on the value of l_0.

To prove the lemma, without loss of generality we can let $d = 1$.

Set $\nu = \lceil 2\pi n \rceil$. Form ν linear forms in ν variables, with only the first n coefficients non-zero:

$$L_m(x_0, \ldots, x_{\nu-1}) = \sum_{k=0}^{\nu-1} \left(b_k e^{2\pi i \frac{km}{\nu}} \right) x_k, \qquad m = 0, \ldots, \nu - 1$$

with $b_k = 0$ for $k > n - 1$. By (5.2.2), there are $u_0, \ldots, u_{\nu-1} \in \{\pm 1\}$ such that, if n is sufficiently large and $R > K$,

$$\left| \sum_{k=0}^{n-1} u_k b_k z^k \right| = \left| \sum_{k=0}^{\nu-1} u_k b_k z^k \right| < 2K\sqrt{\nu} < 2R\sqrt{2\pi n}$$

for every $z = e^{2\pi i m/\nu}$, $m = 0, \ldots, \nu - 1$.

Put

$$M = \max_{|z|=1} \left| \sum_{k=0}^{n-1} u_k b_k z^k \right|.$$

Then

$$M = \left| \sum_{k=0}^{n-1} u_k b_k e^{i\beta k} \right|$$

for some $\beta \in [0, 2\pi)$. There is some $m(\beta) \in \{0, 2\pi, \ldots, (\nu - 1)2\pi\}$ such that

$$\left| \beta - \frac{m(\beta)}{\nu} \right| \leq \frac{2\pi}{2\nu} \leq \frac{1}{2n} \ .$$

Now let

$$f(\theta) = \sum_{k=0}^{n-1} u_k b_k e^{i\theta k}.$$

We have

$$\left| f(\beta) - f\left(\frac{m(\beta)}{\nu}\right)\right| \le \int_{\frac{m(\beta)}{\nu}}^{\beta} \left|f'(\theta)\right| \mathrm{d}\theta, \tag{5.2.4}$$

and by Bernstein's inequality this is no greater than

$$nM\left|\beta - \frac{m(\beta)}{\nu}\right| \le nM\frac{1}{2n} = \frac{M}{2}.$$

This gives

$$\frac{M}{2} = |f(\beta)| - \frac{M}{2} \le \left|f\left(\frac{m(\beta)}{\nu}\right)\right| < 2R\sqrt{2\pi n}.$$

Replacing n by $n+1$ gives the lemma. □

Now we have what we need to prove the theorem. Let g_n be a sequence of "ultra-flat" polynomials, as given by Theorem 5.1.1:

$$g_n(z) = \sum_{k=0}^{n} a_{nk} z^k, \qquad |a_{nk}| = 1, \quad 0 \le k \le n,$$

with

$$(1-\eta_n)\sqrt{n+1} < |g_n(z)| < (1+\eta_n)\sqrt{n+1}, \qquad |z| = 1, \tag{5.2.5}$$

where $\eta_n \to 0$ as $n \to \infty$.

Fix an integer $l \ge 3$, and denote by P_l the regular polygon of which the vertices are the lth roots of unity. The inscribed circle has radius $\rho = \rho(l) = \cos\dfrac{\pi}{l}$.

Now consider the kth coefficient of g_n: $a_k = a_{nk} = e^{2\pi i \alpha_k}$, where $0 \le \alpha_k < 1$. (From this point, for convenience we will drop the n from a_{nk}; it is understood that a_k and α_k depend on n.) For some integer $j = j(n,k)$ with $0 \le j < l$,

$$\frac{j}{l} - \frac{1}{2l} \le \alpha_k < \frac{j}{l} + \frac{1}{2l}.$$

For each $k \in \{0, \dots, n\}$, let Δ_k be the triangle with vertices

$$e^{2\pi i \frac{j-1}{l}},\ e^{2\pi i \frac{j}{l}},\ e^{2\pi i \frac{j+1}{l}}.$$

The diameter of Δ_k is

$$\text{diam } \Delta_k < \frac{4\pi}{l}. \tag{5.2.6}$$

By joining the midpoints of the sides, we obtain four similar triangles $\Delta_k(1;s)$, $s = 1, \dots, 4$. For convenience we define $\Delta_k(1;1)$ to be the triangle containing the arc of the circle inscribed in P_l, so $\Delta_k(1;1)$ has vertices

$$\frac{e^{2\pi i \frac{j-1}{l}} + e^{2\pi i \frac{j}{l}}}{2},\ e^{2\pi i \frac{j}{l}},\ \frac{e^{2\pi i \frac{j}{l}} + e^{2\pi i \frac{j+1}{l}}}{2}.$$

Decomposing each of $\Delta_k(1;s)$ into four similar triangles in the same way, we get 16 triangles $\Delta_k(2;s),\ s=1,\dots,16$. Iterating, we get

$$\Delta_k = \bigcup_{s=1}^{4} \Delta_k(1;s) = \bigcup_{s=1}^{4^2} \Delta_k(2;s) = \cdots = \bigcup_{s=1}^{4^q} \Delta_k(q;s) = \cdots,$$

and

$$\text{diam } \Delta_k(q;s) = 2^{-q}\text{diam } \Delta_k < 2^{-q}\frac{4\pi}{l}.$$

Now fix $q \in \mathbb{Z}$ with $2^q \geq n+1$. Then there are indices $s_2,\dots,s_q$, all depending on k, such that

$$\rho a_k \in \Delta_k(q;s_q) \subset \cdots \subset \Delta_k(2;s_2) \subset \Delta_k(1;1) \subset \Delta_k.$$

Let $\omega_{k,q}$ be any vertex of $\Delta_k(q;s_q)$, arbitrarily chosen for each k. By (5.2.6),

$$\max_{|z|=1}\left|\sum_{k=0}^{n}\rho a_k z^k - \sum_{k=0}^{n}\omega_{k,q}z^k\right| \leq \sum_{k=0}^{n}|\rho a_k - \omega_{k,q}| \leq (n+1)2^{-q}\frac{4\pi}{l} \leq \frac{4\pi}{l}.$$

Now set

$$d = d_q = \frac{1}{2}\text{diam } \Delta_k(q-1;s_{q-1}) = 2^{-q}\frac{4\pi}{l}.$$

If $\omega_{k,q}$ is a vertex of $\Delta_k(q-1;s_{q-1})$, put $\omega^*_{k,q-1} = \omega_{k,q}$. Otherwise, arbitrarily choose one of the endpoints of the side of $\Delta_k(q-1;s_{q-1})$ containing $\omega_{k,q}$, and label it $\omega^*_{k,q-1}$. Then each $\left(\omega_{k,q} - \omega^*_{k,q-1}\right)$ is a complex number of modulus at most d, and by Lemma 5.2.1 there exist $u_k = \pm 1$, for $k = 0,\dots,n$, so that

$$\max_{|z|=1}\left|\sum_{k=0}^{n} u_k\left(\omega_{k,q} - \omega^*_{k,q-1}\right)z^k\right| \leq 4Rd\sqrt{2\pi}\sqrt{n+1}$$

for $R > K$. Now, if $\omega_{k,q}$ was a vertex of $\Delta_k(q-1;s_{q-1})$, set $\omega_{k,q-1} = \omega^*_{k,q-1} = \omega_{k,q}$. Otherwise, if $u_k = 1$, set $\omega_{k,q-1} = \omega^*_{k,q-1}$, and if $u_k = -1$, define $\omega_{k,q-1}$ to be the other endpoint of the side of $\Delta_k(q-1;s_{q-1})$ containing $\omega_{k,q}$, so that

$$\omega_{k,q} - \omega_{k,q-1} = -\left(\omega_{k,q} - \omega^*_{k,q-1}\right).$$

