Indecomposability Over the Max-Min Semiring

Benjamin Baily[1], Henry L. Fleischmann, and Faye Jackson
Department of Mathematics
530 Church St.
University of Michigan
Ann Arbor, MI 48109
United States
bbaily@umich.edu, henryfl@umich.edu, alephnil@umich.edu

Justine Dell
Department of Mathematics
9500 Gilman Dr.
University of California San Diego
La Jolla, CA 92093
United States
jsdell@ucsd.edu

Steven J. Miller
Department of Mathematics and Statistics
Williams College
18 Hoxsey St.
Williamstown, MA 01267
United States
sjm1@williams.edu

Ethan Pesikoff
Department of Mathematics
Yale University
10 Hillhouse Ave.
New Haven, CT 06520
United States
ethan.pesikoff@yale.edu

[1]The authors of this work were supported by NSF Grants DMS1561945 and DMS1659037.

Luke Reifenberg
Department of Mathematics
Univeristy of Notre Dame
255 Hurley
Notre Dame, IN 46556
United States
lreifenb@nd.edu

Abstract

For sets $A, B \subset \mathbb{N}$, their sumset is $A + B := \{a + b : a \in A, b \in B\}$. If we cannot write a set C as $C = A + B$ with $|A|, |B| \geq 2$, then we say that C is (additively) *indecomposable*. The question of whether a given set C is indecomposable arises naturally in additive combinatorics. Equivalently, we can formulate this question as one about the indecomposability of boolean polynomials, which has been discussed in previous work by Kim and Roush (2005) and Shitov (2014).

We use combinatorial and probabilistic methods to prove that almost all polynomials are indecomposable over the max-min semiring, generalizing work of Shitov (2014) and proving a 2011 conjecture by Applegate, Brun, and Sloane concerning lunar numbers. Furthermore, we use measure-theoretic methods and apply Borel's result on normal numbers to prove that almost all power series are asymptotically indecomposable over the max-min semiring. This result generalizes work of Wirsing (1953).

Indecomposability Over the Max-Min Semiring

Benjamin Baily, Justine Dell, Henry L. Fleischmann, Faye Jackson, Steven J. Miller, Ethan Pesikoff, and Luke Reifenberg

December 29, 2022

1 Introduction

The max-min semiring $\mathcal{N}$ consists of the set $\mathbb{N} \cup \{\infty\}$ equipped with the operations $\oplus, \otimes$, where $a \oplus b = \max(a, b), a \otimes b = \min(a, b)$. Previous work [7, 9] has discussed the factorization of polynomials over the *Boolean Semiring*, that is, the subsemiring $\mathcal{B}_2 = \{0, 1\}$. Generally, understanding the factorization of boolean polynomials proves useful in both the classical setting of factoring polynomials over fields [3] as well as in tropical geometry [11]. Remarkably, the study of factorization of boolean polynomials corresponds naturally with the study of sumsets within additive combinatorics, an active area of research [4, 10]. This paper explores the indecomposability (see Definition 6) of polynomials and power series over the sub-semiring $\mathcal{B}_b = \{0, \dots, b-1\}$ of $\mathcal{N}$, also known as the semiring of lunar numbers in base b [1]. Our main results generalize known results in the boolean case [9, 12].

1.1 Preliminaries

Since we deal with asymptotics throughout this paper, we first adopt one standard notation for asymptotic analysis.

Definition 1. If f, g are nonnegative real-valued functions and there exists a constant $c > 0$ such that $f \leq cg$, then we write $f \ll g$.

We now formally define the polynomials over $\mathcal{N}$.

Definition 2. The max-min semiring $\mathcal{N} = (\mathbb{N} \cup \{\infty\}, \oplus, \otimes)$ is defined by the operations

$$a \oplus b \coloneqq \max(a, b)$$
$$a \otimes b \coloneqq \min(a, b)$$

with the operations having units ∞ and 0, respectively. We also define the sub-semiring $\mathcal{B}_b = \{0, \dots, b-1\}$, with units $b-1$ and 0, respectively. For convenience we say $\mathcal{N} = \mathcal{B}_\infty$.

Furthermore, power series (and thus polynomials) in $\mathcal{N}[[x]]$ are defined so that the distributive law holds and for $a, b \in \mathcal{N}$ and $i, j \in \mathbb{N}$ we have

$$a \otimes x^i = ax^i$$
$$ax^i \otimes bx^j = (a \otimes b)x^{i+j}.$$

Note that, in $\mathcal{N}[[x]]$, the unit for $\oplus$ is 0, and the unit for $\otimes$ is ∞. The units in $\mathcal{B}_b[[x]]$ are $b-1$ and 0. We define $\mathcal{B}_b^n[x]$ as the set of polynomials in $\mathcal{B}_b[x]$ whose degree is at most n.

Definition 3. Let $f \in B_b[[x]]$. If $f = g \otimes h$ for $g, h \in \mathcal{B}_b[[x]]$ implies that either g or h is a unit, then f is said to be *prime*. If $f = g \otimes h$ implies that either g or h is a monomial, then f is said to be *indecomposable*. Note that all primes are automatically indecomposable.

Definition 4. Let $f, g \in \mathcal{B}_b[[x]]$. If f and g differ in only finitely many coefficients, then we say $f \sim g$. Furthermore, if $f \sim gh$ implies that either g or h is a monomial, then f is *asymptotically indecomposable*.

As noted previously, the question of whether a polynomial is indecomposable within $\mathcal{B}_2[[x]]$ corresponds precisely to whether a certain subset of $\mathbb{N}$ is indecomposable as a sumset. We recall the definition of the sum of $A, B \subseteq \mathbb{Z}$ and indecomposability of sets below.

Definition 5. Let $A, B \subset G$ for some abelian group G. Their *sumset* is the set $A + B \coloneqq \{a + b : a \in A, b \in B\}$.

