Journal of Integer Sequences, Vol. 28 (2025),
Article 25.2.7

Indecomposability Over the Max-Min Semiring

Benjamin Baily
Department of Mathematics
University of Michigan
530 Church Street
Ann Arbor, MI 48109
USA
bbaily@umich.edu

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

Henry L. Fleischmann
Department of Computer Science
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213
USA
henryfl@umich.edu

Faye Jackson and Ethan Pesikoff
Department of Mathematics
University of Chicago
5734 South University Avenue
Chicago, IL 60637
USA
alephnil@uchicago.edu
epesikoff@uchicago.edu

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

Luke Reifenberg
Department of Mathematics
University of Notre Dame
255 Hurley Building
Notre Dame, IN 46556
USA
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 as well as Shitov.

We use combinatorial and probabilistic methods to prove that almost all polynomials are indecomposable over the max-min semiring, generalizing work of Shitov and proving a conjecture by Applegate, LeBrun, and Sloane concerning lunar numbers.

1 Introduction

Given a positive integer b, let $\mathcal{A}_b$ denote the set $\{0, \ldots, b-1\}$ equipped with the operations $\oplus, \otimes$, where $t \oplus u = \max(t, u), t \otimes u = \min(t, u)$. Previous work [6, 8] has discussed the factorization of polynomials over the *Boolean semiring* $\mathcal{A}_2[x]$. Understanding the factorization of Boolean polynomials proves useful in both the classical setting of factoring polynomials over fields [2] as well as in tropical geometry [10]. The study of factorization of Boolean polynomials corresponds naturally with the study of sumsets within additive combinatorics, an active area of research [3, 9].

More generally, Applegate, LeBrun, and Sloane define a *lunar number* to be an element of the polynomial semiring $\mathcal{A}_b[x]$. In this paper, we show that almost all lunar numbers are indecomposable, and as a consequence we confirm Applegate, LeBrun, and Sloane's conjectured estimate for the number of degree-n lunar primes in base b.

1.1 Preliminaries

Since we deal with asymptotic estimates 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 $f \lesssim g$.

We now define the term *lunar number*.

Definition 2. The semiring $\mathcal{A}_b = (\{0, \ldots, b-1\}, \oplus, \otimes)$ is defined by the operations

$$t \oplus u \coloneqq \max(t, u)$$
$$t \otimes u \coloneqq \min(t, u),$$

where $\{0, \ldots, b-1\}$ is equipped with the usual linear order. The additive identity and multiplicative identity are $0_{\mathcal{A}_b} = 0$ and $1_{\mathcal{A}_b} = b-1$, respectively. The semiring of *lunar numbers*, then, is the polynomial semiring $\mathcal{L}_b \coloneqq \mathcal{A}_b[x]$.

For each $n \geq 0$, we define the set $\mathcal{L}_b^n \subseteq \mathcal{L}_b$ of lunar numbers of degree at most n:

$$\mathcal{L}_b^n = \left\{ \bigoplus_{i=0}^{n} a_i x^i \text{ such that } a_i \in \mathcal{A}_b \text{ for all } i \right\}.$$

For example, we have $\mathcal{A}_b = \mathcal{L}_b^0$ and $\mathcal{L}_b = \bigcup_{n \geq 0} \mathcal{L}_b^n$.

Remark 3. Originally, Applegate, LeBrun, and Sloane referred to these elements as *dismal numbers*. Finding the old name too depressing, the authors have since renamed these objects *lunar numbers*. See the links section of A087636.

Example 4. Working in $\mathcal{L}_3$, the product of $1 \oplus 2x$ with $2 \oplus 1x$ is

$$(1 \oplus 2x) \otimes (2 \oplus 1x) = 1 \oplus (2x \oplus 1x) \oplus 1x^2 = 1 \oplus 2x \oplus 1x^2.$$

Written in the notation of lunar arithmetic used by Applegate, LeBrun, and Sloane, this is

$$\begin{array}{rcc} & 2 & 1 \\ \times_3 & 1 & 2 \\ \hline & 2 & 1 \\ 1 & 1 & \\ \hline 1 & 2 & 1 \end{array}$$

where 21 represents the polynomial $1 \oplus 2x$.