Then, in every case,

$$\left(\omega_{k,q} - \omega_{k,q-1}\right)z^k = u_k\left(\omega_{k,q} - \omega^*_{k,q-1}\right)z^k,$$

and we have

$$\max_{|z|=1}\left|\sum_{k=0}^{n}\omega_{k,q}z^k - \sum_{k=0}^{n}\omega_{k,q-1}z^k\right| \leq 4Rd\sqrt{2\pi}\sqrt{n+1} = 2^{-q}\frac{16R\pi\sqrt{2\pi}}{l}\sqrt{n+1}\ .$$

Iterate, choosing $\omega_{k,q-2},\dots,\omega_{k,1}$, so that, by applying Lemma 5.2.1 with

$$d = d_r = 2^{-r}\frac{4\pi}{l},$$

we have

$$\max_{|z|=1}\left|\sum_{k=0}^{n}\omega_{k,r}z^k-\sum_{k=0}^{n}\omega_{k,r-1}z^k\right|\le 4Rd\sqrt{2\pi}\sqrt{n+1}=2^{-r}\frac{16R\pi\sqrt{2\pi}}{l}\sqrt{n+1}$$

for $r=2,\dots,q-1$.

One last iteration will reach $\omega_k=\omega_{k,0}$. Here $\omega_{k,1}$ is a vertex of $\Delta_k(1:1)$, so either $\omega_k=\omega_{k,1}=e^{2\pi i\frac{j}{l}}$, or $\omega_{k,1}$ is a midpoint of Δ_k. In the latter case, ω_k is one of the roots of unity

$$e^{2\pi i\frac{j-1}{l}},\ e^{2\pi i\frac{j}{l}},\ e^{2\pi i\frac{j+1}{l}}.$$

This time we can take $d=d_1=\dfrac{\pi}{l}$ and choose ω_k according to Lemma 5.2.1 so that

$$\max_{|z|=1}\left|\sum_{k=0}^{n}\omega_{k,1}z^k-\sum_{k=0}^{n}\omega_{k}z^k\right|\le 4Rd\sqrt{2\pi}\sqrt{n+1}=\frac{4R\pi\sqrt{2\pi}}{l}\sqrt{n+1}.$$

Summarizing, we have

$$\begin{aligned}\max_{|z|=1}\left|\sum_{k=0}^{n}\rho a_kz^k-\sum_{k=0}^{n}\omega_kz^k\right| &\le \max_{|z|=1}\left|\sum_{k=0}^{n}\rho a_kz^k-\sum_{k=0}^{n}\omega_{k,q}z^k\right|\\ &\quad+\sum_{r=2}^{q}\max_{|z|=1}\left|\sum_{k=0}^{n}\omega_{k,r}z^k-\sum_{k=0}^{n}\omega_{k,r-1}z^k\right|\\ &\quad+\max_{|z|=1}\left|\sum_{k=0}^{n}\omega_{k,1}z^k-\sum_{k=0}^{n}\omega_kz^k\right|\\ &\le \frac{4\pi}{l}+\sum_{r=2}^{q}2^{-r}\frac{16R\pi\sqrt{2\pi}}{l}\sqrt{n+1}+\frac{4R\pi\sqrt{2\pi}}{l}\sqrt{n+1}\\ &\le \frac{12R\pi\sqrt{2\pi}}{l}\sqrt{n+1}+O(1).\end{aligned}$$

By (5.2.5),

$$(\rho-\xi_n)\sqrt{n+1}<\left|\sum_{k=0}^{n}\rho a_kz^k\right|<(\rho+\xi_n)\sqrt{n+1},$$

where $\rho=\cos\dfrac{\pi}{l}$ and $\xi_n\to 0$ as $n\to\infty$. This gives

$$\begin{aligned}\left(\cos\frac{\pi}{l}-\frac{12R\pi\sqrt{2\pi}}{l}-\xi_n\right)\sqrt{n+1}-O(1) &< \left|\sum_{k=0}^{n}\omega_kz^k\right|\\ &< \left(\cos\frac{\pi}{l}+\frac{12R\pi\sqrt{2\pi}}{l}+\xi_n\right)\sqrt{n+1}+O(1).\end{aligned}$$

By setting

$$l_0 = \min\left\{ l \in \mathbb{Z} :\ l \geq 3,\ \cos\frac{\pi}{l} - \frac{12R\pi\sqrt{2\pi}}{l} > 0 \right\}, \tag{5.2.7}$$

we obtain the theorem. □

The condition $l \geq 3$ is redundant; we state it to emphasize that Beck's method of approximation by the endpoints of triangles requires a largest triangle of which the endpoints must be roots of unity.

5.3 Proof of Spencer's Theorem

Spencer [35] calculated several values of K, of which the best was $K \leq 5.32$. Without developing any new technique, we will slightly improve on this result.

Our goal is to prove Theorem 5.1.3. We will closely follow the method of Spencer, and we will use the following theorem due to Kleitman [21].

Theorem 5.3.1 (Kleitman)**.** *Let $\mathcal{A} \subset \{\pm 1\}^r$ and $t < r/2$ be given, with*

$$|\mathcal{A}| \geq \sum_{i=0}^{t} \binom{r}{i} .$$

Then diam $\mathcal{A} \geq 2t$.

Here, the diameter is taken with respect to the Hamming metric, which counts the number of coordinates where two elements of $\{\pm 1\}^r$ differ. The theorem says that some pair of elements of $\mathcal{A}$ differs in at least $2t$ coordinates.

For this and what follows we will make use of two functions. The first, the binary entropy function, is defined for $0 \leq q \leq 1$ as

$$H(q) = -q\log_2 q - (1-q)\log_2(1-q), \quad 0 < q < 1,$$

and

$$H(0) = H(1) = 0.$$

The second is the normal distribution function, defined for $x \in \mathbb{R}$ by

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} \mathrm{d}t \ .$$

We begin with a combinatorial lemma. The proof is as given by Spencer [35].

Lemma 5.3.1. *Let $1/2 > a_1 > a_2 > \cdots$ be given, and put*

$$\mathbf{B} = \{(b_1, \ldots, b_n) \in \mathbb{Z}^n : |\{i : |b_i| \geq s\}| \leq a_s n,\ s = 1, 2, \ldots\}.$$

Then $|\mathbf{B}| \leq 2^{cn}$, with

$$c = \sum_{s=1}^{\infty} [H(a_s) + a_s].$$

Note that the sum may fail to converge, in which case the lemma gives no information about the cardinality of $\mathbf{B}$.