Definition 6. Let $S \subset \mathbb{N}$. If $S = A + B$ implies either A or B is a singleton, then S is indecomposable. Similarly, if $S \sim A + B$ implies A or B is a singleton, then S is asymptotically indecomposable. Here, $\sim$ denotes difference in finitely many elements.

With these definitions in mind, one may associate with any subset $A \subseteq \mathbb{N}$ the boolean power series $\sum_j 1_A(j)x^j$, where $1_A(j) = 1$ if $j \in A$, and $1_A(j) = 0$ if $j \notin A$. Then the semiring $\mathcal{B}_2[[x]]$ is isomorphic to the semiring of subsets of $\mathbb{N}$ under union and set addition [5]. Under this isomorphism, the notion of indecomposability of a polynomial exactly matches that of indecomposability of a set.

Furthermore, just as products of boolean polynomials correspond to sums of sets, products of min-max polynomials correspond to sums of *multisets*. Gal Gross has previously provided a full account of this correspondence [5].

We also recall the definition of a normal number, and the result that almost all numbers are normal in any base b.

Definition 7. A number $\lambda \in \mathbb{R}$ is *normal* in base b if the base b representation of λ contains an equal proportion of each finite sequence of digits base b. That is, if for all positive integers n, all possible strings of n digits have density b^{-n} in the base b representation.

More formally, let $s = (\delta_1, \ldots, \delta_k)$ be a string of digits in $\{0, \ldots, b-1\}$. Fix a real number λ and let $N_\lambda(n, s)$ denote the number of occurrences of the string s in the first n digits of the base-b expansion of λ. Then the following holds:

$$\lim_{n\to\infty} \frac{N_\lambda(n, s)}{n} \;=\; b^{-k}.$$

An equivalent formulation of this is the following: let $Z \subset \{0, \ldots, b-1\}^k$ and let $N_\lambda(n, Z) = \sum_{s\in Z} N(n, s)$. Then

$$\lim_{n\to\infty} \frac{N(n, Z)}{n} = |Z|b^{-k}. \tag{1}$$

Almost every number is normal. This was first shown by Borel in base two in 1909 [2], and Wirsing extended this result to all bases in 1953 [12].

Theorem 8 (Wirsing [12, Lemma 2'])**.** *For any $b \geq 2$, almost every $\lambda \in \mathbb{R}$ is normal in base b. Consequently, almost every $\lambda \in \mathbb{R}$ is absolutely normal, that is, normal in every base.*

1.2 Summary of previous work

We now state previous work by Shitov in 2014 and by Wirsing in 1953. We begin with Shitov's work concerning polynomials over $\mathcal{B}_2$.

Theorem 9 (Shitov [9, Theorem 2.5])**.** *As $n \to \infty$, the proportion of degree n polynomials in $\mathcal{B}_2[x]$ which are prime tends to 1.*

Theorem 9 answers a question of K. H. Kim and F. W. Roush posed in 2005 [7]. Remarkably, the proof uses only elementary combinatorics and probability. The result of Wirsing stated below is much older, but, unlike Shitov's work, the proof requires more advanced techniques.

Theorem 10 (Wirsing [12, Theorem 2])**.** *Almost every element of $\mathcal{B}_2[[x]]$ is asymptotically indecomposable.*

The proof of Theorem 10 is measure-theoretic and builds heavily off the work of Borel, in particular the result that almost every number is *normal* (Definition 7) in base 2. Wirsing and Shitov phrased these results in two different settings. Wirsing in fact writes that almost every set $A \subset \mathbb{N}$ is asymptotically indecomposable.

We restate Shitov and Wirsing's results in these terms: almost every finite subset of $\mathbb{N}$ is indecomposable and almost every subset of $\mathbb{N}$ is asymptotically indecomposable. As noted previously, the semiring of sets under union and set addition is isomorphic to the semiring of boolean polynomials [5]. Hence, these two formulations are equivalent.

1.3 Summary of results

Our contribution is to generalize these results to the setting of the max-min semiring $\mathcal{B}_b[[x]]$. In particular, we prove the following two results.

Theorem 11. *Fix b, and set $\mathcal{B}_b = \{0, 1, \ldots, b-1\} \subset \mathcal{N}$. Then as $n \to \infty$, the proportion of degree n polynomials in $\mathcal{B}_b[x]$ which are indecomposable tends to 1.*

Theorem 12. *Almost every element of $\mathcal{B}_b[[x]]$ is asymptotically indecomposable.*

The first result is particularly interesting as it relates to a third manner in which to interpret the polynomials over $\mathcal{B}_b$. In particular, Theorem 11 implies a conjecture of Applegate, Le Brun, and Sloane concerning lunar primes [1].

Conjecture 13. Let $\pi_b(n)$ denote the number of degree $n-1$ prime polynomials of $\mathcal{B}_b[x]$. Then we have the asymptotic $\pi_b(n) \sim (b-1)^2 b^{n-2}$.

The paper is organized as follows. In Section 2, we prove Theorem 11 by partitioning the collection of decomposable polynomials in $\mathcal{B}_b[[x]]$ into several subcollections and bounding the size of each. We do this by applying Hoeffding's inequality and a generalization of one of Shitov's lemmas [9, Lemma 2.6]. We then prove Conjecture 13 as a corollary of Theorem 11 in Section 2.1. In Section 3, we prove Theorem 12 using a similar partitioning strategy for $\mathcal{B}_b[[x]]$. We apply the Borel-Cantelli Lemma and the result that almost all numbers are normal in every base [12].

2 Indecomposability in $\mathcal{B}_b^n[x]$

In this section, we generalize Shitov's result to polynomials over the max-min semiring. We begin with some conventions.

