On the Erdős-Turán Conjecture and Related Results

by

Yao Xiao

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2011

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

The Erdős-Turán Conjecture, posed in 1941 in [10], states that if a subset B of natural numbers is such that every positive integer n can be written as the sum of a bounded number of terms from B, then the number of such representations must be unbounded as n tends to infinity. To put it in more precise terms, if $r_{B,h}(n)$ denotes the number of ways that the positive integer n can be written as a sum of h elements of B, then the Erdős-Turán Conjecture states that $\limsup_{n\to\infty} r_{B,h}(n) = \infty$. The origin of this conjecture can be traced back to Sidon [22][1], who asked whether there exist additive bases such that $r_{B,h}(n) = n^{o(1)}$. The case for $h = 2$ was given a positive answer by Erdős in 1956 [6], who proved the existence of additive bases B and positive numbers c_1, c_2 such that $c_1 \log(n) \leq r_{B,2}(n) \leq c_2 \log(n)$. The case for arbitrary h was given by Erdős and Tetali [9] in 1990. Both of these proofs use the probabilistic method, and so the result only shows the existence of such bases but such bases are not given explicitly. I. Ruzsa used the probabilistic method to prove a partial converse to the Erdős-Fuchs Theorem, which is to say that there exists there a subset $A \subset \mathbb{N}$, not necessarily a basis, such that $\sum_{n\leq N} r_{A,2}(n) = cN + O(N^{1/4}\log(N))$ for some positive constant $c > 0$. Kolountzakis [17] gave an effective algorithm that is polynomial with respect to the digits of n to compute such bases. We will discuss these results in the following work.

Erdős, following his 1956 result, strengthened his conjecture to the following form: if B is an additve basis for the natural numbers, then $\limsup_{n\to\infty} r_{B,h}(n)/\log(n) > 0$. Essentially, he conjectured that the thin bases he constructed are as thin as possible in general. Dirac [3] showed that $r_{B,2}(n)$ is eventually non-constant, while Borwein, Choi, and Chu [2] showed that $r_{B,2}(n)$ cannot be bounded by 7. More importantly, Borwein, Choi, and Chu have shown that the Erdős-Turán conjecture is true if certain classes of polynomials are finite sets. The Erdős-Turán conjecture is known to be true for multiplicative bases, and known to be false if we consider additive bases for all of the integers rather than the natural numbers. In particular, Nathanson [19] proved the following striking result: if $f(n)$ is any arithmetic function, then there exists for all positive integers $h > 1$ an additive basis B such that $r_{B,h}(n) = f(n)$ for all $n \in \mathbb{Z}$.

Certainly, a main ingredient of a proof of the Erdős-Turán conjecture would be to decompose a given basis into 'nice' parts, each of which we can deduce that the conjecture holds. More specifically, if it can be shown that each additive basis can be decomposed into a part that approximates an arithmetic progression (for example, containing arbitrarily long arithmetic progressions) and another that is uniform (similar to a random set), then in each case we have known results that will establish the conjecture for that part. Thus it is natural to ask if it is possible to extract a thin basis from a given basis. The first non-trivial result along this direction was given by Wirsing [26], and we will discuss Van Vu's [24] proof that the Waring bases contain thin subbases.

Acknowledgements

First and foremost, I would like to thank my supervisor, Professor Cameron Stewart, for his insightful suggestions and for bringing to my attention to various results that were subsequently included in this thesis. I would like to thank Camellia Chung, Gloria Mak, and Nicole Ngai for their help pointing out grammatical and spelling issues. Lastly, I would like to thank the Pure Mathematics Department at the University of Waterloo for providing me with support during the writing of this thesis.

Dedication

This is dedicated to my parents and my girlfriend, Camellia, whose patience with me was necessary for the completion of this thesis.

Table of Contents

Chapter 1

Introduction

A central question in additive number theory is the following: Given an infinite subset $B \subset \mathbb{N}$, can we write every element of $\mathbb{N}$ as a sum of a bounded number of elements in B? The first non-trivial result obtained in this topic is Lagrange's Theorem that every natural number can be written as the sum of four squares (and not all positive integers can be written as the sum of three squares or less). Hilbert proved that for every positive integer k, every element of $\mathbb{N}$ can be written as a bounded sum of kth powers. I.M. Vinogradov proved that every sufficiently large odd positive integer can be written as the sum of three primes. The infamous Goldbach Conjecture is equivalent to the assertion that every positive integer greater than one can be written as the sum of at most three primes.

Instead of considering a fixed and somewhat well-known set such as the squares, higher integer powers, the polygonal numbers, and the primes, we are concerned with a general set. Here we provide some definitions.

Definition 1.0.1. Let $B \subset \mathbb{N}$ be an infinite subset of the natural numbers and let $h \geq 2$ be a positive integer. Define $r_{B,h}(n) = \#\{(a_1, \cdots, a_h) \in B^h | a_1 + \cdots + a_h = n\}$. We say that B is an *additive basis of order h* if there exists $N \in \mathbb{N}$ such that for all $n \geq N$, $r_{B,h}(n) > 0$.

The function $r_{B,h}(n)$ counts the number of ways (order matters) that n can be represented as a sum of h elements of B. Usually we make the convention of assuming $0 \in B$, so that if B is an additive basis of order $g < h$, then it is also an additive basis of order h. In many proofs that a given set of natural numbers is an additive basis of finite order, one does not show that $r_{B,h}(n) \geq 1$ but instead proves the much more powerful statement that there exists a function f with $\lim_{n\to\infty} f(n) = \infty$ such that $r_{B,h}(n) \gg f(n)$. In particular, in many cases it is not known how to prove that $r_{B,h}(n) > 0$ without showing that $r_{B,h}(n)$ tends to infinity.

This compels an interesting problem, which is the main discussion of this paper. Following the paradigm above, it seems that it is impossible to show that $r_{B,h}(n) > 0$ for all sufficiently large n without $r_{B,h}(n)$ being unbounded as a function of n. Indeed, Erdős and Turán conjectured the following in 1941 [10]:

Conjecture 1.0.2. *(Erdős and Turán) If B is an additive basis of order h, then* $\limsup_{n\to\infty} r_{B,h}(n) = \infty$.

The language used above is modern and not precisely the same as in the original paper. It is noted that Erdős and Turán remarked that "we may mention that the corresponding result for $g(n)$, the number of representations of n as $a_i a_j$, can be proved." [10]. This latter result was proved by Erdős in 1938.

In the original paper of Erdős and Turán in 1941, they proved some estimates on how many terms a *Sidon sequence* can have up to n. A Sidon sequence is a sequence $A = \{a_1, a_2, \cdots\} \subset \mathbb{N}_0$ such that each $n \in \mathbb{N}$ can only be written as a sum of two elements of A in at most one way. In other words, $r_{A,2}(n) \leq 1$ for all $n \geq 1$. See for example [21] for some recent advances on studying Sidon sets.

Indeed, the Erdős-Turán conjecture is motivated by a question posed by Sidon in the 1930's, due to the importance of Sidon sequences in Fourier analysis. If $b_1 + b_2 = n$, then $b_1, b_2 \leq n$ so that

$$n \leq \sum_{j\leq n} r_{B,2}(j) \leq |B \cap [1,n]|^2. \tag{1.0.1}$$

Sidon asked whether or not one can find additive bases of order 2 of "good quality". Specifically those bases such that $|B \cap [1,n]| = n^{1/2+o(1)}$, which means that B is nearly as 'thin' as possible by equation (1.0.1). If $r_{B,2}(n) = O(\log n)$, then equation (1.0.1) is surely satisfied, so we would have a 'thin' basis. This question was answered positively by Erdős in 1956, and together with Tetali in 1990 generalized to account for additive bases of arbitrary order $h > 2$. We will discuss these results in sections 2 and 3. The existence of thin bases of all orders motivated Erdős to strengthen his conjecture to the following:

Conjecture 1.0.3. *(Erdős) Let B be an additive basis of order h. Then* $\limsup_{n\to\infty} \dfrac{r_{B,h}(n)}{\log(n)} > 0$.

Erdős's proof of the existence of a thin basis in the sense noted above, done in [6], is probabilistic, and no explicit example has ever been found.

An easier problem is to examine the 'average' of $r_{B,h}(n)$ when summed over the first N integers for some additive basis B. In other words, we examine the sum

$$\sum_{n\leq N} r_{B,h}(n).$$

If the Erdős-Turán conjecture is true, then this sum should not be too regular; meaning that $\sum_{j\leq n} r_{B,h}(j)$ should not be too similar to cn for some positive number c. To this end, Erdős and Fuchs proved in [8] the following result:

Theorem 1.0.4. (Erdős-Fuchs Theorem) *Let $B \subset \mathbb{N}$ be an infinite subset. Then*

$$\sum_{j \leq n} r_{B,2}(n) = cn + o(n^{1/4} \log^{-1/2}(n))$$

cannot hold for any constant $c > 0$.

Unfortunately, this result is far from being able to settle the Erdős-Turán conjecture, since a slightly larger error term is allowed. This was proven by I. Ruzsa in [20]. Ruzsa gave a square-like random set such that the sum $\sum_{j \leq n} r_{B,h}(j) = cn + O(n^{1/4} \log n)$. We will give Ruzsa's result in chapter 2.

As is suggested by the Erdős conjecture, bases where $r_{B,h}(n) = O(\log n)$ and $r_{B,h}(n) > c \log n$ infinitely often are essentially as thin as possible. A natural question along these lines is to ask whether 'thicker' bases that cannot be any thinner exist. That is, if B is an additive basis, is it always possible to find a subset C of B such that C is an additive basis, and $r_{C,h}(n) = O(\log n)$. In other words, can every additive basis B such that $r_{B,h}(n)$ is large infinitely often be reduced to a thin basis. The general problem is not yet resolved. However, in [26] Wirsing proves that the primes contains a thin sub-basis of any order, and in [25] Van Vu showed that the Waring bases (set of kth powers) contain thin sub-bases of all sufficiently large orders. Vu's approach uses the probabilistic method of Erdős and the Hardy-Littlewood Circle Method. We will examine this result in chapter 4 of this paper.

Lastly, the most definitive and concrete approach to the Erdős-Turán Conjecture is computational. Kolountzakis gave in [17] a fast algorithm to compute an Erdős base, in the sense that at the nth iteration the algorithm generates a set E_n in polynomial time with respect to the number of digits of n, and such that as $n \to \infty$, E_n tends towards a thin additive basis in the Erdős sense with probability 1. Borwein, Choi, and Chu in [2] used a computational approach to prove that if B is an additive basis of order 2, then $r_{B,2}(n)$ cannot be bounded by 7. We will discuss these results in chapter 5.

Chapter 2

The Probabilistic Method - Part I

In this chapter we will discuss the probabilistic method, with the intention of applying it to prove Erdős's 1956 theorem [6], which asserts that thin bases of order 2 exist. We will also use the techniques developed in this section to prove Ruzsa's theorem [20]. In this first section, the main result will be Chernoff's Inequality. Chernoff's Inequality applies when one can decompose a random variable into a sum of independent indicator random variables, as we will see in both Erdős's theorem and Ruzsa's theorem. It fails when one cannot decompose a random variable as such; and a more powerful tool is needed to resolve such cases. This will be discussed in the next section in the context of the Erdős-Tetalli theorem [8].

2.1 Basics and preliminaries

The probabilistic method is based on a very simple idea. If we wish to prove that a certain object B exists with property P, then it suffices to show that in some suitably defined probability space (definition 2.1.2) the event "B has property P" occurs with positive probability. This method was first introduced by Paul Erdős in 1947 when he proved the existence of a graph with a certain Ramsey property without constructing it. Since then, Erdős has proven many significant results in finite mathematics by employing the probabilistic method. In this first subsection we give some of the basic ideas, results, and techniques used in the probabilistic method. Of course, what we cover here is far from complete. The interested reader is recommended to consult [1].

We begin with some definitions and results from elementary probability theory and number theory. We will only give definitions and results that we need for the rest of this paper, and not give statements in their full generality. The interested reader is referred to [13] for a more thorough and comprehensive treatement.

Definition 2.1.1. *(asymptotic notations)* Let Θ, O, o be defined as follows: Given two functions $f, g : \mathbb{R} \to \mathbb{R}^+$, we say that $g = O(f)$ if there exists some $C > 0$ such that $g(x) \leq Cf(x)$ for all x, that $g = o(f)$ if $\lim_{x\to\infty} \frac{g(x)}{f(x)} = 0$, that $g = \Omega(f)$ if there exists a constant $C > 0$ such that $g(x) \geq cf(x)$ for all sufficiently large x, and

$g = \Theta(f(x))$ if there exist constants $c_1, c_2 > 0$ such that $c_1 f(x) \leq g(x) \leq c_2 f(x)$ for all x.

Definition 2.1.2. Let Ω be a non-empty set. We say $\mathcal{F} \subset \mathcal{P}(\Omega)$, where $\mathcal{P}(\Omega)$ is the power set of Ω, is a σ- *algebra* over Ω if $\mathcal{F}$ satisfies the following:

(i) $\emptyset, \Omega \in \mathcal{F}$;
(ii) If $A \in \mathcal{F}$, then the complement of A in Ω is also in $\mathcal{F}$; and
(iii) If $A_1, A_2, \cdots$, is a countable collection of sets in Ω, then $\bigcup_{n=1}^{\infty} A_n \in \mathcal{F}$.

Together we say that the pair $(\Omega, \mathcal{F})$ is a *measureable space*. We say that $\mu : \mathcal{F} \to \mathbb{R}^+$ is a *measure* on $(\Omega, \mathcal{F})$ (or if the σ-algebra $\mathcal{F}$ is understood, simply Ω) if μ satisfies the following:

(i) $\mu(\emptyset) = 0$;
(ii) If $A_1, A_2, \cdots$ are pairwise disjoint subsets of Ω, then $\mu\left(\bigcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty} \mu(A_n)$.

If in addition $\mu(\Omega) = 1$, we say that μ is a *probability measure*. Generally, the space $(\Omega, \mathcal{F}, \mu)$ is a *measure space*, if $\mu = \mathbb{P}$ is a probability measure, then $(\Omega, \mathcal{F}, \mathbb{P})$ is a *probability space*. In this case we call Ω the *sample space* and $\mathcal{F}$ the *event space*.

We will not need the full strength and generality of the above definition in this paper. Indeed, usually Ω will be the set of non-negative integers, $\mathcal{F}$ will be the power-set of Ω. For more details about measure spaces, please refer to [11].

Definition 2.1.3. Let $X : \Omega \to \mathbb{R}$ be a function. We say that X is a (real-valued) *random variable* if $\{\omega : X(\omega) \leq r\} \in \mathcal{F}$ for all $r \in \mathbb{R}$. We say that X is a *discrete* random variable if the range of X is the integers. We say that X is an *indicator* random variable if $X(B) = 1$ for some $B \in \mathcal{F}$, and $X = 0$ otherwise.

Indeed, one can show that a random variable is the same idea as a measureable function on $\mathcal{F}$. Also, we usually denote indicator random variables as $\mathbb{I}$ to separate from the typical random variable.

We now define some central objects in probability, which will be used frequently in this paper.

Definition 2.1.4. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and X be a random variable. Define its *expectation* to be the quantity

$$\mathbb{E}X = \int_{\Omega} X d\mathbb{P}.$$

If $\mathbb{E}|X| < \infty$, we say that X has *finite first moment*, and say that $\mathbb{E}X$ is the *first moment*. Analogously we say X has *finite nth moment* if $\mathbb{E}|X^n| < \infty$, and the nth moment is $\mathbb{E}X^n$.

Definition 2.1.5. Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space and let X be a random variable. Define the *variance* of X to be

$$\mathbf{Var}(X) = \mathbb{E}[(X - \mathbb{E}X)^2] = \mathbb{E}[X^2] - \mathbb{E}[X]^2.$$

Let $\sigma = \sqrt{\mathbf{Var}(X)}$ be the *standard deviation* of X.

It is clear from the definition above that regardless of how a (finite) set of random variables $X_1, \cdots, X_n$ are related, by the linearity of the integral, we must have $\mathbb{E}[X_1 + \cdots + X_n] = \mathbb{E}X_1 + \cdots + \mathbb{E}X_n$. This is not so for higher order moments. Indeed the concept of *independence* must be introduced. According to Gerald Folland [11], the idea of independence is truly unique to the field of probability and has no analogue in analysis. Thus we will give a definition of independence below and discuss some immediate consequences.

Definition 2.1.6. Suppose $F_1, \cdots, F_n \in \mathcal{F}$ are a set of events. Let F be the event that $F_1, \cdots, F_n$ all happen. We say that the events $F_1, \cdots, F_n$ are *jointly independent* if

$$\mathbb{P}(F) = \mathbb{P}(F_1) \cdots \mathbb{P}(F_n).$$

Let $F_{i,j}$ be the event that both F_i, F_j happen. If for all $i \neq j$, $1 \leq i, j \leq n$ we have $\mathbb{P}(F_{i,j}) = \mathbb{P}(F_i)\mathbb{P}(F_j)$, then $F_1, \cdots, F_n$ are said to be *pairwise independent*.

Definition 2.1.7. Let $X_1, \cdots, X_n$ be a set of real-valued random variables. Then $X_1, \cdots, X_n$ are said to be *jointly independent* if the events $F_1 = \{\omega : X_1(\omega) \leq a_1\}, F_2 = \{\omega : X_2(\omega) \leq a_2\}, \cdots, F_n = \{\omega : X_n(\omega) \leq a_n\}$ are jointly independent for all $(a_1, \cdots, a_n) \in \mathbb{R}^n$. Pairwise independence is defined analogously.

Note that joint independence implies pairwise independence, but not conversely (page 13 in [13]). A principal component of our investigations in the following two sections will rely on the concept of independence. In most cases below we will obtain our desired result by showing that a given random variable X will be near its expectation with high probability. To do this, we will attempt to decompose our random variable X into a sum of independent random variables. The idea is that a sum of independent random variables will be tightly concentrated to its mean because it is difficult for independent random variables to 'work together' to significantly deviate from the mean. This is not always possible; as we will see in section 3. In such cases when it is not possible we will have to settle with decomposing X into a sum of random variables that are only 'weakly' related. To measure such a relation, we will need the following definition:

Definition 2.1.8. Let X_1, X_2 be real-valued random variables. Define their *covariance* by

$$\mathbf{Cov}(X_1, X_2) = \mathbb{E}[(X_1 - \mathbb{E}X_1)(X_2 - \mathbb{E}X_2)].$$

An immediate observation of the above definition is that if X_1, X_2 are independent, then $\mathbf{Cov}(X_1, X_2) = 0$. Thus, covariance gives a way to measure how the random

variables X_1, X_2 are related. Note also that if $X_1, \cdots, X_n$ are random variables, then we have for $X = X_1 + \cdots + X_n$, the equation

$$\mathbf{Var}(X) = \sum_{j=1}^{n} \mathbf{Var}(X_j) + \sum_{i \neq j} \mathbf{Cov}(X_i, X_j).$$

In particular, we see that *pairwise independence* is the crucial idea when one desires linearity of the second moment. As we will see, however, pairwise independence is not a sufficiently strong notion to carry on with our results.

We will concern ourselves for the rest of this subsection with various probabilistic methods involving these concepts. In the subsection below and for the rest of the paper, we will not explicitly define our probability space $(\Omega, \mathcal{F}, \mathbb{P})$, as that level of precision is unnecessary. Indeed, issues such as measureability will not come up because we are working with discrete random variables.

The first method we discuss is known as the *First Moment Method* [1][22] and is based on the following simple but extremely useful observation: If $X_1, \cdots, X_n$ are any random variables in some probability space and $c_1, \cdots, c_n$ any scalars, then the expected value is linear, namely if we set $X = c_1X_1 + \cdots c_nX_n$, then

$$\mathbb{E}X = c_1\mathbb{E}X_1 + c_2\mathbb{E}X_2 + \cdots c_n\mathbb{E}X_n$$

The power of this observation lies in the fact that linearity of expectation does not depend on the random variables $X_1, \cdots, X_n$ being independent. In applications, frequently we want to consider some sets we are interested in with some random structure which allow us to express it as some random variable. Then we carefully decompose this random variable into simple random variables, usually indicator variables, and apply linearity of expectation to obtain a specific point in the probability space X such that $X \geq \mathbb{E}X$ or $X \leq \mathbb{E}X$, depending on the question being asked. We demonstrate this technique with a simple example given by Erdős in [7].

Example 2.1.9. Suppose that A is a finite set of non-zero integers. Then there exists a subset B of A such that $|B| > |A|/3$ and such that B is *sum-free*, that is there do not exist three elements x, y, z in B such that $x + y = z$.

Proof. Since A is finite and does not contain zero, there exists a large prime p of the form $p = 3k + 2$ (that such primes exist follows from Dirichlet's Theorem) such that $A \subset [-p/3, p/3] \backslash \{0\}$. Now we can view A as a subset of $G = \mathbb{Z}/p\mathbb{Z}$ instead. If $x, y \in A$ are such that $x + y \in A$, then it does not matter whether one views $x + y$ as an integer or as an element of G. Hence B is sum-free in A in the sense of the integers if and only if B is sum-free in G. Note that the interval $[k+1, 2k+1] = \{k+1, k+2, \cdots, 2k+1\}$ is sum-free in G.

Now choose an element $g \in G \setminus \{0\}$ such that each element in $G \setminus \{0\}$ has an equal probability of being chosen, and form the random set

$$B = \{a \in A : g^{-1}a \in \{k+1, \cdots, 2k+1\}\}.$$

Now it is clear that $g[k+1, 2k+1] = \{g(k+1), g(k+2), \cdots, g(2k+1)\}$ is sum-free in G since $[k+1, 2k+1]$ is. But $B = A \cap (g[k+1, 2k+1])$ and hence B is also sum-free. Now $|B|$ is a random variable taking on values in integers from 0 to k, so it suffices to show that the expectation of $|B|$ is greater than $\frac{|A|}{3}$. By the linearity of expectation, we have

$$\mathbb{E}|B| = \sum_{a \in A} \mathbb{P}(a \in B) = \sum_{a \in A} \mathbb{P}(g^{-1}a \in [k+1, 2k+1]).$$

By the definition of A, we know that for all $a \in A$, a is an invertible element of G, and so since g is uniformly distributed in $G \setminus \{0\}$ we have that $g^{-1}a$ is also uniformly distributed in $G \setminus \{0\}$. Now note that $|[k+1, 2k+1]| = k+1 > \frac{3k+2-1}{3} = \frac{(p-1)}{3}$, so that for all $a \in A$, we have

$$\mathbb{P}(g^{-1}a \in [k+1, 2k+1]) = \frac{k+1}{3k+1} > \frac{1}{3}.$$

This implies that

$$\mathbb{E}|B| = \sum_{a \in A} \mathbb{P}(x^{-1}a \in [k+1, 2k+1]) > \sum_{a \in A} \frac{1}{3} = \frac{|A|}{3}.$$

Hence there exists a specific point B in our probability space that satisfies $|B| > |A|/3$, and we are done.

□

We now introduce another simple yet profoundly powerful tool that arose from measure theory, that of the *Borel-Cantelli Lemma*. In probabilistic terms, the lemma can be stated as:

Theorem 2.1.10. *(Borel-Cantelli Lemma): Let $A_1, A_2, \cdots$ be a sequence of events, possibly dependent, such that $\sum_{n=1}^{\infty} \mathbb{P}(A_n) < \infty$. Define*

$$A = \bigcap_{n=1}^{\infty} \bigcup_{m=n}^{\infty} A_m.$$

Then $\mathbb{P}(A) = 0$.

Proof. Aforementioned this is a result that arose from measure theory, and is proved as such. The events $A_1, A_2, \cdots$ are simply sets of elements in some sample space, and it is clear that $A \subset \bigcup_{m=n}^{\infty} A_m$ for all $n \geq 1$. By the subadditivity of the probability measure, it follows that $\mathbb{P}(A) \leq \sum_{m=n}^{\infty} \mathbb{P}(A_m)$. Since $\sum_{n=1}^{\infty} \mathbb{P}(A_n) < \infty$ it follows that $\lim_{n \to \infty} \sum_{m=n}^{\infty} \mathbb{P}(A_m) = 0$, and hence $\mathbb{P}(A) = 0$ as desired. □

This result essentially says the following: if a sequence of events $A_1, A_2, \cdots$, possibly dependent, are such that $\sum_{n=1}^{\infty} \mathbb{P}(A_n) < \infty$, then with probability 1 at most finitely many of these events occur. This is very powerful and will be used in the next two chapters to establish the existence of thin additive bases of the natural numbers. Indeed in applications we want to say that a random set B satisfies a certain property by proving that the sum of the probabilities of 'bad events' that B does not satisfy the given property is finite. Unfortunately, this result does not give insight into the probability of finitely many bad events occurring and only through careful analysis of the specific problem does one obtain good estimates.

