Université de Montréal

On the structure of sumsets and representation functions with prescribed rates of growth

par

Christian Tafula Santos

Département de mathématiques et de statistique
Faculté des arts et des sciences

Thèse présentée en vue de l'obtention du grade de
Philosophiæ Doctor (Ph.D.)
en mathématiques

Orientation mathématiques pures

Julliet, 2025

Université de Montréal

Faculté des arts et des sciences

Cette thèse intitulée

On the structure of sumsets and representation functions with prescribed rates of growth

présentée par

Christian Tafula Santos

a été évaluée par un jury composé des personnes suivantes :

Matilde Lalín
(président-rapporteur)

Andrew Granville
(directeur de recherche)

Jake Levinson
(membre du jury)

Melvyn Nathanson
(examinateur externe)

(représentant du doyen de la FESP)

Résumé

Cette thèse explore la structure additive et les propriétés de représentation des ensembles en combinatoire additive, en se concentrant sur deux thèmes principaux :

Structure des ensembles somme : Soit $A \subseteq \mathbb{Z}_{\geq 0}$ un ensemble fini avec un élément minimum 0, un élément maximum m, et ℓ éléments entre les deux. Définissons $(hA)^{(t)}$ comme l'ensemble des entiers ayant au moins t représentations sous forme de somme de h éléments de A. Nous prouvons que $(hA)^{(t)}$ est structuré lorsque

$$h \geq (1 + o(1))\frac{1}{e}m\ell t^{1/\ell},$$

dans le régime $\ell \to \infty$, $t^{1/\ell} \to \infty$ et construisons des contre-exemples presque optimaux lorsque $h \ll m\ell t^{1/\ell}$. Des résultats similaires s'étendent aux sous-ensembles de $\mathbb{Z}^d$. De plus, nous interprétons les mouvements des pièces d'échecs comme des ensembles somme, montrant qu'un cavalier atteint une case générique plus efficacement qu'un roi, avec un facteur moyen de 24/13.

Fonctions de représentation avec des taux de croissance prescrits : Étant donné des entiers positifs $b_1, \ldots, b_h$ avec $\gcd(b_1, \ldots, b_h) = 1$, nous étudions la fonction de représentation

$$r_{A,h}(n) = \#\{(x_1, \ldots, x_h) \in A^h : b_1x_1 + \cdots + b_hx_h = n\}.$$

Nous montrons que si $F(n) \leq r_{\mathbb{N},h}(n)$ est régulièrement croissante avec $\lim_{n\to\infty} F(n)/\log n = \infty$, il existe un ensemble $A \subseteq \mathbb{N}$ tel que $r_{A,h}(n) \sim F(n)$. Lorsque F est croissante et que $F(2x) \ll F(x)$, nous construisons un ensemble A satisfaisant $r_{A,h}(n) \asymp F(n)$, et fournissons une heuristique suggérant que si $\limsup_{n\to\infty} r_{A,h}(n)/\log n < 1$, alors $r_{A,h}(n) = 0$ pour une infinité de n.

S'appuyant sur les résultats de Vu et Wooley, nous étudions les fonctions de représentation pour les puissances k-ièmes $\mathbb{N}^k$ et les puissances k-ièmes des premiers $\mathbb{P}^k$. Pour $h \geq h_k = O(8^k k^2)$ et $F(n)$ régulièrement croissante satisfaisant $\lim_{n\to\infty} F(n)/\log n = \infty$, nous montrons l'existence d'un ensemble $A \subseteq \mathbb{N}^k$ tel que

$$r_{A,h}(n) \sim \mathfrak{S}_{k,h}(n)F(n),$$

où $\mathfrak{S}_{k,h}(n)$ est la série singulière associée au problème de Waring. Dans le cas des puissances premières, nous obtenons des résultats analogues pour $F(n) = n^\kappa$. Pour $F(n) = \log n$, nous montrons que pour chaque $h \geq 2k^2(2\log k + \log\log k + O(1))$, il existe un ensemble $A \subseteq \mathbb{P}^k$ tel que $r_{A,h}(n) \asymp \log n$, ce qui montre l'existence de sous-bases minces pour les puissances premières.

Mots-clés: combinatoire additive, ensembles somme, cavalier d'échecs, fonction de représentation, variation régulière, problème de Waring, problème de Waring–Goldbach.

Abstract

This thesis investigates the additive structure and representation properties of sets in additive combinatorics, focusing on two main themes:

Structure of sumsets: Let $A \subseteq \mathbb{Z}_{\geq 0}$ be a finite set with minimum element 0, maximum element m, and ℓ elements in between. Define $(hA)^{(t)}$ as the set of integers with at least t representations as a sum of h elements of A. We prove that $(hA)^{(t)}$ is structured when

$$h \geq (1 + o(1))\frac{1}{e} m\ell t^{1/\ell},$$

in the regime $\ell \to \infty$, $t^{1/\ell} \to \infty$ and construct near-optimal counterexamples when $h \ll m\ell t^{1/\ell}$. Similar results extend to subsets of $\mathbb{Z}^d$. Additionally, we interpret chess piece movements as sumsets, showing that a knight reaches a generic square more efficiently than a king by a factor of 24/13 on average.

Representation functions with prescribed rates of growth: Given positive integers $b_1, \ldots, b_h$ with $\gcd(b_1, \ldots, b_h) = 1$, we study the representation function

$$r_{A,h}(n) = \#\{(x_1, \ldots, x_h) \in A^h : b_1 x_1 + \cdots + b_h x_h = n\}.$$

We show that if $F(n) \leq r_{\mathbb{N},h}(n)$ is regularly varying with $\lim_{n\to\infty} F(n)/\log n = \infty$, there exists $A \subseteq \mathbb{N}$ such that $r_{A,h}(n) \sim F(n)$. When F is increasing and $F(2x) \ll F(x)$, we construct A satisfying $r_{A,h}(n) \asymp F(n)$, and provide a heuristic suggesting that if $\limsup_{n\to\infty} r_{A,h}(n)/\log n < 1$, then $r_{A,h}(n) = 0$ for infinitely many n.

Building on results of Vu and Wooley, we investigate representation functions of k-th powers $\mathbb{N}^k$ and k-th powers of primes $\mathbb{P}^k$. For $h \geq h_k = O(8^k k^2)$ and regularly varying $F(n)$ satisfying $\lim_{n\to\infty} F(n)/\log n = \infty$, we show the existence of $A \subseteq \mathbb{N}^k$ such that

$$r_{A,h}(n) \sim \mathfrak{S}_{k,h}(n) F(n),$$

where $\mathfrak{S}_{k,h}(n)$ is the singular series associated to Waring's problem. In the case of prime powers, we obtain analogous results for $F(n) = n^\kappa$. For $F(n) = \log n$, we show that for every $h \geq 2k^2(2\log k + \log\log k + O(1))$, there exists $A \subseteq \mathbb{P}^k$ such that $r_{A,h}(n) \asymp \log n$, showing the existence of thin subbases of prime powers.

Keywords: additive combinatorics, sumsets, chess knight, representation function, regular variation, Waring's problem, Waring–Goldbach's problem

To the memory of my grandmother,
Vera Lucia

Contents

List of tables

List of figures

Notation and conventions

We start with a list of general notation and definitions that will be used throughout the thesis.

- For a set S, we denote its cardinality by $\#S$ or $|S|$.
- In this thesis, 0 is included in the natural numbers, i.e. $\mathbb{N} = \mathbb{Z}_{\geq 0}$.
- For $m \in \mathbb{N}$, we write $[m] = \{0,1,\ldots,m\}$.
- A multiset is a set that allows multiple instances of the same element, e.g. $\{1,1,2\}$.
- The symbol log denotes the natural logarithm ln.
- We denote the probability measure by Pr.
- li denotes the logarithmic integral $\mathrm{li}(x) = \int_{2^-}^{x} \frac{\mathrm{d}t}{\log t}$.
- The Gamma function is defined as $\Gamma(z) = \int_0^\infty t^{z-1} e^{-t}\, \mathrm{d}t$.
- Let X be a set and f, $g : X \to \mathbb{R}$ be real-valued functions. We write $f(x) \ll g(x)$, or $f(x) = O(g(x))$, or $g(x) \gg f(x)$, if there exists a constant $C \in \mathbb{R}_{>0}$ such that $|f(x)| \leq Cg(x)$ for every $x \in X$. If the constant C depends on some parameters, then we sometimes include these as subscripts on the symbols $\ll$, $\gg$, O.
- We write $f(x) \asymp g(x)$ if $f(x) \ll g(x) \ll f(x)$.
- For f, $g : \mathbb{R} \to \mathbb{R}$, we write $f(x) = o(g(x))$ if $\lim_{x\to\infty} f(x)/g(x) = 0$.
- We write $f(x) \sim g(x)$ if $\lim_{x\to\infty} f(x)/g(x) = 1$, or $f(x) - g(x) = o(g(x))$.
- A real-valued function $\psi : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ is called *slowly varying* if it is measurable and $\lim_{x\to\infty} \psi(\lambda x)/\psi(x) = 1$ for every $\lambda > 0$.
- A real-valued function $F : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ is called *regularly varying* if it is measurable and $\lim_{x\to\infty} F(\lambda x)/F(x)$ exists for every $\lambda > 0$. Regularly varying functions are of the form $F(x) = x^\kappa \psi(x)$, where $\kappa \in \mathbb{R}$ and $\psi(x)$ is slowly varying.
- For a sequence of random variables $(X_n)_{n\geq 1}$ in a probability space Ω, and a real function g, we write $X_n \overset{\text{a.s.}}{\sim} g(n)$ if $X_n(\omega) \sim g(n)$ for almost all $\omega \in \Omega$.
- We write $e(\alpha) = e^{2\pi i\alpha}$.
- For $k \geq 1$, we write $\mathbb{N}^k = \{n^k \mid n \in \mathbb{N}\}$, and $\mathbb{P}^k = \{p^k \mid p \text{ prime}\}$.
- If a, $b \in \mathbb{N}$, we denote $\gcd(a,b)$ by (a,b).
- $\varphi(n) = \#\{1 \leq m \leq n \mid (m,n) = 1\}$ is Euler's totient function.