Definition 14. Let $f \in \mathcal{N}[x]$. Then $|f|$ denotes the number of nonzero coefficients of f.

Definition 15 (Applegate, LeBrun, and Sloane [1, p. 6])**.** A *digit map* is a nondecreasing function $\mathbb{N} \to \mathbb{N}$. If d is a digit map and $f = a_0 \oplus a_1 x \oplus a_2 x^2 \oplus \cdots \in \mathcal{N}[[x]]$, then we let $d(f) = d(a_0) \oplus d(a_1)x \oplus d(a_2)x^2 \oplus \cdots$.

Theorem 16 (Applegate, Lebrun, and Sloane [1, Thm. 3])**.** *If d is a digit map, then $d : \mathcal{N}[[x]] \to \mathcal{N}[[x]]$ is a semiring homomorphism. In particular, if $f = gh$ is a nontrivial factorization and $d(1) \geq 1$, then $d(f) = d(g)d(h)$ is a nontrivial factorization of $d(f)$.*

Theorem 16 provides a framework for our proof, allowing us to reduce the problem of factoring a polynomial over $\mathcal{B}_b$ to factoring one over $\mathcal{B}_2$.

Definition 17. We define the digit maps s_i for each $i \in \mathbb{Z}^+$.

$$s_i(n) := \begin{cases} 0, & n < i; \\ i, & n \geq i. \end{cases} \tag{2}$$

For $f \in \mathcal{N}[[x]]$, we additionally define $f_i = s_1(s_i(f))$. These polynomials, which we refer to as the "i-level support of f," are indicator functions for where the coefficients of f are at least i.

Remark 18. These digit maps are a very useful tool, and it is natural to attempt to prove Theorem 11 as a direct corollary of Theorem 16 and Theorem 9. One observes that almost all degree-n polynomials in $\mathcal{B}_2[x]$ are indecomposable. Additionally, for $f \in \mathcal{B}_b[x]$, f and f_1 are either both decomposable or both indecomposable. Hence, it is reasonable to expect that almost all polynomials f of degree n are indecomposable because, thanks to Theorem 9, almost all f_1 of degree n are indecomposable. Unfortunately, the polynomials f_1 are not uniformly distributed in $\mathcal{B}_2[x]$, so one does not have

$$\mathbb{P}(\{f \in \mathcal{B}_b[x] : f \text{ indecomposable}\}) = \mathbb{P}(\{g \in \mathcal{B}_2[x] : g \text{ indecomposable}\}).$$

Hoeffding's inequality and its corollary eq. (3) imply that if f is a random degree-n polynomial in $\mathcal{B}_b[x]$, the polynomial f_1 will almost surely have approximately $\frac{(b-1)(n+1)}{b}$ nonzero coefficients, whereas a randomly-chosen degree-n polynomial in $\mathcal{B}_2[x]$ will have approximately $\frac{n+1}{2}$ nonzero coefficients. In fact, polynomials with more nonzero coefficients are much more likely to be decomposable.

To fix the issue of this non-uniform distribution in the case that $b = 2a$, one might instead look at f_a. This way, the polynomials f_a are in fact uniformly distributed in $\mathcal{B}_2[x]$. However, a new issue emerges: nontrivial factorizations in $\mathcal{B}_b[x]$ may appear trivial under this digit map. For example, if $b = 4, f = 1 \oplus x$, and $g = 1 \oplus x \oplus x^2$, then $f^2 = g$ and $f_2^2 = g_2$, but $f_2 = g_2 = 0$. Ultimately, this is the correct approach, but we must look at both f_1, f_a together and account for several other possible sources of decomposable polynomials.

Finally, to conclude our setup, we use the following convention for referencing the coefficients of polynomials. Throughout the remainder of this paper, let

$$f = \bigoplus_{k=0}^{\infty} \alpha_k x^k, \quad g = \bigoplus_{k=0}^{\infty} \beta_k x^k, \quad h = \bigoplus_{k=0}^{\infty} \gamma_k x^k, \quad \sigma = \bigoplus_{k=0}^{\infty} \delta_k x^k,$$

for notational convenience. Additionally, set $\alpha_i' = \alpha_i \otimes 1$ and similarly for each other coefficient. This way we have, for instance:

$$f_1 = \bigoplus_{k=0}^{\infty} \alpha_k' x^k, \quad g_1 = \bigoplus_{k=0}^{\infty} \beta_k' x^k, \quad h_1 = \bigoplus_{k=0}^{\infty} \gamma_k' x^k, \quad \sigma_1 = \bigoplus_{k=0}^{\infty} \delta_k' x^k.$$

We may now begin in earnest. In the proof of one lemma, Shitov shows the following statement, which will be of great use to us.

Corollary 19 (Shitov [9, p. 1185])**.** *For any $d > 0$, the number of pairs of boolean polynomials (f, g) satisfying the following conditions is at most $n^{2d+1}2^{(k,n)}$, where (k, n) is used to denote the greatest common divisor of k and n.*

1. *The constant terms of f, g are nonzero;*
2. *$\deg f = k > 0, \deg g = n - k$;*
3. *$|f \otimes g| \leq |f| + |g| + d$.*

We now generalize Corollary 19 to our setting.

Lemma 20. *The number of pairs of boolean polynomials (f, g) satisfying the following conditions is at most $n^{2d+2}2^k$ for any $d > 0$.*

1. *The constant term of f is nonzero;*
2. *$\deg f = k > 0, \deg g = n - k$;*
3. *$|f \otimes g| \leq |f| + |g| + d$.*

Proof. Write $g = x^j \otimes (1 + \cdots + x^{n-k-j})$ and define $\bar{g}$ by $g = x^j \otimes \bar{g}$. Then clearly $|f \otimes g| = |f \otimes \bar{g}|$ and $|g| = |\bar{g}|$. By Corollary 19, there are at most $n^{2d+1}2^{(k,n-j)}$ pairs $(f, \bar{g})$ satisfying the hypotheses of the corollary. Since there are at most n choices for j, the number of pairs (f, g) satisfying the hypotheses of this lemma is at most $\sum_{j=0}^{n-1} n^{2d+1}2^{(k,n-j)} \leq n^{2d+2}2^k$. □

The final ingredient for our proof is Hoeffding's inequality.