Our next technique is called, unsurprisingly, the *Second Moment Method*. As the title suggests the second moment method uses information on the variance of a random variable to obtain better estimates. The main tool in the second moment method is the Chebyshev Inequality, which we state here and provide a short proof.

Theorem 2.1.11. *(Chebyshev's Inequality) Let X be a real valued random variable. For any $\lambda > 0$ we have the inequality*

$$\mathbb{P}(|X - \mathbb{E}X| > \lambda \mathbf{Var}(X)^{1/2}) \leq \frac{1}{\lambda^2}.$$

Proof. We have the trivial inequality $X \geq \lambda \mathbb{I}(X \geq \lambda)$, where $\mathbb{I}$ is the indicator function. Taking expectation of both sides yields $\mathbb{E}X \geq \lambda \mathbb{P}(X \geq \lambda)$ and re-arranging yields

$$\mathbb{P}(X \geq \lambda) \leq \frac{\mathbb{E}X}{\lambda}. \tag{2.1.1}$$

This inequality is known as Markov's Inequality.

Now suppose that $\mathbf{Var}(X) = 0$. By the definition of variance, this is equivalent to $\mathbb{E}(X - \mathbb{E}X)^2 = 0$. Since X is a real-valued random variable, this implies that $\mathbb{P}(X \neq \mathbb{E}X) = 0$, so that $\mathbb{P}(|X - \mathbb{E}X| > \lambda \mathbf{Var}(X)^{1/2}) = \mathbb{P}(|X - \mathbb{E}X| > 0) = 0$ which is surely less than $\frac{1}{\lambda^2}$ for any $\lambda > 0$. Hence we suppose that $\mathbf{Var}(X) > 0$. From inequality (2.1.1), we obtain

$$\mathbb{P}(|X - \mathbb{E}X| > \lambda \mathbf{Var}(X)^{1/2}) = \mathbb{P}(|X - \mathbb{E}X|^2 > \lambda^2 \mathbf{Var}(X)) \leq \frac{\mathbb{E}|X - \mathbb{E}X|^2}{\lambda^2 \mathbf{Var}(X)} = \frac{1}{\lambda^2}.$$

This is what we wished to prove. □

The second moment allows us to control the expected value of a desired quantity in a stronger way, since the upper bound is stronger than if we only considered the expected value. However, we no longer have linearity unless we assume the (rather strong) condition of independence. That is, $\mathbf{Var}(X_1 + \cdots + X_n) = \mathbf{Var}(X_1) + \cdots + \mathbf{Var}(X_n)$ only when the random variables $X_1, \cdots, X_n$ are independent. We give a famous example, a theorem originally produced by Hardy and Ramanujan, given by Turán in 1934 [23].

Example 2.1.12. Let $\omega(n)$ denote the number of distinct prime divisors of n. Let $f : \mathbb{N} \to \mathbb{N}$ be an arithmetic function that tends to infinity. Then the number of integers x satisfying $1 \leq x \leq n$ and $|\omega(x) - \log\log(x)| > f(n)\sqrt{\log\log(n)}$ is $o(n)$.

Proof. Let $n \in \mathbb{N}$ and define $S_n = \{x \in \{1, 2, \cdots, n\} : |\omega(x) - \log\log(x)| > f(n)\sqrt{\log\log(n)}\}$. Then our goal is to show that $|S_n| = o(n)$. Now choose x from $[1, n] = \{1, 2, \cdots, n\}$ uniformly. Then we have

$$\mathbb{P}(|\omega(x) - \log\log(x)| > f(n)\sqrt{\log\log(n)}) = \frac{|S_n|}{n}.$$

And so it suffices to show that

$$\mathbb{P}(|\omega(x) - \log\log(x)| > f(n)\sqrt{\log\log(n)}) = o(1).$$

Define $B_n(x) = \{p : p \leq n^{1/10}, p|x\}$ where p represents a prime. Since $x \leq n$, x cannot have 10 distinct prime divisors larger than $n^{1/10}$ and so $|B_n(x)| \leq \omega(x) \leq |B_n(x)|+10$. Thus it suffices to show that

$$\mathbb{P}(||B_n(x)| - \log\log(n)| \geq f(n)\sqrt{\log\log(n)}) = o(1).$$

We can replace $\mathbb{P}(||B_n(x)|-\log\log(x)| \geq f(n)\sqrt{\log\log(n)})$ with $\mathbb{P}(||B_n(x)|-\log\log(n)| \geq f(n)\sqrt{\log\log(n)})$ by the following: consider for a large n and fixed positive constant $m > 0$, the probability of picking $x \in [1, n]$ uniformly such that $\log\log(x) < \log\log(n)-m$. Since the exponential function is injective, this inequality is equivalent to $\log(x) < e^{-m}\log(n)$, which is then equivalent to $x < e^{e^{-m}\log(n)} = n^{e^{-m}}$. Since we assumed $m > 0$, we see that the probability $\mathbb{P}(\log\log(x) < \log\log(n)-m) \leq \dfrac{n^{e^{-m}}}{n}$ which tends to 0 as $n \to \infty$. That is, the probability $\mathbb{P}(\log\log(x) < \log\log(n) + O(1)) = 1 - o(1)$.

Now we obtain some estimates on $\mathbb{E}|B_n(x)|, \mathbf{Var}(|B_n(x)|)$. First notice that $|B_n(x)| = \sum_{p \leq n^{1/10}} \mathbb{I}(p|x)$ and taking expectations yields

$$\mathbb{E}|B_n(x)| = \sum_{p \leq n^{1/10}} \mathbb{P}(p|x).$$

Likewise, we can estimate the variance by (p, q denote primes)

$$\mathbf{Var}(|B_n(x)|) = \sum_{p \leq n^{1/10}} (\mathbb{P}(p|x) - \mathbb{P}(p|x)^2) - \sum_{p,q \leq n^{1/10}, p \neq q} \mathbf{Cov}(\mathbb{I}(p|x), \mathbb{I}(q|x)).$$

Now note that $\mathbb{I}(p|x)\mathbb{I}(q|x) = \mathbb{I}(pq|x)$, since p, q are distinct primes and hence coprime. But $\mathbb{P}(p|x) = \dfrac{1}{p} + O\left(\dfrac{1}{n}\right)$, and we note that we have the definition of covariance

$$\mathbf{Cov}(\mathbb{I}(p|x), \mathbb{I}(q|x)) = \mathbb{E}[(\mathbb{I}(p|x) - \mathbb{E}[\mathbb{I}(p|x)])(\mathbb{I}(q|x) - \mathbb{E}[\mathbb{I}(q|x)])]$$

And thus we get the estimate

$$\mathbf{Cov}(\mathbb{I}(p|x), \mathbb{I}(q|x)) = \frac{1}{pq} + O\left(\frac{1}{n}\right) - \left(\frac{1}{p} + O\left(\frac{1}{n}\right)\right)\left(\frac{1}{q} + O\left(\frac{1}{n}\right)\right) = O\left(\frac{1}{n}\right).$$

Hence we obtain the estimates

$$\mathbb{E}|B_n(x)| = \sum_{p \leq n^{1/10}} \frac{1}{p} + O(n^{-9/10})$$

$$\mathbf{Var}(|B_n(x)|) = \sum_{p \leq n^{1/10}} \left(\frac{1}{p} - \frac{1}{p^2}\right) + O(n^{-8/10}).$$

We now use a classic theorem of Mertens, which we do not prove, which states that $\sum_{p \leq n} \frac{1}{p} = \log\log(n) + O(1)$. Now let f be a function such that $\lim_{n \to \infty} f(n) = \infty$. By Chebyshev's Inequality, we have

$$\mathbb{P}(||B_n(x)| - \mathbb{E}|B_n(x)| > f(n)\mathbf{Var}(|B_n(x))^{1/2}) \leq \frac{1}{f(n)^2}$$

Which implies for large n

$$\mathbb{P}(||B_n(x) - \log\log(n)| \geq f(n)\sqrt{\log\log(n)}) \leq \frac{1}{f(n)^2} = o(1).$$

This finishes the proof of the example. □

A main theme with the first and second moment methods is that if one can obtain good estimates on the first and second moments of a random variable, we can often obtain non-trivial estimates on the random variable itself. Indeed, there is a method to control all moments simultaneously, and that is the topic of the next subsection; that of the *Exponential Moment Method*.

We start with the definition of the *moment generating function*, defined as $\mathbb{E}[e^{tX}]$ for some real-valued random variable X, provided that it exists. By the Law of the Unconscious Statistician [13], we have that

$$\mathbb{E}[e^{tX}] = \sum_{n=0}^{\infty} \frac{t^n \mathbb{E}[X^n]}{n!}.$$

Similar to the central role that Chebyshev's Inequality plays in the second moment method, there is an analogously important inequality in applications of the exponential moment method. This is Chernoff's Inequality. Roughly speaking, Chernoff's Inequality gives bounds that are much better than those in Chebyshev's Inequality, but requires a much stronger assumption of the joint independence of the random variables involved. In practice it is sometimes possible to massage the problem in the case when the random variables involved are not independent but interact in a weak way. We present Chernoff's Inequality and a proof.

Theorem 2.1.13. *(Chernoff's Inequality) Suppose $X_1, \cdots, X_n$ are independent real-valued random variables with finite first moment such that $|X_i - \mathbb{E}X_i| \leq 1$ for all $1 \leq i \leq n$. Set $X = X_1 + \cdots + X_n$ and let $\sigma = \sqrt{\mathbf{Var}(X)}$ be the standard deviation of X. Then for all $\lambda > 0$ we have*

$$\mathbb{P}(|X - \mathbb{E}X| \geq \lambda\sigma) \leq 2\max(e^{-\lambda^2/4}, e^{-\lambda\sigma/2}).$$

Proof. By replacing each X_i with $X_i - \mathbb{E}X_i$ we can assume that $\mathbb{E}X_i = 0$ for all $1 \leq i \leq n$. Begin with the observation that $\mathbb{P}(|X| \geq \lambda\sigma) = \mathbb{P}(X \geq \lambda\sigma) + \mathbb{P}(X \leq -\lambda\sigma)$. Replacing X with $-X$ we see that it suffices to show that $\mathbb{P}(X \geq \lambda\sigma) \leq e^{-t\lambda\sigma/2}$, where $t = \min(\lambda/2\sigma, 1)$. By the monotonicity of the exponential function and Markov's Inequality, we obtain

$$\mathbb{P}(X \geq \lambda\sigma) = \mathbb{P}(e^{tX} \geq e^{t\lambda\sigma}) \leq e^{-t\lambda\sigma}\mathbb{E}[e^{tX}] = e^{-t\lambda\sigma}\mathbb{E}[e^{tX_1} \cdots e^{tX_n}].$$

By the independence of $X_1, \cdots, X_n$ we obtain

$$\mathbb{P}(X \geq \lambda\sigma) \leq e^{-t\lambda\sigma}\mathbb{E}[e^{tX_1}]\mathbb{E}[e^{tX_2}] \cdots \mathbb{E}[e^{tX_n}].$$

For $x \in [0, 1]$, the Taylor series expansion of $f(x) = e^x$ yields that $e^x = \sum_{m=0}^{\infty} \frac{x^m}{m!} \leq 1 + x + x^2$. Apply this to the random variable tX_i, which takes values in $[0, 1]$ for $0 \leq t \leq 1$, we obtain $e^{tX_i} \leq 1 + tX_i + t^2X_i^2$. Taking expectations yields that $\mathbb{E}[e^{tX_i}] \leq 1 + t\mathbb{E}[X_i] + t^2\mathbb{E}[X_i^2]$. By the assumption of $\mathbb{E}[X_i] = 0$ we see that $\mathbb{E}[e^{tX_i}] \leq 1 + t^2\mathbf{Var}(X_i)$. Now again looking at $f(x) = e^x$ we notice the trivial inequality $1 + x \leq e^x$ for x positive, so that $1 + t^2\mathbf{Var}(X_i) \leq \exp(t^2\mathbf{Var}(X_i))$. Hence we obtain

$$\mathbb{P}(X \geq \lambda\sigma) \leq e^{-t\lambda\sigma} \exp(t^2\mathbf{Var}(X_1)) \cdots \exp(t^2\mathbf{Var}(X_n)).$$

By independence, we have that $\exp(t^2\mathbf{Var}(X_1)) \cdots \exp(t^2\mathbf{Var}(X_n)) = \exp(t^2\mathbf{Var}(X)) = e^{t^2\sigma^2}$. But since $t \leq \lambda/2\sigma$, we have that $e^{-t\lambda\sigma}e^{\sigma^2t^2} \leq e^{-\lambda^2/4}$. Thus the claim is verified. □

We will need the following corollary to Chernoff's Inequality for later use.

Corollary 2.1.14. *Suppose $X_1, X_2, \cdots, X_n$ are independent indicator random variables. Set $X = X_1 + \cdots + X_n$. Then for any $\varepsilon > 0$ we have*

$$\mathbb{P}(|X - \mathbb{E}X| \geq \varepsilon\mathbb{E}X) \leq 2\exp(-\min(\varepsilon^2/4, \varepsilon/2)\mathbb{E}X).$$

In particular, with $\varepsilon = 1/2$, we have

$$\mathbb{P}(|X - \mathbb{E}X| = \Theta(\mathbb{E}X)) \geq 1 - 2\exp(-\mathbb{E}X/16)$$

Proof. It is clear that $|X_i - \mathbb{E}X_i| \leq 1$, since X_i is an indicator random variable. Note also that $\mathbf{Var}(X_i) = \mathbb{E}X_i^2 - (\mathbb{E}X_i)^2 = \mathbb{E}X_i - (\mathbb{E}X_i)^2 \leq \mathbb{E}X_i$. Thus by independence and the linearity of expectation we have $\mathbf{Var}(X) \leq \mathbb{E}X$. Now apply Chernoff's Inequality with $\lambda = \varepsilon\mathbb{E}X/\sigma$ to obtain the result. □

We are now ready to proceed to the next section.

2.2 Thin bases of order 2

The study of additive bases in the natural numbers is classical. It began with such curious questions as which numbers can be written as the sum of two squares. It is clear that not all positive integers can be written as the sum of two squares; for example the number 11 has no such representation. This is clear: if a positive integer n can be written as $n = x^2 + y^2$ where x, y are integers, then $n \equiv 0, 1 \pmod 4$. A slightly harder problem is to determine which positive integers can be written as the sum of three squares. Again there are positive numbers that cannot be written as the sum of three squares, though these are much rarer and difficult to find than those that cannot be written as the sum of two squares. Gauss gave a complete characterization of such integers, which we give as the following theorem. For a proof, see [19].

Theorem 2.2.1. (Gauss) *A positive integer N can be represented as the sum of three squares if and only if N is not of the form*

$$N = 4^a(8k + 7).$$

It is striking then that Lagrange proved that in fact every positive integers can be written as the sum of at most four squares (or exactly four squares if one allows 0 in the sum). This is considered the first major result in additive number theory.

In modern notation, Lagrange's Theorem is equivalent to the following: Let $B = \{n^2 : n \in \mathbb{N}\}$, then $r_{B,4}(n) > 0$ for all $n \in \mathbb{N}$. In other words, B is an additive basis of order 4 (it is in fact a basis). Theorem 2.2.1 show that B is not a basis of any smaller order. Consider the elementary estimate

$$\sum_{j \le n} 1 \le \sum_{j \le n} r_{B,4}(j) \le |B \cap [1, n]|^4 \le \sum_{j \le 4n} r_{B,4}(j).$$

This gives a lower bound on the size of $|B \cap [1, n]|$, which is $n^{1/4}$. We know that this is a rather poor estimate; since we know that $|B \cap [1, n]| \sim n^{1/2}$. In other words the set of squares is a 'thick' basis because it contains many more elements than the lower bound would suggest. In the 1930s, Sidon asked the question of whether there exist 'thin' bases that come arbitrarily close to the lower bound. In other words, bases B of order h such that $|B \cap [1, n]| = n^{1/h+o(1)}$. This question was first answered by Erdős in 1954 with the paper [5]. Soon after in 1956, Erdős would produce a refinement of this result [7], which is the main subject of this section.

Theorem 2.2.2. *(Erdős 1956) There exist a subset $B \subset \mathbb{N}$ and positive constants c_1, c_2 such that for all sufficiently large $n \in \mathbb{N}$, $c_1 \log(n) \le r_{B,2}(n) \le c_2 \log(n)$.*

Notice that this theorem implies that $|B \cap [1, n]| = \Theta(n^{1/2} \log^{1/2}(n))$, which is certainly equal to $n^{1/2+o(1)}$ and so such a basis is thin in Sidon's sense.

To prove this theorem we will need a fairly elementary but powerful tool in analytic number theory, that of partial summation. We give it as a proposition.

Proposition 2.2.3. *(Partial Summation) Let $f, g : \mathbb{R} \to \mathbb{R}$ be two functions such that f is differentiable. Define $A(x) = \sum_{n \leq x} g(n)$. Then*

$$\sum_{n \leq x} f(n)g(n) = f(x)\sum_{n \leq x} g(n) - \int_1^x f'(t)A(t)dt.$$

Proof. We have

$$\begin{aligned}
\sum_{n \leq x} f(n)g(n) &= \sum_{n \leq x} f(n)[A(n) - A(n-1)] \\
&= f(\lfloor x \rfloor)A(x) - \sum_{n \leq x-1} A(n)(f(n+1) - f(n)) \\
&= f(\lfloor x \rfloor)A(x) - \sum_{n \leq x-1} A(n)\int_n^{n+1} f'(t)dt \\
&= f(\lfloor x \rfloor)A(x) - \int_1^{\lfloor x \rfloor} A(t)f'(t)dt
\end{aligned}$$

We are done if x is a positive integer. But we can consider the general case by setting $\lfloor x \rfloor = N$, so that $A(t) = A(N)$ for $N \leq t \leq x$, and note that

$$\int_N^x A(t)f'(t)dt = A(x)[f(x) - f(\lfloor x \rfloor)) = A(x)f(x) - f(\lfloor x \rfloor)A(x)$$

Which implies that

$$\begin{aligned}
f(\lfloor x \rfloor)A(x) - \int_1^N A(t)g'(t)dt &= f(x)A(x) - \int_N^x A(t)f'(t)dt - \int_1^N f'(t)A(t)dt \\
&= f(x)A(x) - \int_1^x A(t)f'(t)dt.
\end{aligned}$$

This proves the required result. □

Now we can begin the proof of Erdős's theorem in earnest.

Proof. (*Erdős's Theorem*) Define the random set B by the following: for each $x \in \mathbb{N}$, we have $\mathbb{P}(x \in B) = p_x = \min\left\{10\sqrt{\frac{\log(x)}{x}}, 1\right\}$ and for distinct x, y the events $x \in B, y \in B$ are independent. Then $r_{B,2}(n)$ is an integer valued random variable, and we have $r_{B,2}(n) = \sum_{x+y=n} \mathbb{I}(x \in B)\mathbb{I}(y \in B)$. Taking expectations, we see that

$$\mathbb{E}[r_{B,2}(n)] = \sum_{x+y=n} p_x p_y.$$

We can simplify this sum by writing

$$\mathbb{E}[r_{B,2}(n)] = \frac{1}{2}\sum_{\substack{x+y=n\\x<y}} p_x p_y + O(1).$$

This is because the probability $p_{n/2}p_{n/2} = 100\dfrac{\log(n/2)}{n/2} = o(1)$.

Now we apply partial summation to obtain

$$50\sum_{x\le n/2}\sqrt{\frac{\log(x)\log(n-x)}{x(n-x)}}$$

$$= 50\log(n/2)\sum_{x\le n/2}\frac{1}{\sqrt{x(n-x)}} - 50\int_1^{n/2}\frac{(n-t)\log(n-t)-t\log(t)}{t(n-t)[\log(t)\log(n-t)]^{1/2}}\sum_{x\le t}\frac{1}{\sqrt{t(n-t)}}dt.$$

In particular, the latter term is negligible for large n, and we have

$$50\sum_{x\le n/2}\sqrt{\frac{\log(x)\log(n-x)}{x(n-x)}} \sim 50\log(n)\sum_{x\le n/2}\frac{1}{\sqrt{x(n-x)}}.$$

Now note that $\displaystyle\sum_{x\le n/2}\frac{1}{\sqrt{x(n-x)}} = \sum_{x\le n/2}\frac{1}{n}\frac{1}{\sqrt{(x/n)(1-x/n)}}$ is the Riemann sum for the integral $\displaystyle\int_0^1\frac{dt}{\sqrt{t(1-t)}} = \pi$, which can be readily evaluated through elementary calculus with the substitution $t = (1+\sin(\theta))/2$. Hence we obtain

$$\mathbb{E}[r_{B,2}(n)] \sim 50\pi\log(n).$$

Now note that since we required $x < n/2$, the random variables $\mathbb{I}(x\in B)\mathbb{I}(n-x\in B)$ for $1 \le x < n/2$ are independent. This is easy to see; knowing the value of $\mathbb{I}(x\in B)\mathbb{I}(n-x\in B)$ for some value x in the range does not give information for any other value, since we required the events $x \in B$ to be independent and $n - x > n/2$.

For simplicity and clarity set $\mu = \mathbb{E}[r_{B,2}(n)]$. Now suppose we choose $\varepsilon > 0$. By the corollary to Chernoff's Inequality, which applies by the independence established in the previous paragraph, we can choose a positive constant c_ε such that

$$\mathbb{P}(|r_{B,2}(n) - \mu| \ge \varepsilon\mu) \le 2\exp(-c_\varepsilon\mu).$$

In particular, for $\varepsilon = 0.9$, we have $\min(\varepsilon^2/4, \varepsilon/2) = 0.2025$ and we can choose $c_\varepsilon = 0.1 < 0.2025$, so that $\exp(-c_\varepsilon) < \exp(-0.2025)$. In this case we obtain the bound

$$\mathbb{P}(|r_{B,2}(n) - \mu| \ge \varepsilon\mu) \le 2\exp(-0.1\mu).$$

Note that $\mu \sim 50\pi \log(n)$, so that for n sufficiently large we have $\mu > 40\pi \log(n)$ and thus $\exp(-c_\varepsilon \mu) < \exp(-4\pi \log(n)) < n^{-2}$ for n sufficiently large.

Now set $c_1 = 5\pi, c_2 = 95\pi$. Let A_n be the event that either $r_{B,2}(n) < c_1 \log(n)$ or $r_{B,2}(n) > c_2 \log(n)$. Then A_n is a subset of the event $|r_{B,2}(n) - \mu| \geq 0.9\mu$, and thus $\mathbb{P}(A_n) < n^{-2}$ for n sufficiently large. In other words, we have

$$\sum_{n=1}^{\infty} \mathbb{P}(A_n) \leq \sum_{n=1}^{\infty} \frac{1}{n^2} < \infty.$$

Now the Borel-Cantelli Lemma applies and so with probability 1 at most finitely many of the $A_1, A_2, \cdots$ occur. Hence there exists a specific set B in our probability space that has the desired property for all n sufficiently large. That is, a specific set B such that $c_1 \log(n) \leq r_{B,2}(n) \leq c_2 \log(n)$ for all sufficiently large n. □

Notice that this proof seems quite innocuous, and that the requirement for independence seems to be just brushed over and is for convenience rather than necessity. This is not so. It turns out that when the independence assumption cannot be made, that is when we are looking at sums of three elements or more, that Chernoff's Inequality no longer applies and we cannot proceed with the proof as written above. Historically, Erdős proved the above theorem in 1956 but had to wait until 1990 before proving the case for bases of higher order. This will be discussed in the next section.

We give an example to illustrate the necessity of the joint independence assumption in Chernoff's Inequality.

Example 2.2.4. Colour the elements of $[1, n] = \{1, 2, \cdots, n\}$ either black or white independently and with equal probability. For each $A \subset [1, n]$, let s_A denote the parity of the black elements of A, so that $s_A = 1$ if the number of black elements in A is odd, and $s_A = 0$ otherwise. Let $X = \sum_{A \subset [1,n]} s_A$. Then the s_A's are pairwise independent, and we have $\mathbb{E}X = 2^{n-1} - 1/2$ and $\mathbf{Var}(X) = 2^{n-2} - 1/4$. Further, $\mathbb{P}(X = 0) = 2^{-n}$ where the upper bound in Chernoff's Inequality would be $2\exp(-2^{n-2})$. Hence Chernoff's Inequality fails for sufficiently large n.