Put $\alpha_s = \lfloor a_s n \rfloor$. We can choose $\{i : |b_i| = s\}$ in $\sum_{k=0}^{\alpha_s} \binom{n}{k}$ ways. For each choice of $\{i : |b_i| = s\}$, there are $2^k \leq 2^{\alpha_s}$ ways of choosing $b_i = \pm s$.

We have, then,

$$|\mathbf{B}| < \prod_{s=1}^{\infty} \left[2^{\alpha_s} \sum_{k=0}^{\alpha_s} \binom{n}{k} \right].$$

A straightforward estimation, given below, yields

$$\sum_{k=0}^{\alpha_s} \binom{n}{k} \leq 2^{nH(\alpha_s/n)}. \tag{5.3.1}$$

Therefore,

$$|\mathbf{B}| < \prod_{s=1}^{\infty} 2^{\alpha_s + nH(\alpha_s/n)} \leq \prod_{s=1}^{\infty} 2^{n(H(a_s)+a_s)},$$

and this is the lemma.

To see (5.3.1), let $p + q = 1$, with $q > p$. For $\alpha = np$,

$$\sum_{k=0}^{\alpha} \binom{n}{k} p^k q^{n-k} = p^\alpha q^{n-\alpha} \sum_{k=0}^{\alpha} \binom{n}{k} \left(\frac{q}{p}\right)^{\alpha-k} < 1.$$

Then

$$\sum_{k=0}^{\alpha} \binom{n}{k} \leq \sum_{k=0}^{\alpha} \binom{n}{k} \left(\frac{q}{p}\right)^{\alpha-k} \leq \frac{1}{p^\alpha q^{n-\alpha}} = 2^{nH(p)}.$$

□

The following lemma is given in more general form in an appendix of [36].

Lemma 5.3.2. *Let $L(\mathbf{u}) = a_1 u_1 + \cdots + a_r u_r$ be a linear form with real coefficients a_i, with $|a_i| \leq 1$ for each i, and let the $u_i = \pm 1$ be independent and uniformly distributed random variables. Then*

$$\mathbf{P}\left[|L(\mathbf{u})| \geq \lambda\sqrt{r}\right] \leq 2e^{-\lambda^2/2}. \tag{5.3.2}$$

By comparing power series, it is easily seen that $\cosh c \le e^{c^2/2}$ for every real c, with equality only when $c = 0$. Then

$$\begin{aligned}\mathbf{E}\left[e^{ca_iu_i}\right] &= \frac{1}{2}e^{ca_i} + \frac{1}{2}e^{c(-a_i)} \\ &= \cosh ca_i \quad \le \quad \cosh c \quad \le \quad e^{c^2/2}.\end{aligned}$$

Since the a_iu_i are independent, we have

$$\begin{aligned}\mathbf{E}\left[e^{cL(\mathbf{u})}\right] &= \prod_{i=1}^{r} \cosh ca_i \\ &\le e^{rc^2/2}.\end{aligned}$$

Now using Markov's inequality, for positive c and α,

$$\begin{aligned}\mathbf{P}\left[|L(\mathbf{u})| \ge \alpha\right] &= 2\mathbf{P}\left[e^{cL(\mathbf{u})} \ge e^{c\alpha}\right] \\ &\le 2\mathbf{E}\left[e^{cL(\mathbf{u})}\right] e^{-c\alpha} < 2e^{rc^2/2-c\alpha}.\end{aligned}$$

Putting $c = \alpha/r$, we have

$$\mathbf{P}\left[|L(\mathbf{u})| \ge \alpha\right] \le 2e^{\alpha^2/(2r)-\alpha^2/r} = 2e^{-\alpha^2/(2r)}.$$

We get (5.3.2) by putting $\alpha = \lambda\sqrt{r}$. □

We prove one more lemma in probability before we turn to Spencer's main lemma.

Lemma 5.3.3. *Let $L(\mathbf{u}) = a_1u_1 + \cdots + a_ru_r$ be a linear form with real coefficients a_i, with $|a_i| \le 1$ for each i, and let the $u_i = \pm 1$ be independent and uniformly distributed random variables. Fix $C > 0$ and $\varepsilon > 0$. Then, for $0 < \lambda < C$,*

$$\mathbf{P}\left[|L(\mathbf{u})| \ge \lambda\sqrt{r}\right] \le 2(1+\varepsilon)\Phi(-\lambda) \tag{5.3.3}$$

when r is sufficiently large.

First, suppose $L(\mathbf{u}) = a_1u_1 + \cdots + a_ru_r$ is as in the lemma, and write $\mathbf{a} = (a_1, \ldots, a_r)$. Each a_iu_i is a random variable of mean 0 and variance a_i^2, and $L(\mathbf{u})$ is a random variable of mean 0 and variance

$$\sigma^2 = \|\mathbf{a}\|_2^2 = \sum_{i=1}^{r} a_i^2.$$

We consider the case $\sigma^2 < \sqrt{r}$. By Markov's inequality,

$$\begin{aligned}\mathbf{P}\left[|L(\mathbf{u})| \ge \lambda\sqrt{r}\right] &= \mathbf{P}\left[L(\mathbf{u})^2 \ge \lambda^2 r\right] \\ &\le \frac{\mathbf{E}\left[L(\mathbf{u})^2\right]}{\lambda^2 r} \\ &= \frac{\sigma^2}{\lambda^2 r} \quad < \quad \frac{1}{\lambda^2\sqrt{r}}.\end{aligned}$$

Thus, (5.3.3) is satisfied in this case if r is sufficiently large.

Now we turn to the general case. Let L_r be a sequence of linear forms

$$L_r(\mathbf{u}) = a_{r1}u_1 + \cdots + a_{rr}u_r, \qquad r = 1, 2, \ldots,$$

with the u_i as stated in the lemma, and write $\mathbf{a}_r = (a_{r1}, \ldots, a_{rr})$. Each $a_{ri}u_i$ is a random variable of mean 0 and variance a_{ri}^2, and $L_r(\mathbf{u})$ is a random variable of mean 0 and variance

$$\sigma_r^2 = \|\mathbf{a}_r\|_2^2 = \sum_{i=1}^{r} a_{ri}^2.$$

In light of the first case we considered, we can assume without loss of generality that $\sigma_r^2 \geq \sqrt{r}$. Then $\sigma_r \to \infty$ as $r \to \infty$, and the Lindeberg condition is satisfied. That is, for every $\eta > 0$,

$$\lim_{r\to\infty} \frac{1}{\sigma_r^2} \sum_{i=1}^{r} \int_{|a_{ri}u_i| \geq \eta\sigma_r} a_{ri}^2 u_i^2 \mathrm{d}\mu = 0,$$

where μ is the probability measure on each u_i. By the Lindeberg central limit theorem (Theorem 1.2.2), the distribution function of $L_r(\mathbf{u})/\|\mathbf{a_r}\|_2$ converges weakly to Φ. This convergence is uniform on $\mathbb{R}$, and therefore uniform on $[-C, C]$. Since $\|\mathbf{a_r}\|_2 \leq \sqrt{r}$, this gives that, for $0 < \lambda < C$ and for any $\varepsilon > 0$, there exists R such that

$$\mathbf{P}\left[|L_r| \geq \lambda\sqrt{r}\right] < 2(1+\varepsilon)\Phi(-\lambda) \tag{5.3.4}$$

when $r > R$. This R is established for the given sequence L_r, and indeed, for each ε there is some R for which (5.3.4) holds for every sequence L_r. If it were otherwise, then one could construct a sequence L_r such that (5.3.4) failed for infinitely many r. □