Definition 5. Let $f \in \mathcal{L}_b$. Provided that h is not a *unit* and that in every decomposition $h = f \otimes g$ for $f, g \in \mathcal{L}_b$ at least one of f, g is a *unit*, we say that h is *prime*. This corresponds to the definition of a *lunar prime* given by Applegate, LeBrun, and Sloane [1, p. 7]. A *monomial* is an element of $\mathcal{L}_b$ of the form tx^n for some $t \in \mathcal{A}_b, n \in \mathbb{Z}^{\geq 0}$. Provided that h is not a *monomial* and that in every decomposition $h = f \otimes g$ for $f, g \in \mathcal{L}_b$ at least one of f, g is a *monomial*, we say that h is *indecomposable*.

Remark 6. If h is a lunar prime that is not a monomial, then h is also indecomposable by definition. On the other hand, there is only one prime monomial in $\mathcal{L}_b$: the monomial $(b-1)x$. Therefore, to bound the number of lunar primes, it suffices to bound the number of indecomposable lunar numbers.

Example 7. Fix a base $b \geq 2$. First, we see that $1 \oplus x \oplus x^2$ is decomposable in $\mathcal{L}_b$, since

$$(1 \oplus x) \otimes (1 \oplus x) = 1 \oplus x \oplus x \oplus x^2 = 1 \oplus x \oplus x^2.$$

In contrast, $1 \oplus x \oplus x^3$ is indecomposable.

The question of whether a polynomial is indecomposable within $\mathcal{L}_2$ 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 8. 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 9 (see [4, Definition 3])**.** Let $S \subset \mathbb{N}$ such that $S \neq \emptyset$. If $S = A + B$ implies either A or B is a singleton, then S is indecomposable. Note that in Gross's thesis [4], indecomposability is referred to as Ostmann irreducibility.

With these definitions in mind, one may associate with a finite nonempty subset $A \subseteq \mathbb{N}$ the polynomial $\sum_j 1_A(j)x^j$, where $1_A(j) = 1$ if $j \in A$, and $1_A(j) = 0$ if $j \notin A$. Then the semiring $\mathcal{L}_2$ is isomorphic to the semiring of finite subsets of $\mathbb{N}$ under union and set addition [4]. 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 [4].

1.2 Summary of results

In 2008, Shitov studied the proportion of degree n polynomials over $\mathcal{A}_2$ which are prime.

Theorem 10 (Shitov [8, Theorem 2.5])**.** *As $n \to \infty$, the proportion of degree n polynomials in $\mathcal{L}_2$ with nonzero constant term which are prime tends to 1.*

Theorem 10 answers a question of K. H. Kim and F. W. Roush posed in 2005 [6]. Remarkably, the proof uses only elementary combinatorics and probability. In particular, Hoeffding's inequality plays a key role in the proof, allowing Shitov to control the degrees of the factors making up composite polynomials. Our contribution is to generalize Shitov's result to the setting of lunar arithmetic in higher bases.

Theorem 11. *Fix an integer $b \geq 2$. Then as $n \to \infty$, the proportion of polynomials in $\mathcal{L}_b^n$ which are indecomposable tends to 1.*

The proportion of polynomials in $\mathcal{L}_b^n$ which have degree n is $\frac{b-1}{b}$, so Theorem 11 is equivalent to the statement that the proportion of degree n polynomials in $\mathcal{L}_b$ which are indecomposable tends to 1. Theorem 11 implies a conjecture of Applegate, LeBrun, and Sloane concerning lunar primes [1] as a corollary.

Corollary 12 (Applegate et al. [1, Conjecture 1])**.** *Let $\pi_b(n)$ denote the number of degree $n-1$ prime lunar numbers in $\mathcal{L}_b$. Then, for fixed $b \geq 2$, we have the asymptotic estimate $\pi_b(n) \sim (b-1)^2 b^{n-2}$ as $n \to \infty$.*

In Section 2, we prove Theorem 11 by partitioning the collection of decomposable polynomials in $\mathcal{L}_b^n$ 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 [8, Lemma 2.6]. We then prove Corollary 12 as a consequence of Theorem 11 in Section 2.1.