Proof. We first establish the pairwise independence of the s_A's. Let A, B be two distinct subsets of $[1, n]$. If $A \cap B = \emptyset$, then clearly s_A, s_B are independent. We first consider the case when $A \subset B$. Suppose we know that $s_A = 1$, so A has an odd number of black elements. Then $\mathbb{P}(s_B = 1 | s_A = 1)$ is equal to $\mathbb{P}(s_{B \setminus A} = 0) = 1/2$, since $B \setminus A \neq \emptyset$. Hence $\mathbb{P}(s_B = 1 | s_A = 1) = \mathbb{P}(s_B = 1)$. Analogous conditions also hold, so that s_A, s_B are independent. It is now clear that if A is not a subset of B, $A \setminus B$ has no bearing on s_B, so we can apply the same analysis above to $C = A \cap B$ to obtain that s_A, s_B are also independent in this case.

It is now a trivial matter to compute the variance and expectation, since the linearity of variance only depends on pairwise independence. Note that $\mathbb{P}(s_\emptyset = 1) = 0$,

since there is no way to obtain an odd number black elements in the empty set. Otherwise, $\mathbb{P}(s_A = 1) = 1/2$. By the linearity of expectation and pairwise independence then we have that

$$\mathbb{E}X = \sum_{A\subset[1,n],A\neq\emptyset} 1/2 = 2^{n-1} - 1/2,$$

$$\mathbf{Var}(X) = \sum_{A\subset[1,n],A\neq\emptyset} (1/2 - 1/4) = 2^{n-2} - 1/4.$$

Also, we have $X = 0$ if and only if all of the elements were coloured white, so that $\mathbb{P}(X = 0) = 2^{-n}$. But then we have for $\lambda = 2^{n/2}$

$$\mathbb{P}(|X - \mathbb{E}X| \geq 2 \cdot 2^{(n-2)/2}\sqrt{2^{n-2} - 1/4}) \geq \mathbb{P}(X = 0) = 2^{-n} \geq 2\exp(-2^{n-2})$$

This shows that Chernoff's Inequality fails. □

So as the above example demonstrates, a much more powerful idea and set of tools is needed to overcome the hurdle of dependence. It is no wonder that even Erdős could not find a solution for 34 years. We will introduce the solution for higher order thin bases in the following section.

Remark 2.2.5. In [5], Erdős actually employed a very different argument to produce an additive basis B with $0 < r_{B,2}(n) < c\log n$ for some $c > 0$. This argument can be converted to give an explicit algorithm to produce a thin basis with almost sure certainty. However, as we will allude to in section 5, Erdős's original argument produces an algorithm that is exponential in nature. The main content of the first half of chapter 5 is to produce an algorithm which furnishes a thin basis that is of polynomial time.

2.3 Ruzsa's converse to the Erdős-Fuchs Theorem

We conclude this section with a discussion of the famous Erdős-Fuchs Theorem. Roughly speaking, this theorem states that the 'average' behaviour of the representation function $r_{B,2}(n)$ for some $B \subset \mathbb{N}$ cannot be too close to a constant. We state the theorem in more precise terms below.

Theorem 2.3.1. (Erdős-Fuchs Theorem) *Let $B \subset \mathbb{N}$ be an infinite subset. Then*

$$\sum_{n\leq N} r_{B,2}(n) = cN + o(N^{1/4}\log^{-1/2}(N))$$

cannot hold for any constant $c > 0$.

Note that there is no assertion that B is an additive basis. Indeed, in most well-known examples of bases it is plain that $\sum_{n\leq N} r_{B,2}(n)$ is much larger. For example, if B is a thin basis as constructed in the previous subsection, then we would have

$\sum_{n \leq N} r_{B,2}(n) \gg N \log(N)$. On the other hand, it is easy to construct a set B for which $\frac{1}{N} \sum_{n \leq N} r_{B,2}(n)$ tends to 0 (for example, $B = \{10^{n!} : n \in \mathbb{N}\}$).

We will not study this theorem much further in this paper, since it is only tangentially related to additive bases and the probabilistic method. What we will study, however, is a partial converse to this theorem by I. Ruzsa given in 1997. In particular, Ruzsa proved the following:

Theorem 2.3.2. (Ruzsa) *There exists $B \subset \mathbb{N}$ such that*

$$\sum_{n \leq N} r_{B,2}(n) = cN + O(N^{1/4} \log(N)).$$

We will prove this theorem in this section. What is interesting is that such an example is furnished using the probabilistic method. Another interesting aspect of this theorem is that there is a very nice, simple subset of $\mathbb{N}$ that might serve as a concrete example of such a set, namely the set of squares. The verification of whether the squares is such a set boils down to the famous Gauss Circle Problem, which can be stated as follows:

Conjecture 2.3.3. (Gauss Circle Problem) *Let $N(r)$ be the number of solutions $(x, y) \in \mathbb{Z}^2$ to the inequality*

$$x^2 + y^2 \leq r.$$

Then for all $\varepsilon > 0$ we have

$$N(r) = \pi r + O(r^{1/3+\varepsilon}).$$

To date there has been no final resolution to this problem. The best current known error bound is $O(r^{131/416})$, due to Martin Huxley in [14].

Before we prove Ruzsa's Theorem, we first give another probabilistic lemma, known as *Hoeffding's Inequality*.

Proposition 2.3.4. (Hoeffding Inequality) *Suppose $X_1, \cdots, X_n$ are bounded independent random variables, so that $a_j \leq X_j \leq b_j$ for each j and constants a_j, b_j, and that*

$$\sum_{j=1}^{n} (b_j - a_j)^2 \leq D^2.$$

Set $X = \sum_{j=1}^{n} X_j$ and $\mu = \mathbb{E}X$. Then

$$\mathbb{P}(|X - \mu| \geq \lambda D) \leq \exp(-2\lambda^2).$$

Note the similarity between this result and Chernoff's Inequality. Here the σ term has been replaced with the upper bound D. In the case of Chernoff's Inequality this would provide a cruder bound, since if $X_1, \cdots, X_n$ were all indicator random variables then $D = \sqrt{n}$ whereas σ could be much smaller. We now proceed with the proof of this proposition.

Proof. Since the quantity $(b_j - a_j)^2$ is unchanged if we shift the interval $[a_j, b_j]$, it suffices to assume that $\mathbb{E}X_j = 0$ for $1 \leq j \leq n$. We first show that if $Z \in [a, b]$ and $\mathbb{E}Z = 0$, then

$$\mathbb{E}[e^{tZ}] \leq \exp\left(\frac{t^2(b-a)^2}{8}\right).$$

To see this, note that $f(z) = e^{tz}$ is a convex function. Hence it follows that $e^{tz} \leq \frac{z-a}{b-a}e^{tb} + \frac{b-z}{b-a}e^{ta}$. Taking expectations on both sides and considering the linearity of expectation and the fact that $\mathbb{E}Z = 0$, we obtain

$$\mathbb{E}[e^{tZ}] \leq \frac{-a}{b-a}e^{tb} + \frac{b}{b-a}e^{ta}.$$

Now set $x = \frac{-a}{b-a}$ to obtain

$$\frac{b}{b-a}e^{ta} - \frac{a}{b-a}e^{tb} = (1 - x + xe^{t(b-a)})e^{-xt(b-a)}.$$

Now set $t(b-a) = u$ and $\varphi(u) = -xu + \log(1 - x + xe^u)$ so that

$$e^{\varphi(u)} = (1 - x + xe^u)e^{-xu}.$$

For u sufficiently small, the Taylor series for $\varphi(u)$ centered at 0 exists. Hence by Taylor's Theorem we have that

$$\varphi(u) = \varphi(0) + \varphi'(0)u + \frac{u^2}{2}\varphi''(v)$$

for some $v \in [0, u]$. Note that $\varphi(0) = \varphi'(0) = 0$, so we simply need to find a good bound for $\varphi''(v)$. But

$$\varphi''(v) = \frac{xe^u}{1 - x + xe^u} - \frac{x^2e^{2u}}{(1 - x + xe^u)^2} = \rho(1 - \rho)$$

where $\rho = \frac{xe^u}{1 - x + xe^u}$. Clearly, $\rho(1 - \rho)$ is maximized when $\rho = 1/2$, so we obtain the bound

$$\varphi(u) \leq \frac{u^2}{2}\frac{1}{4} = \frac{u^2}{8}.$$

Applying this to our original inequality, we obtain

$$\mathbb{E}[e^{tZ}] \leq \exp\left(\frac{t^2(b-a)^2}{8}\right),$$

as desired.

Now we use the same trick as in the proof of Chernoff's Inequality, namely the observation that

$$\mathbb{P}(X \geq \lambda D) \leq e^{-t\lambda D}\mathbb{E}[e^{tX}].$$

Thus we obtain the bound

$$\mathbb{P}(X \geq \lambda D) \leq e^{-t\lambda D}\prod_{j=1}^{n}\exp\left(\frac{t^2(b_j-a_j)^2}{8}\right) \leq \exp(-t\lambda D)\exp\left(t^2\sum_{j=1}^{n}\frac{(b_j-a_j)^2}{8}\right).$$

Setting $t = \dfrac{4\lambda D}{\sum_{j=1}^{n}(b_j-a_j)^2}$ and noting that $\displaystyle\sum_{j=1}^{n}(b_j-a_j)^2 \leq D^2$ yields the desired result. Note that everything we have done applies to $-X$ as well, and hence we obtain the desired inequality. This completes the proof. □

Now we proceed to prove Ruzsa's Theorem.

Proof. (Ruzsa's Theorem) We will define a random set A as follows. Suppose α_i is a uniformly distributed random variable in the interval $[i, i+1]$. Set $a_i = \lfloor \alpha_i^2 \rfloor$. Set $A = \{a_i\}_{i\geq 1}$. We will show that with probability 1, A satisfies

$$\sum_{n\leq N} r_{A,2}(n) = cN + O(N^{1/4}\log(N)),$$

for some $c > 0$.

Set $\delta_{ij} = 1$ if $\alpha_i^2 + \alpha_j^2 \leq n$, and $\delta_{ij} = 0$ otherwise. Set $\sigma_n = \displaystyle\sum_{i,j}\delta_{ij}$ to be the number of ordered pairs (i,j) such that $\alpha_i^2+\alpha_j^2 \leq n$. Now set d_{ij} to be the area of the intersection of the square $[i,i+1]\times[j,j+1]$ with the circle disc $\{(x,y) : x^2+y^2 \leq n\}$. Clearly then $\displaystyle\sum_{i,j} d_{ij} = \frac{\pi n}{4}$. Thus we obtain

$$\sigma_n - \frac{\pi n}{4} = \sum_{i,j}(\delta_{ij} - d_{ij}).$$

Note that since $\alpha_i^2 + \alpha_j^2 \geq i^2 + j^2$, if $i^2+j^2 \geq n$ then $\delta_{ij} = 0$ with probability 1. At the same time if $i^2+j^2 \geq n$, then $d_{ij} = 0$. Conversely, if $(i+1)^2+(j+1)^2 \leq n$, then $\alpha_i^2+\alpha_j^2 \leq n$ with probability 1 and hence $\delta_{ij} = 1$. Similarly, if $(i+1)^2+(j+1)^2 \leq n$ then the square $[i,i+1]\times[j,j+1]$ is contained inside the disc $\{(x,y) : x^2+y^2 \leq n\}$, and hence $d_{ij} = 1$. Hence the only interesting case is

$$i^2 + j^2 < n < (i+1)^2 + (j+1)^2.$$

Now define

$$I = \{(i,j) : 0 \leq i < j, i^2+j^2 < n < (i+1)^2+(j+1)^2\}.$$

Note that if $i^2+j^2 < n < (i+1)^2+(j+1)^2$, then either $(i,j) \in I$ or $(j,i) \in I$, unless $i=j$ which happens for at most one value, namely the i such that $2i^2 < n < 2(i+1)^2$, if $n/2$ is a non-square. Hence we have

$$\sigma_n - \frac{\pi n}{4} = 2 \sum_{(i,j)\in I} (\delta_{ij} - d_{ij}) + O(1).$$

Set $\sum_{(i,j)\in I} (\delta_{ij} - d_{ij}) = \tau$. If $i \neq j$, then (α_i, α_j) is uniformly distributed on the square $[i, i+1] \times [j, j+1]$. By the definition of δ_{ij}, we see that the probability that $\delta_{ij} = 1$ is precisely the area of the intersection of $[i, i+1] \times [j, j+1]$ and the disc $\{(x,y) : x^2+y^2 \leq n\}$, in other words d_{ij}. This implies that $\mathbb{E}[\delta_{ij}] = d_{ij}$, and by the linearity of expectation, we have

$$\mathbb{E}\tau = 0.$$

We would be able to apply Hoeffding's inequality right away, since δ_{ij} are indicator random variables. Unfortunately, $\delta_{ij} : 1 \leq i < j$ are not independent. Thus we would need to first decompose τ into a sum of independent random variables. The following construction does exactly that and is quite ingenious.

If $(i,j) \in I$, then surely $j^2 < i^2+j^2 < n < (i+1)^2+(j+1)^2 \leq j^2+(j+1)^2$. Let k_1, k_2 denote respectively the minimum and maximum value of j such that $j^2 < n < j^2+(j+1)^2$. Then it is clear that $k_1 \sim \sqrt{n/2}, k_2 \sim \sqrt{n}$. Observe that $i \leq k_1 - 1$. This follows from $i^2+(i+1)^2 \leq i^2+j^2 < n$. For each $k_1 \leq j \leq k_2$, let

$$I_j = \{i : i^2+j^2 < n < (i+1)^2+(j+1)^2, i < j\}.$$

Note that I_j (as the notation suggests) is an interval. Set $\beta_j = \sum_{i\in I_j} (\delta_{ij} - d_{ij})$. Then we have

$$\tau = \sum_{j=k_1}^{k_2} \beta_j.$$

Now define

$$\tau_0 = \sum_{j\equiv 0 \pmod 2} \beta_j$$

$$\tau_1 = \sum_{j\equiv 1 \pmod 2} \beta_j.$$

So we have $\tau = \tau_0 + \tau_1$. The key now is to show that both τ_0 and τ_1 are sums of independent random variables, so that Hoeffding's Inequality applies. To this end we show that for $l = 0, 1$ we have that for $j \equiv l \pmod 2$, β_j depends on disjoint sets of α_i's. It is clear that β_j depends on $I_j \cup \{j\}$, so that our goal is to show if $j_1 \equiv j_2 \pmod 2$ and $j_1 \neq j_2$, we have $(I_{j_1} \cup \{j_1\}) \cap (I_{j_2} \cup \{j_2\}) = \emptyset$. Since we verified that $I_{j_1}, I_{j_2} \subset [1, k_1 - 1]$ and $j_1, j_2 \geq k_1$, it follows that we only need to check that $I_{j_1} \cap I_{j_2} = \emptyset$.

We may assume without loss of generality that $j_2 > j_1$, so that $j_2 \geq j_1 + 2$ since they have the same parity. If $i \in I_{j_1}$, then $n < (i+1)^2 + (j_1+1)^2$. If $i \in I_{j_2}$, then $i^2 + (j_1+2)^2 \leq i^2 + j_2^2 < n$ and if $i \in I_{j_1} \cap I_{j_2}$, then both hold simultaneously. This implies that $i^2 + (j_1+2)^2 < (i+1)^2 + (j_1+1)^2$ or equivalently $2j_1 + 3 < 2i + 1$, which contradicts the assumption that $i < j_1$. Hence $I_{j_1} \cap I_{j_2} = \emptyset$ as desired.

To apply Hoeffding's Inequality, we would need a bound D such that $\sum_{j \geq 1} |\max \beta_j - \min \beta_j| \leq D^2$. Since $\beta_j \leq \sum_{i \in I_j} 1 = |I_j|$, it follows that we can choose D such that

$$D^2 = \sum_{j \geq 1} |I_j|^2.$$

Since $i \in I_j$ if and only if $i^2 + j^2 < n < (i+1)^2 + (j+1)^2$, it follows for $j < k_2$ we have that $i < \sqrt{n - j^2}$ and $i > \sqrt{n - (j+1)^2} - 1$. Hence $I_j \subset [\sqrt{n-(j+1)^2} - 1, \sqrt{n - j^2}]$, and so

$$|I_j| \leq 2 + \sqrt{n - j^2} + \sqrt{n - (j+1)^2}.$$

For $j = k_2$, we use the bound $|I_j| = |I_{k_2}| \leq 1 + \sqrt{n - j^2}$ instead. Recall that k_2 was defined to be the largest integer j such that $k_2^2 < n$, so that $k_2 = \lfloor \sqrt{n-1} \rfloor$. Hence

$$|I_{k_2}| \leq 1 + \sqrt{n - k_2^2} \leq 1 + \sqrt{2k_2 + 1} \leq 2\sqrt{k_2}.$$

For $j < k_2$, we write $j = k_2 - r$ for $1 \leq r \leq k_2 - k_1$. Then we have

$$n - j^2 \geq k_2^2 - (k_2 - r)^2 = 2k_2 r - r^2 \geq k_2 r.$$

Consequently, we have

$$\sqrt{n - j^2} - \sqrt{n - (j+1)^2} = \frac{2j+1}{\sqrt{n - j^2} + \sqrt{n - (j+1)^2}}$$

$$\leq \frac{2j+1}{\sqrt{n - j^2}} \leq \frac{2(j+1)}{\sqrt{k_2 r}} \leq 2\sqrt{\frac{k_2}{r}}.$$

In particular, we obtain the bound $|I_j| \leq 2 + 2\sqrt{k_2/r}$. Summing, we obtain the bound for D^2:

$$D^2 = \sum_{j \geq 1} |I_j|^2 \leq 4k_2 + \sum_{r=1}^{k_2 - k_1} (2 + 2\sqrt{k_2/r})^2 \leq C\sqrt{n}\log(n),$$

for some $C > 0$, since $k_2 \sim \sqrt{n}, k_1 \sim \sqrt{n/2}$.

Now we apply Hoeffding's Inequality with $\lambda = 3\sqrt{\log(n)}$ and $D = n^{1/4}\sqrt{C\log(n)}$. Thus we obtain

$$\mathbb{P}(|\tau| \geq \lambda D) = \mathbb{P}(|\tau| \geq 3n^{1/4}\sqrt{C}\log(n)) \leq \exp(-2(9\log(n))) = n^{-18}.$$

Recall that $\sigma - \frac{\pi n}{4} = 2\tau + O(1)$, so the above inequality implies that

$$\mathbb{P}\left(\left|\sigma - \frac{\pi n}{4}\right| > C' n^{1/4}\log(n)\right) \leq n^{-18}$$

for some suitably chosen constant $C' > 6\sqrt{C}$. Now let A_n be the event that $\left|\sigma - \frac{\pi n}{4}\right| > C' n^{1/4}\log(n)$. Then since $\mathbb{P}(A_n) \leq n^{-18}$, the Borel-Cantelli Lemma applies and with probability one at most finitely many of the A_n's occur. In particular, with probability one we have

$$\sigma = \sigma_n = \frac{\pi n}{4} + O(n^{1/4}\log(n)).$$

Now, from the definition of a_i, we have that $\alpha_i^2 - 1 < a_i \leq \alpha_i^2$, and so

$$\alpha_i^2 + \alpha_j^2 - 2 < a_i + a_j \leq \alpha_i^2 + \alpha_j^2.$$

This implies that

$$\sigma_{N+2} \leq \sum_{n \leq N} r_{A,2}(n) \leq \sigma_N.$$

Hence with probability 1, there exists a set A that satisfies

$$\sum_{n \leq N} r_{A,2}(n) = \frac{\pi n}{4} + O(n^{1/4}\log(n)),$$

and this completes the proof. □

We discuss briefly the motivation for this construction. If instead of a random set A we consider the set of all squares, then we know (almost trivially) that

$$\sum_{n \leq N} r_{\mathbb{N}^2,2}(n) = \pi N + O(\sqrt{N}).$$

The last term is not an optimal error term. Indeed it is conjectured that

$$\sum_{n \leq N} r_{\mathbb{N}^2,2}(n) = \pi N + O(N^{1/4+\varepsilon}),$$

for any given $\varepsilon > 0$. This conjecture is known as the Gauss Circle Problem, since Gauss was the first one to investigate it. Unfortunately, the problem seems to remain unresolved, though in 2007 a paper by Cappell and Shaneson appeared on the arXiv claiming to have resolved the problem. Their proof is not currently accepted by the mathematical community, though no retraction has been made. If this conjecture is true, then the set of squares themselves give an example of Ruzsa's thin sumset.

Indeed, it is clear that Ruzsa's insight was to notice that the set of squares have the correct main term, and conjecturally the correct error term. Hence he attempted and succeeded in generating a 'square like' random set that actually does the job.

Unfortunately, one can see that Ruzsa's construction relies much on the same machinery that was used in Erdős's theorem. Namely, the approach is to define a suitable random set B, calculate $\mathbb{E}[r_{B,2}(n)]$, break $r_{B,2}(n)$ (or something sufficiently close to it, as in Ruzsa's theorem) into a sum of independent indicator random variables, then apply something like Chernoff's Inequality to show that the 'bad' events have summable probability, and then apply the Borel-Cantelli Lemma to finish the job. The key difficulty that Ruzsa did not circumvent in his theorem is how to deal with the case when $r_{B,k}(n)$ (when k could be larger than 2) cannot be decomposed into a sum of independent indicator random variables, but nonetheless correlation of the summands remain 'small'. The key insight needed to overcome this difficulty is discussed in the next chapter, where we discuss the proof of the Erdős-Tetali Theorem.

Chapter 3

The Probabilistic Method - Part II

3.1 Two needed inequalities

Before we present the Erdős-Tetali theorem, we will need to introduce the significant breakthrough that allowed the aforementioned authors to make the jump from the $k = 2$ case to the general case, that of Janson's Inequality. Roughly speaking, if $X_1, \cdots, X_n$ are independent, then $X = X_1 + \cdots + X_n$ is a sum of independent random variables. However we may wish to consider other polynomials of $X_1, \cdots, X_n$. Namely, if $X = X(X_1, \cdots, X_n)$ is a convex polynomial of $X_1, \cdots, X_n$, then we wish to obtain some sort of statement saying that X should be close to(or concentrated near) its mean. From this perspective, we can view Janson's Inequality as a generalization of Chernoff's Inequality.

We first begin with a correlation inequality due to Fortuin, Kasteleyn, and Ginibre [12].

3.1.1 FKG Inequality

The FKG inequality, a fundamental inequality in the study of lattices in combinatorics, has a clear generalization in the context of independent random variables. The idea here is that X, Y are two monotone functions of jointly independent random variables $X_1, X_2, \cdots, X_n$, then $X(X_1, \cdots, X_n), Y(X_1, \cdots, X_n)$ should be positively correlated. We give the following definition:

Definition 3.1.1. Let $X_1, \cdots, X_n$ be jointly independent indicator random variables. Let $X = X(X_1, \cdots, X_n)$ be a function of the variables $X_1, \cdots, X_n$. We say that X is *monotone increasing* if $X(X_1, \cdots, X_n) \geq X(X_1', \cdots, X_n')$ whenever $X_j \geq X_j'$, for $1 \leq j \leq n$. Say that X is *monotone decreasing* if $-X$ is monotone increasing.

With this definition, we can state the FKG inequality needed for our context.

Proposition 3.1.2. (FKG Inequality) *Suppose $X_1, \cdots, X_n$ are independent indicator random variables. Then if X, Y are monotone increasing random variables, then*

$$E[XY] \geq E[X]E[Y]$$

or equivalently

$$\mathbf{Cov}(X, Y) \geq 0.$$

The same holds if X, Y are both monotone decreasing.

Proof. By replacing X and Y with $-X, -Y$ if necessary, it suffices to assume that X, Y are monotone increasing. Note that by definition, X, Y are functions of the set of independent variables $\{X_1, \cdots, X_n\}$. We thus establish the truth of the inequality by induction on n. If $n = 0$ then the set of independent random variables is empty, hence X, Y are deterministic and the inequality is vacuously true. If $n \geq 1$, assume that the inequality is proved for $n - 1$. We now show that this implies the truth of the inequality for n as well.