Notation for Chapter 2: $\mathbb{Z}$

Let A, $B \subseteq \mathbb{Z}$ be finite sets, h, $t \geq 1$ be integers.

- $A + B = \{a + b \mid a \in A, b \in B\}$ and $A - B = \{a - b \mid a \in A, b \in B\}$.
- $hA = \{a_1 + \cdots + a_h \mid a_1, \ldots, a_h \in A\}$ is the h-fold sumset of A.
- $R_{A,h}(n) := \#\{(k_a)_{a\in A} \in \mathbb{Z}_{\geq 0}^{|A|} \mid \sum_{a\in A} k_a a = n, \sum_{a\in A} k_a = h\}$ is the representation function of A.
- $R_A(n) := \#\{(k_a)_{a\in A} \in \mathbb{Z}_{\geq 0}^{|A|} \mid \sum_{a\in A} k_a a = n\}$ is the total representation function of A.
- $(hA)^{(t)} := \{n \in \mathbb{Z} \mid R_{A,h}(n) \geq t\}$ is the t-representable h-fold sumset of A.

After possibly an affine transformation, assume now that $0 \in A$ is the smallest element of A, $\gcd A = 1$, and let $m = \max_{a\in A} a$ and $\ell := |A| - 2$.

- $\mathcal{P}_t(A) = \bigcup_{h\geq 1} (hA)^{(t)}$ (with $\mathcal{P}_1 = \mathcal{P}$).
- $\mathcal{E}_t(A) = \mathbb{Z}_{\geq 0} \setminus \mathcal{P}_t(A)$ is the t-exceptional set of A (with $\mathcal{E}_1 = \mathcal{E}$).
- $\mathrm{Fr}_t(A) := \max_{n\in\mathcal{E}_t(A)} n$ is a generalization of the Frobenius number.

Notation for Chapter 2: $\mathbb{Z}^d$

Let A, $B \subseteq \mathbb{Z}^d$ be finite sets, h, $t \geq 1$ be integers.

- $A + B = \{\mathbf{a} + \mathbf{b} \mid \mathbf{a} \in A, \mathbf{b} \in B\}$ and $A - B = \{\mathbf{a} - \mathbf{b} \mid \mathbf{a} \in A, \mathbf{b} \in B\}$.
- $hA = \{\mathbf{a}_1 + \cdots + \mathbf{a}_h \mid \mathbf{a}_1, \ldots, \mathbf{a}_h \in A\}$ is the h-fold sumset of A.
- $R_{A,h}(\mathbf{p}) = \#\{(k_\mathbf{a})_{\mathbf{a}\in A} \in \mathbb{Z}_{\geq 0}^{|A|} \mid \sum_{\mathbf{a}\in A} k_\mathbf{a} \mathbf{a} = \mathbf{p}, \sum_{\mathbf{a}\in A} k_\mathbf{a} = h\}$ is the representation function of A.
- $R_A(\mathbf{p}) = \#\{(k_\mathbf{a})_{\mathbf{a}\in A} \in \mathbb{Z}_{\geq 0}^{|A|} \mid \sum_{\mathbf{a}\in A} k_\mathbf{a} \mathbf{a} = \mathbf{p}\}$ is the total representation function of A.
- $(hA)^{(t)} = \{\mathbf{p} \in \mathbb{Z}^d \mid R_{A,h}(\mathbf{p}) \geq t\}$ is the t-representable h-fold sumset of A.
- $\mathcal{H}(A) := \{\sum_{\mathbf{a}\in A} c_\mathbf{a} \mathbf{a} \mid c_\mathbf{a} \in \mathbb{R}_{\geq 0}, \sum_{\mathbf{a}\in A} c_\mathbf{a} = 1\}$ is the convex hull of A.
- $\mathrm{ex}(\mathcal{H}(A))$ is the set of extremal points (or "corners") of $\mathcal{H}(A)$, which consists of those points in $\mathcal{H}(A)$ that cannot be written as convex combinations of other points in $\mathcal{H}(A)$.

After possibly an affine transformation, suppose that $\mathbf{0} \in \mathrm{ex}(\mathcal{H}(A))$.

- $\mathcal{C}_A := \{\sum_{\mathbf{a}\in A} c_\mathbf{a} \mathbf{a} \mid c_\mathbf{a} \in \mathbb{R}_{\geq 0}\}$ is the cone of A.
- $\Lambda_A := \mathrm{span}_\mathbb{Z}(A) = \{\sum_{\mathbf{a}\in A} c_\mathbf{a} \mathbf{a} \mid c_\mathbf{a} \in \mathbb{Z}\}$ is the $\mathbb{Z}$-span of A.
- $\mathcal{P}_t(A) = \bigcup_{h\geq 1} (hA)^{(t)}$ (with $\mathcal{P}_1 = \mathcal{P}$)
- $\mathcal{E}_t(A) = (\mathcal{C}_A \cap \Lambda_A) \setminus \mathcal{P}_t(A)$ is the t-exceptional set of A (with $\mathcal{E}_1 = \mathcal{E}$).

Notation for Chapter 3

- $A(x,y) = \min\{h \geq 1 \mid (x,y) \in hA\}$.
- $\mathrm{K} = \{(1,0), (1,1), (0,1), (-1,1), (-1,0), (-1,-1), (0,-1), (1,-1)\}$ is the king.
- $\mathrm{N}_{a,b} = \{(b,a), (a,b), (-a,b), (-b,a), (-b,-a), (-a,-b), (a,-b), (b,-a)\}$ is the (a,b)-knight.
- $\mathcal{B}_h = \{(x,y) \in \mathbb{Z}^2 \mid \max\{|x|,|y|\} \leq h\}$ is the ball of radius h with respect to the max norm.

Notation for Chapters 4 and 5

Let $A \subseteq \mathbb{Z}_{\geq 0}$ be a subset of integers, $h \geq 2$ be an integer, and $b_1, \ldots, b_h$ be positive integers with gcd = 1. In Chapter 4, the representation function is defined as

$$r_{A,h}^{(b_1,\ldots,b_h)}(n) = \#\{(x_1, \ldots, x_h) \in A^h \mid b_1x_1 + \cdots + b_hx_h = n\}.$$

When we write simply $r_{A,h}(n)$, in Chapter 4 this means $b_1, \ldots, b_h$ are fixed, and in Chapter 5 it means $b_1 = \cdots = b_h = 1$.

- $\rho_{A,h}^{(b_1,\cdots,b_h)}(n) = \#\{(x_1, \ldots, x_h) \in A^h \mid b_1x_1 + \cdots + b_hx_h = n, x_i \neq x_j \text{ if } i \neq j\}$ is the exact representation function. If $b_1, \ldots, b_h$ are fixed, we write simply $\rho_{A,h}(n)$.
- $r_{A,h}^{(\delta\text{-small})}(n) = \#\{(x_1, \ldots, x_h) \in A^h \mid b_1x_1 + \cdots + b_hx_h = n, \exists j : x_j < n^\delta\}$ counts δ-small solutions. $\rho_{A,h}^{(\delta\text{-small})}(n)$ is defined similarly.
- $r_{A,h}^{(\delta\text{-normal})}(n) = \#\{(x_1, \ldots, x_h) \in A^h \mid b_1x_1 + \cdots + b_hx_h = n, \forall j, x_j \geq n^\delta\}$ counts δ-normal solutions. $\rho_{A,h}^{(\delta\text{-normal})}(n)$ is defined similarly.
- $r^*_{A,\ell}(n) = \max_{1 \leq i_1 < \ldots < i_\ell \leq h} \#\{(x_1, \ldots, x_\ell) \in A^\ell \mid b_{i_1}x_1 + \cdots + b_{i_\ell}x_\ell = n\}$, for $1 \leq \ell \leq h$.
- $\widehat{r}_{A,h}(n)$ = size of a maximum disjoint family of representations $(x_1, \ldots, x_h) \in A^h$ such that $b_1x_1 + \cdots + b_hx_h = n$. Define similarly: $\widehat{\rho}_{A,h}(n)$, $\widehat{r}_{A,h}^{(\delta\text{-small})}(n)$, $\widehat{\rho}_{A,h}^{(\delta\text{-small})}(n)$, $\widehat{r}_{A,h}^{(\delta\text{-normal})}(n)$, $\widehat{\rho}_{A,h}^{(\delta\text{-normal})}(n)$, and $\widehat{r}^*_{A,\ell}(n)$. I.e., a hat "$\widehat{\ }$" signifies we are counting a maximum disjoint family of representations given the restrictions of the representation function.

Let $q \geq 1$, $1 \leq a \leq q$ be integers with $(a,q) = 1$.

- $S(a,q) = \sum_{r=1}^{q} e(ar^k/q)$.
- $\mathfrak{S}_{k,h}(n) = \sum_{q \geq 1} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} S(a,q)^h/q^h \, e(-na/q)$ is the singular series associated to Waring's problem.
- $\mathfrak{S}^*_{k,h}(n) = \sum_{q \geq 1} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} S(a,q)^h/\varphi(q)^h \, e(-na/q)$ is the singular series associated to Waring–Goldbach's problem.