2 Indecomposability in $\mathcal{L}_b^n$

We begin with some conventions.

Definition 13. Let $f \in \mathcal{L}_b$. Then $|f|$ denotes the number of nonzero coefficients of f.

Definition 14 (Applegate, LeBrun, and Sloane [1, p. 6])**.** A *base-b digit map* is a nondecreasing function from $\mathcal{A}_b$ to itself. Let d be a digit map such that $d(0) = 0$. If we set $b' = d(b-1)+1$, we have $d(b) = 1_{\mathcal{A}_{b'}}$. Consequently, by restricting the codomain to $\mathcal{A}_{b'}$, we obtain a semiring homomorphism.

Moreover, such a digit map extends naturally to a map $d : \mathcal{L}_b \to \mathcal{L}_{b'}$ by the rule

$$d\left(\bigoplus_{i=0}^{n} a_i x^i\right) = \bigoplus_{i=0}^{n} d(a_i) x^i.$$

This theory can be extended to include all nondecreasing functions from $\mathbb{N} \cup \{\infty\}$ to itself, though we do not need this extended notion for our application.

Theorem 15 (Applegate, LeBrun, and Sloane [1, Thm. 3])**.** *If d is a base-b digit map and $f, g \in \mathcal{L}_b$, then*

$$d(f) \oplus d(g) = d(f \oplus g) \text{ and } d(f) \otimes d(g) = d(f \otimes g).$$

Theorem 15 provides a framework for our proof, allowing us to reduce the problem of factoring polynomials over $\mathcal{L}_b$ to factoring polynomials over $\mathcal{L}_2$.

Definition 16. Fix an integer $b \geq 2$. We define the digit maps s_i for each $1 \leq i \leq b-1$.

$$s_i(n) := \begin{cases} 0, & n < i; \\ 1, & n \geq i. \end{cases} \tag{1}$$

As discussed in Definition 14, these digit maps extend naturally to maps $s_i : \mathcal{L}_b \to \mathcal{L}_2$. For $f \in \mathcal{L}_b$, we additionally define $f_i = s_i(f)$. These polynomials, which can be thought of as the "i-level support of f", are indicator functions for where the coefficients of f are at least i.

Remark 17. By Shitov's result, almost all degree-n polynomials in $\mathcal{L}_2$ are indecomposable. Additionally, for $h \in \mathcal{L}_b$, we have that $h = f \otimes g$ implies $h_1 = f_1 \otimes g_1$, and f_1, g_1 are monomials if and only if f, g are. As a consequence, if h_1 is indecomposable, so is h. If the polynomials h_1 were uniformly distributed in $\mathcal{L}_2^n$, then we would have

$$\text{Prob}(\{f \in \mathcal{L}_b^n : f \text{ indecomposable}\}) \geq \text{Prob}(\{g \in \mathcal{L}_2^n : g \text{ indecomposable}\}),$$

where the probability measure is the uniform measure on the finite set $\mathcal{L}_b^n$. The polynomials h_1, however, are not uniformly distributed in $\mathcal{L}_2^n$. Hoeffding's inequality and its corollary eq. (2) imply that if f is a random degree-n polynomial in $\mathcal{L}_b$, the polynomial f_1 will almost surely have approximately $\frac{(b-1)(n+1)}{b}$ nonzero coefficients, whereas a degree-n polynomial chosen uniformly from $\mathcal{L}_2$ will have approximately $\frac{n+1}{2}$ nonzero coefficients. In fact, polynomials with more nonzero coefficients are much more likely to be decomposable.

Instead, we consider the polynomials f_a, where $a = \lfloor b/2 \rfloor$. When $b = 2a$, Theorem 11 is a corollary of Theorem 10 and Lemma 19. When $b = 2a+1$, Theorem 11 is not a direct corollary of Theorem 10, but our proof is along the lines of Shitov's argument.

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 18 (Shitov [8, p. 1185])**.** *For $d \in \mathbb{R}^+$, the number of pairs of Boolean polynomials (f, g) satisfying the following conditions is at most $n^{2d+1}2^{\gcd(k,n)}$.*

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 18 to our setting.