By the inductive hypothesis, it suffices to assume that $\mathbb{P}(X_n = 0), \mathbb{P}(X_n = 1)$ are non-zero. Otherwise the random variable X_n is a constant and so $X(X_1, \cdots, X_n) = X(X_1, \cdots, X_{n-1})$. By the inductive hypothesis, we are done. Now note that since $\mathbf{Cov}(X, Y) = \mathbb{E}[(X - \mathbb{E}[X])(Y - \mathbb{E}[Y])]$ is unaffected if X, Y are shifted, we may assume without loss of generality that the conditional expectations $\mathbb{E}[X|X_n = 0], \mathbb{E}[Y|X_n = 0] = 0$. By the monotonicity assumption, it follows that $\mathbb{E}[X|X_n = 1], \mathbb{E}[Y|X_n] \geq 0$. By monotonicity again and the inductive hypothesis, we have that

$$\mathbb{E}[XY|X_n = 0] \geq \mathbb{E}[X|X_n = 0]\mathbb{E}[Y|Y_n = 0] = 0.$$

Likewise, we have

$$\mathbb{E}[XY|X_n = 1] \geq \mathbb{E}[X|X_n = 1]\mathbb{E}[Y|X_n = 1].$$

By the law of total probability, we have

$$\mathbb{E}[XY] = \mathbb{E}[XY|X_n = 1]\mathbb{P}(X_n = 1) + \mathbb{E}[XY|X_n = 0]\mathbb{P}(X_n = 0)$$

$$\geq \mathbb{E}[X|X_n = 1]\mathbb{E}[Y|X_n = 1]\mathbb{P}(X_n = 1).$$

On the other hand, we have $\mathbb{E}[X] = \mathbb{E}[X|X_n = 0]\mathbb{P}(X_n = 0) + \mathbb{E}[X|X_n = 1]\mathbb{P}(X_n = 1) = \mathbb{E}[X|X_n = 1]\mathbb{P}(X_n = 1)$ and similarly $\mathbb{E}[Y] = \mathbb{E}[Y|X_n = 1]\mathbb{P}(X_n = 1)$. Here we used the fact that $\mathbb{E}[X|X_n = 0] = \mathbb{E}[Y|X_n = 0] = 0$. Together, these imply that

$$\mathbb{E}[X]\mathbb{E}[Y] = \mathbb{E}[X|X_n = 1]\mathbb{E}[Y|X_n = 1]\mathbb{P}(X_n = 1)^2.$$

But $\mathbb{P}(X_n = 1) \leq 1$, and hence

$$\mathbb{E}[XY] \geq \mathbb{E}[X]\mathbb{E}[Y],$$

as desired. □

Now we proceed to prove Janson's Inequality. Note that the result we prove here is an improved version of the original. To see a statement and proof of the original Janson's Inequality, see [1]. This new Janson's Inequality is taken from [15] and [22]. Janson's Inequality is part of a larger scheme called Poisson's paradigm, which deals

with the case when a random variable can be decomposed into a sum of 'mostly independent' indicator random variables. This is precisely the context that is needed to overcome the difficulty of dependence when dealing with a basis of order $k > 2$.

The Poisson paradigm has spawned a large amount of research that cannot be covered in this paper. See [1] and [22] for more details. We now introduce Janson's Inequality.

3.1.2 Janson's Inequality

Proposition 3.1.3. (Janson's Inequality) *Suppose $X_1, \cdots, X_n$ are independent indicator random variables. Let $\mathcal{A}$ be a collection of non-empty subsets of $[1, n] = \{1, 2, \cdots, n\}$. Define*

$$X = \sum_{A \in \mathcal{A}} \prod_{j \in A} X_j,$$

and

$$\Delta(X_1, \cdots, X_n) = \sum_{A,B \in \mathcal{A}, A \cap B \neq \emptyset} \mathbb{E}\left(\prod_{j \in A \cup B} X_j \right).$$

Then for any real number $0 \leq x \leq \mathbb{E}X$, we have the inequality

$$\mathbb{P}(X \leq \mathbb{E}X - x) \leq \exp\left(\frac{-x^2}{2\Delta}\right), \mathbb{P}(X = 0) \leq \exp\left(\frac{-\mathbb{E}[X]^2}{2\Delta}\right).$$

Proof. We will establish Janson's Inequality using techniques from the exponential moment method from the first sub-section of this chapter. If $\mathbb{P}(X_j = 1) = 0$, then $\mathbb{E}[X'] = \mathbb{E}[X_1 + \cdots + X_{j-1} + X_{j+1} + \cdots + X_n] = \mathbb{E}[X]$ and we can instead look at the random variable $X' = X_1 + \cdots + X_{j-1} + X_{j+1} + \cdots + X_n$. If $\mathbb{P}(X_j = 0) = 0$ then we see that

$$\mathbb{P}(X \leq \mathbb{E}[X] - x) = \mathbb{P}(X' + 1 \leq \mathbb{E}[X] + 1 - x) = \mathbb{P}(X' \leq \mathbb{E}[X'] - x),$$

and from the definition of Δ it is clear that $\Delta(X_1, \cdots, X_n) = \Delta(X_1, \cdots, X_{j-1}, X_{j+1}, \cdots, X_n)$. Hence it suffices to assume that $\mathbb{P}(X_j = 0) > 0, \mathbb{P}(X_j = 1) > 0$ for all j.

Define the function $F(t) = \mathbb{E}[e^{-tX})$ for positive t. Recall Markov's Inequality implies that for any random variable and $\lambda > 0$, we have

$$\mathbb{P}(X \leq -\lambda) = \mathbb{P}(e^{-tX} \geq e^{t\lambda}) \leq \frac{\mathbb{E}[e^{-tX}]}{e^{t\lambda}}.$$

This implies that

$$\mathbb{P}(X \leq \mathbb{E}[X] - x) \leq \frac{F(t)}{\exp(-t(\mathbb{E}[X] - x))}.$$

Thus it suffices to show, after taking logarithms, that the stronger inequality $\log(F(t)) + t(\mathbb{E}[X] - x) \leq \frac{-x^2}{2\Delta}$ holds for some $t > 0$. Because the summands in X, being $\prod_{j \in A} X_j$

are no longer independent necessarily when two index sets $A, B \in \mathcal{A}$ intersect non-trivially, we cannot hope for an easy factorization of $\mathbb{E}[e^{-tX}]$ as we did with Chernoff's Inequality. Getting around this difficulty with dependence is the crucial insight that allowed Erdős and Tetalli to show the existence of thin bases of arbitrary order. We will bypass the difficulty of dependence as follows. It is clear that $F(0) = 1$. By the Fundamental Theorem of Calculus, we have

$$\log(F(t)) = \int_0^t \frac{F'(s)}{F(s)} ds.$$

By the chain rule, we have

$$F'(t) = -\mathbb{E}[Xe^{-tX}]$$

which implies that

$$F'(t) = -\sum_{A \in \mathcal{A}} \mathbb{E}\left(e^{-tX} \prod_{j \in A} X_j\right).$$

Clearly, $\prod_{j \in A} X_j = 1$ if and only if $X_j = 1$ for all $j \in A$. Thus we can define E_A to be the event that $X_j = 1$ for all $j \in A$. Then we obtain the following equality

$$F'(t) = -\sum_{A \in \mathcal{A}} \mathbb{E}[e^{-tX}|E_A]\mathbb{P}(E_A).$$

Making this substitution into the equation $\log F(t) = \int_0^t \frac{F'(s)}{F(s)} ds$, we obtain

$$-\log F(t) = \int_0^t \frac{\sum_{A \in \mathcal{A}} \mathbb{E}[e^{-sX}|E_A]\mathbb{P}(E_A)}{F(s)} ds = \sum_{A \in \mathcal{A}} \mathbb{P}(E_A) \int_0^t \frac{\mathbb{E}[e^{-sX}|E_A]}{F(s)} ds.$$

The exchange of the sum and the integral is trivial, due to the sum being finite. It thus suffices to show the inequality

$$\sum_{A \in \mathcal{A}} \mathbb{P}(E_A) \int_0^t \frac{\mathbb{E}[e^{-sX}|E_A]}{F(s)} ds + t(\mathbb{E}[X] - x) \geq \frac{x^2}{2\Delta}.$$

Again, recall that the summands of X are not necessarily independent. However, if $A, B \in \mathcal{A}$ are such that $A \cap B = \emptyset$, then $\prod_{j \in A} X_j, \prod_{j \in B} X_j$ are independent. Thus it is natural to introduce the ancillary random variables $Y_A = \sum_{B \in \mathcal{A}: A \cap B \neq \emptyset} \prod_{j \in B} X_j$ and $Z_A = \sum_{B \in \mathcal{A}: A \cap B = \emptyset} \prod_{j \in B} X_j$.

By the FKG inequality, we have

$$\mathbb{E}[e^{-tX}|E_A] = \mathbb{E}[e^{-t(Y_A + Z_A)}|E_A] \geq \mathbb{E}[e^{-tY_A}|E_A]\mathbb{E}[e^{-tZ_A}|E_A].$$

But Z_A is independent from E_A, hence $\mathbb{E}[e^{-tZ_A}|E_A] = \mathbb{E}[e^{-tZ_A}]$. Since $X \geq Z_A$, we have that $e^{-tX} \leq e^{-tZ_A}$ and so $\mathbb{E}[e^{-tZ_A}] \geq F(t)$. Now, we can replace

$$\sum_{A\in\mathcal{A}} \mathbb{P}(E_A) \int_0^t \frac{\mathbb{E}[e^{-sX}|E_A]}{F(s)} ds + t(\mathbb{E}[X] - x) \geq \frac{x^2}{2\Delta}$$

with

$$\sum_{A\in\mathcal{A}} \mathbb{P}(E_A) \int_0^t \mathbb{E}[e^{-sY_A}|E_A] ds + t(\mathbb{E}[X] - x) \geq \frac{x^2}{2\Delta}.$$

Now for any positive number t, the function $f(z) = e^{-tz}$ is convex. Now we can apply *Jensen's Inequality*, which states for any convex function φ, we have $\mathbb{E}[\varphi(X)] \geq \varphi(\mathbb{E}[X])$. In particular, we have

$$\mathbb{E}[e^{-sY_A}|E_A] \geq \exp\left(-s\mathbb{E}[Y_A|E_A]\right).$$

Now, we apply the classic, finite version of Jensen's Inequality to the convex function $f(u) = \exp(-su)$ and noting that $\mathbb{E}[X] = \sum_{A\in\mathcal{A}} \mathbb{P}(E_A)$ to obtain

$$\sum_{A\in\mathcal{A}} \mathbb{P}(E_A) \exp(-s\mathbb{E}[Y_A|E_A]) \geq E[X] \exp\left(-s \sum_{A\in\mathcal{A}} \frac{\mathbb{P}(E_A)\mathbb{E}[Y_A|E_A]}{\mathbb{E}[X]}\right).$$

On the other hand, we have

$$\sum_{A\in\mathcal{A}} \mathbb{P}(E_A)\mathbb{E}[Y_A|E_A] = \sum_{A\in\mathcal{A}} \sum_{B\in\mathcal{A}:A\cap B\neq\emptyset} \mathbb{E}\left(\mathbb{I}(E_A) \prod_{j\in B} X_j\right) = \Delta(X_1, \cdots, X_n) = \Delta.$$

This implies that

$$\begin{aligned}
&\int_0^t \sum_{A\in\mathcal{A}} \mathbb{P}(E_A)\mathbb{E}[e^{-sY_A}|E_A] ds + t(\mathbb{E}[X] - x) \\
&\geq \mathbb{E}[X] \int_0^t \exp\left(-s\frac{\Delta}{\mathbb{E}[X]}\right) ds - t(\mathbb{E}[X] - x) \\
&= \frac{\mathbb{E}[X]^2}{\Delta}\left(1 - \exp\left(-t\frac{\Delta}{\mathbb{E}[X]}\right)\right) - t(\mathbb{E}[X] - x).
\end{aligned}$$

Now set $t = x/\Delta$ so that $\dfrac{t\Delta}{\mathbb{E}[X]} = \dfrac{x}{\mathbb{E}[X]} \leq 1$, and thus we obtain

$$1 - \exp\left(-t\frac{\Delta}{\mathbb{E}[X]}\right) = 1 - \exp\left(\frac{-x}{\mathbb{E}[X]}\right) \geq \frac{x}{\mathbb{E}[X]} - \frac{x^2}{2\mathbb{E}[X]^2}.$$

Finally, we obtain

$$\begin{aligned}
&\int_0^t \sum_{A\in\mathcal{A}} \mathbb{P}(E_A)\mathbb{E}[e^{-sY_A}|E_A] ds + t(\mathbb{E}[X] - x) \\
&\geq \frac{x\mathbb{E}[X]}{\Delta} - \frac{x^2}{2\Delta} - \frac{x}{\Delta}(\mathbb{E}[X] - x) = \frac{x^2}{2\Delta}.
\end{aligned}$$

This completes the proof. □

The FKG inequality showed that if X, Y are two increasing functions of the random variables $X_1, \cdots, X_n$ then their covariance is non-negative. Janson's Inequality asserts that one can obtain an exponential type bound for a specific type of convex polynomial of independent indicator random variables. Note however that with the case of Chernoff's Inequality, we were able to obtain a bound on $|X - \mathbb{E}X|$, not just $X - \mathbb{E}X$. This turns out to be crucial if we are to obtain a thin basis. For example, with the $k = 2$ case we saw that both ends of the inequality were needed to obtain the $\Theta(\log(n))$ behaviour. In the next subsection some better estimates will be obtained to deal with the general case.

3.2 Thin bases of order $k > 2$

We present here the original argument of Erdős and Tetali in their 1990 paper, [9]. It is noted that an alternative proof has since been discovered using more refined machinery on polynomial concentration, which can be seen as generalizing both Chernoff's bounds and Janson's Inequality. We direct the reader to [22] for such results. We begin with the classic *sunflower lemma*.

Definition 3.2.1. We say a collection of sets S is a *sunflower* if there exists a set G such that for every $A_i, A_j \in S$ we have $A_i \cap A_j = G$. The sets A_i are called *petals* of the sunflower. G is then called the *core* of the sunflower.

Proposition 3.2.2. (Sunflower Lemma) *Let $\mathcal{F}$ be a finite collection of sets, each containing n elements. Suppose that for some positive integer $l > 0$ we have $|\mathcal{F}| > (l-1)^n n!$. Then $\mathcal{F}$ contains l sets that form a sunflower.*

Proof. We proceed by induction on n. For the $n = 1$ case, $\mathcal{F}$ contains at least l singletons, no two are the same, so their pairwise intersection is $\emptyset$. Pick any l elements in $\mathcal{F}$ and they form a sunflower with core $\emptyset$. Now suppose that $n > 1$ and that the claim has been verified for all values less than n. Let $\mathcal{A} = \{A_1, \cdots, A_s\} \subset \mathcal{F}$ be a collection of disjoint sets that is maximal, in other words $\mathcal{A} \cup \{B\}$ is not a disjoint family for any $B \in \mathcal{F}$. If $s \geq l$, then we are done since we can find a sunflower with core the empty set. Hence suppose that $s \leq l - 1$. Set $B = \bigcup_{j=1}^{s} A_j$. Then $|B| \leq n(l-1)$. By the maximality of $\mathcal{A}$, B intersects non-trivially with every element in $\mathcal{F}$. By the pigeon hole principle there is an $x \in B$ that is contained in at least $\frac{|\mathcal{F}|}{|B|} > \frac{n!(l-1)^n}{n(l-1)} = (n-1)!(l-1)^{n-1}$ many elements of $\mathcal{F}$. Now consider the family $\mathcal{F}_x = \{S \setminus \{x\} : S \in \mathcal{F}\}$. By the inductive hypothesis, since each of the elements in $\mathcal{F}_x$ contains $n-1$ elements, it follows that $\mathcal{F}_x$ contains a sunflower with l petals, say $C_1, \cdots, C_l$. But then $C_1 \cup \{x\}, \cdots, C_l \cup \{x\}$ is still a sunflower with l petals, and each $C_j \cup \{x\} \in \mathcal{F}$. This completes the proof of the proposition. □

We will now establish the Erdős-Tetali Theorem in the following manner. We define a random set B as per the proof of Erdős's theorem for the case $k = 2$, with

a suitable probability. Next we define $r_{B,k}(n)$ to be the number of ways of writing n as k elements of B, and show that the expected value of $r_{B,k}(n)$, which we denote μ, is $\Theta(\log(n))$. Next we will be done if we can show that if A_n is the event that $|r_{B,k}(n) - \mu| \geq (1-\varepsilon)\mu$ then the probabilites $\mathbb{P}(A_n)$ are summable as a series, and hence with probability one at most finitely many of the A_n's occur. This will establish the theorem. For technical reasons, we want to work with a slightly modified definition for $r_{B,k}(n)$; where we want to only consider the sum of k DISTINCT elements. This choice is largely to simplify the discourse. For detailed discussions on how to deal with the case when repeat summands are allowed, see [22].

We now construct the random set B as follows. Fix the absolute constant

$$D_k = \left(\frac{k^{k-1}}{k-1}\right)^{\frac{k-1}{k}} \prod_{j=1}^{k-2}((j+1)^{\frac{1}{k}} - j^{\frac{1}{k}}).$$

Choose C so that $C^k D_k > 3$. Define $\mathbb{P}(x \in B) = p_x = C\frac{\log^{1/k}(x)}{x^{1-1/k}}$ if the right hand side is at most $1/2$, and 0 otherwise. Notice with this definition, if n is sufficiently large, then we only need to consider summands x where $p_x = C\frac{\log^{1/k}(x)}{x^{1-1/k}}$.

We are now ready to state our first result.

Proposition 3.2.3. *With the notation as in the above definition, we have* $\mu = \Theta(\log(n))$.

Proof. First note that

$$\mu = \sum_{\substack{x_1+\cdots+x_k=n \\ 1\leq x_1<\cdots<x_k}} p_{x_1}\cdots p_{x_k}$$

$$= \sum_{\substack{x_1+\cdots+x_k=n \\ 1\leq x_1<\cdots<x_k}} \left(C\frac{\log^{1/k}(x_1)}{x_1^{1-1/k}}\right)\left(C\frac{\log^{1/k}(x_2)}{x_2^{1-1/k}}\right)\cdots\left(C\frac{\log^{1/k}(x_k)}{x_k^{1-1/k}}\right).$$

We now break the sum into two parts. Let

$$\mathcal{F}_1 = \left\{(x_1,\cdots,x_k) \in B^k : \frac{n}{\log n} \leq x_1 < \cdots < x_k\right\}$$

and

$$\mathcal{F}_2 = \left\{(x_1,\cdots,x_k) \in B^k : x_1 < \cdots < x_k, x_1 \leq \frac{n}{\log n}\right\}.$$

Then define

$$\mu_1 = \sum_{\mathcal{F}_1}\left(C\frac{\log^{1/k} x_1}{x_1^{1-1/k}}\right)\left(C\frac{\log^{1/k} x_2}{x_2^{1-1/k}}\right)\cdots\left(C\frac{\log^{1/k} x_k}{x_k^{1-1/k}}\right)$$

and

$$\mu_2 = \sum_{\mathcal{F}_2} \left(C \frac{\log^{1/k} x_1}{x_1^{1-1/k}} \right) \left(C \frac{\log^{1/k} x_2}{x_2^{1-1/k}} \right) \cdots \left(C \frac{\log^{1/k} x_k}{x_k^{1-1/k}} \right).$$

Then it is clear that $\mu = \mu_1 + \mu_2$. Thus to show that $\mu = \Theta(\log n)$ it suffices to show that $\mu_1 = \Theta(\log n)$ and $\mu_2 = o(\log n)$.

By partial summation, we have

$$\begin{aligned} \mu_1 &= \sum_{\mathcal{F}_1} \left(C \frac{\log^{1/k} x_1}{x_1^{1-1/k}} \right) \left(C \frac{\log^{1/k} x_2}{x_2^{1-1/k}} \right) \cdots \left(C \frac{\log^{1/k} x_k}{x_k^{1-1/k}} \right) \\ &= C^k (1 + o(1))(\log n) \sum_{\mathcal{F}_1} \frac{1}{(x_1 \cdots x_k)^{(k-1)/k}}. \end{aligned}$$

Now set $S_1 = \displaystyle\sum_{\mathcal{F}_1} \frac{1}{(x_1 \cdots x_k)^{(k-1)/k}}$. It suffices to show that $S_1 = \Theta(1)$.

Now note that since x_k is the largest of the x_i's, and the summands are distinct, we have $x_k > \dfrac{n}{k}$. Hence we obtain the trivial bound

$$S_1 < \frac{1}{(n/k)^{(k-1)/k}} \sum_{\mathcal{F}_1} \frac{1}{(x_1 \cdots x_{k-1})^{(k-1)/k}}.$$

We can bound this latter sum by summing over all possible tuples $(x_1, \cdots, x_k) \in [1, n]^k$, and hence

$$S_1 < \frac{1}{(n/k)^{(k-1)/k}} \sum_{1 \le x_i \le n} \frac{1}{(x_1 \cdots x_k)^{(k-1)/k}} = \frac{1}{(n/k)^{(k-1)/k}} \left(\sum_{1 \le x \le n} \frac{1}{x^{(k-1)/k}} \right)^{k-1}.$$

Now note that the function $f(x) = \dfrac{1}{x^{(k-1)/k}}$ is strictly decreasing, and hence we can approximate the above sum by an integral. An elementary argument yields that

$$S_1 < \frac{1}{(n/k)^{(k-1)/k}} \left(\sum_{1 \le x \le n} \frac{1}{x^{(k-1)/k}} \right)^{k-1} \le \left(\frac{k}{n} \right)^{(k-1)/k} \left(\int_1^n \frac{dx}{x^{(k-1)/k}} + O(1) \right)^{k-1}$$

Evaluating the integral, we obtain

$$\left(\int_1^n \frac{dx}{x^{(k-1)/k}} + O(1) \right)^{k-1} = (kn^{1/k} + O(1))^{k-1} = k^{k-1}(n^{(k-1)/k} + o(n^{(k-1)/k})).$$

Thus we obtain the bound

$$S_1 < \left(\frac{k}{n} \right)^{(k-1)/k} (k^{k-1} n^{(k-1)/k} + o(n^{(k-1)/k})) = (1 + o(1)) k^{(k^2-1)/k}.$$

This shows that $\mu_1 = O(\log n)$. Now we seek to obtain a lower bound for μ_1. Note that $x_k < n$ vacuously, and hence the (also trivial) lower bound for S_1:

$$S_1 > \frac{1}{n^{(k-1)/k}} \sum_{\mathcal{F}_1} \frac{1}{(x_1 \cdots x_{k-1})^{(k-1)/k}}.$$

The objective again is to have a good lower bound for $\sum_{\mathcal{F}_1} \frac{1}{(x_1 \cdots x_{k-1})^{(k-1)/k}}$. Since the range of summation $\mathcal{F}_1$ is defined for $\frac{n}{\log n} \leq x_1 < \cdots < x_k$, we can only obtain a smaller sum by replacing $\mathcal{F}_1$ with the more restricting range $\mathcal{G}_1$ which is $\frac{n}{\log n} < x_1 < \frac{n}{k(k-1)}, \frac{n}{k(k-1)} < x_2 < \frac{2n}{k(k-1)}, \cdots, \frac{(k-2)n}{k(k-1)} < x_{k-1} < \frac{n}{k}$. Note that this restriction automatically forces $x_k > \frac{n}{k}$, and so $x_k > x_{k-1}$. Note that the sum

$$\sum_{\mathcal{G}_1} \frac{1}{(x_1 \cdots x_{k-1})^{(k-1)/k}}$$

can be factored into

$$\sum_{\frac{n}{\log n} < x_1 < \frac{n}{k(k-1)}} \frac{1}{x_1^{(k-1)/k}} \cdots \sum_{\frac{(k-2)n}{k(k-1)} < x_{k-1} < \frac{n}{k}} \frac{1}{x_{k-1}^{(k-1)/k}}.$$

Note that each of the sums involving x_i can be approximated by an integral that is easy to evaluate, and we obtain

$$\sum_{\frac{n}{\log n} < x_1 < \frac{n}{k(k-1)}} \frac{1}{x_1^{(k-1)/k}} \cdots \sum_{\frac{(k-2)n}{k(k-1)} < x_{k-1} < \frac{n}{k}} \frac{1}{x_{k-1}^{(k-1)/k}}$$

$$= \left(\int_{\frac{n}{\log n}}^{\frac{n}{k(k-1)}} \frac{dx_1}{x_1^{(k-1)/k}} + O(1) \right) \cdots \left(\int_{\frac{(k-2)n}{k(k-1)}}^{\frac{n}{k}} \frac{dx_{k-1}}{x_{k-1}^{(k-1)/k}} + O(1) \right)$$

$$= (1+o(1))k^{k-1} \left(\frac{n}{k(k-1)} \right)^{(k-1)/k} [1-(n/k(k-1)\log(n))^{1/k}][2^{1/k}-1] \cdots [(k-1)^{1/k}-(k-2)^{1/k}].$$

Dividing by $n^{(k-1)/k}$ and recalling the definition of D_k yields that

$$S_1 > D_k + o(1)$$

Which is a non-trivial lower bound indeed, since $D_k > 0$.