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my advisor, Professor Andrew Granville, for his unwavering support, encouragement, and belief in me throughout this journey. His guidance has been invaluable, not only in shaping my mathematical thinking but also in teaching me how to be an independent researcher. I am truly fortunate to have had him as a mentor.

I am also sincerely grateful to the members of my jury, Professors Matilde Lalín, Jake Levinson, and Melvyn Nathanson, for their careful reading of my thesis and their insightful feedback. Their time and effort in evaluating my work are deeply appreciated. Additionally, I extend my gratitude to the Institut des Sciences Mathématiques, the Faculté des Études Supérieures et Postdoctorales, the Département de Mathématiques et Statistique at UdeM, and the Centre de Recherches Mathématiques for their financial support, which made this research possible.

The PhD journey is long and demanding, and I am incredibly thankful for the camaraderie and support of my friends in the math department. Jeremy, Mohammad, Siva, Stelios, Subham, Tony, and Xurui – our mathematical discussions and the unforgettable moments we shared made this experience far more enjoyable. I am especially grateful to my academic brothers, Cihan and Sun-Kai, whose friendship and shared passion for mathematics enriched my journey in countless ways. My friends from Brazil, particularly João and Lucas, have been a constant source of support, and I will always cherish our late-night phone conversations.

Finally, I wish to express my deepest gratitude to my family. My parents, Miguel and Simone, have always been my greatest pillars of support, and I would not be where I am today without their love and encouragement. To my grandmother Vera, who is deeply missed, thank you for everything. To Júlia, Letícia, Mário, Ricardo, Sandra, and Sônia – thank you for always being there for me.

This thesis is the result of not just my efforts, but the collective support and kindness of all these wonderful people. I am forever grateful.

Chapter 1

Introduction

1.1. Structure of sumsets

Let $d \geq 1$ be an integer, $A \subseteq \mathbb{Z}^d$ be a finite set, and for each $h \geq 1$, define the sumset

$$hA := \{\mathbf{a}_1 + \cdots + \mathbf{a}_h \mid \mathbf{a}_i \in A \text{ for all } i\}.$$

This sumset hA represents the collection of all points that can be formed by summing h (possibly repeated) elements of A, and it plays a fundamental role in the study of additive combinatorics. As h becomes sufficiently large, the set hA not only expands but also reveals patterns that connect its size and structure to geometric and arithmetic properties of the original set A, which has been the subject of extensive study.

Two complementary notions of structure emerge in the analysis of hA and are considered in the literature. The more classical perspective concerns the *size of* hA, or more specifically the growth rate of the cardinality $|hA|$ as $h \to \infty$. This topic dates back to the work of Khovanskii [**20**] in 1992, who showed that for sufficiently large h, the cardinality $|hA|$ is given by a polynomial $P_A(h)$ in h, whose degree is at most d, the dimension of the lattice $\mathbb{Z}^d$. That is,

$$|hA| = P_A(h),$$

where the coefficients of $P_A(h)$ encode geometric and combinatorial properties of A. For example, the leading term of $P_A(h)$ is determined by the volume of the convex hull of A. This has been generalized to abelian semigroups (cf. Nathanson–Ruzsa [**31**]).

The second notion of structure focuses on the internal organization of hA, and is referred to as the *stability* or simply *structure of* hA. This concept was first introduced by Nathanson [**26**] in the context of one-dimensional sets (i.e., when $d = 1$) and later generalized by Granville and Shakan [**13**] to higher dimensions. The idea of stability concerns the eventual behavior of hA as $h \to \infty$, and posits that for sufficiently large h, the sumset hA becomes as large as it can possibly be. The least h_1 for which hA is structured for $h \geq h_1$ has been studied by several authors in $\mathbb{Z}$ [**26, 6, 13, 16, 24**] and in $\mathbb{Z}^d$ [**7, 14, 15**].

1.1.1. Structure in $\mathbb{Z}$

For an integer $m \geq 0$, define $[m] := \{0,1,\ldots,m\}$. Given a finite subset A of integers, our focus lies in characterizing the elements of the sumset hA. Without loss of generality, assume $\min_{a \in A} a = 0$ and $\gcd(A) = 1$,[1] and express A as:

$$A = \{0 = a_0 < a_1 < \cdots < a_\ell < a_{\ell+1} = m\}$$

where $|A| = \ell + 2$ and m denotes the largest element of A.

Defining

$$\mathcal{P}(A) := \bigcup_{h \geq 1} hA,$$

which represents all integers expressible as finite sums of elements in A, we introduce the *exceptional set* of A:

$$\mathcal{E}(A) := \mathbb{Z}_{\geq 0} \setminus \mathcal{P}(A).$$

Since $A \subseteq 2A \subseteq 3A \subseteq \ldots$, it follows that $hA \subseteq [hm] \setminus \mathcal{E}(A)$. Moreover, defining the reflection $m - A = \{m - a \mid a \in A\}$, we obtain the identity $h(m - A) = hm - hA$, implying that if $n \in \mathcal{E}(m - A)$, then $hm - n \notin hA$. Consequently, we derive the containment:

$$hA \subseteq [hm] \setminus \Big(\mathcal{E}(A) \cup (hm - \mathcal{E}(m - A))\Big). \tag{1.1}$$

When equality holds in (1.1), the sumset hA is said to be *structured*.[2]

The existence of a threshold $h_1 = h_1(A)$ beyond which hA is structured for all $h \geq h_1$ was first established by Nathanson [**26**] in 1972, who obtained the bound $h_1 \leq m^2(\ell + 1)$. Subsequent refinements include:

- Chen–Chen–Wu [**6**]: $h_1 \leq \sum_{i=2}^{\ell+1}(a_i - 1) - 1$.
- Granville–Shakan [**13**]: $h_1 \leq 2\lfloor m/2 \rfloor$.
- Granville–Walker [**16**]: $h_1 \leq m - \ell$.

In 2022, Lev [**24**] further refined this bound, showing that hA is structured for all h satisfying $h \leq \max\{m - \frac{3}{2}(\ell - 1), \frac{2}{3}(m - \ell)\}$, except when A or $m - A$ takes the specific form $\{0,1,h + 2,\ldots,m\}$. In such cases, Granville–Walker's bound $m - \ell$ is optimal.

1.1.2. Structure of t-representables

Imagine that instead of counting numbers that can be written at least once as a sum of h elements from A, we seek those that can be written at least t times. To formalize this, we

[1] If we define $A' := \{(a - a_0)/d \mid a \in A\}$, where $a_0 := \min_{a \in A} a$ and $d := \gcd\{a - a_0 \mid a \in A\}$, then hA can be reconstructed from hA' through an affine transformation: $hA = ha_0 + d \cdot (hA')$, where $d \cdot B = \{d \cdot b \mid b \in B\}$.

[2] Alternatively, hA is said to *stabilize* for large h.

define the *representation function* of hA as:

$$R_{A,h}(n) := \#\{(k_0,\ldots,k_{\ell+1}) \in \mathbb{Z}_{\geq 0}^{\ell+2} \mid k_0a_0 + \cdots + k_{\ell+1}a_{\ell+1} = n, \textstyle\sum_{i=0}^{\ell+1} k_i = h\}$$
$$= \#\{(k_1,\ldots,k_{\ell+1}) \in \mathbb{Z}_{\geq 0}^{\ell+1} \mid k_1a_1 + \cdots + k_{\ell+1}a_{\ell+1} = n, \textstyle\sum_{i=1}^{\ell+1} k_i \leq h\},$$

where the second equality follows from the fact that $a_0 = 0$. For $t \geq 1$, define the t-representable sumset:

$$(hA)^{(t)} := \{n \in \mathbb{Z}_{\geq 0} \mid R_{A,h}(n) \geq t\}.$$

In 2021, Nathanson [**30**] showed that $(hA)^{(t)}$ exhibits a similar notion of structure for sufficiently large h. Define:

$$\mathcal{P}_t(A) := \bigcup_{h\geq 1} (hA)^{(t)}$$

and introduce the *t-exceptional set*:

$$\mathcal{E}_t(A) := \mathbb{Z}_{\geq 0} \setminus \mathcal{P}_t(A).$$

Then, there exists a smallest integer $h_t = h_t(A)$ such that for all $h \geq h_t$, we have:

$$(hA)^{(t)} = [hm] \setminus \Big(\mathcal{E}_t(A) \cup (hm - \mathcal{E}_t(m - A))\Big). \tag{1.2}$$

When this relation holds, $(hA)^{(t)}$ is said to be *structured*. Nathanson established the bound $h_t \leq m\ell(tm-1)+1$, which was later refined by Yang–Zhou [**45**] to $h_t \leq \sum_{i=2}^{\ell+1}(ta_i - 1) - 1$.

The bound we obtain for the structure threshold involves the Frobenius number of the set A. The *Frobenius number*,

$$\mathrm{Fr}(A) := \max_{n\in\mathcal{E}(A)} n,$$

is known to be finite,[3] with $\mathrm{Fr}(A) := 0$ if $\mathcal{E}(A) = \varnothing$. The study of $\mathrm{Fr}(A)$ dates back to Sylvester [**34**, p. 134], who showed that for $A = \{0 < a_1 < a_2\}$, we have $\mathrm{Fr}(A) = a_1a_2 - a_1 - a_2$. Similarly, define

$$\mathrm{Fr}_t(A) := \max_{n\in\mathcal{E}_t(A)} n,$$

which is shown to be finite in Corollary 2.5.