Now we state and prove Spencer's main result as a lemma, closely following Spencer's argument. This is Spencer's Lemma 20 ([35], p 704), although the bulk of the proof is given with his Lemma 4 ([35], p 681). Our statement of the lemma corrects a typographic error in the original work.[1]

For the purpose of the lemma, we construct a function $\Psi = \Psi_{C,\varepsilon}$ for each choice of large $C > 0$ and small $\varepsilon > 0$. Let $M > 0$ be such that $\Phi(-M) = e^{-C^2/4}$. Define

$$\Psi(t) = 2(1+\varepsilon)e^{-t^2/2}$$

if $t \geq C$, and

$$\Psi(t) = 2(1+\varepsilon)\Phi(-t)$$

if $0 < t \leq M$. For $M < t < C$, set

$$\Psi(t) = 2(1+\varepsilon)\exp\left(-\frac{C^2}{2} + \frac{C^2}{4}\frac{C-t}{C-M}\right).$$

[1]The inequality in $H\left(\frac{1}{2} - p\right) < 1 - \beta$ is reversed in the original.

From our construction of Ψ, it will be clear that, for $L(\mathbf{u})$ as in Lemmas 5.3.2 and 5.3.3, and for $t > 0$,

$$\mathbf{P}\left[|L(\mathbf{u})| \geq t\sqrt{r}\right] \leq \Psi(t), \tag{5.3.5}$$

by those lemmas.

We should point out that Spencer uses

$$\mathbf{P}\left[|L(\mathbf{u})| \geq t\sqrt{r}\right] \leq 2\Phi(-t) + o(1)$$

here. Without more information about the error term, we cannot guarantee convergence of the sum defining β in the following lemma. We therefore use our admittedly more awkward construction, here and in Lemma 5.6.1.

Lemma 5.3.4 (Spencer)**.** *Fix large $C > 0$, small $\varepsilon > 0$, and the function $\Psi = \Psi_{C,\varepsilon}$ as above. Let a rational number $\alpha \leq 1$, a real number $K > 0$, and a real sequence γ_s such that $\sum_{s=1}^{\infty} \gamma_s^{-1} < 1$, be given. Suppose that*

$$\Psi(K(2s+1))\gamma_{s+1} < \Psi(K(2s-1))\gamma_s$$

for $s = 1, 2, \ldots$; define

$$\beta = \alpha^{-1} \sum_{s=1}^{\infty} \left[H\left(\Psi(K(2s-1))\gamma_s\right) + \Psi(K(2s-1))\gamma_s\right]$$

and suppose that $\beta < 1$. Choose p, with $0 < p < 1/2$, so that

$$H\left(\frac{1}{2} - p\right) < 1 - \beta\ .$$

Let L_i, $i = 1, 2, \ldots, n$, be n linear forms in r variables,

$$L_i(\mathbf{x}) = a_{i1}x_1 + \cdots + a_{ir}x_r, \qquad 1 \leq i \leq n\ ,$$

with $r \leq \alpha n$, and real coefficients $|a_{ij}| \leq 1$.

Then for n sufficiently large, there exists $\mathbf{u} = (u_1, \ldots, u_r)$, with each $u_i \in \{-1, 0, 1\}$, so that

$$|\{i : u_i = 0\}| \leq 2p(\alpha n) \tag{5.3.6}$$

and

$$|L_i(\mathbf{u})| \leq K\sqrt{r} \leq K\sqrt{\alpha}\sqrt{n}, \qquad 1 \leq i \leq n\ . \tag{5.3.7}$$

Without loss of generality, we can assume $r = \alpha n$. To see this, write $\alpha = w/v$ in reduced form, where w and v are positive integers. We can make the argument letting $n_k \to \infty$, where $n_k = kv$. For $n_k < n < n_{k+1}$, we can add forms and variables with zero coefficients to obtain $|L_i(\mathbf{u})| \leq K\sqrt{\alpha}\sqrt{n_{k+1}} \leq K\sqrt{\alpha}\sqrt{n+v}$.

Let $\mathbf{u} = (u_1, \ldots, u_n)$, and let the u_i be independent random variables such that each $u_i = \pm 1$ with equal probability.

Define $T : \{\pm 1\}^r \to \mathbb{Z}^n$ by

$$T(u_1, \dots, u_r) = (b_1, \dots, b_n),$$

with

$$b_i = 0 \qquad \text{if} \qquad |L_i(\mathbf{u})| \le K\sqrt{r}$$

and

$$b_i = s \qquad \text{if} \qquad (2s-1)K\sqrt{r} < |L_i(\mathbf{u})| \le (2s+1)K\sqrt{r}$$

for $s = 1, 2, \dots$.

Now define

$$\mathbf{B} = \{\mathbf{b} \in \mathbb{Z}^n : |\{i : |b_i| \ge s\}| \le n\Psi(K(2s-1))\gamma_s, \qquad s = 1, 2, \dots\}.$$

We have

$$\mathbf{P}[b_i \ge s] = \mathbf{P}\left[|L((u)| \ge K(2s-1)\sqrt{r}\right] \le \Psi(K(2s-1))$$

for r sufficiently large, by (5.3.5).

The expected number of i such that $b_i \ge s$ is at most $n\Psi(K(2s-1))$. By Markov's inequality,

$$\mathbf{P}[|\{i : b_i \ge s\}| \ge n\Psi(K(2s-1))\gamma_s] \le \frac{1}{\gamma_s}. \tag{5.3.8}$$

We have

$$\mathbf{P}\left[\mathbf{b} \in \boldsymbol{B}\right] \ge 1 - \sum_{s=1}^{\infty} \gamma_s^{-1}$$

since the union of the sets in (5.3.8) is the complement of $\boldsymbol{B}$.

Put $\kappa = 1 - \sum_{s=1}^{\infty} \gamma_s^{-1}$. Then $|T^{-1}(\boldsymbol{B})| \ge \kappa 2^r$, since we are using the uniform probability measure on $\{\pm 1\}^r$.