The above calculations combined yields the following information:

$$C^k(D_k + o(1)) \log n \leq \mu_1 \leq C^k(k^{(k^2-1)/k} + o(1)).$$

Now we direct our attention to μ_2. Recall that

$$\mu_2 = C^k \sum_{\mathcal{F}_2} \frac{(\log(x_1)\log(x_2)\cdots\log(x_k))^{1/k}}{(x_1 x_2 \cdots x_k)^{(k-1)/k}}.$$

Clearly, we have the inequality

$$\mu_2 < C^k \log n \sum_{\mathcal{F}_2} \frac{1}{(x_1 \cdots x_k)^{(k-1)/k}}.$$

Set

$$S_2 = \sum_{\mathcal{F}_2} \frac{1}{(x_1 \cdots x_k)^{(k-1)/k}}.$$

Then we want to show that $S_2 = o(1)$, as that would imply that $\mu_2 = o(\log n)$ which is what we want. The approach is very similar to getting the upper bound for S_1. Indeed, we can allow $1 \leq x_1 \leq \dfrac{n}{\log n}$, and $1 \leq x_i \leq n$ for $2 \leq i \leq k-1$, and bound $\dfrac{1}{x_k} < \dfrac{k}{n}$. We hence obtain the upper bound

$$S_2 < \left(\frac{k}{n}\right)^{(k-1)/k} \left(\sum_{1 \leq x_1 \leq \frac{n}{\log n}} \frac{1}{x_1^{(k-1)/k}} \right) \left(\sum_{1 \leq x_2 \leq n} \frac{1}{x_2^{(k-1)/k}} \right)^{k-2}.$$

Again we approximate by integrals to obtain

$$S_2 < \left(\frac{k}{n}\right)^{(k-1)/k} \left(\int_1^{\frac{n}{\log n}} \frac{dx_1}{x_1^{(k-1)/k}} + O(1) \right) \left(\int_1^{n} \frac{dx_2}{x_2^{(k-1)/k}} + O(1) \right)^{k-2}$$

$$= \left(\frac{k}{n}\right)^{(k-1)(k-2)/k} \left[\frac{1}{\log^{1/k} n} n^{(k-1)/k} + o\left(\frac{1}{\log^{1/k}(n)} n^{(k-1)/k} \right) \right].$$

This implies that

$$S_2 = O\left(\frac{1}{\log^{1/k} n} \right) = o(1).$$

Hence $\mu_2 = o(\log(n))$, as desired.

Combining the estimates for μ_1, μ_2, we get that $C^k(D_k + o(1)) \log n \leq \mu \leq C^k(k^{(k^2-1)/k} + o(1)) \log(n)$. This completes the proof of this propostion. □

Now that we have established that the expected value μ of our random variable $r_{B,k}(n)$ is of the right size, namely $\Theta(\log n)$, we have to prove that $r_{B,k}(n)$ is close to its expected value with high probability. Our next step will be to show that $r_{B,k}(n) = O(\log n)$ with high probability. We will finish the proof of the Erdős-Tetalli Theorem by showing that $r_{B,k}(n) = \Omega(\log n)$ as well.

To show that $r_{B,k}(n) = O(\log n)$ with high probability, let A_n be the event that $|r_{B,k}(n) > d\mu|$ for some constant $d > 0$. We will show that with an appropriate choice of d, we have $\displaystyle\sum_{n=1}^{\infty} \mathbb{P}(A_n) < \infty$. Then the Borel-Cantelli Lemma will apply to show

that with probability one at most finitely many of the A_n's occur.

We follow a similar strategy as in the proof of the previous proposition, namely we will break $r_{B,k}(n)$ into two components. First, we consider representations of n that are totally disjoint; meaning they do not share even one summand. Then we will consider representations with at least one overlap. The idea is to show that the disjoint representations make up the bulk of the representations, and the ones with overlap are negligible.

To do this, we first consider disjoint representations; that is, two representations $n = a_1 + \cdots + a_k = b_1 + \cdots + b_k$, and $a_i \neq b_j$ for $1 \leq i, j \leq k$. To do this we first need another probabilistic lemma, which is called the disjointness lemma.

Proposition 3.2.4. (Disjointness Lemma) *Suppose that $A_1, A_2, \cdots$ is a sequence of events such that $\sum_{n=1}^{\infty} \mathbb{P}(A_n) \leq u < \infty$. Then*

$$\sum_{\substack{\{A_1,\cdots,A_l\} \\ \mathbb{P}(A_1\cap\cdots\cap A_l)=\mathbb{P}(A_1)\cdots\mathbb{P}(A_l)}} \mathbb{P}(A_1 \cap \cdots \cap A_l) \leq \frac{u^l}{l!}.$$

Proof. The proof is elementary, but we provide it here for completeness. By independence, it follows that

$$\sum_{\substack{\{A_1,\cdots,A_l\} \\ \mathbb{P}(A_1\cap\cdots\cap A_l)=\mathbb{P}(A_1)\cdots\mathbb{P}(A_l)}} \mathbb{P}(A_1 \cap \cdots \cap A_l) = \sum_{\substack{\{A_1,\cdots,A_l\} \\ \mathbb{P}(A_1\cap\cdots\cap A_l)=\mathbb{P}(A_1)\cdots\mathbb{P}(A_l)}} \mathbb{P}(A_1)\cdots\mathbb{P}(A_l).$$

The latter is certainly bounded above by the sum over all $A_1, \cdots, A_l$ where each set is distinct, as opposed to only mutually independent ones, and hence we obtain

$$\sum_{\substack{\{A_1,\cdots,A_l\} \\ \mathbb{P}(A_1\cap\cdots\cap A_l)=\mathbb{P}(A_1)\cdots\mathbb{P}(A_l)}} \mathbb{P}(A_1)\cdots\mathbb{P}(A_l) \leq \sum_{\{A_1,\cdots,A_l\}} \mathbb{P}(A_1)\mathbb{P}(A_2)\cdots\mathbb{P}(A_l).$$

Since the latter sum is indexed by sets instead of tuples, we can adjust it to include permutations of $A_1, \cdots, A_l$ by multiplying by $\frac{1}{l!}$. Hence we obtain

$$\sum_{\{A_1,\cdots,A_l\}} \mathbb{P}(A_1)\mathbb{P}(A_2)\cdots\mathbb{P}(A_l) = \frac{1}{l!} \sum_{(A_1,\cdots,A_l)} \mathbb{P}(A_1)\cdots\mathbb{P}(A_l).$$

By the convergence of the series $\sum_{n=1}^{\infty} \mathbb{P}(A_n) \leq u < \infty$, we obtain

$$\frac{1}{l!} \sum_{(A_1,\cdots,A_l)} \mathbb{P}(A_1)\cdots\mathbb{P}(A_l) = \frac{1}{l!} \left(\sum_{n=1}^{\infty} \mathbb{P}(A_n) \right)^l \leq \frac{u^l}{l!}.$$

This completes the proof. □

Before we can use the disjointness lemma, we have to give some definitions. Essentially, to bypass the fact that our random variable $r_{B,k}(n)$ cannot be decomposed into a sum of independent random variables, we will pursue the following idea: first consider collections of representations $n = a_1 + \cdots + a_k = b_1 + \cdots + b_k$ where $a_i \neq b_j$ for $1 \leq i, j \leq k$, then show that contributions made by non-disjoint representations is small. Hence we are motivated to make the following definition:

Definition 3.2.5. Suppose $T_1 = \{a_1, \cdots, a_k\}, T_2 = \{b_1, \cdots, b_k\}$ with $T_1, T_2 \subset B$ where B is the random set we defined at the beginning of this section. Suppose that $n = a_1 + \cdots + a_k = b_1 + \cdots + b_k$. We say that T_1, T_2 are *disjoint representations* if $T_1 \cap T_2 = \emptyset$.

The idea of the following propositions is to show that there cannot be a collection of pairwise disjoint collections T_j. In particular, we will show that a maximal collection is of size $O(\log(n))$. We now prove the following corollary to the disjointness lemma.

Corollary 3.2.6. *Let $\mathcal{T}$ be a collection of pairwise disjoint sets T_j such that $\sum_{x \in T_j} x = n$. Then*

$$\sum_{\mathcal{T}} \mathbb{P}(T_1 \cap \cdots \cap T_{6\mu}) \leq \frac{\mu^{6\mu}}{(6\mu)!}.$$

Where we understand T_j to be the event that all elements of T_j are chosen to be in our random set B.

Proof. This is just the disjointness lemma with $u = \mu, l = 6\mu$. □

Set $r^*_{B,k}(n)$ to be the size of a maximal collection of pairwise disjoint representations. We will show that with the appropriate choice of our constant C, that $r^*_{B,k}(n)$ is bounded above by an absolute multiple of μ with high probability.

Proposition 3.2.7. *Choose $C > (1/3D_k)^{1/k}$. Then for all sufficiently large n we have $r^*_{B,k}(n) \leq 6\mu$ with probability 1.*

Proof. Let A_n denote the event that $r^*_{B,k}(n) > 6\mu$. Let $\mathcal{T}$ be as in the corollary above. Then surely, we have

$$\mathbb{P}(A_n) < \sum_{\mathcal{T}} \mathbb{P}(T_1 \cap \cdots \cap T_{6\mu}) \leq \frac{\mu^{6\mu}}{(6\mu)!}.$$

Now using Stirling's Formula [11], we have $m! \sim \sqrt{2\pi m}\left(\frac{m}{e}\right)^m$. We also have $m! > m^m e^{-m}$ for $m = 1, 2, \cdots$. Using this estimate, we obtain

$$\mathbb{P}(A_n) < \frac{1}{(6\mu/e)^{(6\mu)}} = \left(\frac{e}{6}\right)^{(6\mu)}.$$

Since we $e/6 < 1$, it follows that we have the bound $(e/6)^{6\mu} < (e/6)^{6(C^k(D_k + o(1)))\log(n)}$. Hence, we obtain

$$\mathbb{P}(A_n) < n^{-6C^k D_k + o(1)}.$$

By our choice of C, we see that $C^k D_k > 1/3$, so that

$$\mathbb{P}(A_n) < n^{-2+o(1)}.$$

Now the Borel-Cantelli Lemma applies, and we see that $\sum_{n=1}^{\infty} \mathbb{P}(A_n) < \infty$, so with probability one at most finitely many of the A_n's occur. This completes the proof. □

Remark 3.2.8. Our next step is to obtain a non-trivial bound on the number of representations of n as a sum of $k-1$ elements of our random set B. To see why this is needed, note the following argument: Let $\mathcal{T}$ be a maximal collection of disjoint representations. Then, we have proven that $|\mathcal{T}| = r^*_{B,k}(n) < 6\mu$. Since each representation contains exactly k elements, it follows that $\left|\bigcup_{T\in\mathcal{T}} T\right| < 6\mu k$. If we set $r_{B,k-1}(n)$ to be the number of ways that n can be written as the sum of $k-1$ elements of B, then for each x the number of representations that contain x is precisely $r_{B,k-1}(n-x)$. Thus if we obtain a uniform upper bound c on $r_{B,k-1}(n)$, then we can conclude that $r_{B,k}(n) < 6\mu kc = (6C^k k^{(k^2-1)/k} c + o(1))\log(n)$.

Thus to prove the appropriate upper bound for $r_{B,k}(n)$, it remains to show that $r_{B,k-1}(n)$ is bounded above. In fact, we will prove the following:

Proposition 3.2.9. *There exists a constant $c > 0$ such that $r_{B,k-1}(n) < c$ for all n almost surely.*

Proof. For $2 \le l \le k-1$, define $\mu_l = \mathbb{E}[r_{B,l}(n)]$. We will follow the same general strategy: we will show that μ_l has the right size, and then show that $r_{B,l}(n)$ is close to μ_l with high probability. Let $\mathcal{F}_l$ denote the set $\{(x_1, \cdots, x_l) \in B^l : x_1 + \cdots + x_l = n, 1 \le x_1 < \cdots < x_l < n\}$. Then we have

$$\begin{aligned}\mu_l &= \sum_{\mathcal{F}_l} \mathbb{P}(x_1 \in B) \cdots \mathbb{P}(x_l \in B) \\ &= \sum_{\mathcal{F}_l} C\left(\frac{\log(x_1)}{x_1^{k-1}}\right)^{1/k} \cdots C\left(\frac{\log(x_l)}{x_l^{k-1}}\right)^{1/k}.\end{aligned}$$

By arguments similar to those presented earlier, we can obtain the cruder estimate that

$$\mu_l = n^{o(1)} \sum_{\mathcal{F}_l} \left(\frac{1}{x_1^{k-1}}\right)^{1/k} \cdots \left(\frac{1}{x_l^{k-1}}\right)^{1/k} = n^{o(1)} S_l.$$

Using the bound $n/l < x_l$, we see that

$$S_l = n^{-(k-1)/k+o(1)} \sum_{\mathcal{F}_l} \frac{1}{(x_1 \cdots x_{l-1})^{(k-1)/k}}.$$

Again, we can estimate by replacing summation over $\mathcal{F}_l$ to summation over all $1 \leq x_i \leq n$, to obtain the bound

$$\begin{aligned} S_l &< n^{-(k-1)/k+o(1)} \sum_{\substack{1 \leq x_i \leq n \\ i=1,\cdots,l-1}} \frac{1}{(x_1 \cdots x_{l-1})^{(k-1)/k}} \\ &= n^{-(k-1)/k+o(1)} \left(\sum_{1 \leq x \leq n} \frac{1}{x^{(k-1)/k}} \right)^{l-1} \\ &= n^{-(k-1)/k+o(1)} (n^{1/k+o(1)})^{l-1} = n^{-1+l/k+o(1)}. \end{aligned}$$

Since $\mu_l = n^{o(1)} S_l$, it follows that $\mu_l \leq n^{-1+l/k+o(1)}$.

Now we will use another application of the disjointness lemma and the Borel-Cantelli Lemma to prove that, in fact, $r^*_{B,k-1}(n) < c$ almost surely. First, denote T_i^l denote a representation of n as the sum of l *distinct* numbers. Then, if T_i^l, T_j^l are *disjoint*, then they are in fact independent events (recall earlier that by an abuse of notation we treat the set T_i^l and the event that all elements in T_i^l are in B the same). Hence the disjointness lemma applies, and we see that summing over all collections of $\{T_1^l, \cdots, T_{2k}^l\}$, we obtain

$$\sum \mathbb{P}(T_1^l \cap \cdots \cap T_{2k}^l) < \frac{\mu_l^{2k}}{(2k)!}.$$

From this we obtain

$$\begin{aligned} \mathbb{P}(r^*_{B,l}(n) > 2k) &\leq \sum \mathbb{P}(T_1^l \cap \cdots \cap T_{2k}^l) \\ &< \frac{\mu_l^{2k}}{(2k)!} \\ &< \frac{(n^{-1+l/k+o(1)})^{2k}}{(2k)!} = n^{-2k+2l+o(1)}. \end{aligned}$$

Recall that $l \leq k-1$, and so $-2k+2l \leq -2$, and hence

$$\mathbb{P}(r^*_{B,l}(n) > 2k) < n^{-2+o(1)}.$$

Applying the Borel-Canteli Lemma to the events A_n such that $r^*_{B,l}(n) > 2k$, we obtain that almost surely $r^*_{B,l}(n) \leq 2k$ for n sufficiently large. Choosing a larger constant c_l if necessary, we also obtain that $r^*_{B,l}(n) \leq c_l$ almost surely.

Next we will show that $r_{B,k-1}(n)$ is bounded above by a constant almost surely. This will involve a clever application of the Sunflower Lemma, which was covered earlier in this section. Without further ado, we state and prove our next result.

We have established that for all $2 \leq l \leq k-1$ we have $r^*_{B,l}(n) < c_l$ almost surely for all n. Set $c_{\max} = \max\limits_{2 \leq l \leq k-1} \{c_l\}$. We claim that it suffices to set $c = (c_{\max})^{k-1}(k-1)!$.

We will establish this by contradiction. If the claim is false, then there exists a positive integer N for which $r_{B,k-1}(N) > c$ with positive probability. In particular, there are more than $(c_{\max})^{k-1}(k-1)!$ representations T_i^{k-1} of N with positive probability, and hence by the Sunflower Lemma there exists $c_{\max}+1$ representations $\{T_1^{k-1}, \cdots, T_{c_{\max}+1}^{k-1}\}$ forming a sunflower, with core R. Let $R = \{x_1, \cdots, x_r\}$, with $0 \leq r \leq k-2$. If $x_1 + \cdots + x_r = m$, then removing R from each of the T_i^{k-1} will yield at least $c_{\max}+1$ representations of $N-m$ as a sum of $k-r-1$ elements, contradicting the choice of $c_{\max}$. Hence the claim follows. □

By the remark earlier, we have now successfully proved that $r_{B,k}(n) = O(\log(n))$. To complete the proof of the Erdős-Tetali Theorem, it remains to show that $r_{B,k}(n) = \Omega(\log(n))$.

To do this, we would like to apply Janson's Inequality. To apply our version of Janson's Inequality, we define the random variables X_i such that $X_i = 1$ if $i \in B$, and $X_i = 0$ otherwise. By our definition of the random set B, it follows that the X_j's are jointly independent indicator random variables. Now, if we are interested in representations of n as a sum of k distinct numbers, denote T_j a representation of n as a sum of k distinct elements of B, and consider $X(n) = \sum_{T_j} \prod_{i \in T_j} X_i$. Note that $\prod_{i \in T_j} X_i = 1$ if and only if $T_j \subset B$, and hence $X(n) = r^*_{B,k}(n)$. Let $\mu^* = \mathbb{E}[r^*_{B,k}(n)]$. Then, by the notation used in proposition 3.2 (Janson's Inequality), we set $x = \varepsilon\mu^*$ and $\delta = \dfrac{\Delta}{\mu^*}$. We can then conclude the following:

$$\mathbb{P}(r^*_{B,k}(n) \leq (1-\varepsilon)\mu^*) \leq \exp\left(\frac{-2\varepsilon^2\mu^*}{2\delta}\right) \leq \exp\left(\frac{-2\varepsilon^2\mu^*}{1+\delta}\right).$$

We can then use this form of Janson's Inequality to prove that $r^*_{B,k}(n)$, and consequently $r_{B,k}(n)$, is $\Omega(\log(n))$ almost surely. To do this, we need a good bound on Δ. Indeed, we will show in the next proposition that $\Delta = o(1)$.

Proposition 3.2.10. *Let T_j, X_i be as above. Recall that we have $\Delta(X_1, \cdots, X_n) = \sum_{T_s, T_t, T_s \cap T_t \neq \emptyset} \mathbb{E}\left(\prod_{i \in T_s \cup T_t} X_i\right)$. In this setting we have*

$$\Delta = o(1).$$

Proof. Say $T_s \sim T_t$ if they share at least one element in common and at most $k-2$ elements in common (for if they share $k-1$ elements in common then they are in fact the same). Then we can rewrite Δ as

$$\Delta = \sum_{T_s \sim T_t} \mathbb{P}(T_s \cap T_t).$$

To see this, note that $\prod_{i\in T_s\cup T_t} X_i = 1$ if and only if $i \in B$ for every i in $T_s \cup T_t$, in other words $T_s \cup T_t \subset B$, or that the events T_s, T_t both happened. Thus the probability that $\prod_{i\in T_s\cup T_t} X_i = 1$ is precisely the probability that both $T_s, T_t \subset B$.

Now, we can organize the sum by the size of the intersection of $T_s \cap T_t$. Indeed, we have

$$\sum_{T_s\sim T_t} \mathbb{P}(T_s \cap T_t) = \sum_{l=1}^{k-2} \sum_{|T_s\cap T_t|=l} \mathbb{P}(T_s \cap T_t).$$

Now consider T_s, T_t such that $|T_s \cap T_t| = l$. Write $T_s = \{z_1, \cdots, z_l, x_1, \cdots, x_{k-l}\}$ and $T_t = \{z_1, \cdots, z_l, y_1, \cdots, y_{k-l}\}$. Write $z_1 + \cdots + z_l = m$. Then $x_1 + \cdots + x_l = y_1 + \cdots + y_l = n - m$. Thus, we have the rather unpleasant decomposition

$$\sum_{|T_s\cap T_t|=l} \mathbb{P}(T_s \cap T_t) = \sum_m \sum_{\substack{z_1+\cdots+z_l=m \\ x_1+\cdots+x_{k-l}=n-m \\ y_1+\cdots+y_{k-l}=n-m}} [p_{z_1}\cdots p_{z_l}][p_{x_1}\cdots p_{x_{k-l}}][p_{y_1}\cdots p_{y_{k-l}}].$$

By disjointness and hence independence, we can rewrite the right hand side as

$$\sum_m \left(\sum_{z_1+\cdots+z_l=m} p_{z_1}\cdots p_{z_l}\right)\left(\sum_{x_1+\cdots+x_{k-l}=n-m} p_{x_1}\cdots p_{x_l}\right)^2 = \sum_m \mu_l(m)[\mu_{k-l}(n-m)]^2.$$

As shown in proposition 3.11, for $\varepsilon < l/2k$ we can choose m_0 such that $\mu_l \le n^{-1+l/k+\varepsilon}$ for $1 \le l \le k-1$ and all $m > m_0$. Then we will break the latter sum into four pieces: s_1, s_2, s_3, s_4, respectively over the ranges $m \le m_0$, $m_0 < m \le n/2$, $n/2 < m < n - m_0$, and $n - m_0 \le m$. Note that since m_0 is fixed, we have $\mu_l(m) < M$ for some fixed constant M. The first sum is

$$s_1 = \sum_{m\le m_0} \mu_l(m)[\mu_{k-l}(n-m)]^2 < n^{-2+2(k-l)/k+o(1)} \sum_{m\le m_0} M = n^{-2+2(k-l)/k+o(1)} = o(1),$$

since $l < k$.

The second sum is

$$s_2 = \sum_{m_0<m\le n/2} \mu_l(m)[\mu_{k-l}(n-m)]^2 < n^{-2+2(k-l)/k+o(1)} \sum_{m_0<m\le n/2} m^{-1+l/k+\varepsilon}.$$

We can estimate the last sum by an integral, as usual, by noting that

$$\sum_{m_0<m\le n/2} m^{-1+l/k+\varepsilon} < \sum_{m\le n} m^{-1+l/k+\varepsilon} = \int_0^n x^{-1+k/l+\varepsilon}dx + O(1) = n^{l/k+\varepsilon} + O(1).$$

Using this estimate, we get

$$s_2 < n^{-l/k+\varepsilon+o(1)},$$

and since $\varepsilon < l/2k$ we see that $s_2 = o(1)$.

Now we estimate s_3 by

$$s_3 = \sum_{n/2<m\leq n-m_0} \mu_l(m)[\mu_{k-l}(n-m)]^2 < n^{-1+l/k+o(1)} \sum_{n/2<m\leq n-m_0} (n-m)^{-2+2(k-l)/k+2\varepsilon}.$$

Again, by bounding the last sum from above by a very generous integral estimate, we get

$$\sum_{n/2<m\leq n-m_0} (n-m)^{-2+2(k-l)/k+2\varepsilon} < \int_0^n (n-x)^{-2+2(k-l)/k+2\varepsilon} dx + O(1) = n^{1-2l/k+2\varepsilon} + O(1).$$

And so, we get

$$s_3 < n^{-l/k+2\varepsilon+o(1)}.$$

But $\varepsilon < l/2k$, so $s_3 = o(1)$.

Finally, we estimate s_4.

$$s_4 = \sum_{m>n-m_0} \mu_l(m)[\mu_{k-l}(n-m)]^2 < n^{-1+l/k+o(1)} \sum_{m>n-m_0} M^2.$$

But since $m \leq n$, we see that there are only finitely many choices of m (depending on m_0 only) such that $m > n-m_0$, and so the last sum is a constant. Thus, $s_4 = o(1)$.

Since $\Delta = s_1 + s_2 + s_3 + s_4$, we see that $\Delta = o(1)$, which is what we wanted to prove. □

Now that we have shown that the T_i's are 'weakly' correlated, we can apply Janson's Inequality to finish the proof of the Erdős-Tetali Theorem.

Proof. (Lower bound on $r_{B,k}(n)$) By proposition 3.5, we have $\mu > C^k(D_k + o(1))\log(n)$. Let $0 < \varepsilon < 1$. Apply Janson's Inequality to get

$$\mathbb{P}(r^*_{B,k}(n) \leq (1-\varepsilon)\mu) \leq \mathbb{P}(r_{B,k}(n) \leq (1-\varepsilon)\mu) \leq \exp\left(\frac{-\varepsilon(C^k(D_k + o(1))\log(n))}{1+\delta}\right).$$

Since $\delta = \Delta/\mu^*$, we have $\delta = o(1)$. Thus, by choosing $C^k D_k > 4$ and controlling ε, we see that $\mathbb{P}(r_{B,k}(n) \leq (1-\varepsilon)\mu) < n^{-2+o(1)}$ eventually, so that by Borel-Cantelli at most finitely many of these events occur. Hence almost surely we have $r_{B,k}(n) > C'\log(n)$ for some constant C', which establishes our lower bound. □

Hence we have shown that $r_{B,k}(n) = \Theta(\log(n))$ almost surely, and so there exists a particular set B that is in fact a thin basis.