Theorem 1.1. *If $|A| \geq 4$, then $(hA)^{(t)}$ is structured as in* (1.2) *for all*

$$h \geq \left\lfloor \frac{\mathrm{Fr}_t(A) + m}{a_1} \right\rfloor + \left\lfloor \frac{\mathrm{Fr}_t(m-A) + m}{m - a_\ell} \right\rfloor.$$

This bound can be simplified to:

[3]As is well-known, there are $x_1,\ldots,x_{\ell+1} \in \mathbb{Z}$ such that $\sum_{i=1}^{\ell+1} a_ix_i = 1$. Taking $M := a_1 \max_i |x_i|$ and $N := \sum_{i=1}^{\ell+1} Ma_i$, we have $N + k = \sum_{i=1}^{\ell+1}(M + kx_i)a_i \in \mathcal{P}(A)$ for every $0 \leq k < a_1$. Therefore, since $a_1 + \mathcal{P}(A) \subseteq \mathcal{P}(A)$, we have $\{N, N+1, \ldots\} \in \mathcal{P}(A)$, so $\mathrm{Fr}(A) < N$.

Theorem 1.2. *If $|A| \geq 4$, then $(hA)^{(t)}$ is structured as in* (1.2) *for all*

$$h \geq C_{A,t}\,\frac{1}{e} m\ell t^{1/\ell},$$

where

$$C_{A,t} \leq \left(1+\frac{4}{\ell}\right)\frac{e}{t^{1/\ell}} + \left(1+\frac{2}{\ell}\right)\frac{1+(\log 4\ell)/\ell}{\min\{a_1, m-a_\ell\}}.$$

In particular, $C_{A,t} \leq 3e$ if $\ell \geq 4$, and $C_{A,t} \leq 1+o(1)$ as $\ell \to \infty$, $t^{1/\ell} \to \infty$.

This refines the bound of Yang–Zhou for, e.g., $t \geq 8\ell \geq 32$ – see Remark 2.12.

Remark (Case $\ell = 1$)**.** The case $|A| = 3$, examined in Appendix A, shows that $(hA)^{(t)}$ is structured for all $h, t \geq 1$. The special case $t = 1$ was proven by Granville–Shakan [**13**]. Therefore, Theorems 1.1 and 1.2 consider $\ell \geq 2$.

In Section 2.3, we construct a family of finite sets $A = A(m,\ell,t)$ for certain $m \geq 5$, $\ell \geq 2$, $t \geq 2$, each containing $1, m-1$, for which

$$h_t(A) \geq (1+o(1))\,\frac{1}{e} m\ell t^{1/\ell}$$

as $\ell \to \infty$, $t^{1/\ell} \to \infty$. Thus, Theorem 1.2 is asymptotically optimal in this regime.

1.1.3. Structure in $\mathbb{Z}^d$

A generalization of Theorem 1.1 holds for finite sets A in arbitrary dimensions. Let $d \geq 1$ be a fixed integer and consider a finite set $A \subseteq \mathbb{Z}^d$. Without loss of generality, assume that $\operatorname{span}_{\mathbb{R}}(A) = \mathbb{R}^d$, meaning that A spans the entire space.[4]

The *convex hull* of A is defined as

$$\mathcal{H}(A) := \left\{ \sum_{\mathbf{a}\in A} c_{\mathbf{a}}\mathbf{a} \;\middle|\; c_{\mathbf{a}} \in \mathbb{R}_{\geq 0},\ \sum_{\mathbf{a}\in A} c_{\mathbf{a}} = 1 \right\}$$

which represents the smallest convex set containing A. The set of *extremal points* $\operatorname{ex}(\mathcal{H}(A))$, also known as the "corners" of $\mathcal{H}(A)$, consists of those points $\mathbf{v} \in \mathcal{H}(A)$ where there exists a supporting hyperplane that is tangent to $\mathcal{H}(A)$ at $\mathbf{v}$ and separates the rest of $\mathcal{H}(A)$ onto one side. Explicitly, we define:

$$\operatorname{ex}(\mathcal{H}(A)) := \left\{ \mathbf{v} \in \mathcal{H}(A) \;\middle|\; \begin{array}{c} \exists \mathbf{n} = \mathbf{n}(\mathbf{v}) \in \mathbb{Z}^d, \exists c \in \mathbb{R} \text{ such that} \\ \langle \mathbf{n}, \mathbf{v}\rangle = c \text{ and } \langle \mathbf{n}, \mathbf{x}\rangle > c, \forall \mathbf{x} \in \mathcal{H}(A) \setminus \{\mathbf{v}\} \end{array} \right\}.$$

This characterization ensures that the extremal points of $\mathcal{H}(A)$ are precisely those that cannot be written as convex combinations of other points in $\mathcal{H}(A)$.

[4]If $\operatorname{span}_{\mathbb{R}}(A) \simeq \mathbb{R}^{d'}$ for some $d' < d$, then after a suitable change of basis, we can assume $A \subseteq \mathbb{Z}^{d'} = \mathbb{R}^{d'} \cap \mathbb{Z}^d$.

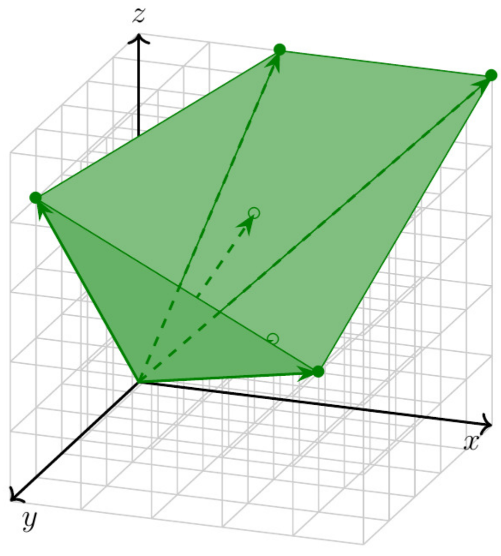

Fig. 1. The set $A = \{(\mathit{0,0,0}), (\mathit{0,4,4}), (\mathit{2,0,5}), (2,1,3), (3,3,2), (\mathit{4,4,2}), (\mathit{5,0,5})\}$. Points written in italics compose $\mathrm{ex}(\mathcal{H}(A))$.

Analogous to the one-dimensional case, suppose without loss of generality that $\mathbf{0} \in \mathrm{ex}(\mathcal{H}(A))$. For each integer $h \geq 1$, define the *representation function* of hA as

$$\begin{aligned} R_{A,h}(\mathbf{p}) &:= \#\left\{(k_{\mathbf{a}})_{\mathbf{a}\in A} \in \mathbb{Z}_{\geq 0}^{|A|} \;\middle|\; \sum_{\mathbf{a}\in A} k_{\mathbf{a}}\mathbf{a} = \mathbf{p},\ \text{with } \sum_{\mathbf{a}\in A} k_{\mathbf{a}} = h\right\} \\ &= \#\left\{(k_{\mathbf{a}})_{\mathbf{a}\in A\setminus\{\mathbf{0}\}} \in \mathbb{Z}_{\geq 0}^{|A|-1} \;\middle|\; \sum_{\mathbf{a}\in A\setminus\{\mathbf{0}\}} k_{\mathbf{a}}\mathbf{a} = \mathbf{p},\ \text{with } \sum_{\mathbf{a}\in A\setminus\{\mathbf{0}\}} k_{\mathbf{a}} \leq h\right\}. \end{aligned}$$

For any integer $t \geq 1$, define the t-representable sumset:

$$(hA)^{(t)} := \{\mathbf{p} \in \mathbb{Z}^d \mid R_{A,h}(\mathbf{p}) \geq t\}.$$

Defining the *cone* of A as

$$\mathcal{C}_A := \left\{\sum_{\mathbf{a}\in A} c_{\mathbf{a}}\mathbf{a} \;\middle|\; c_{\mathbf{a}} \in \mathbb{R}_{\geq 0}\right\},$$

noting that $\mathcal{H}(A) \subseteq \mathcal{C}_A$, and defining the $\mathbb{Z}$-span of A as

$$\Lambda_A := \mathrm{span}_{\mathbb{Z}}(A) = \left\{\sum_{\mathbf{a}\in A} c_{\mathbf{a}}\mathbf{a} \;\middle|\; c_{\mathbf{a}} \in \mathbb{Z}\right\},$$

we introduce the *t-exceptional set* $\mathcal{E}_t(A)$:

$$\mathcal{P}_t(A) := \bigcup_{h\geq 1} (hA)^{(t)}, \quad \mathcal{E}_t(A) := (\mathcal{C}_A \cap \Lambda_A) \setminus \mathcal{P}_t(A).$$

We will establish the existence of a minimal threshold $h_t = h_t(A)$ such that for all $h \geq h_t$,

$$(hA)^{(t)} = (h\mathcal{H}(A) \cap \Lambda_A) \setminus \left(\bigcup_{\mathbf{v} \in \mathrm{ex}(\mathcal{H}(A))} (h\mathbf{v} - \mathcal{E}_t(\mathbf{v} - A)) \right). \tag{1.3}$$

Here, $h\mathcal{H}(A) = \{h\mathbf{p} \mid \mathbf{p} \in \mathcal{H}(A)\}$ denotes the h-dilate of $\mathcal{H}(A)$.