Lemma 19. *The number of pairs of Boolean polynomials (f, g) satisfying the following conditions is at most $n^{2d+2}2^k$ for every $d > 0$.*

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 18, there are at most $n^{2d+1}2^{\gcd(k,n-j)}$ 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 $\sum_{j=0}^{n-1} n^{2d+1}2^{\gcd(k,n-j)} \leq n^{2d+2}2^k$. □

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

Proposition 20 (Hoeffding's Inequality [5, Thm. 2])**.** *Let X_n be a sum of n independent Bernoulli random variables X with $\mathbb{E}[X] = p$. Then* $\text{Prob}(|X_n - np| > \epsilon n) \leq 2e^{-2\epsilon^2 n}$.

When we choose a degree $n-1$ polynomial f uniformly at random from $\mathcal{L}_b$, 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 uniformly from $\mathcal{L}_b$, then

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

We now prove a quantitative version of Theorem 11. Let Σ_b^n denote the set of decomposable lunar numbers of base b and degree at most n.

Proposition 21. *Fix $b, n \geq 2$ and let $a = \lfloor b/2 \rfloor$. Then for every $d, v > 0$ we have*

$$|\Sigma_b^n| \lesssim b^{n+1} \left(n^2 e^{\frac{-d^2}{4(n+2)}} + n^{2d+4} 2^{\frac{d}{2} - \frac{n+1}{3}} + vn^{2d+2} 2^v b^{\frac{d}{2} - \frac{n}{b}} + n^2 2^{-v}\right).$$

We partition Σ_b^n into two subsets, then control the size of each. Let $\mathcal{D}_b^n \subseteq \Sigma_b^n$ denote the set of h that admit a factorization $h = f \otimes g$ such that f_a, g_a are not monomials and let $\mathcal{I}_b^n = \Sigma_b^n \setminus \mathcal{D}_b^n$.

Remark 22. When $b = 2a$, the size of $\mathcal{D}_b^n$ is easy to control. As each $h \in \mathcal{D}_b^n$ has a factorization $h = f \otimes g$ such that $h_a = f_a \otimes g_a$ is nontrivial, we have that $s_a(\mathcal{D}_b^n) \subseteq \Sigma_2^n$ (though the inclusion may be strict, as $h_a = \overline{f} \otimes \overline{g}$ may not lift to a factorization of h). As the cardinality of $s_a^{-1}(f)$ is a^{n+1} for all $f \in \mathcal{L}_2^n$, we have

$$\frac{|\mathcal{D}_b^n|}{b^n} \leq \frac{|s_a^{-1}(\Sigma_2^n)|}{b^n} = \frac{a^{n+1}|\Sigma_2^n|}{b^n} = \frac{a|\Sigma_2^n|}{2^n},$$

a quantity which goes to zero as a consequence of Theorem 10.

Definition 23. Let $d \in \mathbb{R}^+$. A polynomial $h \in \mathcal{L}_b^n$ is *d-Hoeffding extremal* if there exists $1 \leq i \leq b-1$ such that

$$\left||h_i| - \frac{(b-i)n}{b}\right| > \frac{d}{2}, \tag{3}$$

or if h admits a factorization $h = f \otimes g$ such that

$$\left||f_i| + |g_i| - \frac{(b-i)(n+1)}{b}\right| > \frac{d}{2}. \tag{4}$$

Let $\mathcal{H}_b^n(d)$ denote the set of all $h \in \mathcal{L}_b^n$ that are d-Hoeffding extremal.

We will show individually that $\mathcal{H}_b^n(d), \mathcal{D}_b^n \setminus \mathcal{H}_b^n(d)$, and $\mathcal{I}_b^n \setminus \mathcal{H}_b^n(d)$ are small, from which it follows that Σ_b^n is small.