However, there are some further questions that remains to be answered. First, can we improve the Θ to an asymptotic? That is, does there exist a thin basis B such

that $r_{B,k}(n) \sim c\log(n)$ for some constant $c > 0$? Or we can ask a weaker question and see if there exist a thin basis B such that $c_1 \log(n) \leq r_{B,k}(n) \leq c_2 \log(n)$, but c_1, c_2 can be made arbitrarily close. Neither of these questions have been answered in the literature. The difficulty it seems is that the probabilistic method of Erdős remains the only effective way to generate a thin basis, and unfortunately when using exponential type bounds such as Janson's Inequality or Chernoff's Inequality, the constants c_1, c_2 matter as one needs to achieve a $n^{-\alpha}, \alpha > 1$ type bound on the bad events to apply Borel-Cantelli. Because one requires the control of the constants c_1, c_2 to use the Borel-Cantelli Lemma, it does not seem easy to answer either of the two questions above without a stronger inequality.

Another question is whether one can explicitly construct a thin basis B. This seems to be a very difficult problem. It seems a notoriously difficult problem in additive number theory to prove that an explicitly given set is indeed a basis, since it is often an extremely non-trivial task to find a good lower bound (at the very least, eventually positive) for the function $r_{B,k}(n)$. Indeed, finding a non-trivial lower bound for $r_{\mathcal{P},2}(n)$ where $\mathcal{P}$ is the set of primes amounts to resolving the infamous Goldbach Conjecture. The two most famous bases in the literature, being the Waring bases and the primes, are both very 'thick' bases. Hence one can see the difficulty in showing that a specific set is indeed a thin basis, since it would likely be extremely hard to get a good lower bound on something that is already very small.

Though it seems difficult to give a specific example of a thin basis, one can hope that a thin basis can be computed effectively. Indeed this is possible, and we will give Kolountzakis' proof that an effective thin basis exists in section 5.

As per conjecture 1.3, we see that Erdős conjectured that in fact bases cannot be arbitrarily thin in the sense that $r_{B,k}(n)$ cannot approach infinity much slower than $\log n$. Thus another important question to ask is the following: given a set A that is known to be a basis of order k, can we then show that it must necessarily contain a thin basis B? Of course, one cannot hope for $r_{B,k}(n) = \Theta(\log(n))$ since there are easy obstructions to this (take, for example, the set $A = \{1\} \cup \{2\} \cup \{3k : k \in \mathbb{N}\}$. Then A is clearly an additive basis of order 2; but $r_{A,2}(3k+1) = r_{A,2}(3k+2) = 1$ for all $k \geq 1$). However, one might hope for a sub-basis B with $r_{B,k}(n) = O(\log(n))$. Even this modest question is very difficult. Fortunately, there has been some progress on this, and we will give Van Vu's application of the probabilistic method to show that there is a thin sub-basis in any Waring basis in the next chapter.

Chapter 4

Thin Subbases of Waring Bases

4.1 A relatively thin sub-basis for the set of squares

In this chapter we identify some progress made towards resolving Erdős's stronger conjecture (Conjecture 1.0.3), namely to show that the representation function of an additive basis cannot tend arbitrarily slowly towards infinity. One way to address this problem is to extract a thin basis B from a given basis A, which may not be thin. This turns out to be a very difficult problem in general, but if the given basis A is sufficiently thick, then it is possible to extract a thin basis from it. In this section we will present some results by Nathanson, Erdős, and Vu regarding the existence of thin subbases in the Waring bases.

By classical results of Hardy, Littlewood, and Vinogradov, we can see that if $B = \mathbb{N}^r$ for some $r > 1$, we can choose $k > r$ such that B is an additive basis of order k and $r_{B,k}(n)$ is large. In particular, we have the following result due to Vinogradov [19]

Theorem 4.1.1. *For any fixed positive integer $r \geq 2$, there exists a constant $k_1(r)$ such that for all $k > k_1(r)$ then*

$$r_{\mathbb{N}^r,k}(n) = \Theta(n^{\frac{k}{r}-1})$$

for every $n \in \mathbb{N}$.

The integer powers are attractive because they provide natural examples of additive bases with relatively low density. In all of the results presented in this section, the number theoretic properties of $\mathbb{N}^r = \{n^r : n \in \mathbb{N}\}$ will be essential; and so there is little hope of generalizing these ideas to relatively sparse additive bases B whose number theoretic properties are not well understood or available without some significant paradigm shift.

Meanwhile, Wirsing in [26] gave a general result that proves any additive basis B with a sufficiently high natural density while satisfying some regularity conditions also contain thin sub-bases, but in order for his results to be relevant the function

$r_{B,k}(n)$ has to be very large. Nevertheless, the primes satisfy the hypotheses in Wirsing's theorem. We will discuss Wirsing's result in the next section.

We begin the discourse in this section with a result due to Nathanson, Choi, and Erdős, found in [19]. Recall what is widely accepted as the first result in additive number theory, which is Lagrange's theorem that $\mathbb{N}^2$ is an additive basis of order 4. Also recall that the set of squares is a 'thick' basis in the following sense: if B is an additive basis of order h, then we would expect that

$$\sum_{n \leq N} r_{B,h}(n) \leq |B \cap [1, N]|^h \leq \sum_{n \leq hN} r_{B,h}(n)$$

or in other words

$$N^{1/h} \leq |B \cap [1, N]|.$$

If $B = \mathbb{N}^2$, we have $h = 4$ and $|B \cap [1, N]| = N^{1/2+o(1)}$. This is much larger than the lower bound of $N^{1/4}$, which justifies why the squares are not 'thin'. Indeed, it was asked whether it is possible to find a subset B of the squares that is thin in the sense that $|B \cap [1, N]|/N^{1/2} \to 0$. This is a much weaker requirement then the desired result of $|B \cap [1, N]| = N^{1/4+o(1)}$, but nonetheless represents an advancement. We will present the following result due to Nathanson, Choi, and Erdős [19]. Here we work with a slightly different context, more similar to the previous subsection. In particular, instead of asserting that a set A is an additive basis for $\mathbb{N}$, we look at sets A_N which are additive bases for the set $\{1, \cdots, N\}$. We begin with a definition along these lines.

Definition 4.1.2. Let $N, h \geq 1$ be a positive integer. Let $A_{N,h} \subset \{0, \cdots, N\}$, and $r_{A_{N,h}}(n)$ be the number of ways of writing n as a sum of h elements from $A_{N,h}$. We say that $A_{N,h}$ is an *additive basis* of order h for N if $r_{A,N,h}(n) > 0$ for $n = 1, \cdots, N$. If h is understood, then we simply write A_N or $r_{A_N}(n)$.

The essence of this theorem is to start with all of the squares up to $4N^{2/3}$, then show that only a small portion of squares between $4N^{2/3}$ and N is needed to form a basis for N. This proof heavily relies on the number theoretic properties of the squares. However, the benefit is that we obtain an explicit construction, which is preferable to the existential proofs obtained via the probabilistic method.

Theorem 4.1.3. *For every $N \geq 2$, there exists a set $A_N \subset \mathbb{N}^2$ such that A_N is an additive basis of order 4 for N and*

$$|A_N| \leq \left(\frac{4}{\log 2}\right) N^{1/3} \log N.$$

Proof. Note that this proof is quite elementary and does not appeal to the probabilistic method. We will begin by stating that $A_2 = A_3 = \{0, 1\}$ and $A_4 = A_5 = \{0, 1, 4\}$ satisfies the requirements of the theorem for $N = 2, 3, 4, 5$. It suffices to assume that $N \geq 6$ from now on.

By the characterization of those numbers that are the sum of three squares (see Theorem 2.2.1), we see that if $l \equiv 1, 2 \pmod 4$ then l can be written as the sum of three squares. $a^2 \equiv 0 \pmod 4$ if a is even and $a^2 \equiv 1 \pmod 4$ if a is odd, it follows that if $m \not\equiv 0 \pmod 4$ and a is a positive integer such that $a^2 \leq m$, then either $m - a^2$ is the sum of three squares or $m - (a-1)^2$ is the sum of three squares.

For $N \geq 6$, denote by $A_N^{(1)}$ the set of squares of all non-negative integers up to $2N^{1/3}$. Then it is plain that

$$|A_N^{(1)}| \leq 2N^{1/3} + 1.$$

Let $A_N^{(2)}$ be the set of squares of all integers of the form

$$\lfloor k^{1/2} N^{1/3} \rfloor, \lfloor k^{1/2} N^{1/3} \rfloor - 1,$$

where

$$4 \leq k \leq N^{1/3}.$$

Then

$$|A_N^{(2)}| \leq 2(N^{1/3} - 3) = 2N^{1/3} - 6.$$

Set $A_N^{(0)} = A_N^{(1)} \cup A_N^{(2)}$. Then we have

$$|A_N^{(0)}| < 4N^{1/3}.$$

Since $A_N^{(0)}$ contains all of the squares up to $4N^{2/3}$, then Lagrange's Theorem implies that every non-negative integer up to $4N^{2/3}$ is the sum of four squares in $A_N^{(0)}$.

Let m be an integer satisfying

$$4N^{2/3} < m \leq N, m \not\equiv 0 \pmod 4.$$

We now find $a_0 \in A_N^{(2)}$ such that

$$0 \leq m - a_0^2 \leq 4N^{2/3}$$

and $m - a_0^2$ is the sum of three squares. We have

$$4 \leq k = \left\lfloor \frac{m}{N^{2/3}} \right\rfloor \leq N^{1/3}.$$

Set $a = \lfloor k^{1/2} N^{1/3} \rfloor$. Then $a^2 \in A_N^{(2)}, (a-1)^2 \in A_N^{(2)}$,

$$a^2 \leq kN^{2/3} \leq m < (k+1)N^{2/3},$$

with

$$a > k^{1/2} N^{1/3} - 1.$$

It now suffices to choose $a_0^2 \in \{a^2, (a-1)^2\} \subset A_N^{(2)}$ so that $m - a_0^2$ is a sum of three squares, which is possible by the remark at the beginning of this proof. Since $N \geq 6$ we have $4 < 3N^{1/6}$, so we have

$$\begin{aligned} 0 \leq m - a^2 &\leq m - a_0^2 \leq m - (a-1)^2 \\ &< (k+1)N^{2/3} - (k^{1/2}N^{1/3} - 2)^2 \\ &< (k+1)N^{2/3} - kN^{2/3} + 4k^{1/2}N^{1/3} \\ &= N^{2/3} + 4k^{1/2}N^{1/3} \\ &\leq N^{2/3} + 4N^{1/2} \\ &< 4N^{2/3}. \end{aligned}$$

This shows that $m - a_0^2$ is the sum of three squares in $A_N^{(1)}$. Consequently, if $0 \leq m \leq N$ and $m \not\equiv 0 \pmod 4$, then m is the sum of four squares belonging to $A_N^{(0)}$. Now set

$$A_N = \left\{ (2^i a)^2 : 0 \leq i \leq \frac{\log N}{\log 4}, a \in A_N^{(0)} \right\}.$$

Therefore A_N is a set of squares and

$$\begin{aligned} |A_N| &\leq \left(\frac{\log N}{\log 4} + 1 \right) |A_N^{(0)}| \\ &< \left(\frac{2 \log N}{\log 4} \right) 4N^{1/3} \\ &= \left(\frac{4}{\log 2} \right) N^{1/3} \log N. \end{aligned}$$

Let $n \in \{0, 1, \cdots, N\}$. If $n \not\equiv 0 \pmod 4$, then we demonstrated that n is the sum of four squares in $A_N^{(0)} \subset A_N$. If $n \equiv 0 \pmod 4$, then $n = 4^i m, m \not\equiv \pmod 4$ and $0 \leq i \leq \log(N)/\log(4)$. Then

$$m = a_1^2 + a_2^2 + a_3^2 + a_4^2, a_1, a_2, a_3, a_4 \in A_N^{(0)}.$$

This shows that

$$n = 4^i m = (2^i a_1)^2 + (2^i a_2)^2 + (2^i a_3)^2 + (2^i a_4)^2.$$

Hence n is the sum of four squares belonging to A_N. This completes the proof. □

The above example shows that specific number theoretic information about the squares is essential. After some success in find thin sub-bases of the squares, Nathanson asked [25] whether there exist a thin sub-basis of all sufficiently large orders for all Waring bases. The question was partially answered by Wirsing in [26] but was conclusively answered by Vu in [25]. In subsequent subsections we will introduce Vu's work proving that all Waring bases $\mathbb{N}^r$ contain thin sub-bases of all sufficiently large orders.

4.2 Polynomial concentration results

The construction of thin sub-bases in the Waring bases is part of a much more general framework. The fundamental breakthrough that allowed Erdős and Tetali to generalize Erdős's method used to prove a thin basis of order 2 exists to all orders k and Vu's proof of the existence of thin sub-bases in the Waring bases relies on proving results stating when certain polynomials of indicator random variables are tightly concentrated about their mean. The results in this subsection can be seen as generalizations of Chernoff's Inequality as well as Janson's inequality.

The results in this subsection are motivated by the following classical inequality found in [22].

Theorem 4.2.1. (Lipschitz concentration inequality) *Let $Y : \{0,1\}^n \to \mathbb{R}$ be a function such that $|Y(s) - Y(t)| \leq K$ whenever $s, t \in \{0,1\}^n$ differ in only one coordinate. Then if $X_1, \cdots, X_n$ are independent indicator random variables, we have*

$$\mathbb{P}(|Y(X_1, \cdots, X_n) - \mathbb{E}[Y(X_1, \cdots, X_n)]| \geq \lambda K\sqrt{n}) \leq 2e^{-\lambda^2/2}$$

for all $\lambda > 0$.

This result can be compared with Hoeffding's inequality (proposition 2.21) in that if we have a good bound on the influence of each indicator random variable X_j on Y, then Y is concentrated within $O(K\sqrt{n})$ of its mean. A proof of this result can be found in [22].

However, the Lipschitz-type control over the random variable Y is very stringent. One can see that if we have good control over the partial derivatives of Y with respect to each X_j, then the conditions of the theorem would apply. This is often not the case in applications to number theory, particularly with thin bases. Hence we will need to weaken the hypotheses and obtain good bounds in more specific settings. We will now present a few definitions and results due to Vu in [25].

Definition 4.2.2. Let $X_1, \cdots, X_n$ be indicator random variables. We say that Y is *totally positive* if all of its coefficients are non-negative, and that Y is *regular* if all of its coefficients are between 0 and 1. We also say that Y is *simplified* if its monomials are square-free, that is does not contain a term of the form X_j^2 for any $1 \leq j \leq n$. We say that Y is homogeneous if all of its monomials have the same degree.

Definition 4.2.3. For any non-negative integers $\alpha_1, \cdots, \alpha_n$ define the *multi-index* α by $\alpha = (\alpha_1, \cdots, \alpha_n)$. Define the partial derivative $\partial^\alpha(Y)$ with respect to the multi-index α as

$$\partial^\alpha(Y) = \left(\frac{\partial}{\partial X_1}\right)^{\alpha_1} \cdots \left(\frac{\partial}{\partial X_n}\right)^{\alpha_n} Y(X_1, \cdots, X_n),$$

and denote the *order* of α to be

$$|\alpha| = \alpha_1 + \cdots + \alpha_n.$$

Definition 4.2.4. Let $d \in \mathbb{N} \cup \{0\}$. Denote by $\mathbb{E}_d[Y]$ the maximum value of all expected values of partial derivatives of Y of order d. That is,

$$\mathbb{E}_d[Y] = \max_{\alpha:|\alpha|=d} \mathbb{E}[\partial^\alpha Y].$$

One sees immediately that $\mathbb{E}_0[Y] = \mathbb{E}Y$ and $\mathbb{E}_d[Y] = 0$ for d exceeding the degree of Y.

Theorem 4.2.5. (Vu) *Let $n, k \in \mathbb{N}$ and $\beta, \xi, \varepsilon > 0$. Consider jointly independent indicator random variables $X_1, \cdots, X_n$. Let $Q = Q(k, \varepsilon, \beta, \xi)$ be a large constant independent of n. If $Y = Y(X_1, \cdots, X_n)$ is a regular homogeneous polynomial (not necessarily simplified) of degree k and satisfies the expectation bounds*

$$Q \log n \leq \mathbb{E}Y \leq n/Q;\ \mathbb{E}_1(Y), \cdots, \mathbb{E}_{k-1}(Y) \leq n^{-\xi},$$

then

$$\mathbb{P}(|Y - \mathbb{E}Y| \geq \varepsilon \mathbb{E}Y) \leq n^{-\beta}.$$

As a consequence to the proof of the above theorem is the following, which will be the main tool to establish thin sub-bases in Waring bases.

Theorem 4.2.6. *Suppose $X_1, \cdots, X_n$ are jointly independent indicator random variables. Set $\partial^\alpha_* Y(t) = \partial^\alpha Y(t) - \partial^\alpha Y(0)$. Let $Y = Y(X_1, \cdots, X_n)$ be a simplified regular (not necessarily homogeneous) polynomial such that for all multi-index α and some $\gamma > 0$*

$$\mathbb{E}(\partial^\alpha_* Y) \leq n^{-\gamma}.$$

Then, for any $\beta > 0$ we can find a constant $K = K_{\beta,\gamma}$, independent of n and Y, such that we have the bound

$$\mathbb{P}(Y \geq K_{\beta,\gamma}) < n^{-\beta}.$$

The above two results are consequences of the main theorem in [25]. Since the main theorem and its proof is highly technical and only the theorems mentioned above are needed for showing the existence of thin sub-bases in the Waring bases, we refer the reader to [16] and [25] for details on the proof.

We note that the above theorems can be adapted to prove the Erdős-Tetali theorem. Indeed, one can easily see that the Erdős-Tetali theorem is simply a special case of Vu's result in [24]. We now proceed to present the main result of this section.

4.3 Thin Waring bases

Due to the length of this proof, we begin this subsection with some comments. The main ingredients of the proof here are the probabilistic method of Erdős, Vinogradov's Theorem giving an asymptotic for $r_{\mathbb{N}^r,k}(n)$ [19], the polynomial concentration results of Kim and Vu [16][25], and a technical lemma in [24] that gives a bound on the number of solutions in "boxes" $[1, P_1] \times \cdots \times [1, P_s]$ for positive integers $P_1, \cdots, P_s$.

Let $r \geq 2$ be fixed, and consider $\mathbb{N}_0^r$. We begin with introducing a random subset $B \subset \mathbb{N}_0^r$ defined as follows

Definition 4.3.1. For $r \geq 2, r \in \mathbb{N}$ define the random set $B \subset \mathbb{N}_0^r$ by the following

$$x \in \mathbb{N}_0; p_x = \mathbb{P}(x^r \in B) = x^{-1+k/r} \log^{1/k}(x).$$

Here $k > r$ is a large positive integer such that $\mathbb{N}_0^r$ is an additive basis of order k.

Definition 4.3.2. Let B be the random set defined above. Let X_j be the indicator random variable such that $X_j = 1$ if and only if $j^r \in B$.

Now we can see that we can write $r_{B,k}(n)$ as a polynomial in $\{X_1, \cdots, X_{\lfloor n^{1/r} \rfloor}\}$. In particular, we have

$$r_{B,k}(n) = \sum_{x_1^r + \cdots + x_k^r = n} \prod_{j=1}^{k} X_{x_j}.$$

As was done in the case of the Erdős-Tetalli theorem, we proceed as follows. First, we break up $r_{B,k}(n)$ into two parts μ_1 and μ_2, and show that $\mu_1 = \Theta(\log n)$ while $\mu_2 = o(\log n)$. Then we show, for some small $\varepsilon > 0$, that with probability at least $1 - O(1/n^2)$ we have

$$1 - \varepsilon \leq \frac{r_{B,k}(n)}{\mathbb{E}[r_{B,k}(n)]} \leq 1 + \varepsilon.$$

The Borel-Cantelli Lemma then applies at once, showing that B is indeed an additive basis of order k.

We examine $\mathbb{E}[r_{B,k}(n)]$ to see what issues arise as we write $\mu = \mathbb{E}[r_{B,k}(n)]$ and see that

$$\mu = \sum_{x_1^r + \cdots + x_k^r = n} c^k \prod_{j=1}^{k} x_j^{-1+r/k} \log^{1/k}(x_j).$$

Heuristically, one expects that since $x_1^r + \cdots + x_k^r = n$ that each of the x_j to be of order $\Theta(n^{1/r})$. Hence, we would expect the term $c^k \prod_{j=1}^{k} x_j^{-1+r/k} \log^{1/k}(x_j)$ be of order $\Theta(n^{k/r(-1+r/k)} \log n) = \Theta(n^{-k/r+1} \log n)$. This together with Vinogradov's Theorem that there should be $\Theta(n^{\frac{k}{r}-1})$ summands, yields that $\mu = \Theta(\log n)$. This naive approach is dashed when one considers sums of the form $x_1^r + \cdots + x_k^r = n$ where x_1 is very small, say $x_1 = O(n^\delta)$ for some $\delta < 1/r$. The remedy for this problem is to split μ into two parts.

Vu in [24] circumvented the problem with sums $x_1^r + \cdots + x_k^r = n$ with small x_1 by obtaining estimates for the number of tuples $(x_1, \cdots, x_k), x_1^r + \cdots + x_k^r = n$ in

boxes. That is, for any positive integers $P_1, \cdots, P_k$, we obtain estimates for the number of solutions to $x_1^r + \cdots + x_k^r = n$ with $1 \leq x_1 \leq P_1, \cdots, 1 \leq x_k \leq P_k$. We denote

$$R(P_1, \cdots, P_k)(n) = \#\{(x_1, \cdots, x_k) : x_1^r + \cdots + x_k^r = n, 1 \leq x_1 \leq P_1, \cdots, 1 \leq x_k \leq P_k\}.$$

The main work horse for our approach is the following result, which is the main lemma in [24]. Due to its length and technicality we will not present the full proof, but rather a sketch of the main ideas, including applying the Hardy-Littlewood circle method.

Theorem 4.3.3. (Vu's main lemma in [24]) *For fixed $r \geq 2$, there exists a constant $k_3(r) = O(8^k k^2)$ such that the following holds: For any $k > k_3(r)$ there is a positive constant $\delta = \delta(r, k)$ such that for every finite sequence of positive integers $P_1, \cdots, P_k$ and all $n \in \mathbb{N}$, we have*

$$R(P_1, \cdots, P_k)(n) = O\left(n^{-1} \prod_{j=1}^{k} P_j + \prod_{j=1}^{k} P_j^{1-r/k-\delta}\right).$$

As mentioned before, the proof of the above result relies on the Hardy-Littlewood circle method. In fact, the circle method was originally introduced to tackle Waring's problem, which was first solved by Hilbert. The idea is that one can naturally encode additive problems using generating functions. In particular, if we start with a set $A = \{a_0, a_1, \cdots, \} \subset \mathbb{N}_0$, we can consider the *generating function* of A as

$$f(z) = \sum_{n=0}^{\infty} z^{a_n}.$$

Then one can easily see that

$$(f(z))^k = \left(\sum_{n=0}^{\infty} z^{a_n}\right)^k = \sum_{n=0}^{\infty} r_{A,k}(n) z^n.$$

We can restrict $f(z)$ to the unit circle (hence the term 'circle method'). Set $e^{2\pi i\alpha} = e(\alpha)$. Note that $r_{A,k}(n)$ is the n-th Fourier coefficient of the series $f(e(\alpha))^k$. That is, we have the equality

$$r_{A,k}(n) = \int_0^1 f(e(\alpha))^k e(-n\alpha) d\alpha.$$

The key to applying this method is to evaluate the integral on the right hand side. This technique was devised by Hardy and Littlewood (hence its namesake) but vastly improved by Vinogradov [19]. Vinogradov's key insight was that one can replace the series $f(z)$ with a finite truncation, say

$$f_N(z) = \sum_{n=0}^{N} z^{a_n}.$$

For fixed n, we can choose a large N so that the j-th coefficient of $(f_N(z))^k$ for $0 \leq j \leq n$ is equal to $r_{A,k}(j)$. This truncation allows one to forget about issues of convergence and usually makes estimating the integral much easier. Nonetheless, Hardy and Littlewood's original insight was to break the unit circle into 'major arcs' and 'minor arcs'. The idea is that the integral over the major arcs is the main contribution to $r_{A,k}(n)$ and the integral over the minor arcs is negligible.

Let $P_1, \cdots, P_k$ be positive integers. Define, for each j, the function $f_j(\alpha) = \sum_{m=1}^{P_j} e(\alpha m^r)$. Then we have

$$R(P_1, \cdots, P_k)(n) = \int_0^1 \prod_{j=1}^{k} f_j(\alpha) e(-n\alpha) d\alpha.$$

The difficulty of estimating this integral is the possibility that the sequence $P_1, \cdots, P_k$ can be very irregular. Thus a good definition of major and minor arcs has to account for any information available regarding the P_j's. This leads to a convoluted definition below. First, we introduce some constants. Let ν, τ, χ be defined as follows

$$\nu = \frac{1}{2(26(2^{r-1}) + 17)}, \tau = \frac{7\nu}{2r}, \chi = \frac{(26(2^{r-1}) + 4)\nu}{r}.$$

Set $k_3(r) = d2^{3r-3}r^2 = O(8^r r^2)$, where d is chosen so that for all $k > k_3(r)$ the following inequality holds

$$\frac{\tau\nu k}{\sum_{j=1}^{k} \frac{1}{j}} \geq 2^{r-1}(r+1). \tag{4.3.1}$$

We will need the following lemma in order to properly define the major and minor arcs.