Granville–Shakan [**13**] proved the finiteness of h_1 in 2020, and in 2023, Granville–Shakan–Walker [**14**] provided the explicit bound:

$$h_1(A) \leq (d+1)2^{11d^2} d^{12d^6} |A|^{3d^2} \left(\max_{\mathbf{a},\mathbf{b} \in A} \|\mathbf{a} - \mathbf{b}\|_\infty \right)^{8d^6} \leq \left(d|A| \max_{\mathbf{a},\mathbf{b} \in A} \|\mathbf{a} - \mathbf{b}\|_\infty \right)^{13d^6}.$$

This was further improved in 2024 by Granville–Smith–Walker [**15**], who obtained the refined bound:

$$h_1(A) \leq (d+1)(d!)^2(|\mathrm{ex}(\mathcal{H}(A))| - d)\mathrm{Vol}(\mathcal{H}(A))^2.$$

Our result provides a bound for h_t in terms of specific geometric quantities associated with A. Let $\mathfrak{n}$ be a unit vector in $\mathbb{R}^d$ such that $\langle \mathfrak{n}, \mathbf{v} \rangle > 0$ for all $\mathbf{v} \in \mathcal{C}_A \setminus \{\mathbf{0}\}$, ensuring that $\mathcal{C}_A \setminus \{\mathbf{0}\}$ lies entirely on one side of the hyperplane orthogonal to $\mathfrak{n}$. Define

$$\delta_A = \delta_{A,\mathfrak{n}} := \min_{\mathbf{a} \in A \setminus \{\mathbf{0}\}} \langle \mathbf{a}, \mathfrak{n} \rangle, \qquad \Delta_A = \Delta_{A,\mathfrak{n}} := \max_{\mathbf{a} \in A \setminus \{\mathbf{0}\}} \langle \mathbf{a}, \mathfrak{n} \rangle. \tag{1.4}$$

That is, we project the elements of A onto the one-dimensional cone $\mathbb{R}_{\geq 0}\,\mathfrak{n}$ and define δ_A (resp. Δ_A) as the smallest (resp. largest) nonzero projection length. These constants play a key role in the estimates of the structure theorem.

Lemma 1.3. *There exists a minimum $\varphi = \varphi_{A,t} \in \mathbb{R}_{\geq 1}$ such that, for every real $\lambda \geq \varphi$, we have*

$$\Big((\lambda\mathcal{H}(A) \cap \Lambda_A) \setminus \mathcal{E}_t(A) \Big) + A = \Big((\lambda + 1)\mathcal{H}(A) \cap \Lambda_A \Big) \setminus \mathcal{E}_t(A).$$

Theorem 1.4 (t-structure)**.** *The set $(hA)^{(t)} \subseteq \mathbb{Z}^d$ is structured as in* (1.3) *for every*

$$h \geq \max_{\substack{\mathbf{0} \in B \subseteq \mathrm{ex}(\mathcal{H}(A)) \\ |B| = d+1 \\ \mathrm{span}_{\mathbb{R}}(B) = \mathbb{R}^d}} \left(\sum_{\mathbf{b} \in B} \left\lceil \frac{\Delta_{\mathbf{b}-A}}{\delta_{\mathbf{b}-A}} \varphi_{\mathbf{b}-A,t} \right\rceil \right),$$

where $\varphi_{\mathbf{b}-A,t}$ is the constant from Lemma 1.3 for the set $\mathbf{b} - A$.

Remark. Note that the bound in Theorem 1.4 depends on the choice of $\mathbf{n}$ in (1.4). The bound is valid for all valid choices of $\mathfrak{n}$, so one could, in principle, find the $\mathfrak{n}$ that yields the minimum Δ_A/δ_A.

Lemma 1.3 and Theorem 1.4 are proven in Section 2.4. We note that Theorem 1.4 can be seen as a generalization of Theorem 1.1 for $d \geq 2$ – see Remark 2.22.

1.1.4. Size of $(hA)^{(t)}$

In 1992, Khovanskii [**20**] showed that for every finite set $A \subseteq \mathbb{Z}^d$ there exists a polynomial $P_A \in \mathbb{Q}[x]$ of degree at most d, and a threshold $h_1^{\mathrm{Kh}} = h_1^{\mathrm{Kh}}(A)$, such that $hA = P_A(h)$ provided $h \geq h_1^{\mathrm{Kh}}$. His proof, however, did not give a concrete estimate for h_1^{Kh}. Later, Nathanson–Rusza [**31**] gave a combinatorial proof of this result, but this did not produce an effective bound on h_1^{Kh} either. Curran–Goldmakher [**7**] obtained explicit bounds for h_1^{Kh} when $\mathcal{H}(A)$ is a d-simplex, or when $\mathcal{H}(A)$ is d-dimensional and $|A| = d+1$ or $d+2$. The first effective bounds for arbitrary d and arbitrary $A \subseteq \mathbb{Z}^d$ were obtained by Granville–Shakan–Walker [**14**], who showed that

$$h_1^{\mathrm{Kh}}(A) \leq \left(2|A| \max_{\mathbf{a},\mathbf{b} \in A} \|\mathbf{a} - \mathbf{b}\|_\infty\right)^{(d+4)|A|}$$

This was improved by Granville–Smith–Walker [**15**], who showed that

$$h_1^{\mathrm{Kh}} \leq d!|A|^2 \mathrm{Vol}(\mathcal{H}(A)) - |A| + 1.$$

In Section 2.4, we will prove a generalization of Khovanskii's theorem for $(hA)^{(t)}$:

Theorem 1.5 (t-Khovanskii)**.** *If $A \subseteq \mathbb{Z}^d$ is finite, then for every $t \geq 1$ there is $h_t^{\mathrm{Kh}}(A) \in \mathbb{Z}_{\geq 1}$ such that, for every $h \geq h_t^{\mathrm{Kh}}(A)$, we have*

$$|(hA)^{(t)}| = P_{A,t}(h),$$

where $P_{A,t}(x) \in \mathbb{Q}[x]$ is a polynomial of degree $\leq d$.

1.2. Knights are 24/13 times faster than the king

Using the theory of sumsets, we will address the following question in Chapter 3: On an infinite chess board, how much faster can the knight reach a square when compared to the king, on average? More generally, for coprime $b > a \in \mathbb{Z}_{\geq 1}$ such that $a+b$ is odd, define the (a,b)-knight and the king as

$$\mathrm{N}_{a,b} = \{(a,b), (b,a), (-a,b), (-b,a), (-b,-a), (-a,-b), (a,-b), (b,-a)\},$$

$$\mathrm{K} = \{(1,0), (1,1), (0,1), (-1,1), (-1,0), (-1,-1), (0,-1), (1,-1)\} \subseteq \mathbb{Z}^2,$$

respectively. One way to formulate this question is by asking for the average ratio, for $\mathbf{p} \in \mathbb{Z}^2$ in a box, between $\min\{h \in \mathbb{Z}_{\geq 1} \mid \mathbf{p} \in h\mathrm{N}\}$ and $\min\{h \in \mathbb{Z}_{\geq 1} \mid \mathbf{p} \in h\mathrm{K}\}$, where hA is the h-fold sumset of A. We show that this ratio equals $2(a+b)b^2/(a^2+3b^2)$.

1.2.1. The king and the (a,b)-knight

Let $A \subseteq \mathbb{Z}^2$ be a finite set. For each $\mathbf{p} \in \mathbb{Z}^2$, we are interested in determining the smallest $h \geq 1$ for which we can write $\mathbf{p} = \mathbf{a}_1 + \cdots + \mathbf{a}_h$, where $\mathbf{a}_i \in A$ for $1 \leq i \leq h$ are not necessarily distinct. Writing $hA = \{\mathbf{a}_1 + \cdots + \mathbf{a}_h \mid \mathbf{a}_1, \ldots, \mathbf{a}_h \in A\}$, we define $A(0,0) := 0$ and, for $(x,y) \neq (0,0)$,

$$A(x,y) := \min\{h \geq 1 \mid (x,y) \in hA\}. \tag{1.5}$$

In Chapter 3, we will study the behaviour of $A(x,y)$ for a particular class of sumsets. Thinking of $\mathbb{Z}^2$ as an infinite chess board, a finite set A may be thought of as a *piece* placed at the origin, being able to move only to $\mathbf{a} \in A$. Then, in two moves, the piece is able to reach every point in $2A$, and so on. We say that A is:

- *Primitive* if $A(x,y)$ is well-defined for every $x,y \in \mathbb{Z}$;
- *Symmetric* if $(a,b) \in A$ implies $(\delta_1 a, \delta_2 b)$, $(\delta_1 b, \delta_2 a) \in A$ for every choice of $\delta_1,\delta_2 \in \{-1,+1\}$;

The two pieces that will concern us are the following:

a) The *king* $\mathrm{K} = \{(1,0),(1,1),(0,1),(-1,1),(-1,0),(-1,-1),(0,-1),(1,-1)\}$ is the smallest symmetric piece with $(1,0),(1,1) \in \mathrm{K}$.

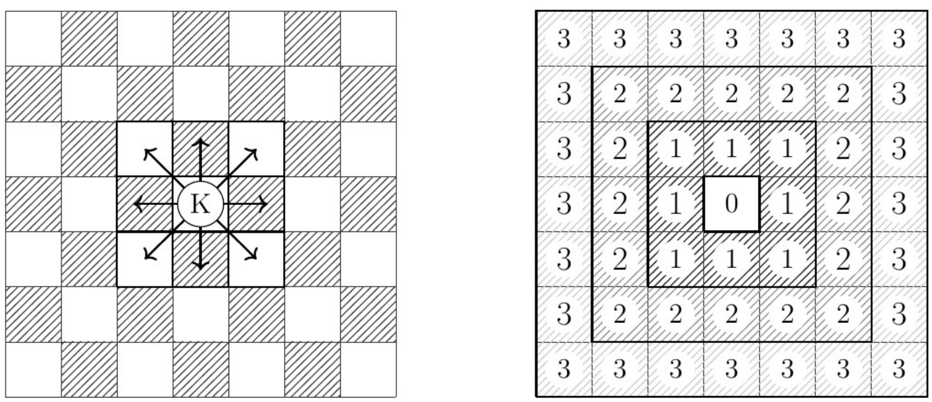

Fig. 2. The king's movements (left) and $\mathrm{K}(x,y)$ (right).

b) For $a,b \in \mathbb{Z}_{\geq 1}$, we define the (a,b)-*knight* $\mathrm{N}_{a,b}$ by the set of moves

$$\begin{aligned}\mathrm{N}_{a,b} := \{\, &(b,a),(a,b),(-a,b),(-b,a),\\ &(-b,-a),(-a,-b),(a,-b),(b,-a)\,\};\end{aligned}$$

in other words, $\mathrm{N}_{a,b}$ is the smallest symmetric piece with $(a,b) \in \mathrm{N}_{a,b}$. The usual chess knight is the (1,2)-knight, which we call just *knight* and denote by N.