Proposition 21 (Hoeffding's Inequality [6, Thm. 2])**.** *Let X_n be a sum of n independent Bernoulli random variables X with $\mathbb{E}[X] = p$. Then $\mathbb{P}(|X_n - np| > \epsilon n) \leq 2e^{-2\epsilon^2 n}$.*

When we choose a degree $n - 1$ polynomial f at random from $\mathcal{B}_b[x]$, the quantity $|f_i|$ is a sum of n independent Bernoulli random variables Z_i with $\mathbb{E}[Z_i] = \frac{b-i}{b}$. As a consequence, if f is a degree $n - 1$ polynomial chosen randomly from $\mathcal{B}_b[x]$, then

$$\mathbb{P}\left(\left||f_i| - \frac{(b-i)n}{b}\right| > \epsilon n\right) \leq 2e^{-2\epsilon^2 n}. \tag{3}$$

We now prove a quantitative version of Theorem 11.

Proposition 22. *Let $b > 1$ and $a = \lfloor b/2 \rfloor$ and let $\Sigma_{b,n}$ denote the set of decomposable degree $n-1$ polynomials in $\mathcal{B}_b[x]$. Then for any $d, v > 0$ we have*

$$|\Sigma_{b,n}| \ll b^n \left(ne^{-d^2/4(n+1)} + vn^{2d+1}2^v b^{-n} + n^2 2^{-v} + n^{2d+3}2^{\frac{d}{2}-\frac{n}{3}} \right).$$

We define sets $E_i = E_i^n(d, v), 1 \le i \le 7$, such that $\Sigma_{b,n} \subseteq E_1 \cup \dots E_7$. Our proposition follows from the trivial bound $|\Sigma_{b,n}| \le |E_1| + \cdots + |E_7|$ and a series of lemmas concerning the size of $|E_1|, \dots, |E_7|$.

We now detail the partition. Though we will not write this after each set, we stipulate that $h \in E_i$ only if $h \notin E_j$ for any $j < i$.

E_1 is the set of polynomials h such that $\left| |h_1| - \frac{(b-1)n}{b} \right| > \frac{d}{2}$.

E_2 is those $h = f \otimes g$ such that $\left| |f_1| + |g_1| - \frac{(b-1)(n+1)}{b} \right| > \frac{d}{2}$.

E_3 is those h such that $\left| |h_a| - \frac{(b-a)n}{b} \right| > \frac{d}{2}$.

E_4 is those $h = f \otimes g$ such that $\left| |f_a| + |g_a| - \frac{(b-a)(n+1)}{b} \right| > \frac{d}{2}$.

E_5 is those $h = f \otimes g$ with $\deg f \le v$.

E_6 is those $h = f \otimes g$ with $|f_a| \le 1$ or $|g_a| \le 1$.

E_7 is all remaining decomposable degree $n-1$ polynomials h.

The size of $E_1, \dots, E_4$ can be bounded using Equation (3). The purpose of these sets is to control the size of the supports of the polynomials in the remaining sets. In particular, we want $|h_i| \le |f_i| + |g_i| + d$ for $i = 1, a$. This is so that when $h_i = f_i \otimes g_i$ is a nontrivial factorization, the hypotheses of Lemma 20 apply and we can conclude that there are few possible pairs (f, g).

Lemma 23. *For $j = 1, 3$ we have $|E_j| \ll e^{-d^2/4(n+1)} b^n$.*

Proof. Applying Equation (3) with $\epsilon = \frac{d}{2n}$, we obtain

$$|E_j| \le 2e^{-d^2/4n} b^n \ll e^{-d^2/4n} b^n \le e^{-d^2/4(n+1)} b^n.$$

□

Lemma 24. *For $j = 2, 4$ we have $|E_j| \ll ne^{-d^2/4(n+1)} b^n$.*

Proof. Each pair (f, g) corresponds to only one choice of h, thus it suffices to bound the number of pairs (f, g). If we fix $\deg f = k$, then we must have $\deg g = n - k - 1$ as

$\deg(f \otimes g) = n-1$. The set of pairs $(f,g) \in (\mathcal{B}_b[x])^2$ such that $\deg f = k, \deg g = n-k-1$ is in bijection with $\mathcal{B}_b^n[x]$, with the bijection given below:

$$\begin{aligned} \phi(f,g) &= f \oplus \left(((b-1)x^{k+1}) \otimes g\right) \\ \phi^{-1}(h) &= \left(\bigoplus_{j=0}^{k} \gamma_j x^j, \bigoplus_{j=k+1}^{n} \gamma_j x^{j-k-1}\right). \end{aligned}$$

Moreover, $|f_i| + |g_i| = |(\phi(f,g))_i|$. Thus, choosing $\epsilon = \frac{d}{2n+2}$ and applying Equation (3), we obtain that there are at most $2e^{-d^2/4(n+1)}b^{n+1}$ such pairs (f,g). Since there are $n/2$ choices for $\deg f$, we use this bound for each choice and obtain

$$|E_j| \leq ne^{-d^2/4(n+1)}b^{n+1} \ll ne^{-d^2/4(n+1)}b^n.$$

□

Lemma 25. *We have* $|E_5| \leq vn^{2d+1}2^v$.