Proposition 4.3.4. *Let $k > k_3(r)$ and $P_1, \cdots, P_k$ be positive integers, with τ, ν, χ defined as above. Set $P = \prod_{j=1}^{k} P_j$. Then there is a $1 \leq j \leq k$ such that*

$$P_j \geq P^{\frac{1}{k}(1-\tau) + \frac{2^{r-1}(r+1)}{\nu k(k-j+1)}}.$$

Proof. We will prove this by contradiction. Suppose that the inequality fails for all $1 \leq j \leq k$. Then, multiplying from $j = 1$ to $j = k$ we obtain

$$P < P^{(1-\tau) + \frac{2^{r-1}(r+1)}{\nu k} \sum_{j=1}^{k} \frac{1}{k-j+1}} = P^{(1-\tau) + \frac{2^{r-1}(r+1)}{\nu k} \sum_{j=1}^{k} \frac{1}{j}}.$$

This implies that $\tau < \frac{2^{r-1}(r+1)}{\nu k} \sum_{j=1}^{k} \frac{1}{j}$, which contradicts equation (4.3.1). □

Let l be the smallest index j that satisfies the inequality in the above proposition. It follows at once that

$$P_l^{(k-l+1)\nu} \geq P^{2^{r-1}(r+1)/k}, P_l \geq P^{\frac{1}{s}(1-\tau)}. \tag{4.3.2}$$

Finally, we are ready to define the arcs. Set $\rho = P_l^{\nu}$ and $B = P_l^{r-\nu}$. For $1 \leq a < q \leq \rho$ with $(a,q) = 1$, define $I_{a,q} = (a/q - B^{-1}, a/q + B^{-1})$. The intervals $I_{a,q}$ will be the *major arcs*, and $\mathfrak{M}$ will be their union. The set $\mathfrak{m} = [0,1] \setminus \mathfrak{M}$ is called the *minor arcs*.

We will prove that the contribution of the minor arcs is of the same order of magnitude as the second term in the estimate in theorem 4.12. For the major arc contributions please refer to [24]. We will need to first state a classic result due to Weyl [19].

Theorem 4.3.5. (Weyl's inequality) *Let $f(x) = \alpha x^r + \cdots$ be a polynomial of degree $r \geq 2$ with real coefficients, and suppose that α has the rational approximation a/q with $q \geq 1, (a,q) = 1$ and*

$$\left| \alpha - \frac{a}{q} \right| \leq \frac{1}{q^2}.$$

Let $S(f) = \sum_{m=1}^{N} e(f(m))$ and set $\varepsilon > 0$. Then

$$S(f) \ll N^{1+\varepsilon}(N^{-1} + q^{-1} + N^{-r}q)^{1/2^{r-1}}.$$

In particular, the result holds for $f(x) = \alpha x^r$.

The proof of this result can be found in [19]. We now proceed to prove the bound for the minor arcs.

Proposition 4.3.6. *Let $f_j(\alpha) = \sum_{m=1}^{P_j} e(\alpha m^r)$, and set $g(\alpha) = \prod_{j=1}^{k} f_j(\alpha)$. Then there is a positive constant $\delta = \delta(r,k)$ such that*

$$\left| \int_{\mathfrak{m}} g(\alpha) e(-n\alpha) d\alpha \right| = O(P^{1-r/k-\delta}).$$

Proof. Suppose $\alpha \in \mathfrak{m}$. Then by Dirichlet's lemma, there exists a, q such that $(a,q) = 1, \rho \leq q \leq B$ and $|a/q - \alpha| \leq 1/q^2$. By Weyl's inequality, for all $j \geq l$ we have

$$|f_j(\alpha)| \leq P_j(q^{-1} + P_j^{-1} + qP_j^{-r})^{1/2^{r-1}} = O(P_j q^{-1/2^{r-1}}).$$

On the other hand, for $j < l$ we have $|f_j(\alpha)| \leq P_j$. We now have

$$\left| \int_{\mathfrak{m}} g(\alpha) e(-n\alpha) d\alpha \right| \leq \max_{\alpha \in \mathfrak{m}} |g(\alpha)|$$

$$= O\left(\prod_{j=1}^{l-1} P_j \prod_{j=l}^{k} (P_j q^{-1/2^{r-1}}) \right) = O(Pq^{-(k-l+1)/2^{r-1}}).$$

Since $q \geq \rho = P_l^{\nu}$, by (4.2) we have

$$q^{-(k-l+1)/2^{r-1}} \leq P_l^{-\nu(k-l+1)/2^{r-1}} \leq P^{-(r+1)/k}.$$

It now suffices to set $\delta = 1/k$. This completes the proof. □

The major arcs estimate requires a series of very technical and tedious lemmas, which is why the constants ν, τ, χ were chosen the way that they were. The details are found in [25]. Nevertheless, the result obtained is recorded here

Proposition 4.3.7. *There is a positive constant $\delta = \delta(r,k)$ such that for every sequence $2 \leq P_1 \leq P_2 \leq \cdots \leq P_k = n^{1/r}$ and $P = \prod_{j=1}^{k} P_j$ we have*

$$\left| \int_{\mathfrak{M}} g(\alpha) e(-n\alpha) d\alpha \right| = O(Pn^{-1} + P^{1-r/k-\delta}).$$

We proceed now in the same manner as in proposition 3.2.3 to establish the estimate for $\mu = \mathbb{E}[r_{B,k}(n)]$. We will require some preliminary definitions. As always, we adopt the convention that $x_1 \leq x_2 \leq \cdots \leq x_k$.

Definition 4.3.8. Define

$$\mathcal{S}_1 = \{(x_1, \cdots, x_k) : \sum_{j=1}^{k} x_j^r = n, x_j \in \mathbb{N}_0, x_1 \geq n^{1/kr}\}$$

and

$$\mathcal{S}_2 = \{(x_1, \cdots, x_k) : \sum_{j=1}^{k} x_j^r = n, x_j \in \mathbb{N}_0, x_1 < n^{1/kr}\}.$$

Further, we will set

$$\mathcal{F}_1 = \mathcal{S}_1 \cap B, \mathcal{F}_2 = \mathcal{S}_2 \cap B$$

where $B \subset \mathbb{N}_0^r$ is our random set.

Definition 4.3.9. Define

$$\mu_1 = \sum_{\mathcal{S}_1} c^k \prod_{j=1}^{k} x_j^{-1+r/k} \log^{1/k}(x_j),$$

and

$$\mu_2 = \sum_{\mathcal{S}_2} c^k \prod_{j=1}^{k} x_j^{-1+r/k} \log^{1/k}(x_j).$$

It is clear that $\mu = \mu_1 + \mu_2$.

We write $F(X_1, \cdots, X_{\lfloor n^{1/r} \rfloor}) = \sum_{(x_1,\cdots,x_k)\in\mathcal{S}_1} \prod_{j=1}^{k} X_{x_j}$. We will apply the polynomial concentration results to control the size of F. We proceed to prove some necessary propositions first.

Proposition 4.3.10. *If $k > k_3(r)$, then for all m*

$$Y_{k,m} = \sum_{m=x_1^r+\cdots+x_k^r} \left(\prod_{j=1}^{k} x_j \right)^{-1+r/k} = O(1).$$

Proof. We will decompose $Y_{k,m}$ into dyadic subsums. Let $\mathcal{P}$ denote the set of k-tuples $\{P_1, \cdots, P_k\}$ where $P_j \in \{2, 4, \cdots, 2^t\}$ where 2^t is the smallest power of 2 larger than $m^{1/r}$. If $A = \{P_1, \cdots, P_k\} \in \mathcal{P}$, let σ_A denote the subsum of $Y_{k,m}$ taken over all k-tuples $(x_1, \cdots, x_k)$ satisfying $P_j/2 \leq x_j \leq P_j$ for all $1 \leq j \leq k$. It follows that

$$Y_{k,m} \leq \sum_{A \in \mathcal{P}} \sigma_A.$$

Let $P_A = \prod_{P_j \in A} P_j$. By definition, we see that each term in σ_A is of order $\Theta(P_A^{-1+r/k})$. By Theorem 4.3.3, the number of terms in σ_A is $O(P_A m^{-1} + P_A^{1-r/k-\delta})$. Hence, we have

$$\sigma_A = O(P_A^{r/k} m^{-1} + P_A^{-\delta}).$$

We can improve the second term by the following argument. If $P_A < (m/k)^{1/r}$, then $\sigma_A = 0$ since there are no solutions to $x_1^r + \cdots + x_k^r = m$ with $x_1 \leq P_1, \cdots, x_k \leq P_k$. Hence we lose nothing by assuming $P_A \geq (m/k)^{1/r}$ and so $P_A^{-\delta} \leq (m/k)^{-\delta/r}$. This shows that for some $\eta > 0$ we have

$$\sigma_A = O(P_A^{r/k} m^{-1} + m^{-\eta}).$$

Now, by construction, there are at most $O(\log^k m)$ elements in $\mathcal{P}$. This implies

$$\sum_{A \in \mathcal{P}} \sigma_A = O\left(m^{-1} \sum_{A \in \mathcal{P}} P_A^{r/k} + m^{-\eta} \log^k m \right).$$

The second term on the right hand side is $o(1)$. The first term can be estimated as follows:

$$\sum_{A \in \mathcal{P}} P_A^{r/k} \leq \left(2^{r/k} + 2^{2(r/k)} + \cdots 2^{t(r/k)}\right)^k$$

$$< \left(\frac{2^{(t+1)(r/k)}}{2^{r/k} - 1} \right)^k \ll 2^{r(t+1)} < (4m^{1/r})^r = O(m).$$

This proves the required estimate. □

Again, just like in the proof of the Erdős-Tetali theorem, we show that $r_{B,s}(n)$ is small when $s < k$. We formalize this as the following proposition.

Proposition 4.3.11. *Suppose $k > rk_3(r)$. Then there is a positive constant $\gamma > 0$ such that $\mathbb{E}[r_{B,s}(m)] = O(m^{-\gamma})$ for $1 \leq s < k$.*

Proof. It suffices to show that there exists $\gamma > 0$ such that

$$Z_{s,m} = \sum_{m = x_1^r + \cdots + x_s^r} \left(\prod_{j=1}^{s} x_j \right)^{-1+r/k} = O(m^{-\gamma}),$$

since the log terms are negligible compared to $m^{-\gamma}$. If $s > k_3(r)$, the previous proposition applies and we have $x_s \leq (m/s)^{1/r}$, so

$$Z_{s,m} \leq Y_{s,m} \left(\frac{m}{s}\right)^{\frac{1}{r}(r/k - r/s)} = O(m^{-(k-s)/ks})$$

and we are done. If $s \leq k_3(r)$, then since $k > rk_3(r)$ we see that $s/k < 1/r$. Again, from $x_s \geq (m/s)^{1/r}$ we obtain

$$Z_{s,m} = O\left(m^{\frac{1}{r}(-1+r/k)} \left(\sum_{x=1}^{m^{1/r}} x^{-1+r/k}\right)^{s-1}\right).$$

This is an upper bound. As in the case with the Erdős-Tetali theorem we can approximate the sum by an integral. To wit, we have

$$\sum_{x=1}^{m^{1/r}} x^{-1+r/k} = \int_1^{m^{1/r}} x^{-1+r/k} dx + O(1) = O(m^{1/k}).$$

So we have

$$Z_{s,m} = O(m^{-1/r+1/k+(s-1)/k}) = O(m^{-(1/r-s/k)}).$$

Since $s/k < 1/r$, we are done. □

Proposition 4.3.12. *With k sufficiently large, we have $\mu_1 = \Theta(\log n)$.*

Proof. Note that $\prod_{j=1}^{k} \log^{1/k}(x_j) \leq \log n$ for all $x_1 \leq \cdots \leq x_k$ such that $x_1^r + \cdots + x_k^r = n$. Hence, $\mu = O(\log n)$ follows from proposition 4.3.10.

To get the lower bound, by convexity we have that the contribution of a term $(x_1, \cdots, x_k)$ with $x_j \neq 0, 1$ is

$$\prod_{j=1}^{k} c x_j^{-1+r/k} \log^{1/k}(x_j) \geq c^k (n/k)^{\frac{k}{r}\left(\frac{r}{k}-1\right)} \log(n/k).$$

By Vinogradov's Theorem, there are $\Theta(n^{\frac{k}{r}-1})$ terms that do not contain $x_j = 0, 1$, and we are done. □

Remark 4.3.13. We note that by choosing c large, we can assume that $\mu_1/\log(n)$ is arbitrarily large.

Recall that $F(X_1, \cdots, X_{\lfloor n^{1/r} \rfloor}) = \sum_{(x_1,\cdots,x_k)\in\mathcal{S}_1} \prod_{j=1}^{k} X_{x_j}$. We will now prove that $F = \Theta(\log n)$.

Theorem 4.3.14. *Almost surely, we have*

$$F(X_1, \cdots, X_{\lfloor n^{1/r} \rfloor}) = \sum_{(x_1,\cdots,x_k)\in\mathcal{S}_1} \prod_{j=1}^{k} X_{x_j} = \Theta(\log n).$$

Proof. From proposition 4.3.12, we see that there exist constants c_1, c_2 such that

$$c_1 \log n \leq \mathbb{E}[F] \leq c_2 \log n.$$

Consider a set $A = \{i_1, \cdots, i_s\}$, with $i_j \in \{1, 2, \cdots, \lfloor n^{1/r} \rfloor\}$ and $s \leq k-1$. Let $m = n - \sum_{y\in A} y^k$ and $l = k - |A|$. Consider the partial derivative of F with respect to A

$$\partial_A(F) = \frac{\partial^{|A|} F}{\partial X_{i_1} \cdots \partial X_{i_s}}.$$

From the definition of $Z_{l,m}$, we see that

$$\mathbb{E}[\partial_A(F)] = \mathbb{E}\left[\sum_{(x_1,\cdots,x_k)\in\mathcal{F}_1 A\subset\{x_1,\cdots,x_k\}} \prod_{x_j\in\{x_1,\cdots,x_k\}\setminus A} X_{x_j}\right]$$

$$= O(Z_{l,m} \log n) = O(m^{-\gamma})$$

for some positive γ. Recall that $\mathcal{S}_1$ consists of solutions with $x_1^r \geq n^{1/k}$, it follows that if $|A| < k$ then $m \geq x_1^r \geq n^{1/k}$. This implies that

$$\mathbb{E}[\partial_A(F)] = O(n^{-\gamma/k}) = O(n^{-\xi})$$

for all A with $1 \leq |A| \leq k-1$ and $\xi = \gamma/k$.

Now we are ready to apply Theorem 4.2.5. By remark 4.3.13, we can choose c and consequently c_1 so that

$$c_1 > Q(k, \varepsilon, 2r, \xi)$$

In which case we get

$$\mathbb{P}(|F - \mathbb{E}[F]| \geq \varepsilon \mathbb{E}[F]) \leq n^{-2r}$$

Then the Borel-Cantelli Lemma applies and we see that almost surely $F = \Theta(\log n)$ for all sufficiently large n. This completes the proof. □

We now show that μ_2 is small.

Proposition 4.3.15. *There exists a positive constant $\gamma > 0$ such that $\mu_2 = O(n^{-\gamma})$.*

Proof. Recall that if $(x_1, \cdots, x_k) \in \mathcal{S}_2$, then $x_1 < n^{1/rk}$. Hence, we have

$$\mu_2 = O(\log n) \sum_{(x_1,\cdots,x_k)\in\mathcal{S}_2} \prod_{j=1}^{k} x_j^{r/k-1}$$

$$= O\left(\log n \sum_{x=1}^{n^{1/rk}} x^{-1+r/k} \max_{n-n^{1/k} \leq m \leq n} Z_{k-1,m}\right).$$

By proposition 4.20 and the fact that $m > n/2$, we see that $Z_{k-1,m} = O(n^{-1/k(k-1)})$. We can also approximate the sum in the above estimate by integrals to yield

$$\sum_{x=1}^{n^{1/rk}} x^{-1+r/k} = O(n^{1/k^2}).$$

Since $\dfrac{1}{k(k-1)} - \dfrac{1}{k^2} > 0$, we see that $\mu_2 = O(n^{-\gamma})$ as desired. □

Now an application of the disjointness lemma and the sunflower lemma as in the proof of the Erdős-Tetali theorem in section 3 yields the main result. For the specific details, see [24].

Currently, this is the best result we have on extracting a thin basis from a 'not-so-thick' additive basis. It is not known if other additive bases with similar densities as $\mathbb{N}_0^r$ contain thin subbases, since the highly technical and essential number theoretic arguments here would not apply. Another point to note is that the threshold that is essential in this proof, namely $k_3(r) = O(8^r r^2)$, is far from optimal. In a 2003 paper [27], T. D. Wooley proved that in fact one can take the threshold down to only $O(r \log r)$. His arguments essentially refined the circle method arguments used by Vu.

The results presented here can be adapted to prove the Erdős-Tetali theorem. However, the proof is not much simpler in this case. The main difference is the use of polynomial concentration results instead of appealing to Janson's Inequality.

We now turn our attention to the final section of this paper where we discuss computational aspects of the Erdős-Turán conjecture. In particular, we will see Kolountzakis' result that one can compute a set in polynomial time, where with probability one the resulting set will be an additive basis of order 2. Next we will see Borwein, Choi, and Chu's decisive result that if B is an additive basis of order 2, then $r_{B,2}(n)$ cannot be bounded above by 7. This is the most conclusive result we have regarding the Erdős-Turán conjecture to date. Their arguments are somewhat similar to the circle method arguments we gave above, but resort to computation rather than estimating integrals over major and minor arcs.

Chapter 5

Computational and Algorithmic Results

5.1 Effective thin basis of order 2

In the previous sections we established the existence of additive bases B with the property that $r_{B,2}(n) = \Theta(\log(n))$. However, it is not clear what any particular B looks like. Indeed, a large part of the arguments to show the existence of such bases is to use the Borel-Cantelli Lemma, which asserts that almost surely only finitely many of the bad events occur. However, there is no information on how big the threshold is after which the bad events no longer happen.

Prior to his 1956 result, proved using the probabilistic method, Erdős was able to use a counting argument to produce an additive basis B with $0 < r_{B,2}(n) < c \log n$ for some $c > 0$ in [5]. One can convert this argument into an algorithm to produce such a basis. Unfortunately, it is clear from the proof that such an algorithm is exponential in complexity. In this subsection we give a result that shows a thin basis B can in fact be computed effectively in polynomial time. The result is due to Kolountzakis in [17]. We note, however, that there does not seem to be an analogous result for bases of higher order.

The main result of this subsection will be to construct an algorithm which gives the elements of a thin basis B one by one, so that the time it takes to generate all elements of $B \cap [1, k]$ is polynomial in k. To this end, define $g(n) = n^{1/2} \log^{1/2}(n)$ and $R_B(n) = \#\{(x, y) \in B^2 : g(n) \leq x \leq y, x + y = n\}$. Then we claim the following:

Proposition 5.1.1. *There exist positive constants c_1, c_2, c_3 with $c_2 < c_3$ such that one can find a set B with the following two properties simultaneously:*

$$c_2 \log(n) \leq R_B(n) \leq c_3 \log(n),$$

for sufficiently large n, and

$$|B \cap [n - g(n), n]| \leq c_1 \log(n).$$

Proof. As usual, we first define the random set B by setting

$$\mathbb{P}(x \in B) = p_x = C\left(\frac{\log(x)}{x}\right)^{1/2}.$$

Where the event $x \in B$ is independent for distinct $x \in \mathbb{N}$. The strategy, of course, is to show that with high probability the random set so defined satisfies the two conditions in the proposition with appropriately chosen constants. Again, we define

$$\mu = \mathbb{E}[R_B(n)] = \sum_{x=g(n)}^{n/2} p_x p_{n-x}.$$

We introduce another notation to deal with the second condition in the proposition, namely

$$s(n) = |B \cap [n - g(n), n]|.$$

Further, it is convenient to define

$$\nu = \mathbb{E}[s(n)] = \sum_{x=n-g(n)}^{n} p_x.$$

Now, we will follow a familiar strategy: we will show that μ, ν are the sizes that we want, and show that the two random variables are both tightly concentrated to their means, and thus establish the proposition.

We first obtain an estimate for μ. Note that for large n, we have $g(n) < \dfrac{n}{\log(n)}$, and hence

$$\begin{aligned}\mu &\geq \sum_{x=n/\log n}^{n/2} C\left(\frac{\log x}{x}\right)^{1/2} C\left(\frac{\log(n-x)}{n-x}\right)^{1/2} \\ &\geq C^2 \log\left(\frac{n}{\log n}\right) \sum_{x=n/\log n}^{n/2} (x(n-x))^{-1/2}.\end{aligned}$$

But we see that $\displaystyle\sum_{x=n/\log n}^{n/2} (x(n-x))^{-1/2} = \int_0^{1/2} (x(1-x))^{-1/2} dx + O(1)$, as per our our results in section 2, and choosing $k_2 < C^2 \displaystyle\int_0^{1/2} (x(1-x))^{-1/2} dx$ we obtain the lower bound

$$\mu \geq k_2 \log n.$$

Likewise, we see that

$$\mu \leq C^2 \log(n/2) \sum_{x=1}^{n/2} (x(n-x))^{-1/2}$$

Thus, choosing $k_3 > C^2(x(1-x))^{-1/2}dx$ we see that

$$\mu \leq k_3 \log(n).$$

This confirms that μ is of the right size.

The estimates for ν are even easier, as we see that

$$Cg(n)\left(\frac{\log(n-g(n))}{n}\right)^{1/2} \leq \nu \leq Cg(n)\left(\frac{\log n}{n-g(n)}\right)^{1/2}.$$

This shows immediately that $\nu = (1+o(1))C\log n$.

Now define A_n to be the event that $|R_B(n) - \mu| > \varepsilon\mu$ and C_n to be the even that $|s(n) - \nu| > \varepsilon\nu$. Since $R_B(n), s(n)$ are sums of jointly independent indicator random variables, we can apply Chernoff's Inequality to obtain

$$\mathbb{P}(A_n) \leq 2\exp(-c_\varepsilon \mu) = 2n^{-\alpha},$$

and

$$\mathbb{P}(C_n) \leq 2\exp(-c_\varepsilon \nu) = 2n^{-\beta},$$

where $\alpha = \frac{1}{2}c_\varepsilon C^2 \int_0^{1/2} (x(1-x))^{-1/2}dx$ and $\beta = \frac{1}{2}c_\varepsilon C$. Choose $\varepsilon = 1/2$ and C sufficiently large so that $\alpha, \beta > 1$. Recall from chapter 1 that c_ε depends only on and can be effectively computed given ε, and hence C can also be effectively computed given ε. Then, we have that

$$\sum_{n=1}^{\infty} [\mathbb{P}(A_n) + \mathbb{P}(C_n)] < \infty,$$

and consequently the Borel-Cantelli Lemma applies, and so with probability 1 at most finitely many of the events A_n, C_n occur. And so there exists n_0 such that for all $n \geq n_0$ we have $\mu/2 \leq R_B(n) \leq 3\mu/2$ and $s(n) \leq 3\nu/2$. Since n_0 depends solely on C, ε, it can be effectively computed given these two quantities. Also, in the language of the proposition, we may set $c_1 = C/2$, $c_2 = \frac{C}{2}\int_0^{1/2} (x(1-x))^{-1/2}dx$, and $c_3 = \frac{3C}{2}\int_0^{1/2} (x(1-x))^{-1/2}dx$. This completes the proof. □

Now that we have established that a candidate set B exists with positive probability, we give an algorithm to compute such a B. To do this, we identify B as an element of $\{0,1\}^{\mathbb{N}}$. Our algorithm will output either a 0 or 1 at the n-th iteration to indicate whether n is in B or not.