Lemma 24. *For fixed b and all $d \in \mathbb{R}^+$, we have $|\mathcal{H}_b^n(d)| \lesssim n^2 e^{\frac{-d^2}{4(n+2)}} b^n$.*

Proof. Let $i \in \{1, \ldots, b\}$. By Equation (2) with $\epsilon = \frac{d}{2(n+1)}$, the number of polynomials h satisfying Equation (3) for a given value of i is at most $e^{\frac{-d^2}{4(n+1)}} b^{n+1}$. To bound the number of $h = f \otimes g$ such that h is d-Hoeffding extremal due to Equation (4), it suffices to bound the number of pairs (f, g) such that $\deg f \otimes g \leq n$ and (f_i, g_i) satisfies Equation (4).

For each $m \leq n$, we bound the number of pairs (f, g) with $\deg f \otimes g = m$. If we fix $\deg f = k$, then we must have $\deg g = m - k$ as $\deg(f \otimes g) = m$. The set of pairs $(f, g) \in (\mathcal{L}_b)^2$ such that $\deg f = k, \deg g = m-k$ is in bijection with $\mathcal{L}_b^{m+1}$ with the bijection given below:

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

Moreover, $|f_i| + |g_i| = |(\phi(f, g))_i|$. Thus, choosing $\epsilon = \frac{d}{2(m+2)}$ and applying Equation (2), we obtain that there are at most $2e^{\frac{-d^2}{4(m+2)}} b^{m+2}$ such pairs (f, g) with $\deg f = k, \deg g = m - k$. As there are m choices for $\deg f$, b choices for i, and n choices for m, we have

$$|\mathcal{H}_b^n| \leq e^{\frac{-d^2}{4(n+1)}} b^{n+1} + \sum_{m=1}^{n} 2me^{\frac{-d^2}{4(m+2)}} b^{m+3} \lesssim \sum_{m=1}^{n} me^{\frac{-d^2}{4(m+2)}} b^{m+1} \leq n^2 e^{\frac{-d^2}{4(n+2)}} b^{m+1}.$$

□

Lemma 25. *If $h = f \otimes g \in \Sigma_b^n \setminus \mathcal{H}_b^n(d)$ and $1 \leq i \leq b-1$, then $|h_i| \leq |f_i| + |b_i| + d$.*

Proof. We have $|h_i| < \frac{(b-a)(n+1)}{b} + d/2$ and $|f_a| + |g_a| > \frac{(b-a)(n+2)}{b} - d/2 \geq |h_i| - d$. □

Lemma 26. *For fixed b and all $d > 0$, we have $|\mathcal{D}_b^n \setminus \mathcal{H}_b^n(d)| \leq n^{2d+4} 2^{\frac{d}{2} - \frac{n}{3}} b^{n+1}$.*

Proof. Let $h \in \mathcal{D}_b^n \setminus \mathcal{H}_b^n(d)$ and fix a nontrivial factorization $h_a = f_a \otimes g_a$. We count the number of pairs (f_a, g_a) with $\deg h_a = m$ for each $2 \leq m \leq n$. Since h is not d-Hoeffding extremal, we have $|h_a| \leq |f_a| + |g_a| + d$. It follows that the pair (f_a, g_a) satisfies the hypotheses of Lemma 19. Being non-monomials, f_a, g_a must both have positive degree, so $\deg f = m - \deg g \leq m-1$. Using the fact that $\gcd(\deg f_a, m) \leq \frac{m}{2}$ for $1 \leq \deg f_a \leq m-1$, the number of possible choices for h_a is at most

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

The total number of possibilities for h_a, therefore, is bounded by

$$\sum_{m=2}^{n} m^{2d+3} 2^{\frac{m}{2}} \leq n^{2d+4} 2^{\frac{n}{2}}.$$

Once h_a is known, if $|h_a| = k$, there are $a^{n+1-k}(b-a)^k$ choices for h. This is because each 0 coefficient of h_a can correspond to any coefficient in $\{0, \dots, a-1\}$, and each 1 corresponds to a coefficient in $\{a, \dots, b-1\}$. Let s denote the quantity $\frac{(b-a)(n+1)}{b} + d/2$. As h is not d-Hoeffding extremal, we have $k \le s$. Recalling that $a = \lfloor b/2 \rfloor$, we have $a \le b/2 \le (b-a)$, with equality of all terms when b is even, we see that the quantity $a^{n+1-k}(b-a)^k$ is maximized when k is maximized. This gives the following upper bound:

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

By the AM-GM inequality, we have $a^{\frac{n+1}{2}}(b-a)^{\frac{n+1}{2}} \le \left(\frac{b}{2}\right)^{n+1}$. For $b \ge 2$, we have the bounds $1 \le \frac{b-a}{a} \le 2$ and $0 \le \frac{b-a}{b} - \frac{1}{2} \le \frac{1}{6}$, thus for every $b \ge 2$ we have $\left(\frac{b-a}{a}\right)^{(\frac{b-a}{b}-\frac{1}{2})(n+1)} \le 2^{\frac{n+1}{6}}$. Altogether, this yields

$$\begin{aligned}|\mathcal{D}_b^n \setminus \mathcal{H}_b^n(d)| \;&\le\; n^{2d+4}2^{\frac{n}{2}} \left(\frac{b}{2}\right)^{n+1} \left(\frac{b-a}{a}\right)^{\frac{d}{2}} \left(\frac{b-a}{a}\right)^{(\frac{b-a}{b}-\frac{1}{2})n+1} \\ &\le n^{2d+4}2^{\frac{n}{2}} \left(\frac{b}{2}\right)^{n+1} 2^{\frac{n+1}{6}+\frac{d}{2}} \le n^{2d+4}2^{\frac{d}{2}-\frac{n}{3}}b^{n+1}.\end{aligned}$$

□

Lemma 27. *For all $d, v \in \mathbb{R}^+$, the number of lunar numbers in $\Sigma_b^n \setminus \mathcal{H}_b^n(d)$ that can be factored as $h = f \otimes g$ where $\deg f \le v$ is at most $vn^{2d+3}2^v(b-1)^{\frac{(b-1)n}{b}+\frac{d}{2}}$.*

Proof. Let $h \in \mathcal{I}_b^n \setminus \mathcal{H}_b^n(d)$ such that $\deg h = m$. Let $h = f \otimes g$ be a nontrivial factorization where $\deg f \le v$. As h is not d-Hoeffding extremal and f_1, g_1 are both not monomials, the factorization $h_1 = f_1 \otimes g_1$ satisfies the hypotheses of Lemma 19. Applying Lemma 19 once for each choice of $1 \le k \le v$, we conclude that the number of possible pairs (f_1, g_1) with $\deg h_1 = m$ is at most $\sum_{k=1}^{v} m^{2d+2}2^{\gcd(k,m)} \le vm^{2d+1}2^v$. Summing over all possible values of m, the number of pairs (f_1, g_1) is at most

$$\sum_{m=2}^{n} vm^{2d+2}2^v \le vn^{2d+3}2^v.$$

Each pair (f_1, g_1) corresponds to $(b-1)^{|f_1|+|g_1|}$ possible pairs (f, g), and since (f_1, g_1) do not satisfy Equation (4), the claim follows. □

Lemma 28. *For all $d, v \in \mathbb{R}^+$, we have $|\mathcal{I}_b^n \setminus \mathcal{H}_b^n(d)| \lesssim vn^{2d+2}2^v b^{\frac{(b-1)n}{b}+\frac{d}{2}} + n^2 2^{-v} b^{n+1}$.*

Proof. For fixed k, there are at most $(k+1)(a-1)^k b$ possible lunar numbers f with $\deg f \le k$ and $|f_a| \le 1$: pick the index of the coefficient with no constraint, then pick its value from $\{0, \dots, b-1\}$, then pick the remaining coefficients from $\{0, \dots, a-1\}$. Additionally, there are

b^{n+1-k} lunar numbers g of degree $\leq n-k$. It follows that there are at most $(k+1)a^k b^{n-k+2}$ lunar numbers h such that $\deg h \leq n, h = f \otimes g, \deg f = k$, and $|f_a| \leq 1$. As

$$\sum_{k=v}^{n} (k+1)a^k b^{n-k+2} \leq n(n+1)(a-1)^v b^{n-v+2} \lesssim n^2 b^{n+1} 2^{-v},$$

the claimed bound follows from Lemma 27. □

These bounds lead to an immediate proof of Proposition 21. With the right choice of d, v, this gives us a proof of Theorem 11.