Proof. Let $h = f \otimes g \in E_5$. Since $h \notin E_1 \cup E_3$, we have $|h_1| \leq \frac{(b-1)n}{b} + \frac{d}{2}, |f_1| + |g_1| \geq \frac{(b-1)(n+1)}{b} - \frac{d}{2}$. Thus $|h_1| \leq |f_1| + |g_1| + d$. If $|f_1| \leq 1$ or $|g_1| \leq 1$, then f or g is a monomial in contradiction to the assumption that $f \otimes g$ is a nontrivial factorization, hence (f_1, g_1) satisfy every hypothesis of Lemma 20. We apply this lemma once for each choice of $1 \leq \deg f \leq v$, and conclude

$$|E_5| \leq \sum_{\deg f=1}^{v} n^{2d+1}2^{\deg f} \leq vn^{2d+1}2^v.$$

□

Lemma 26. *We have* $|E_6| \ll n^2 2^{-v} b^n$.

Proof. Suppose $|f_a| \leq 1$. Then fix $\deg f = k$. Since $h \notin E_5$, we can assume $k > v$. Then there are $(k+1)(b-a)(a-1)^k$ choices[1] for f and b^{n-k} choices for g, hence there are $\leq (k+1)(a-1)^k b^{n-k+1}$ pairs (f,g). There are at most n choices for k, hence

$$\begin{aligned} |E_6| &\leq \sum_{k=v}^{n} (k+1)(a-1)^k b^{n-k+1} \leq n(n+1)(a-1)^v b^{n-v+1} \\ &\ll n^2(a-1)^v b^{n-v} \leq n^2 \left(\frac{b}{2}\right)^v b^{n-v} \leq n^2 2^{-v} b^n. \end{aligned}$$

If instead $|g_a| \leq 1$, then we have that $\deg(g) \geq \deg(f) \geq v$. By symmetry, there are at most twice as many pairs with either $|f_a| \leq 1$ or $|g_a| \leq 1$ as there are with $|f_a| \leq 1$. This doubles the size of our upper bound, but that is only a constant factor. □

Lemma 27. *We have* $|E_7| \leq n^{2d+3} 2^{\frac{d}{2} - \frac{n}{3}} b^n$.

[1] Pick the index of the coefficient to be at least a, then pick its value, then pick the remaining coefficients from $\{0, \cdots, a-1\}$.

Proof. Let $h = f \otimes g$. Since $h \notin E_3 \cup E_4$, we have $|h_a| < \frac{(b-a)n}{b} + \frac{d}{2}$ and $|f_a| + |g_a| > \frac{(b-a)(n+1)}{b}$, hence $|h_a| \leq |f_a| + |g_a| + d$. Moreover, as $h \notin E_6$, neither f_a nor g_a is a monomial and thus the pair (f_a, g_a) is a nontrivial factorization of h_a and satisfies the hypotheses of Lemma 20. Thus, using the fact that $(\deg f_a, n-1) \leq \frac{n-1}{2} \leq \frac{n}{2}$ for $1 \leq \deg f \leq n-2$, the number of possible choices for h_a is at most

$$\sum_{\deg f_a = 1}^{n-2} n^{2d+2} 2^{(\deg f_a, n-1)} \;\leq\; n^{2d+3} 2^{\frac{n}{2}}.$$

Once h_a is known, if $|h_a| = k$, there are $a^{n-k}(b-a)^k$ choices for h. This is because each 0 coefficient of h_a can correspond to any coefficient in $\{0, \ldots, a-1\}$, and any 1 corresponds to a coefficient in $\{a, \ldots, b-1\}$. To clean up our expressions, let s denote the quantity $\frac{(b-a)n}{b} + \frac{d}{2}$. Since $h \notin E_3$, we can say $k \leq s$. Recalling that $a := \lfloor b/2 \rfloor$, we have $a \leq b/2 \leq (b-a)$, with equality of all terms when b is even. This gives the following upper bound:

$$a^{n-k}(b-a)^k \;\leq\; a^{n-s}(b-a)^s \;\leq\; \left(\frac{b}{2}\right)^n \left(\frac{b-a}{a}\right)^{\left(\frac{b-a}{b} - \frac{1}{2}\right)n} \left(\frac{b-a}{a}\right)^{\frac{d}{2}}.$$

For $b \geq 2$, we have the bounds $1 \leq \frac{b-a}{a} \leq 2$ and $0 \leq \frac{b-a}{b} - \frac{1}{2} \leq \frac{1}{6}$, both of which are achieved when $b = 3$. Moreover, for $b = 2$, we have $\left(\frac{b-a}{b}^{\frac{b-a}{b} - \frac{1}{2}}\right) = 1$, thus for any $b \geq 2$ we have $\left(\frac{b-a}{b}\right)^{\left(\frac{b-a}{b} - \frac{1}{2}\right)n} \leq 2^{\frac{n}{6}}$. Altogether, this yields:

$$\begin{aligned} |E_7| \;&\leq\; n^{2d+3} 2^{\frac{n}{2}} \left(\frac{b}{2}\right)^n \left(\frac{b-a}{a}\right)^{\frac{d}{2}} \left(\frac{b-a}{b}\right)^{\left(\frac{b-a}{b} - \frac{1}{2}\right)n} \\ &\leq n^{2d+3} 2^{\frac{n}{2}} \left(\frac{b}{2}\right)^n 2^{\frac{n}{6} + \frac{d}{2}} \leq n^{2d+3} 2^{\frac{d}{2} - \frac{n}{3}} b^n. \end{aligned}$$

□

These bounds lead to an immediate proof of Proposition 22, and with the right choice of d, v, this gives us a proof of Theorem 11.