Let $\chi = \{\chi_1, \chi_2, \cdots\} \in \{0,1\}^{\mathbb{N}}$ be a generic element, and let $E(a_1, \cdots, a_k)$ be the event that $\chi_1 = a_1, \chi_2 = a_2, \cdots, \chi_k = a_k$, where $a_1, \cdots, a_k \in \{0,1\}$. Let n_0 be the

threshold for which $\sum_{n\geq n_0}[\mathbb{P}(A_n)+\mathbb{P}(C_n)]<1$. Now, we wish to construct a sequence $\{a_k\}$ so that

$$\{b_k\}=b_k(a_1,\cdots,a_k)=\sum_{n\geq n_0}[\mathbb{P}(A_n|E(a_1,\cdots,a_k))+\mathbb{P}(C_n|E(a_1,\cdots,a_k))]$$

is non-increasing. Since $\{b_n\}$ is constructed to be monotone (non-increasing), we see from the condition that $\mathbb{P}(A_n)+\mathbb{P}(C_n)$ being summable that

$$\sum_{n\geq n_0}[\mathbb{P}(A_n|E(a_1,\cdots,a_k,\cdots))+\mathbb{P}(C_n|E(a_1,\cdots,a_k,\cdots))]<1.$$

But each of the probabilities $\mathbb{P}(A_n|E(a_1,\cdots,a_k,\cdots)),\mathbb{P}(C_n|E(a_1,\cdots,a_k,\cdots))\in\{0,1\}$, so this inequality implies that they are all zero. In particlar, the point $\chi=(a_1,\cdots,a_k,\cdots)$ is not in the union of "bad" events $\bigcup_{n\geq n_0}(A_n\cup C_n)$.

Hence our task is to choose $\{a_k\}$ so that $\{b_k\}$ does not increase. Notice that we have the following recursion for $\{b_k\}$:

$$b_{k-1}(a_1,\cdots,a_{k-1})=p_kb_k(a_1,\cdots,a_{k-1},1)+(1-p_k)b_k(a_1,\cdots,a_{k-1},0).$$

Since all quantities above are non-negative, it follows that at least one of $b_k(a_1,\cdots,a_{k-1},1)$ and $b_k(a_1,\cdots,a_{k-1},0)$ is not greater than $b_{k-1}(a_1,\cdots,a_{k-1})$. Choose $a_k=1$ if the first is smaller than the latter, and $a_k=0$ otherwise.

Define $\xi=b_k(a_1,\cdots,a_{k-1},1)-b_k(a_1,\cdots,a_{k-1},0)$. Let $G(k)$ be the largest integer x such that $g(x)\leq k$. Then we obtain

$$\xi=\sum_{n=k}^{G(k)}[\mathbb{P}(A_n|E(a_1,\cdots,a_{k-1},1))-\mathbb{P}(A_n|E(a_1,\cdots,a_{k-1},0))]$$

$$+\sum_{n=k}^{G(k)}[\mathbb{P}(C_n|E(a_1,\cdots,a_{k-1},1))-\mathbb{P}(C_n|E(a_1,\cdots,a_{k-1},0))].$$

To see this, note that A_n,C_n with $n>G(k)$ are independent of $a_1,\cdots,a_k$, by the definition of the random variables $R_B(n),s(n)$. Hence their contribution to the sum cancels. Note that $G(k)=\dfrac{(1+o(1))k^2}{\log(k)}$, and that ξ contains $\dfrac{(1+o(1))k^2}{\log(k)}$ summands. Our objective is to decide if $\xi\geq 0$ in polynomial time in k. This is possible as long as we can compute each summand in polynomial time. We will show that this is indeed possible in the next proposition.

Proposition 5.1.2. *Let $X=X(k)=X_1+\cdots+X_k$ be a sum of jointly independent indicator random variables, where $\mathbb{P}(X_j=1)=p_j$ for $j=1,2,\cdots,k$. Then the distribution of X can be computed in polynomial time in k.*

Proof. Note that $\mathbb{P}(X = k) = \prod_{j=1}^{k} p_j$, and $\mathbb{P}(X = 0) = \prod_{j=1}^{k}(1 - p_j)$. Otherwise, we have the recursion $\mathbb{P}(X = j) = p_k\mathbb{P}(X(k-1) = j-1) + (1-p_k)\mathbb{P}(X(k-1) = j)$. We can eventually reduce this expression into a polynomial in $p_1, \cdots, p_k$, which can certainly be computed in polynomial time in k, say $O(f(k))$ where $f(k)$ is a polynomial. Further, X takes on values in $\{0, 1, \cdots, k\}$, and the distribution of X can be computed in polynomial time, namely $O((k+1)f(k))$. □

Now, as we noted, both $R_B(n), s(n)$ are sums of jointly independent indicator random variables. This means that the events $[A_n|E(a_1, \cdots, a_k)], [B_n|E(a_1, \cdots, a_k)]$ can be computed efficiently, and this establishes the existence of the desired algorithm.

Again, we see that the requirement of expressing a desired random variable as the sum of jointly independent indicator random variables. This immediately means that the same argument will not work verbatim for bases of higher order, unless proposition 5.2 can be generalized in a non-trivial way to cases where X is not the sum of jointly independent indicator random variables but nonetheless the correlation between summands is small, akin to how Janson's Inequality extends Chernoff's Inequality.

5.2 A partial Erdős-Turán result: $r_{B,2}(n)$ cannot be bounded by 7

So far, we have discussed many results relating to the probabilistic argument of Erdős, while only tangentially touching on the main conjectures we are concerned with. This difficulty cannot be avoided as it is probably fair to say that currently no one has a clue as to how to attack either of the main conjectures (Conjectures 1.2 and 1.3). However, there is a rather old result of Dirac [3] that states $r_{B,2}(n)$ cannot be eventually constant. A much more recent result by Borwein, Choi, and Chu in 2006 asserts that in fact, $r_{B,2}(n)$ cannot be bounded from above by 7. We give this result in this subsection.

We can rephrase the Erdős-Turán conjecture as follows: if $B \subset \mathbb{N} \cup \{0\}$ is an additive basis, and let $B = \{\beta_n\}_{n=0}^{\infty}$. Then the generating function for B is simply

$$f(z) = \sum_{n=0}^{\infty} z^{\beta_n}.$$

It is clear that

$$f^2(z) = \left(\sum_{n=0}^{\infty} z^{\beta_n}\right)^2 = \sum_{n=0}^{\infty} r_{B,2}(n) z^n.$$

And, as we will see more of in section 5 when we discuss the Hardy-Littlewood circle method, we can in fact replace f with a polynomial trunction, namely $f_N(z) =$

$\sum_{n=0}^{N} z^{\beta_n}$, and we see that

$$f_N^2(z) = a_0 + \cdots + a_{2\beta_N} z^{2\beta_N},$$

and $a_n = r_{B,2}(n)$ for all $n \leq \beta_N$. This is the key simplification that allows the arguments of this subsection to work. In fact, our main result in this section is the following:

Theorem 5.2.1. *Let $B \subset \mathbb{N} \cup \{0\}$ be an additive basis. Then $r_{B,2}(n) \geq 8$ for all sufficiently large n.*

The proof of this theorem is remarkably simple. The idea is to show that an upper bound k on $r_{B,2}(n)$ is equivalent to showing that a certain class $E(k)$ of polynomials contains infinitely many members. One can use an exhaustive computer search to verify that $E(7)$ is in fact finite, and thus obtaining the bound. This will also give a program to prove the Erdős-Turán conjecture, which we will give later in this section. We will proceed with a few propositions.

Proposition 5.2.2. *Consider the truncated polynomial $f_N(z) = \sum_{n=0}^{N} z^{\beta_n}$ and $(f_N(z))^2 = \sum_{n=0}^{2\beta_N} a_n(N) z^n$. Then for all n we have $a_n(N) \leq a_n(N+1)$, and $a_n(N) = a_n(N+1)$ for $n = 0, 1, \cdots, \beta_N$.*

Proof. The proof is almost entirely clear. By increasing N, the number of representations can only increase, and for $n = 0, 1, \cdots, \beta_N$ we see that n cannot be written as anything bigger than β_N, and hence increasing N would not increase the number of representations of n. □

As we remarked earlier, proving the main theorem of this subsection amounts to counting certain classes of polynomials. To this end, we have the following definition and proposition.

Definition 5.2.3. Let $E_N(k)$ denote the set of polynomials with the following properties: each element of $E_N(k)$ is of the form

$$f_N(z) = \sum_{n=0}^{N} z^{\beta_n},$$

where $0 = \beta_0 < \beta_1 < \cdots < \beta_N$. Also we have for

$$(f_N(z))^2 = \sum_{n=0}^{2\beta_N} a_n(N) z^n,$$

that $a_n(N) > 0$ for $n = 0, 1, \cdots, \beta_N$, and $a_n(N) \leq k$ for $0 \leq n \leq 2\beta_N$.

Proposition 5.2.4. *With $E_N(k)$ defined as above, each element $p(z) \in E_N(k)$ is an extension of an element $q(z) \in E_{N-1}(k)$ of at most one more than twice the degree. That is, we have*

$$p(z) = z^\gamma + q(z),$$

where $\deg(q) < \gamma \leq 2\deg(q) + 1$. *In particular, for all $p(z) \in E_N(k)$, we have* $\deg(p) \leq N^2 + 2N - 2$ *and*

$$|E_N(k)| \leq (N^2 - 2)|E_{N-1}(k)|.$$

Proof. Suppose $f_N(z) = 1 + z^{\beta_1} + \cdots + z^{\beta_N} \in E_N(k)$, with $0 = \beta_0 < \beta_1 < \cdots < \beta_N$, then from the previous lemma we have that $a_n(N-1) \leq a_n(N) \leq k$ for all n and $a_n(N-1) = a_n(N) > 0$ for $n = 1, 2, \cdots, \beta_{N-1}$. In particular, $f_{N-1}(z) = 1 + z^{\beta_1} + \cdots + z^{\beta_{N-1}} \in E_{N-1}(k)$, and $f_N(z) = z^{\beta_N} + f_{N-1}(z)$. Now suppose that $\beta_N > 2\beta_{N-1}+1$. Then $\beta_i+\beta_j < 2\beta_{N-1}+1$ for $0 \leq i, j \leq N-1$ and $\beta_n+\beta_N > 2\beta_{N-1}+1$ for $0 \leq n \leq N-1$, and so $\beta_i + \beta_j \neq 2\beta_{N-1} + 1$ for any $0 \leq i, j \leq N$. Hence, we have $a_{2\beta_{N-1}+1}(N) = 0$. This contradicts $f_N(z) \in E_N(k)$, since $\beta_N > 2\beta_{N-1} + 1$. Thus, we established the inequality

$$\beta_{N-1} < \beta_N \leq 2\beta_{N-1} + 1.$$

On the other hand, we have the trivial equality

$$\begin{aligned}(N+1)^2 &= f_N^2(1) \\ &= \sum_{n=0}^{2\beta_N} a_n(N) \\ &\geq (a_0(N) + \cdots + a_{\beta_N}(N)) + a_{\beta_N+\beta_1}(N) + a_{2\beta_N}(N).\end{aligned}$$

Note that on the right hand side, we have $a_{\beta_N}(N), a_{\beta_N+\beta_1}(N), a_{2\beta_N}(N) \geq 1$, and also $(a_0(N) + \cdots + a_{\beta_N-1}(N)) \geq \beta_N$, so we have

$$(N+1)^2 - 3 \geq \beta_N.$$

Now, we also obtain that $\beta_{N-1} \leq N^2 - 3$, and so the number of admissible β_N is at $2\beta_{N-1}+1-\beta_{N-1} = \beta_{N-1}+1 \leq N^2-2$, which completes the proof of the proposition. □

We are now ready to present the main theorem of this subsection, then discuss computational aspects.

Theorem 5.2.5. *Let $k \geq 1$ be fixed. Set*

$$E(k) = \bigcup_{N=0}^{\infty} E_N(k).$$

If for some $N \in \mathbb{N}$ we have $E_N(k) = \emptyset$, or equivalently if $E(k)$ is finite, then no series of the form

$$f(z) = \sum_{n=0}^{\infty} z^{\beta_n}$$

where

$$f^2(z) = \sum_{n=0}^{\infty} a_n z^n$$

with $0 < a_n \leq k$ for all n can exist. If $E(k)$ is a finite set for every $k \geq 1$, then the Erdős-Turán conjecture on additive bases is true.

Remark 5.2.6. This theorem essentially translates this immensely difficult problem on arbitrary additive bases into a computation problem involving exhaustively finding all elements of certain classes of polynomials. Unfortunately, we will soon see that $E(k)$, if finite, grows very rapidly; and computing even $E(8)$ seems an extremely difficult task.

Proof. If $f(z) = \sum_{n=0}^{\infty} z^{\beta_n}$ is such a series such that $f^2(z) = \sum_{n=0}^{\infty} a_n z^n$ has coefficients satisfying $0 < a_n \leq k$, then any truncation $f_N(z) = \sum_{n=0}^{\infty} z^{\beta_n}$ with $f_N^2(z) = \sum_{n=0}^{2\beta_N} a_n(N) z^n$ will have $0 < a_n(N) \leq k$ for $n = 0, 1, \cdots, \beta_N$ and $a_n(N) \leq k$ for all $n \geq 0$, and so $f_N(z) \in E_N(k)$. Since this holds for any $N \geq 1$, we see that $E_N(k)$ is non-empty for any N and hence $E(k)$ is infinite. □

Now we can go on to verify that $E(k)$ is a finite set for $k = 2, \cdots, 7$. Aforementioned, the size of $E(k)$ grows very rapidly; with $|E(7)| = 1,268,361,281,038$.

We have $E_0(2) = \{1\}$, $E_1(2) = \{x+1\}$, $E_2(2) = \{1+x+x^3\}$. To see this, clearly $E_0(2), E_1(2)$ are as stated. The maximal degree of an element in $E_2(2)$ is 3. Clearly the constant and linear terms are needed, and so the only candidates for elements in $E_2(2)$ are $1+x+x^2, 1+x+x^3$. We quickly check that $1+x+x^2$ does not work because $(1+x+x^2)^2 = x^4+2x^3+3x^2+2x+1$, so the coefficient of x^3 is greater than 2. Now, if $E_3(2)$ is non-empty, then $g \in E_3(2)$ would look like $1+x+x^3+x^\beta$, where $4 \leq \beta \leq 7$. If $\beta = 4$, then $a_4(2) = 4 > 2$, if $\beta = 5, 6$, then $a_6(2) = 3 > 2$, and if $\beta = 7$, then $a_5(2) = 0$. Hence $E_3(2)$ is empty, and we are done.

We now give a list of $E_0(3), E_1(3), E_2(3), E_3(3), E_4(3)$. Also, it is verified that $E_N(3) = \emptyset$ for all $N > 4$.

$$E_0(3) = \{1\}$$

$$E_1(3) = \{1+x\}$$

$$E_2(3) = \{1+x+x^2, 1+x+x^3\}$$

$$E_3(3) = \{1+x+x^2+x^4, 1+x+x^2+x^5, 1+x+x^3+x^5\}$$

$$E_4(3) = \{1+x+x^2+x^4+x^7, 1+x+x^2+x^5+x^8\}$$

Below gives the sizes of $E(2), \cdots, E(7)$:

$$|E(2)| = 3$$

$$|E(3)| = 9$$
$$|E(4)| = 404$$
$$|E(5)| = 6,355$$
$$|E(6)| = 11,482,910,373$$
$$|E(7)| = 1,268,361,281,038$$

We are also interested in how many terms can an element of $E(k)$ have, and what is the maximal degree. Define $m(k)$ to be the maximal number of summands of an element in $E(k)$, and define $M(k)$ to be the maximum degree of an element in $E(k)$. Then we have:

$$m(2) = 3, m(3) = 5,$$
$$m(4) = 12, m(5) = 14$$
$$m(6) = 35, m(7) = 41$$

And

$$M(2) = 3, M(3) = 8$$
$$M(4) = 40, M(5) = 52$$
$$M(6) = 264, M(7) = 328$$

The above data is extracted from [2]. Notice that the jumps in all of these values seem to be much larger when going from $2k-1$ to $2k$. This is likely due to the fact that two representations of N are gained when $z^i, z^j, i+j = N$ are added, but only one representation if $N = 2s$ and z^s is added. However, it is unknown whether this effect will persist for larger values of k.

It remains a challenge to find an effective algorithm to compute the size of $E(k)$ when k is large, since the growth seems at least expontential. It is possible through extensive computer search to be able to compute the size of $E(k)$ for $k = 8, 9, \cdots$ up to some relatively small upper bound, but it seems infeasible at this point to generate compelling evidence that the Erdős-Turán conjecture in fact holds. It seems that working with polynomial truncations, when N is large, is not much easier than working with the Erdős-Turán conjecture in full generality. Nevertheless, this is to date the most conclusive result regarding the classical Erdős-Turán conjecture.

Chapter 6

Concluding Remarks

The Erdős-Turán conjecture remains mysterious and largely unresolved despite significant attention. There are several different approaches to tackle the problem, as we have exhibited throughout this paper. The problem arose from studying how thin an additive basis of $\mathbb{N}$ can be in the sense of natural density, and it is known that there exist additive bases of all orders that are essentially as thin as possible. Another way to think about thin bases is not in terms of natural density but in terms of the size of the representation function $r_{B,k}(n)$. Erdős and Tetali proved that there are bases of all orders for which $r_{B,k}(n) = \Theta(\log n)$. The probabilistic method developed by Erdős remains the only effective tool to generate thin bases to date. However, the probabilistic method is only good for showing that thin bases exist, but is powerless to address whether a given basis is thin or not.

Many authors later applied Erdős's method to work with bases that are known to be thick. For one, Wirsing and Vu independently adapted Erdős's method to prove that in certain cases one can find thin sub-bases in certain 'thick' additive bases. In particular, Vu in [24] showed that one can find thin sub-bases of all sufficiently large order k in any Waring base $\mathbb{N}_0^r$. Wooley in [27] improved on how big k has to be to only $r \log r$. By comparison, Vu required k to be as large as $O(8^r r^2)$. However, these results are either too crude to apply to interesting cases (for example, Wirsing required bases to be much thicker than optimal to deal with more sensitive cases) or too reliant on the specific number theoretic properties of a set to apply in general. It would appear that a significant new idea would be needed to advance this direction further.

One critical weakness of the probabilistic method is that it only allows us to prove thin bases (or other objects of interest) exist but cannot give us an explicit example. It is still not known whether or not it is possible to rigorously prove a specific set $A \subset \mathbb{N}_0$ is such that $r_{A,k}(n) = \Theta(\log n)$. A partial result in this direction is Kolountzaki's algorithmic result [17] that produces the terms of a thin basis in polynomial time in terms of k.

Of course, it is very natural to consider the Erdős-Turán conjecture as a computational

problem. Since it is an easy observation that for any set $A = \{a_1, a_2, \cdots\} \subset \mathbb{N}_0$, the representation function $r_{A,k}(n)$ only depends on the first finitely many terms where the exact dependence is determined by A and n. Hence we can get a good idea of how small $r_{A,k}(n)$ can be while still satisfying $r_{A,k}(m) > 0$ for $1 \leq m \leq n$. This is the exact motivation behind the work of Borwein, Choi, and Chu in [2]. Their results are to date the most conclusive, but nonetheless their work did not give an idea on how to prove the conjecture in general.

It would appear that with the study of the Erdős-Turán conjecture one would need to understand how to decompose a given basis into 'ordered' and 'random parts'. As the probabilistic method demonstrates, suitably 'random' sets A are very likely to be additive bases, and that $r_{A,k}(n)$ grows in a fairly uniform fashion. On the other hand, there exist sets that very closely approximate arithmetic progressions which have very non-uniform representation functions. An easy example of such a set is say $B = \{1, 2\} \cup \{3k : k \in \mathbb{N}_0\}$. Then it is clear that $r_{B,2}(3k+1) = r_{B,2}(3k+2) = 1$ for all $k \geq 0$. Due to these obstructions, some decomposition of this type is necessary. If one does have such a decomposition for an additive basis A of order k into an ordered set A_1 and a random set A_2, then one can hopefully use different theorems to show that $r_{A_j,k}(n), j = 1, 2$ is unbounded in both cases and thus establish the theorem. Unfortunately, to date no fruitful results are available in this direction.

The interested reader might note that there are two other natural settings in which to consider the Erdős-Turán conjecture; additive bases of $\mathbb{Z}$, and *multiplicative* bases of $\mathbb{N}$. For the former, since $\mathbb{Z}$ is a group under addition, many tools become available. Unfortunately the conjecture is decisively false. In particular, Nathanson proved in [18] that for any function $f : \mathbb{Z} \to \mathbb{N}_0$ and any $h > 1$ one can find a subset $B \subset \mathbb{Z}$ such that $r_{B,h}(n) = f(n)$ for all $n \in \mathbb{Z}$. To state the multiplicative case, we first define what it means to be a multiplicative basis.

Definition 6.0.7. Let $A = \{a_1, a_2, \cdots\} \subset \mathbb{N}$. Say that A is a *multiplicative basis* of order 2 of $\mathbb{N}$ if there exists a finite set C such that

$$\mathbb{N} \setminus C = \{a_i a_j : a_i, a_j \in A\}.$$

The analogous question for multiplicative bases was settled by Erdős in 1938 [4]. In particular, if $\mathcal{R}_A(n)$ denotes the number of ways n can be written as the product of two elements of A, then $\limsup_{n\to\infty} \mathcal{R}_A(n) = \infty$.

For applications of the probabilistic method and other additive methods discussed in this paper, readers are recommended to peruse [1] and [22].

Bibliography

[1] N. Alon and J. H. Spencer, *The Probabilistic Method*, Third Edition, Wiley and Sons, New Jersey, 2008.

[2] P. Borwein, S. Choi, and F. Chu, *An old conjecture of Erdős-Turán on additive bases*, Mathematics of Computation, **75**(253), 475-484, 2006.

[3] G. A. Dirac, *Note on a problem in additive number theory*, Journal of the London Mathematical Society, **26**, (1951), 313-313.

[4] P. Erdős, *On sequences of integers no one of which divides the product of two others and on some related problems*, Mitt.Tomsk Univ., **2** (1938), 74-82.

[5] P. Erdős, *On a problem of Sidon in additive number theory*, Acta. Sci. Math. Szeged, **15**, (1954), 255-259.

[6] P. Erdős, *Problems and results in additive number theory*, Colloque sur le Théorie des Nombres, CBRM, Bruselles, (1956), 127-137.

[7] P. Erdős, *Extremal problems in number theory*, Proceedings of the Symposium of Pure Mathematics. VIII, American Mathematical Society, (1965), 181-189.

[8] P. Erdős and W. H. J. Fuchs, *On a problem of addditive number theory*, Journal of the London Mathematical Society, **31** (1956), 67-73.

[9] P. Erdős and P. Tetali, *Representations of integers as the sum of k terms*, Random Structures Algorithms. **1**(3) (1990), 245–261.

[10] P. Erdős and P. Turán, *On a problem of Sidon in additive number theory, and some related problems*, Journal of the London Mathematical Society, **16** (1941), 212-215.

[11] G. B. Folland, *Real Analysis - Modern Techniques and Their Applications*, Wiley-Interscience, Canada, 1999.

[12] C. M. Fortuin, P. W. Kasteleyn and J. Ginibre, *Correlation inequalities on some partially ordered sets*, Comm. Math. Phy. **22** (1971), 89-103.

[13] G. Grimmett and D. Stirzaker, *Probability and Random Processes*, Oxford University Press, Oxford, 2006.

[14] M. N. Huxley, *Integer points in plane regions and exponential sums*, Number theory, 157-166, Trends Math., Birkhauser, Basel, 2000.

[15] S. Janson, *Poisson approximation for large deviations*, Random structures Algorithms. **1** (1990), 221-229.

[16] J. H. Kim and V. Vu, *Concentration of multi-variate polynomials and its applications*, Combinatorica, **20**(3) (2000), 417-434.

[17] M. N. Kolountzakis, *An effective additive basis for the integers*, Discrete Math. **145** (1995), 307-313.

[18] M. B. Nathanson, *Every function is the representation function of an additive basis for the integers*, Acta Arithmetica, **108**(1) (2003), 1-8.

[19] M. B. Nathanson, *Additive Number Theory - The Classical Bases*, Springer, New York, 2010.

[20] I. Ruzsa, *A converse to a theorem of Erdős*, Journal of Number Theory. **62** (1997), 397-402.

[21] I. Ruzsa, *Additive and multiplicative Sidon sets*, Acta Arithmetica, **112**(4) (2006), 345-354.

[22] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge University Press, Cambridge, 2010.

[23] P. Turán, *On a theorem of Hardy and Ramanujan*, Journal of the London Mathematical Society, **9** (1934), 274-276.

[24] V. Vu, *On a refinement of Waring's problem*, Duke Mathematical Journal, **105**(1) (2000), 107-134.

[25] V. Vu, *On the concentration of multivariate polynomials with small expectation*, Random Structures Algorithms, **16**(4) (2000), 344-363.

[26] E. Wirsing, *Thin subbases*, Analysis, **6** (1986) 285-308.

[27] T. D. Wooley, *On Vu's thin basis theorem in Waring's problem*, Duke Mathematical Journal, **120**(1) (2004), 1-34.