Proof. Our goal is to show that $|\Sigma_{b,n}|/b^{n+1} \to 0$, from which the result follows. Setting $d = 2\sqrt{n+2}\log n$ and $v = 3\log_2 n$, we then apply Proposition 21 to conclude $|\Sigma_{b,n}|/b^{n+1} \to 0$ for fixed b as $n \to \infty$.

□

2.1 Proof of Conjecture 12

We are now prepared to state and prove Corollary 12 using Theorem 11. Recall from Definition 5 the distinction between a prime polynomial (one factor is always a *unit*) and an indecomposable polynomial (one factor is always a *monomial*). Applegate, LeBrun, and Sloane discuss prime polynomials, but primality 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 $\mathcal{L}_b$.

Definition 29. A *prime candidate* of $\mathcal{L}_b$ is a polynomial with nonzero constant term and maximum coefficient $b-1$.

It is easy enough to see that a lunar number 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, if $\pi_b^{\text{cand}}(n)$ is the number of prime candidates in base b with degree $n-1$, then $\pi_b^{\text{cand}}(n) \sim (b-1)^2 b^{n-2}$. Furthermore, their data suggests that almost all prime candidates are in fact prime as $n \to \infty$. See OEIS sequences A169912 and A087636 for the number of prime elements of $\mathcal{L}_2^n$ and $\mathcal{L}_{10}^n$. 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 re-prove here.

Lemma 30 (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, Corollary 12 is a simple corollary of Theorem 11.

Proof. For fixed b, the proportion of prime candidates of $\mathcal{L}_b^n$ which are decomposable is at most a quantity which vanishes as $n \to \infty$:

$$\frac{\pi_b(n)}{(b-1)^2 b^{n-2}} \leq \frac{\left|\Sigma_b^{n-1}\right|}{(b-1)^2 b^{n-2}} \lesssim \frac{\left|\Sigma_b^{n-1}\right|}{b^n} \to 0. \tag{5}$$

It follows that almost all prime candidates are prime. □

3 Acknowledgments

The authors of this work were supported by NSF grants DMS1561945 and DMS1659037. We thank the other participants of the 2021 Williams SMALL REU for constructive comments. Thanks to Leo Goldmakher for helpful feedback throughout. Thanks also to the referees for valuable feedback across several versions which allowed us to greatly simplify the article. Finally, we are grateful to the OEIS [7], 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, *J. Integer Sequences* **14** (2011), Article 11.9.8.

[2] Shuhong Gao and Alan G. B. Lauder, Decomposition of polytopes and polynomials, *Discrete Comput. Geom.* **26** (2001), 89–104.

[3] Andrew Granville and Aled Walker, A tight structure theorem for sumsets, *Proc. Amer. Math. Soc.* **149** (2021), 4073–4082.

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

[5] Wassily Hoeffding, Probability inequalities for sums of bounded random variables, *J. Amer. Statist. Assoc.* **58** (1963), 13–30.

[6] Ki H. 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.

[7] OEIS Foundation Inc., The On-Line Encyclopedia of Integer Sequences, 2025. Published electronically at https://oeis.org.

[8] Yaroslav Shitov, How many boolean polynomials are irreducible?, *Internat. J. Algebra Comput.* **24** (2014), 1183–1189.

[9] Ilya D. Shkredov, Any small multiplicative subgroup is not a sumset, *Finite Fields Appl.* **63** (2020), 101645.

[10] David Speyer and Bernd Sturmfels, Tropical mathematics, *Math. Mag.* **82** (2009), 163–173.

2020 *Mathematics Subject Classification*: Primary 11B13; Secondary 15A80.
Keywords: sumset, irreducible set, lunar arithmetic.

(Concerned with sequences A087636 and A169912.)

Received January 2 2023; revised versions received January 3 2023; March 25 2024; March 2 2025; March 11 2025. Published in *Journal of Integer Sequences*, March 26 2025.

Return to Journal of Integer Sequences home page.