Proof. Our goal is to show that $|\Sigma_{b,n}|/b^n \to 0$, from which the result follows. Setting $d = 2\sqrt{n+1}\log n$ and $v = 3\log_2 n$, we then apply Proposition 22 to conclude $|\Sigma_{b,n}|/b^n \to 0$. □

2.1 Proof of Conjecture 13

We are now prepared to state and prove Conjecture 13 using Theorem 11. Recall from Definition 3 the distinction between a prime polynomial (one factor is a *unit*) and an indecomposable polynomial (one factor is a *monomial*). Applegate, LeBrun, and Sloane discuss prime polynomials, but primeness and indecomposability are sufficiently similar that our results can be applied to the conjecture [1]. These authors instead use the term *pseudoprime*

to refer to indecomposability. We choose to use the term indecomposability for its relation to ring theory more generally.

Motivating their conjecture, Applegate et al. observed that only certain polynomials can be prime by leveraging the fact that $b-1$ is the only unit in $\mathcal{B}_b[x]$.

Definition 28. A *prime candidate* of $\mathcal{B}_b[x]$ is a polynomial with nonzero constant term and maximum coefficient $b-1$.

It is easy enough to see that a polynomial is prime only if it is a prime candidate. If $h = a_j x^j \oplus \cdots \oplus a_{n-1}x^{n-1}$ for $j > 1$, then $h = (b-1)x^j \otimes (a_j \oplus \cdots \oplus a_{n-1}x^{n-j-1})$ which is a nontrivial factorization in their convention. Moreover, if $c < b-1$ is the maximum coefficient of h, then $h = c \otimes h$.

They showed that the number of prime candidates is asymptotic to $(b-1)^2 b^{n-2}$ (i.e., if $\pi_b^{\text{cand}}(n)$ is the number of prime candidates then $\frac{\pi_b^{\text{cand}}(n)}{(b-1)^2 b^{n-2}} \to 1$ as $n \to \infty$). Furthermore, their data shows that, almost all prime candidates are in fact prime as $k \to \infty$. See OEIS sequences A169912 and A087636 for the number of prime elements of $\mathcal{B}_2[x]$ and $\mathcal{B}_{10}[x]$ of each degree n. As evidence for this fact, Applegate et al. produced the following lower bound:

$$(b-1)^{n-2} + 2(b-2)^{n-2} + \cdots \leq \pi_b(n).$$

Moreover, they observed the following, which we will re-prove here.

Lemma 29 (Applegate, LeBrun, and Sloane [1, p. 10])**.** *An indecomposable prime candidate is prime.*

Proof. If h is indecomposable, then $h = fg$ implies either f, g is a monomial. Without loss of generality, assume that f is a monomial. Since the constant term of h is nonzero, we must have that f is a constant. Since the maximum coefficient of h is $b-1$, we must also have that $f = b-1$, thus h is prime. □

With this lemma, Conjecture 13 is a simple corollary of Theorem 11.

Proof. The proportion of prime candidates of $\mathcal{B}_b^{n-1}[x]$ which are indecomposable is at most a quantity which vanishes as $n \to \infty$:

$$\frac{|\Sigma_{b,n}|}{(b-1)^2 b^{n-2}} \ll \frac{|\Sigma_{b,n}|}{b^n} \to 0. \tag{4}$$

It follows that almost all prime candidates are prime. □

3 Asymptotic indecomposability

Before we prove this, we first must clarify what we mean by "almost all." It turns out, there is a very natural measure to associate with the set $\mathcal{B}_b[[x]]$.

Definition 30. To each element of $\mathcal{B}_b[[x]]$ we associate a real number in $[0, b]$, given by

$$\rho_b\left(\bigoplus_{k=0}^{\infty} a_k x^k\right) := \sum_{k=0}^{\infty} a_k b^{-n}. \tag{5}$$

In other words, each power series corresponds to a string of digits in $[0, 1, \ldots, b-1]$, which we can interpret as the base-b expansion of a number. This allows us to define a probability measure m on $\mathcal{B}_b[[x]]$.

Definition 31. For a set $A \subset \mathcal{B}_b[[x]]$ such that $\rho_b(A)$ is a measurable subset of $\mathbb{R}$, let $m(A) = b^{-1}\mathcal{L}(\rho_b(A))$, where $\mathcal{L}$ denotes the Lebesgue measure.

This reframing allows us to ask and answer questions about these polynomials measure-theoretically. We will use Borel's theorem that every number is normal, regardless of base [12] (see Theorem 8). We deduce Theorem 12 from a second theorem, which is simpler to relate to normality.

Theorem 32. *Let $\mathcal{C}^b \subset \mathcal{B}_b[[x]]$ denote the set of decomposable polynomials. Then $m(\mathcal{C}^b) = 0$.*

We show first how Theorem 12 follows from Theorem 32.

Proof. For $f \in \mathcal{B}_b[[x]]$, let $[f]$ denote the set of all g such that $f \sim g$, and for a set $S \subseteq \mathcal{B}_b[[x]]$ we let $[S]$ denote $\bigcup_{s\in S}[s]$. The set of asymptotically decomposable f is precisely the set $[\mathcal{C}^b]$. Fix a natural number n. Notice the set of polynomials which can be obtained from an element of C^b by editing only the first n coefficients has measure at most $b^n m(\mathcal{C}^b)$, which evaluates to 0. Thus, $[C^b]$ is a countable union of measure 0 sets, hence it has measure 0 and almost all power series over $\mathcal{B}_b[[x]]$ are asymptotically indecomposable. □

We now prove Theorem 32. Our proof is essentially a reformulation of Wirsing's original argument, but as the authors are not aware of an English translation of Wirsing's result [12], we reproduce it here for the sake of completeness.

Definition 33. For $n \in \mathbb{N}$ and $f = \bigoplus_{k=0}^{\infty} a_k x^k \in \mathcal{N}[[x]]$, define $f(n) := \bigoplus_{k=0}^{n} a_k x^k \in \mathcal{N}[x]$.