Not all (a,b)-knights are primitive. In fact, for $\mathrm{N}_{a,b}$ to be primitive, it is necessary and sufficient that $\gcd(a,b) = 1$ and $a+b$ be odd. To see this, color $\mathbb{Z}^2$ like a chess board:

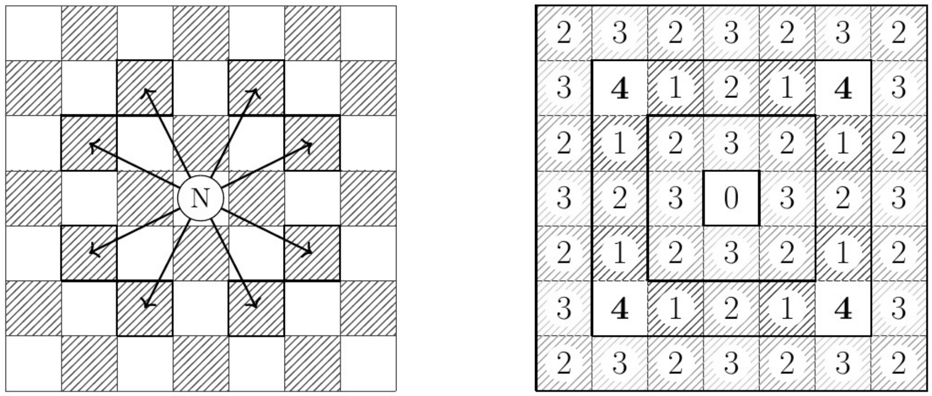

Fig. 3. The knight's movements (left) and $\mathrm{N}(x,y)$ (right).

paint (x,y) white if $2 \mid x+y$, and black otherwise. The necessary direction is then easy: $\gcd(a,b) \mid \gcd(x,y)$ for every point (x,y) accessible to $\mathrm{N}_{a,b}$, and if $a+b$ is even then $\mathrm{N}_{a,b}$ never accesses black points.

For the sufficient direction, by the symmetries of $\mathrm{N}_{a,b}$, it suffices to show that it can access $(1,0)$. Since $(b,a)+(b,-a)=(2b,0)$ and $(a,b)+(a,-b)=(2a,0)$, the (a,b)-knight can access every point of the form $(2(ax+by),0)$ for $x,y \in \mathbb{Z}$; which, since $\gcd(a,b)=1$, implies that $\mathrm{N}_{a,b}$ can access $(2,0)$. By symmetry, it also access $(2x,2y)$ for every $x,y \in \mathbb{Z}$. If a is odd (so b is even), then $(1-a,-b)$ is of the form $(2x,2y)$; applying the move (a,b), we get to $(1,0)$. The argument for a odd and b even goes similarly.

By the symmetries of $\mathrm{N}_{a,b}$, to understand the behaviour of $\mathrm{N}_{a,b}(x,y)$ it suffices to study $x \geq y \in \mathbb{Z}_{\geq 0}$, where $\mathrm{K}(x,y)=x$. We will show the following:

Theorem 1.6. *Let $b > a \geq 1$ be integers with $\gcd(a,b)=1$ and $a+b$ odd, and let $x \geq y \in \mathbb{Z}_{\geq 0}$.*

(i) *If $y \leq \frac{a}{b}x$, then $\mathrm{N}_{a,b}(x,y) = \frac{x}{b} + O(b)$.*

(ii) *If $y > \frac{a}{b}x$, then $\mathrm{N}_{a,b}(x,y) = \frac{x+y}{a+b} + O(b)$.*

In Subsection 3.1.2, we describe the distribution of N/K.

1.2.2. Average velocity in a box

Every finite set A induces a metric $d_A(\mathbf{p},\mathbf{q}) := A(\mathbf{q}-\mathbf{p})$ for $\mathbf{p},\mathbf{q} \in \mathbb{Z}^2$. The king's metric coincides with the one induced by the max norm

$$\|(x,y)\|_\infty = \max\{|x|,|y|\},$$

and thus we equip $\mathbb{Z}^2$ with this metric. For $h \geq 1$, write

$$\mathcal{B}_h := \{\mathbf{p} \in \mathbb{Z}^2 \mid \|\mathbf{p}\|_\infty \leq h\}, \qquad \mathcal{B}_h^* := \mathcal{B}_h \setminus \{(0,0)\}$$

for the ball and punctured ball of radius h, respectively. Note that $\mathcal{B}_h = \bigcup_{\ell=1}^{h} \ell\mathrm{K}$ and $\partial\mathcal{B}_h = \{\mathbf{p} \in \mathbb{Z}^2 \mid \|\mathbf{p}\|_\infty = h\} = h\mathrm{K} \setminus \bigcup_{\ell=0}^{\ell-1} \ell\mathrm{K}$. We have $|\partial\mathcal{B}_h| = 8h$ and $|\mathcal{B}_h^*| = 4h(h+1)$.

What is the average value of $A(x,y)$ in $\mathcal{B}_h$? For instance, the king K is such that $\mathrm{K}(x,y) = \ell$ if and only if $(x,y) \in \partial\mathcal{B}_\ell$; hence,

$$\frac{1}{|\mathcal{B}_h^*|} \sum_{\mathbf{p}\in\mathcal{B}_h^*} \mathrm{K}(\mathbf{p}) = \frac{1}{4h(h+1)} \sum_{\ell=1}^{h} \ell \cdot 8\ell = \frac{2h}{3} + \frac{1}{3}.$$

Thus, we consider the following notion of velocity, which can be understood intuitively as how fast the king K sees the piece A moving (see Remark 3.3): For a finite primitive piece $A \subseteq \mathbb{Z}^2$, the *average velocity* $v = v_{\mathrm{K}}$ of A is given by

$$v(A) := \lim_{h\to\infty} \frac{2h}{3} \left(\frac{1}{|\mathcal{B}_h|} \sum_{\mathbf{p}\in\mathcal{B}_h} A(\mathbf{p}) \right)^{-1}. \tag{1.6}$$

The number $v(A)$ may be thought of as controlling how fast A spreads through $\mathcal{B}_h$. Intuitively, from Theorem 1.6, one might conclude that the knight is almost, although not quite, *twice* as fast as the king. Points of the type $(x,0)$, for example, can be accessed by the knight in around $x/2$ moves, while points of the form (x,x) can be accessed in around $2x/3$ moves. We will show that

$$\frac{\sum_{\mathbf{p}\in\mathcal{B}_h} \mathrm{K}(\mathbf{p})}{\sum_{\mathbf{p}\in\mathcal{B}_h} \mathrm{N}(\mathbf{p})} \xrightarrow{h\to+\infty} \frac{24}{13}.$$

More generally:

Theorem 1.7. *Let $b > a \geq 1$ be integers with $\gcd(a,b) = 1$ and $a+b$ odd. Then:*

$$v(\mathrm{N}_{a,b}) = \frac{2(a+b)b^2}{a^2+3b^2}.$$

See Remark 3.4 for a consequence of Theorem 1.7 when one takes a, b to be consecutive Fibonacci numbers — which we call *Fiboknights*.

1.3. Representation functions with prescribed rates of growth

The representation of integers as sums of elements drawn from specific subsets of natural numbers has been a longstanding focus in additive number theory, with applications ranging from understanding the distribution of prime numbers to uncovering the behavior of structured sets like squares, cubes, or higher k-th powers.

Let $A \subseteq \mathbb{Z}$ be a subset of the integers and $h \geq 2$ be an integer. The function

$$R_{A,h}(n) := \#\{\{x_1, \ldots, x_h\} \subseteq A \text{ multiset} \mid x_1 + \cdots + x_h = n\}$$

counts the number of ways to express n as a sum of h elements from A, ignoring order. In 2004, Nathanson [**28**] showed that for any $h \geq 2$ and any function $F : \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ with finitely many zeros, there exists a set $A \subseteq \mathbb{Z}$ such that $R_{A,h}(n) = F(n)$. This completely characterizes representation functions for subsets of $\mathbb{Z}$ that represent all but finitely many integers. Nathanson later posed the more challenging problem of determining what could be said about the case $A \subseteq \mathbb{Z}_{\geq 0}$.