Here we apply Lemma 5.3.1, with $r = \alpha n$ and

$$c = \alpha\beta = \sum_{s=1}^{\infty} \left[H\left(\Psi(K(2s-1))\gamma_s\right) + \Psi(K(2s-1))\gamma_s\right],$$

to get

$$|\boldsymbol{B}| \le 2^{r\beta} = 2^{\alpha\beta n}.$$

Now we look for $\mathcal{A} \subset \{\pm 1\}^r$ on which T is constant, and so that

$$|\mathcal{A}| \ge \kappa 2^r / 2^{\beta r} > 2^{rH(1/2-p)}; \tag{5.3.9}$$

note that the constant κ is absorbed in the latter inequality if r is sufficiently large. By the pigeonhole principle, there is some $\mathbf{b} \in \boldsymbol{B}$ so that, if

$$\mathcal{A} = T^{-1}(\mathbf{b}),$$

then

$$\begin{aligned} |\mathcal{A}| &\geq \left|T^{-1}(\boldsymbol{B})\right| / |\boldsymbol{B}| \\ &\geq \kappa 2^r / 2^{\beta r} \\ &= \kappa 2^{r(1-\beta)} \end{aligned}$$

as desired.

From the proof of Lemma 5.3.1, we have $2^{rH(1/2-p)} \geq \sum_{k=0}^{r(1/2-p)} \binom{r}{k}$. We can apply Kleitman's theorem (Theorem 5.3.1), using (5.3.9), to get

$$\text{diam } \mathcal{A} \geq (1-2p)r. \tag{5.3.10}$$

Then there exist vectors $\mathbf{u_1}$ and $\mathbf{u_2} \in \mathcal{A}$ with

$$\rho(\mathbf{u_1}, \mathbf{u_2}) = \text{diam } \mathcal{A},$$

where ρ is the Hamming metric.

Put $\mathbf{u} = \dfrac{\mathbf{u_1} - \mathbf{u_2}}{2}$. This is not in general an element of $\{\pm 1\}^r$; we have $\mathbf{u} = (u_1, \ldots, u_r)$, with $u_i \in \{-1, 0, 1\}$. Now $u_i = 0$ if and only if $\mathbf{u_1}$ and $\mathbf{u_2}$ have the same ith coordinate, so

$$\begin{aligned} |\{i : u_i = 0\}| &= r - \rho(\mathbf{u_1}, \mathbf{u_2}) \\ &= r - \text{diam } \mathcal{A} \\ &\leq r - (1-2p)r = 2pr. \end{aligned}$$

This gives (5.3.6). For each $i \in 1, \ldots, n$,

$$L_i(\mathbf{u}) = \frac{L_i(\mathbf{u_1}) - L_i(\mathbf{u_2})}{2}.$$

Since $\mathbf{u_1}$ and $\mathbf{u_2}$ belong to $\mathcal{A}$, we have $T(\mathbf{u_1}) = T(\mathbf{u_2})$, and so $L_i(\mathbf{u_1})$ and $L_i(\mathbf{u_2})$ differ by less than $2K\sqrt{r}$. Thus

$$|L_i(\mathbf{u})| \leq K\sqrt{r} = K\sqrt{\alpha}\sqrt{n},$$

and this is (5.3.7). □

With the main lemma in hand, we now turn to the proof of Theorem 5.1.3. First, fix $\alpha < 1$. We will show that K and $\{\gamma_s\}$ can be chosen to satisfy the conditions of Lemma 5.3.4, and indeed that β can be made arbitrarily small.

Note that $H(q) + q$ is dominated by $H(q) \sim -q \log_2 q$ for small q. By considering ratios of the partial sums of the power series for the two sides, one can see that

$$\Phi(-t) \sim \frac{e^{-t^2/2}}{t\sqrt{2\pi}}$$

as t grows large. (The power series for Φ is easily obtained by term-by-term integration of $e^{-t^2/2}$.) Thus, given any choice of γ_1, we can make $H(\Psi(K)\gamma_1) + \Psi(K)\gamma_1$, the first term in the sum for β, arbitrarily small by choosing K large enough. This gives

$$H(\Psi(K)\gamma_1) + \Psi(K)\gamma_1 < \eta$$

for some suitably small η. With M and C as in the definition of Ψ, a straightforward calculation shows that

$$\frac{\Psi(K(2s+1))\gamma_{s+1}\log_2(\Psi(K(2s+1))\gamma_{s+1})}{\Psi(K(2s-1))\gamma_s\log_2(\Psi(K(2s-1))\gamma_s)} \sim \frac{\gamma_{s+1}}{\gamma_s}e^{-4sK^2}$$

if $K(2s+1) < M$ or if $K(2s-1) > C$, and otherwise

$$\frac{\Psi(K(2s+1))\gamma_{s+1}\log_2(\Psi(K(2s+1))\gamma_{s+1})}{\Psi(K(2s-1))\gamma_s\log_2(\Psi(K(2s-1))\gamma_s)} < \frac{\gamma_{s+1}}{\gamma_s}e^{-CK/2}.$$

Thus, if γ_s grows slowly enough, say

$$\frac{\gamma_{s+1}}{\gamma_s} < \min\left(e^{K^2}, e^{CK/4}\right),$$

we can ensure that the sum for β is less than, say, 2η. If we choose $\eta < \alpha/2$, then $\beta < 1$. Since H maps $[0, 1/2]$ continuously onto $[0, 1]$, the p of Lemma 5.3.4 exists, and the conclusions apply.

Our strategy now is to apply Lemma 5.3.4 repeatedly. Note that the lemma ensures the existence of R so that the conclusions of the lemma apply for $\alpha n = r > R$.

On the first iteration, we set $\alpha = \alpha_1 = 1$. For simplicity, we make an appropriate choice of $\{\gamma_s\}$ for all iterations, though it is not strictly necessary that $\{\gamma_s\}$ be the same in every iteration. We choose $K = G_1$ so that $\beta = \beta_1 < 1$. We set $p = p_1 < 1/2$. Then, if $r_1 = \alpha_1 n = n > R$, there exists $\mathbf{u} = \mathbf{u}_1 \in \{-1, 0, 1\}^n$ so that

$$|L_i(\mathbf{u})| \le K\sqrt{\alpha}\sqrt{n} = G_1\sqrt{n}$$

for each $i \in 1, \ldots, n$, and

$$|\{j : u_j = 0\}| \le 2p_1 n.$$

We define $m_2 = |\{j : u_j = 0\}|$.

Now construct new linear forms of reduced length by indexing the j for which $u_j = 0$: $j_1, \ldots, j_{m_2}$. The coefficient a_{ik} of

$$L_i^{(2)}(\mathbf{x}) = a_{i1}x_1 + \cdots + a_{1m_2}x_{m_2}$$

is defined to be the coefficient a_{ij_k} of L_i.