First, partition $\mathcal{C}^b$ into three sets T_1^b, T_2^b, T_3^b:

$$\begin{aligned}
T_1^b &:= \{h : h = f \otimes g \text{ with } 2 \le |g_1| < \infty\} \\
T_2^b &:= \left\{h : h = f \otimes g \text{ with } \liminf_{n\to\infty} \frac{|f_1(n)| + |g_1(n)|}{n} < \frac{1}{5} \text{ and } |f_1| = \infty = |g_1|\right\} \\
T_3^b &:= \left\{h : h = f \otimes g \text{ with } \liminf_{n\to\infty} \frac{|f_1(n)| + |g_1(n)|}{n} \ge \frac{1}{5} \text{ and } |f_1| = \infty = |g_1|\right\}.
\end{aligned}$$

Since $T_1^b \cup T_2^b \cup T_2^b = C^b$, it suffices to show that $\mathcal{L}(T_1^b) = \mathcal{L}(T_2^b) = \mathcal{L}(T_3^b) = 0$. In proving that the measures of T_1^b and T_3^b are 0, we rely extensively on the following idea.

We now state an important lemma with an elementary proof.

Lemma 34. *If $h = f \otimes g$, then $\bigoplus_{k=0}^{n} \alpha_k \otimes \beta_{n-k} = \gamma_n$.*

Proof. To elucidate this fact, all we need to do is rewrite the product $f \otimes g$:

$$f \otimes g \;=\; \bigoplus_{i=0}^{\infty} \alpha_i x^i \bigoplus_{j=0}^{\infty} \beta_j x^j \;=\; \bigoplus_{n=0}^{\infty} \left(\bigoplus_{k=0}^{n} \alpha_k \otimes \beta_{n-k} \right) x^n \;=\; \bigoplus_{n=0}^{\infty} \gamma_n x^n.$$

□

Lemma 35. *We have $m(T_1^b) = 0$.*

Proof. We show that no element of T_1^b is normal, whence the result follows. Specifically, we claim that the following sequence of digits can never occur in $\rho_b(h)$ for any $h = f \otimes g \in T_1^b$:

$$\underbrace{00\ldots0}_{\deg g+1}1\underbrace{00\ldots0}_{\deg g+1}. \tag{6}$$

Let $f_1 = \bigoplus_{k=0}^{\infty} \alpha_k x^k, g_1 = \bigoplus_{k=0}^{\deg g_1} \beta_k x^k, h_1 = \bigoplus_{k=0}^{\infty} \gamma_k x^k$. We can write

$$h_1 \;=\; g_1 \otimes f_1 \;=\; \bigoplus_{k=0}^{\deg g} \beta_k x^k \otimes f_1.$$

If $\gamma_k = 1$, then by Lemma 34 there exist i, j such that $\alpha_i = \beta_j = 1$ and $i + j = k$. Since g_1 is not a monomial, there exists another index $j' \neq j$ such that $\beta_{j'} = 1$. Then by Lemma 34: $1 \leq \gamma_{i+j'}$ and $\gamma'_{i+j'} = 1$. The gap between the two indices $i + j, i + j'$ is at most $\deg g_1$ (but either index can come first), thus $\rho_b(h_1)$ does not have a "1" without another "1" at most $\deg g$ indices away. Thus the string Equation (6) does not occur in $\rho_b(h_1)$. □

Lemma 36. *We have $m(T_2^b) = 0$.*

Proof. We begin by defining a finite counterpart to T_2^b:

$$T_2^b(n) \;:=\; \left\{\rho_b(h) : h = f \otimes g : \frac{|f_1(n)| + |g_1(n)|}{n} < \frac{1}{5} \text{ and } |f_1| = \infty = |g_1|\right\}.$$

Notice that

$$T_2^b \subseteq \limsup(\{T_2^b(n)\}) \;=\; \bigcap_{N\geq 1} \bigcup_{n\geq N} T_2^b(n).$$

By the Borel-Cantelli Lemma, we know that if $\sum_{n=1}^{\infty} m(T_2^b(n)) < \infty$, then

$$m\left(\limsup_{n\to\infty}(T_2^b(n))\right) = m(T_2^b) = 0.$$

As such, it suffices to show that $\sum_{n=1}^{\infty} m(T_2^b(n)) < \infty$.

Fix an integer k and consider all possible f and h such that $|f_1(n)| + |g_1(n)| = k$. There are $\binom{2n+2}{k}$ possibilities for $f_1(n)$ and $g_1(n)$: each has $n + 1$ coefficients, and we distribute k nonzero coefficients among them. Additionally, for a given choice of $f_1(n)$ and $g_1(n)$, there are $(b-1)^k$ polynomials $f(n)$ and $g(n)$ since each 1 coefficient of f_1 or g_1 can correspond to any value in $\{1, \ldots, b-1\}$. Thus, for a given k, there are at most $(b-1)^k\binom{2n+2}{k}$ possibilities for $f(n) \otimes g(n)$. Therefore, $T_2^b(n)$ is a subset of a union of at most $\sum_{0\leq k\leq \frac{n}{5}}(b-1)^k\binom{2n+2}{k}$ intervals, each of length b^{-n}.

We then compute

$$\begin{aligned} m(T_2^b(n)) &\leq \frac{1}{b^n} \sum_{0 \leq k \leq \frac{n}{5}} (b-1)^k \binom{2n+2}{k} \\ &\leq \frac{n}{5b^n}(b-1)^{n/5}\binom{2n+2}{\lfloor n/5 \rfloor} \leq \frac{n}{b^n}(b-1)^{n/5}\binom{2n}{\lfloor n/5 \rfloor} \\ &\leq \frac{n}{b^n}(b-1)^{n/5}\left(\frac{2ne}{n/5}\right)^{n/5} \leq n\left(\frac{1.94(b-1)^{1/5}}{b}\right)^n. \end{aligned}$$

Notice that $\frac{1.94(b-1)^{1/5}}{b} < 1$ for $b \geq 2$. Hence, the sum $\sum_{n=1}^{\infty} m(T_2^b(n))$ converges, and thus $m(T_2^b) = 0$.