In Chapter 4 we address this question. For a subset $A \subseteq \mathbb{Z}_{\geq 0}$, an integer $h \geq 2$, and fixed positive integers $b_1, \ldots, b_h$ with gcd $= 1$, we consider the representation function

$$r_{A,h}(n) = r_{A,h}^{(b_1,\ldots,b_h)}(n) := \#\{(x_1, \ldots, x_h) \in A^h \mid b_1x_1 + \cdots + b_hx_h = n\} \tag{1.7}$$

We investigate for which functions $F : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ satisfying $F(n) \leq r_{\mathbb{Z}_{\geq 0},h}(n)$, we can find $A \subseteq \mathbb{Z}_{\geq 0}$ such that $r_{A,h}(n) \sim F(n)$. Building on work by Erdős–Tetali [**10**], Kim–Vu [**21**] and Vu [**40**], we show that if F is regularly varying, such an A exists if $F(n)/\log n \to \infty$. If only $r_{A,h}(n) \asymp F(n)$ is required, we can slightly broaden the range, proving the existence of A satisfying $r_{A,h}(n) \asymp F(n)$ for any increasing F with $F(2n) \ll F(n)$ satisfying either $\log n \ll F(n) \ll n^{\frac{1}{h-1}}$ or $(\log n)^{2h^2} \ll F(n) \ll n^{h-1}$, extending the original work of Erdős and Tetali.

A real-valued function $F : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ is called *regularly varying* if it is measurable and $\lim_{x\to\infty} F(\lambda x)/F(x)$ exists for every $\lambda > 0$. Regularly varying functions are of the form

$$F(x) = x^\kappa \psi(x),$$

where $\kappa \in \mathbb{R}$ and $\psi(x)$ is *slowly varying*, meaning $\lim_{x\to\infty} \psi(\lambda x)/\psi(x) = 1$ for every $\lambda > 0$. Slowly varying functions satisfy $\psi(x) = x^{o(1)}$ (see Bingham–Goldie–Teugels [**2**]). These functions provide a broad and flexible framework for describing growth conditions, encompassing a variety of natural cases.

1.3.1. Asymptotics

It is a classical result in additive combinatorics that there are

$$\left(1 + O\left(\frac{1}{n}\right)\right) \frac{1}{(h-1)!} \frac{n^{h-1}}{b_1 \cdots b_h} \tag{1.8}$$

nonnegative integer solutions to the equation $b_1x_1 + \cdots + b_hx_h = n$. Now let $A \subseteq \mathbb{Z}_{\geq 0}$, $h \geq 2$ be an integer, and suppose $b_1 = \cdots = b_h = 1$. In 1956, inspired by a problem of Sidon, Erdős [**8**] used probabilistic methods to show that there exists a subset $A \subseteq \mathbb{Z}_{\geq 0}$ such that $r_{A,2}(n) \asymp \log n$. Later work by Erdős [**9**, Corollary 3] established that for certain functions F

satisfying $\lim_{x\to\infty} F(x)/\log x = \infty$ (e.g., $F(x) = \log n \log\log n$), there exist subsets $A \subseteq \mathbb{Z}_{\geq 0}$ such that $r_{A,2}(n) \sim F(n)$.

In 1990, Erdős and Tetali [**10**] extended this result for any $h \geq 2$, showing the existence of subsets $A \subseteq \mathbb{Z}_{\geq 0}$ such that $r_{A,h}(n) \asymp \log n$. The restriction $b_1 = \cdots = b_h = 1$ was removed by Vu [**40**] in 2000. In Chapter 4, we will address the following:

Problem. *For which functions $1 \ll F(x) \ll x^{h-1}$ can we find a subset $A \subseteq \mathbb{Z}_{\geq 0}$ satisfying $r_{A,h}(n) \sim F(n)$? Or $r_{A,h}(n) \asymp F(n)$?*

This is a weaker form of a question asked by Nathanson (cf. [**28**, Problem 1]). In order to attack this question with analytic methods, we will assume certain regularity conditions on F, and that $F(x) \gg \log x$. In fact, Erdős [**8**, p. 132] inquired whether, if $b_1 = b_2 = 1$ and $r_{A,2}(n) > 0$ for large n, it is always the case that

$$\limsup_{n\to\infty} \frac{r_{A,2}(n)}{\log n} > 0. \tag{1.9}$$

This conjecture[5] naturally extends to general $r_{A,h}$ as defined in (1.7), and a heuristic in its favor is the subject of Theorem 1.12.

Our next theorem deals with F such that $F(x)/\log x \to \infty$ as $x \to \infty$, where Kim–Vu's inequality [**21**] paired with an inequality by Vu [**40**, Theorem 1.4] allows us to obtain asymptotics for regularly varying functions.

Theorem 1.8. *Let $h \geq 2$ be a given integer. Let F be a regularly varying function for which*

$$\frac{F(x)}{\log x} \xrightarrow{x\to\infty} \infty \quad \textit{and} \quad F(x) \leq (1+o(1))\frac{1}{(h-1)!}\frac{x^{h-1}}{b_1\cdots b_h}.$$

Then, there exists $A \subseteq \mathbb{Z}_{\geq 0}$ such that $r_{A,h}(n) \sim F(n)$.

Note that by (1.8), the upper bound covers as wide a range as possible. The proof also implies that we can take A satisfying $|A\cap[1,x]| \sim C\,(xF(x))^{1/h}$, where, if $F(x) = x^\kappa \phi(x)$,

$$C = \frac{h}{1+\kappa}\frac{\Gamma(1+\kappa)^{\frac{1}{h}}}{\Gamma(\frac{1+\kappa}{h})}(b_1\cdots b_h)^{(1+\kappa)/h^2}.$$

When $F(x) = x^\kappa$, we obtain power savings from Kim–Vu's inequality.

Corollary 1.9. *Let $h \geq 2$ be a given integer, and $0 < \kappa \leq h-1$ a real number. Then, for any $C \in \mathbb{R}_{>0}$, there exists $A \subseteq \mathbb{Z}_{\geq 0}$ such that $|A\cap[1,x]| = Cx^{(1+\kappa)/h} + O(x^{(1+\kappa)/2h}\log x)$ and*

$$r_{A,h}(n) = C^h\frac{(1+\kappa)^h}{h^h}\frac{\Gamma(\frac{1+\kappa}{h})^h}{\Gamma(1+\kappa)}\frac{n^\kappa}{(b_1\cdots b_h)^{\frac{1+\kappa}{h}}} + O(E_{h,\kappa}),$$

[5]This is a strong version of the Erdős–Turán conjecture for additive bases: Does $A + A = \mathbb{Z}_{\geq 0}$ necessarily imply that $r_{A,2}(n)$ is unbounded? More generally, if $|A\cap[1,x]| \gg x^{1/2}$, then is $r_{A,2}(n)$ necessarily unbounded?

where $E_{2,\kappa} := n^{\frac{\kappa}{2}}(\log n)^2$, $E_{3,\kappa} := n^{\frac{\kappa}{2}+\max\{0,\frac{\kappa}{3}-\frac{1}{2}\}}(\log n)^3$, *and for* $h \geq 4$,

$$E_{h,\kappa} := \begin{cases} n^{\frac{\kappa}{2}}(\log n)^h & \text{if } 0 \leq \kappa \leq \frac{2}{h-2}, \\ n^{(1-\frac{1}{h})\kappa-\frac{1}{h}} & \text{if } \frac{2}{h-2} < \kappa < h-2, \\ n^{(1-\frac{1}{2h})\kappa-\frac{1}{2}}(\log n)^h & \text{if } h-2 \leq \kappa \leq h-1. \end{cases}$$

Remark. An interesting subcase is the following: Writing $r_{A,h+1}(n) = r^{(1,\ldots,1)}_{A,h+1}(n)$ for the number of solutions $(x_1,\ldots,x_{h+1}) \in A^{h+1}$ to $x_1 + \cdots + x_{h+1} = n$, we obtain the existence of a set $A \subseteq \mathbb{Z}_{\geq 0}$ with $|A \cap [1,x]| = x^{1/h} + O(x^{1/2h}\log x)$ and

$$r_{A,h+1}(n) = \Gamma(1+1/h)^h\, n^{1/h} + O\Big(n^{1/2h}(\log n)^{h+1}\Big).$$

1.3.2. Order of magnitude

Under significantly weaker regularity hypotheses, one can still show the existence of sets $A \subseteq \mathbb{Z}_{\geq 0}$ such that $r_{A,h}(n) \asymp F(n)$, though we no longer obtain asymptotics.

Theorem 1.10. *Let $h \geq 2$ be a fixed integer, and let F be a positive, increasing, locally integrable real function satisfying $F(2x) \ll F(x)$. Suppose further that either*

$$\log x \ll F(x) \ll x^{\frac{1}{h-1}} \tag{1.10}$$

or

$$(\log x)^{2h^2} \ll F(x) \ll x^{h-1} \tag{1.11}$$

Then, there exists $A \subseteq \mathbb{Z}_{\geq 0}$ such that $|A \cap [1,x]| \asymp (xF(x))^{1/h}$ and $r_{A,h}(n) \asymp F(n)$.

The range (1.11) includes all regularly varying functions $x^\kappa\phi(x)$ with $\kappa > 0$, since $x^\kappa\phi(x) \asymp F(x)$ for some increasing F. Moreover, it includes some functions of the form $x^{k(x)}$ where $k(x)$ varies, such as $F(x) = x^{2+\sin(\log\log x)}$. The assumption $F(2x) \ll F(x)$ prevents rapid fluctuations but allows for mild oscillation.

The reason for dividing into the two ranges (1.10) and (1.11) lies in the different methods required to handle them. In the higher-growth case (1.11), the assumption that F is increasing plays a crucial role in the argument. The lower-growth case (1.10) can be treated under more general conditions and follows from the more technical result below, a direct generalization of the main theorem in [**35**], incorporating the weakest regularity assumptions our methods allow.