On the next iteration, set $\alpha = \alpha_2 = m_2/n \le 2p_1\alpha_1$, and $r_2 = \alpha_2 n$. Choose $K = G_2$ so that β_2 is small enough to give $p_2 \le p_1$. Then, if $r_2 > R$, Lemma 5.3.4 gives $\mathbf{u}_2 \in \{-1, 0, 1\}^{\alpha_2 n}$ so that

$$|L_i^{(2)}(\mathbf{u}_2)| \le K\sqrt{\alpha}\sqrt{n} = G_2\sqrt{\alpha_2}\sqrt{n}.$$

Proceed in this way, obtaining at the hth iteration

$$\begin{aligned} |L_i(\mathbf{u}^*)| &\leq |L_i(\mathbf{u}_1)| + |L_i^{(2)}(\mathbf{u}_2)| + \cdots + |L_i^{(h)}(\mathbf{u}_h)| \\ &\leq G_1\sqrt{\alpha_1}\sqrt{n} + G_2\sqrt{\alpha_2}\sqrt{n} + \cdots + G_h\sqrt{\alpha_h}\sqrt{n}. \end{aligned}$$

Here the vector $\mathbf{u}^*$ is obtained from the nonzero coordinates of $\mathbf{u_1}, \ldots, \mathbf{u_k}$ inserted in the appropriate positions. From the estimates beginning on page 47, if G_1 is large enough, $\{\gamma_s\}$ is chosen appropriately, and

$$G_1 < G_2 < \cdots,$$

then

$$\begin{aligned} \beta_k &< -\alpha_k^{-1} 2\Psi(G_k)\gamma_1 \log_2(\Psi(G_k)\gamma_1) \\ &\sim \alpha_k^{-1} \frac{2G_k\gamma_1 e^{-G_k^2/2}}{\log 2\sqrt{2\pi}} \end{aligned}$$

if $\Psi(G_k) = 2(1+\varepsilon)\Phi(-G_k)$. Otherwise, if $\Psi(G_k) = 2(1+\varepsilon)e^{-G_k^2/2}$,

$$\beta_k < \alpha_k^{-1} \frac{2G_k^2\gamma_1 e^{-G_k^2/2}}{\log 2}.$$

Note that, for small p, $H(1/2-p) \sim 1 - 2p^2/\log 2$ (from the power series), so for small β,

$$p \sim \sqrt{\frac{\beta \log 2}{2}}.$$

Since

$$\alpha_{k+1} \sim 2p_k\alpha_k,$$

we can certainly choose $\{G_k\}$ so that

$$S = \sum_{k=1}^{\infty} G_k\sqrt{\alpha_k}$$

converges.

After some iteration, say the hth, we get $r_{h+1} < R$. Now the vector $\mathbf{u}^*$ is constructed first from the nonzero coordinates of $\mathbf{u_1}, \ldots, \mathbf{u_h}$, as before, and then the remaining r_{h+1} zero coordinates are replaced arbitrarily with ± 1. Then we have

$$\begin{aligned} |L_i(\mathbf{u}^*)| &\leq G_1\sqrt{\alpha_1}\sqrt{n} + \cdots + G_h\sqrt{\alpha_h}\sqrt{n} + r_{h+1} \\ &\leq S\sqrt{n} + R. \end{aligned}$$

For $\eta > 0$, if $n = r_1$ is sufficiently large we get

$$|L_i(\mathbf{u}^*)| \leq (S+\eta)\sqrt{n}.$$

Then $\mathbf{u}^*$ is the $\mathbf{u}$ of Theorem 5.1.3, and $S+\eta$ is the absolute constant K of the theorem. □

5.4 The Value of K

Spencer ([35]) proved two versions of Theorem 5.1.3. Beck ([4]) used the first result, $K \approx 9$. At the end of his paper, Spencer gave a calculation improving this to $K \approx 5.32$. Here we repeat the calculation, slightly improving the value to $K \approx 5.2$. Spencer made no attempt to optimize his calculation. While our calculation is not rigorously optimized, we did a crude automated search among choices of G_i, and we believe we are close to the best result available by Spencer's method as it stands.

The calculation is based on the iteration argument given in the previous section. We set $\gamma_1 = 1.01$, and $\gamma_s = 103^{s-1}$ for $s > 1$. For convenience, we put

$$b_{j,k} = \left[H\left(\Psi(G_j(2k-1))\gamma_k\right) + \Psi(G_j(2k-1))\gamma_k\right],$$

and write

$$\beta_j = \sum_{k=1}^{\infty} \alpha_j^{-1} b_{j,k}$$

at the jth iteration. Setting $\alpha_1 = 1$ and $G_1 = 4$, we get

$$\alpha_1^{-1} b_{1,1} \approx 0.0010475$$

and

$$\alpha_1^{-1} b_{1,2} \approx 3.74 \times 10^{-29}.$$

Clearly, the sum for β_1 is dominated here by the first term:

$$\beta_1 \approx 0.0010475.$$

We can take $p_1 = 0.019054$, giving $2p_1\alpha_1 < 0.03811$ and $G_1\sqrt{\alpha_1} = 4$.

On the second iteration, we set $\alpha_2 = 0.03811$ and $G_2 = 5$. Again (and in every iteration), β_i is dominated by the first term and we get

$$\beta_2 \approx 0.0035193$$

and can take $p_2 = 0.011044$. This gives $2p_2\alpha_2 < 0.00084177$ and $G_2\sqrt{\alpha_2} < 0.9761$.

We set $\alpha_3 = 0.00084177$ and $G_3 = 5.1$ and continue, taking $\alpha_4 = 0.000097814$ and $G_4 = 6$, and $\alpha_5 = 2.91067 \times 10^{-6}$ and $G_5 = 9$.

On the next iteration, $\alpha_6 \approx 7 \times 10^{-12}$, and we can choose G_6 and subsequent values giving such rapid convergence of $\sum_{j=1}^{\infty} G_j\sqrt{\alpha_j}$ that this sum is dominated by the first five terms. Thus,

$$K = \sum_{j=1}^{\infty} G_j\sqrt{\alpha_j} + \varepsilon < 4 + .9761 + .1480 + .0594 + .01536 < 5.199.$$

We can therefore take $K = 5.199$ in Theorem 5.1.3.

There is no reason to think that Spencer's result could not be substantially improved, giving a significantly lower value of K. On the other hand, Spencer showed that K has a positive lower bound, and indeed K must be greater than 1 ([35], Theorem 19). If the coefficients of n linear forms, each in n real coefficients, form a Hadamard matrix with each entry ± 1, then any choice of $\mathbf{u} \in \{\pm 1\}^n$ gives $L_i(\mathbf{u}) \geq \sqrt{n}$ for some i.

5.5 The Value of l_0

Using $K = 5.199$ and (5.2.1), we immediately find

$$l_0 = 492.$$

Thus, there exist flat polynomials of which the coefficients are 492nd roots of unity.

Spencer suggested that one should not expect to do better than $K \approx 3$ by some refinement of his method. For $K = 3$, (5.2.1) would give $l_0 = 284$.

In principle, if K were sufficiently small, Beck's method would yield the existence of flat polynomials with coefficients that were 3rd roots of unity. However, not even a result of the type $K \to 0$ as $n \to \infty$ could be used to extend Beck's method to Littlewood polynomials, and Beck himself recognised this limitation. Since K is bounded below by 1, the best we can hope to achieve by this method is $l_0 = 95$.