□

Lemma 37. *We have $m(T_3^b) = 0$.*

Proof. As in the case of T_1^b, we will show that no element of T_3^b is normal, from which the result will follow.

Without loss of generality, we know that $\liminf_{n\to\infty} \frac{|f_1(n)|}{n} \geq \frac{1}{10}$. Let k be a positive integer such that

$$\left(\frac{b-1}{b}\right)^k < \frac{1}{10}.$$

Pick a positive integer r such that $|g_1(r-1)| = k$. This is equivalent to choosing r such that $\rho_b(g_1(r-1))$ has exactly k ones. Let Z denote the polynomials $\sigma \in \mathcal{B}_b^{r-1}[x]$ such that $\sigma_1 \oplus g_1 = \sigma_1$. In other words, Z is the set of $\sigma \in \mathcal{B}_b^{r-1}[x]$ such that $\beta_i \neq 0 \implies \delta_i \neq 0$. We can compute $|Z|$ using a counting argument: If $\beta_i \neq 0$, then $\delta_i \in \{1, \ldots, b-1\}$, otherwise $\delta_i \in \{0, \ldots, b-1\}$. As $|g_1| = k$ and σ has r coefficients, there are $(b-1)^k b^{r-k}$ possible choices for σ.

If $\rho_b(h)$ is normal, we expect the digit strings in $\rho_b(Z)$ to occur at a frequency of $\frac{(b-1)^k b^{r-k}}{b^r} = \left(\frac{b-1}{b}\right)^k$ in $\rho_b(h)$. We show that they instead occur at a frequency of at least $\frac{1}{10}$, from which it follows that $\rho_b(h)$ is not normal.

Suppose $\alpha'_s = 1$. Then from Lemma 34, it follows that

$$\left(\gamma'_s x^s \oplus \cdots \oplus \gamma'_{s+r-1} x^{s+r-1}\right) \oplus \left(\alpha'_s x^s \otimes g_1(r-1)\right) = \left(\alpha'_s x^s \otimes g_1(r-1)\right).$$

Thus $\gamma_s \oplus \cdots \oplus \gamma_{s+r-1} x^{r-1} \in Z$. This observation allows us to lower-bound the frequency of these strings in $\rho_b(h)$:

$$\frac{1}{10} \leq \liminf_{n\to\infty} \left(\frac{|f_1(n)|}{n}\right) \leq \liminf_{n\to\infty} \left(\frac{N_{\rho(h)}(n+r-1, Z)}{n}\right) = \liminf_{n\to\infty} \left(\frac{N_{\rho(h)}(n, Z)}{n}\right).$$

The above contradicts Equation (1), thus h is not normal. □

We now prove Theorem 32, from which Theorem 12 is a corollary.

Proof. By construction, $\mathcal{C}^b = T_1^b \cup T_2^b \cup T_3^b$. As a consequence of Lemma 35, Lemma 36, and Lemma 37, we have

$$m(\mathcal{C}^b) \leq m(T_1^b) + m(T_2^b) + m(T_3^b) = 0.$$

□

4 Acknowledgments

We thank the other participants of the 2021 Williams SMALL REU for constructive comments. Thanks also to Leo Goldmakher for translating Wirsing's paper from the original German and for helpful feedback throughout. Finally, we are grateful to the OEIS [8], in particular sequence A169912, without which we may never have made the connection between lunar arithmetic and sumsets which inspired this project.

References

[1] David L. Applegate, Marc LeBrun, and Neil J. A. Sloane, Dismal arithmetic, *Journal of Integer Sequences* **14** (2011), 11.9.8.

[2] M. Émile Borel, Les probabilités dénombrables et leurs applications arithmétiques., *Rendiconti del Circolo Matematico di Palermo (1884-1940)* **27** (1909), 247–271.

[3] Shuhong Gao and Alan GB Lauder, Decomposition of polytopes and polynomials, *Discrete & Computational Geometry* **26** (2001), 89–104.

[4] Andrew Granville and Aled Walker, A tight structure theorem for sumsets, *Proceedings of the American Mathematical Society* **149** (2021), 4073–4082.

[5] Gal Gross, Maximally additively reducible subsets of the integers, Master's thesis, University of Toronto (Canada), 2019.

[6] Wassily Hoeffding, Probability inequalities for sums of bounded random variables, *Journal of the American Statistical Association* **58** (1963), 13–30.

[7] Ki Hang Kim and Fred. W. Roush, Factorization of polynomials in one variable over the tropical semiring, arxiv preprint arXiv:math/0501167 [math.CO], 2005. https://arxiv.org/abs/math/0501167.

[8] OEIS Foundation Inc., The On-Line Encyclopedia of Integer Sequences, 2022. Published electronically at http://oeis.org.

[9] Yaroslav Shitov, How many boolean polynomials are irreducible?, *International Journal of Algebra and Computation* **24** (2014), 1183–1189.

[10] Ilya D Shkredov, Any small multiplicative subgroup is not a sumset, *Finite Fields and Their Applications* **63** (2020), 101645.

[11] David Speyer and Bernd Sturmfels, Tropical mathematics, *Mathematics Magazine* **82** (2009), 163–173.

[12] Eduard Wirsing, Ein metrischer satz über mengen ganzer zahlen, *Archiv der Mathematik* **4** (1953), 392–398.

2020 *Mathematics Subject Classification*: Primary 11B13; Secondary 15A80.
Keywords: Sumset, irreducible set, lunar arithmetic, asymptotic indecomposability, max-min semiring, normal number.

(Concerned with sequences A087636 and A169912.)