Beck used the value $K \approx 9$, taken from the first version Spencer gave of his theorem. With the proof of Beck's theorem corrected, this gives the value $l_0 = 851$. Had Beck used $K \approx 5.32$, the best value given by Spencer, he would have found $l_0 = 503$.

5.6 Further Improvements

Kai-Uwe Schmidt has calculated a value of $K \approx 3.65$ (personal communication), using a refinement of Spencer's technique. This, on its own, improves the value of l_0 to 345.

He has very kindly agreed to allow us to use the following lemma and his outline of the proof. This lemma is an improvement of Lemma 5.3.4 above. The overall strategy of the proof is as already given for Lemma 5.3.4, and we will be able to refer to that proof for some of the details. Other details are from [1], p. 188. The function Ψ is as defined just before Lemma 5.3.4.

Lemma 5.6.1 (Schmidt)**.** *Let t be real, with $\Psi(t) < 1/e$, and define*

$$h = -(1 - \Psi(t)) \log_2(1 - \Psi(t)) - \sum_{s=1}^{\infty} \Psi\left((2s-1)t\right) \log_2 \Psi\left((2s-1)t\right).$$

Let

$$L_i(\mathbf{x}) = a_{i1}x_1 + \cdots + a_{ir}x_r, \qquad i = 1, \ldots, n,$$

be a set of n linear forms in r variables, with $r \leq n$, and with real coefficients of absolute value at most 1.

Then, if r is large enough, and

$$h \le \frac{r}{(2\log 2)n}, \tag{5.6.1}$$

there is some $\mathbf{u} = (u_1, \ldots, u_r) \in \{-1, 0, 1\}^r$ such that

$$|\{k : u_k = 0\}| \le r\left(1 - \sqrt{\frac{(2\log 2)hn}{r}}\right)$$

and

$$|L_i(\mathbf{u})| \le t\sqrt{r}$$

for each i.

Let $\mathbf{u}$ be random, distributed uniformly on $\{\pm 1\}^r$, and set

$$b_i = L_i(\mathbf{u})$$

for each $i \in \{1, \ldots, n\}$. Let c_i be the closest integer to $|b_i|/(2t\sqrt{r})$, so

$$c_i = \left\lfloor \frac{|b_i|}{2t\sqrt{r}} + \frac{1}{2} \right\rfloor.$$

The entropy function in this context is defined to be

$$\mathcal{H}(c_i) = -\sum_{s=0}^{\infty} \mathbf{P}\left[c_i = s\right] \log_2 \mathbf{P}\left[c_i = s\right].$$

By 5.3.5,

$$\mathbf{P}\left[c_i = 0\right] = \mathbf{P}\left[|L_i(\mathbf{u})| < t\sqrt{r}\right] \ge 1 - \Psi(t),$$

and

$$\begin{aligned} \mathbf{P}\left[c_i = s\right] &= \mathbf{P}\left[\frac{2s-1}{2} \le \frac{|b_i|}{2t\sqrt{r}} < \frac{2s+1}{2}\right] \\ &\le \mathbf{P}\left[|L_i(\mathbf{u})| \ge (2s-1)t\sqrt{r}\right] \\ &\le \Psi((2s-1)t) \end{aligned}$$

for $s \ge 1$, if r is large enough. The function $x \log_2 x$ is decreasing for $1/e < x < 1$, and from our assumption that $\Psi(t) < 1/e$, we have that $1 - \Psi(t) > 1/e$. Therefore,

$$\mathcal{H}(c_i) \le h.$$

Since entropy is subadditive, we have

$$\mathcal{H}(c_1, \ldots, c_n) \le \sum_{i=1}^{n} \mathcal{H}(c_i) \le nh.$$

If a discrete random variable X assumes no value with probability greater than 2^{-v}, then $\mathcal{H}(X) \ge v$. Therefore, some particular value of $(c_1, \ldots, c_n)$ must have probability at least 2^{-nh}. This implies that there is some set $\mathcal{A} \subset \{\pm 1\}^r$, on which $(c_1, \ldots, c_n)$ is constant, and so that

$$|\mathcal{A}| \ge 2^{r-nh}. \tag{5.6.2}$$

The binary entropy function was defined in Section 5.3, for $0 \le q \le 1$, as

$$H(q) = -q \log_2 q - (1-q) \log_2 (1-q), \quad 0 < q < 1,$$

and

$$H(0) = H(1) = 0.$$

On examining the derivative of the difference between the sides, we see that

$$H(\frac{1}{2} - q) \le 1 - \frac{2}{\log 2} q^2$$

for $-1/2 \le q \le 1/2$ (with equality only when $q = 0$).

Putting

$$\delta = \frac{1}{2} - \sqrt{\frac{hn \log 2}{2r}},$$

we get

$$H(\delta) < 1 - \frac{hn}{r}$$

as long as condition (5.6.1) of the lemma holds. Now, from (5.6.2) and (5.3.1), we have

$$|\mathcal{A}| \ge 2^{rH(\delta)} \ge \sum_{k=0}^{\lfloor \delta r \rfloor} \binom{r}{k}.$$

This implies, by Kleitman's theorem, that

$$\text{diam } \mathcal{A} \ge 2\delta r.$$

From here, the argument follows the same lines as the conclusion of the proof of Lemma 5.3.4 (page 47). □

Now it is relatively straightforward to show that h satisfies condition (5.6.1) of the lemma, as long as t is chosen large enough. We can use the estimates of Section 5.3 to do this. As in that section, we can show that an iteration, choosing suitable successive values

of t, converges and gives the K of Spencer's theorem (Theorem 5.1.3). Finally, we can compute a value for K.

Schmidt (personal communication) has carried out the iteration, using the successive values

$$t = 2.9, 3.8, 4.7, 6.$$

In this way he has shown $K \approx 3.65$. It is immediate, from (5.2.1) of Theorem 5.2.1, that

$$l_0 = 345.$$

Schmidt has pointed out that the constant $4\sqrt{2\pi}$ in Lemma 5.2.1 can be improved in two ways. First, instead of splitting the complex coefficients of the linear forms into their real and imaginary parts, one can look at projections on lines through the origin. Second, one can seek to use a tighter version of the Bernstein inequality. These techniques may very well improve the value of l_0 even more than the refinement of Spencer's work.

Appendix

Open Questions

In the study of the normality of numbers, the main open question is generic: are any of the familiar irrational constants such as π, e, $\log 2$, and $\sqrt{2}$ normal in any base? This question seems to be harder than questions of irrationality and transcendence.

When it comes to strong normality, the subject is very much open for exploration. What numbers, known to be normal, are also strongly normal? Can a computable construction of a strongly normal number be given?

The subject of modular normality is also wide open. We wonder whether our theorem on base-r normality modulo q can be extended to the case $q < r$, possibly with some additional condition. Is α necessarily normal in the base r if $\{\lfloor r^n\alpha \rfloor\}$ is uniformly distributed modulo $\mathbb{Z}$? There are various classes of sequences known to be uniformly distributed modulo $\mathbb{Z}$ (see, for example, [22]); are any of these normal modulo $\mathbb{Z}$? If "almost all" is suitably defined, we conjecture that almost all integer sequences are normal modulo $\mathbb{Z}$.

The premier question about flat sequences of polynomials is Littlewood's problem: do there exist flat sequences of polynomials with ± 1 coefficients?

While it is clear that Beck's approach cannot reach the Littlewood problem, we do wonder how close this approach can get. Can we improve Spencer's constant, perhaps by placing suitable constraints on the systems of linear forms? How far can we improve on Beck's method itself?

The method of approximation by triangles has to stop at third roots of unity. We are led to wonder whether there may be some other approximation technique, different from Beck's, that would allow us to connect Kahane's result to Littlewood's question.

Bibliography

[1] N. Alon, J. H. Spencer, and P. Erdös, *The Probabilistic Method*, Wiley-Interscience [John Wiley & Sons], New York, 1992.

[2] D. H. Bailey and R. E. Crandall, *Random generators and normal numbers*, Experimental Mathematics **11** (2002), no. 4, 527–546.

[3] V. Becher and S. Figueira, *An Example of a Computable Absolutely Normal Number*, Theoretical Computer Science **270** (2002), 947–958.

[4] J. Beck, *Flat polynomials on the unit circle –note on a problem of Littlewood*, Bulletin of the London Mathmatical Society **23** (1991), no. 3, 269–277.

[5] A. Belshaw, *On the Normality of Numbers*, Simon Fraser University, 2005. M.Sc. thesis.

[6] A. Belshaw and P. Borwein, *Champernowne's Number, Strong Normality, and the X Chromosome*, Computational and Analytical Mathematics (Simon Fraser University, 2011), Springer Proceedings in Mathematics & Statistics, vol. 50, Springer, New York, 2013, pp. 29–44.

[7] L. Berggren, J. Borwein, and P. Borwein, *Pi: a source book*, 3rd ed., Springer-Verlag, New York, 2004.

[8] W. A. Beyer, N. Metropolis, and J. R. Neergaard, *Statistical study of digits of some square roots of integers in various bases*, Math. Comp. **24** (1970), 455–473.

[9] P. Billingsley, *Probability and Measure*, Wiley-Interscience [John Wiley & Sons], New York, 1979.

[10] É. Borel, *Les probabilités dénombrables et leurs applications arithmétiques*, Supplemento ai rendiconti del Circolo Matematico di Palermo **27** (1909), 247-271.

[11] É. Borel, *Sur les chiffres décimaux de* $\sqrt{2}$ *et divers problèmes de probabilités en chaîne*, C. R. Acad. Sci. Paris **230** (1950), 591–593.

[12] J. Borwein and D. Bailey, *Mathematics by Experiment*, A K Peters Ltd., Natick, MA, 2004.

[13] P. Borwein, *Computational Excursions in Analysis and Number Theory*, Springer-Verlag, New York, 2002.

[14] D. G. Champernowne, *The Construction of Decimals Normal in the Scale of Ten*, Journal of the London Mathematical Society **3** (1933), 254–260.

[15] K. L. Chung, *Markov Chains with Stationary Transition Probabilities*, Third edition, Springer-Verlag, New York, 1967.

[16] Y. Dodge and G. Melfi, *On the reliability of random number generators.* http://pictor.math.uqam.ca/ plouffe/articles/reliability.pdf.

[17] T. Erdélyi, *Polynomials with Littlewood-type Coefficient Constraints*, Approximation theory, X (St. Louis, MO, 2001), Innov. Appl. Math., Vanderbilt Univ. Press, Nashville, TN, 2002, pp. 153–196.

[18] W. Feller, *An Introduction to Probability Theory and its Applications. Vol. I*, Third edition, John Wiley & Sons, New York, 1968.

[19] J.-P. Kahane, *Sur les polynômes à coefficients unimodulaires*, Bulletin of the London Mathematical Society **12** (1980), no. 5, 321-342.

[20] Y. Kanada, *Vectorization of Multiple-Precision Arithmetic Program and 201,326,395 Decimal Digits of π Calculation*, Supercomputing 88 **II, Science and Applications** (1988).

[21] D. Kleitman, *On a Combinatorial Conjecture of Erdös*, Journal of Combinatorial Theory (1966), 209-214.

[22] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley-Interscience [John Wiley & Sons], New York, 1974. Pure and Applied Mathematics.

[23] R. G. Laha and V. K. Rohatgi, *Probability Theory*, John Wiley & Sons, New York, 1979.

[24] R. S. Lehman, *On Liouville's function*, Mathematics of Computation **14** (1960), 411–320.

[25] M. Levin, *On the Discrepancy Estimates of Normal Numbers*, Acta Arithmetica **88(2)** (1999), 99–111.

[26] J.E. Littlewood, *Some Problems in Real and Complex Analysis*, D. C. Heath and Co., Lexington, MA, 1968.

[27] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences II. The Champernowne, Rudin-Shapiro, and Thue-Morse sequences, a further construction*, Journal of Number Theory **73** (1998), 256-276.

[28] I. Niven, *Irrational numbers*, The Carus Mathematical Monographs, No. 11, The Mathematical Association of America. Distributed by John Wiley and Sons, Inc., New York, N.Y., 1956.

[29] ———, *Uniform distribution of sequences of integers*, Compositio Math. **16** (1964), 158–160.

[30] ———, *Uniform distribution of sequences of integers*, Trans. Amer. Math. Soc. **98** (1961), 52–61.

[31] I. Niven and H. S. Zuckerman, *On the definition of normal numbers*, Pacific Journal of Mathematics **1** (1951), 103-109.

[32] K. G. Paterson and V. Tarokh, *On the existence and construction of good codes with low peak-to-average power ratios*, IEEE Trans. Inform. Theory **46** (2000), no. 6, 1974–1987.

[33] S.S. Pillai, *On Normal Numbers*, Proceedings of the Indian Academy of Sciences (Series A) **12** (1940), 179-184.

[34] W. Sierpiński, *Démonstration Élémentaire du Théorème de M. Borel sur les Nombres Absolument Normaux et Déteermination Effective d'un Tel Nombre*, Bulletin de la Société Mathématique de France **45** (1917), 125–132.

[35] J. Spencer, *Six Standard Deviations Suffice*, Transactions of the American Mathematical Society **289** (1985), no. 2, 679–706.

[36] ———, *Sequences with Small Discrepancy Relative to n Events*, Compositio Math. **47** (1982), 365–392.

[37] H. Queffelec and B. Saffari, *On Bernstein's Inequality and Kahane's Ultraflat Polynomials*, J. Fourier Anal. Appl. **2** (1996), 519–582.

[38] C. L. Vanden Eynden, *On the Uniform Distribution of Sequences of Integers*, University of Oregon, 1982. Ph.D. dissertation.

[39] *UCSC Genome Browser.*
http://hgdownload.cse.ucsc.edu/goldenPath/hg19/chromosomes/.

[40] D. D. Wall, *Normal Numbers*, Berkeley, 1949. Ph.D. thesis.