Theorem 1.11. *Let $h \geq 2$ be a given integer, and let $\psi(x) \gg \log x$ be an increasing slowly varying function. If*

(i) (Range) $(x\,\psi(x))^{1/h} \ll f(x) \ll \min\{(x\,\psi(x))^{1/(h-1)},\, x\}$,

(ii) (Regularity) $\int_1^x \frac{f(t)}{t}\,\mathrm{d}t \asymp f(x)$;

then there exists $A \subseteq \mathbb{Z}_{\geq 0}$ *such that* $|A \cap [1,x]| \asymp f(x)$ *and* $r_{A,h}(n) \asymp \frac{f(n)^h}{n}$.

Writing $f(x) := (xF(x))^{1/h}$, Theorem 1.11 implies that for every positive, locally integrable F in the range $\psi(x) \ll F(x) \ll x^{\frac{1}{h-1}}\psi(x)^{1+\frac{1}{h-1}}$ that satisfies

$$\frac{1}{x}\int_1^x F(t)\,\mathrm{d}t \asymp F(x)$$

(this is a consequence of Lemma 4.1), there exists $A \subseteq \mathbb{Z}_{\geq 0}$ such that $r_{A,h}(n) \asymp F(n)$.

Remark. Can the ranges (1.10) and (1.11) in Theorem 1.10 be merged to include all functions F satisfying $\log x \ll F(x) \ll x^{h-1}$? More ambitiously, can Theorem 1.11 be extended to cover the full range $(x \log x)^{1/h} \ll f(x) \ll x$?

1.3.3. What about $F(x) \ll \log(x)$?

Again taking $f(x) := (xF(x))^{1/h}$, we will use the probabilistic space of random subsets $0 \in \mathscr{A} \subseteq \mathbb{Z}_{\geq 0}$ generated by the measure $\Pr(n \in \mathscr{A}) = \min\{c\frac{f(n)}{n}, 1\}$ $(n \geq 1)$, where $c > 0$ is some real number, which is constructed in order to have, essentially,

$$|\mathscr{A} \cap [1,x]| \asymp f(x) \text{ with probability } 1,^6 \quad \text{and } \mathbb{E}(r_{\mathscr{A},h}(n)) \asymp c^h F(n).$$

Theorems 1.8–1.11 are proven by showing that $r_{\mathscr{A},h}$ concentrates around its mean; e.g., $r_{\mathscr{A},h}(n) \asymp \mathbb{E}(r_{\mathscr{A},h}(n))$ with probability 1 in Theorems 1.10, 1.11.[7] The next theorem shows that if $cf(n)$ is too small (i.e., the space is constructed so that $\mathbb{E}(r_{\mathscr{A},h}(n))$ is small), then not only will $r_{\mathscr{A},h}$ not concentrate, but also have infinitely many zeros with probability 1.

Theorem 1.12. *Fix* $0 < \varepsilon < \frac{1}{2}$. *Define the random set* $\mathscr{A} \subseteq \mathbb{Z}_{\geq 0}$ *by taking* $0 \in \mathscr{A}$ *and*

$$\Pr(n \in \mathscr{A}) = \min\left\{c\frac{(n\log(n))^{1/h}}{n}, 1\right\} \qquad (n \geq 1),$$

for $c = (1-\varepsilon)^{1/h}(b_1 \cdots b_h)^{1/h^2}/\Gamma(\frac{1}{h})$. *Then* $\mathbb{E}(r_{\mathscr{A},h}(n)) \sim (1-\varepsilon)\log n$ *as* $n \to \infty$, *but*

$$\Pr(r_{\mathscr{A},h}(n) = 0 \text{ infinitely often}) = 1. \tag{1.12}$$

This suggests a stronger version of (1.9):

[6] Precisely, $\Pr(\mathscr{A} \subseteq \mathbb{Z}_{\geq 0} \mid \exists C_1,C_2 \in \mathbb{R}_{>0} : \forall x \geq 1,\ C_1 f(x) \leq |\mathscr{A} \cap [1,x]| \leq C_2 f(x)) = 1$.

[7] Since finite intersections of events of probability 1 have probability 1 (and hence are non-empty), there must exist $A \subseteq \mathbb{Z}_{\geq 0}$ satisfying both $|A \cap [1,x]| \asymp f(x)$ and $r_{A,h}(n) \asymp F(n)$.

Conjecture 1.13. *If $r_{A,h}(n) > 0$ for all large n, then*

$$\limsup_{n\to\infty} \frac{r_{A,h}(n)}{\log n} \geq 1.$$

Note that the existence of thin bases does not directly contradict Conjecture 1.13 – cf., for instance, the constructions described in Nathanson [**29**].[8]

1.4. Waring and Waring–Goldbach subbases

Chapter 5 investigates subsets A of k-th powers $\mathbb{N}^k = \{n^k \mid n \in \mathbb{N}\}$ and k-th powers of primes $\mathbb{P}^k = \{p^k \mid p \text{ is prime}\}$, aiming to construct additive subbases that satisfy certain growth conditions on their representation functions. In this chapter,

$$r_{A,h}(n) := \{(x_1, \dots, x_h) \in A^h \mid x_1 + \cdots + x_h = n\}$$

(that is, $b_1 = \cdots = b_h = 1$).

1.4.1. Waring subbases

In 2000, Vu [**40**] showed that for each $k \geq 2$, there exists an integer $h_k \ll 8^k k^2$ such that for all $h \geq h_k$, there exists a subset $A \subseteq \mathbb{N}^k$ for which $r_{A,h}(n) \asymp \log n$. Later, Wooley [**42**] refined this bound, proving that

$$h_k \leq k\left(\log k + \log\log k + 2 + O\left(\frac{\log\log k}{\log k}\right)\right).$$

More recently, drawing from the work of Brüdern–Wooley [**5**], Pliego [**32**] further improved the bound to

$$h_k \leq \lceil k(\log k + 4.20032)\rceil,$$

showing that bounds for h_k essentially align with those for the asymptotic order of $\mathbb{N}^k$, as derived using the circle method. Pliego also established that for certain functions $\psi(x) = x^{o(1)}$ with $\lim_{x\to\infty} \psi(x)/\log x = \infty$ (e.g., $\psi(x) = \log n \log\log n$), there exist $A \subseteq \mathbb{N}^k$ such that

$$r_{A,h}(n) \sim \mathfrak{S}_{k,h}(n)\psi(n),$$

where $\mathfrak{S}_{k,h}(n)$ denotes the singular series associated with Waring's problem, defined by

$$S(a,q) := \sum_{r=1}^{q} e\left(\frac{ar^k}{q}\right), \qquad \mathfrak{S}_{k,h}(n) := \sum_{q\geq 1} \sum_{\substack{a=1\\(a,q)=1}}^{q} \frac{S(a,q)^h}{q^h} e\left(-\frac{na}{q}\right). \tag{1.13}$$

[8]E.g. Raikov–Stöhr's construction: In the case $h = 2$, take $A := S_1 \sqcup S_2$, where S_1 consists of only those non-negative integers which can be written as a sum of odd powers of 2, and S_2 of even powers. One has that $|A \cap [1,x]| \ll x^{1/2}$, yet $A + A = \mathbb{Z}_{\geq 0}$. However, the numbers $n_1 := 2 = 10_2$, $n_2 := 10 = 1010_2$, $n_3 := 42 = 101010_2$, etc., can be shown to have at least 2^{k-1} ($> \sqrt{n_k/3}$) representations.

For $h \geq 4k$, this series converges absolutely, and $\mathfrak{S}_{k,h}(n) \asymp 1$ (cf. Vaughan [**38**, Theorems 4.3, 4.6]).

For values of h as large as those in Vu's work, we show the existence of subbases of $\mathbb{N}^k$ with prescribed asymptotics:

Theorem 1.14. *Let $k \geq 2$ be an integer.*

(i) *There exists $h_k \leq k^2(\log k + \log\log k + O(1))$ such that the following holds: Let $h \geq h_k$, and $0 < \kappa < h/k - 1$. Then, for every $c > 0$, there exists a subset $A \subseteq \mathbb{P}^k$ such that*

$$r_{A,h}(n) \sim \mathfrak{S}_{k,h}(n)\, cn^{\kappa}.$$

The same holds for $\kappa = h/k - 1$ but with $0 < c \leq \frac{\Gamma(1+1/k)^h}{\Gamma(h/k)}$.

(ii) *There exists $h_k' \ll 8^k k^2$ such that the following holds: Let $h \geq h_k'$, and F be a regularly varying function satisfying*

$$\lim_{x\to\infty} \frac{F(x)}{\log x} = \infty, \qquad F(x) \leq (1 + o(1)) \frac{\Gamma(1+1/k)^h}{\Gamma(h/k)} x^{h/k-1}.$$

Then, there exists a subset $A \subseteq \mathbb{N}^k$ such that

$$r_{A,h}(n) \sim \mathfrak{S}_{k,h}(n) F(n).$$

In both cases, $\mathfrak{S}_{k,h}(n)$ is the singular series for Waring's problem (1.13)*.*

1.4.2. Waring–Goldbach subbases

Let $k \geq 1$. Given a prime p, let $\theta = \theta(k,p)$ be the unique integer such that $p^\theta \mid k$ but $p^{\theta+1} \nmid k$. Define

$$\gamma = \gamma(k,p) := \begin{cases} \theta + 2 & \text{if } p = 2, 2 \mid k, \\ \theta + 1 & \text{otherwise,} \end{cases} \qquad K(k) := \prod_{(p-1)\mid k} p^{\gamma}. \tag{1.14}$$

If a prime q is coprime to $K(k)$, then $q^k \equiv 1 \pmod{p^\gamma}$ whenever $(p-1) \mid k$, since $\varphi(p^\gamma) = p^\theta(p-1) \mid k$ for p odd (and $\varphi(2^\gamma)/2 \mid k$), where $\varphi(n) := |\{m \leq n \mid (m,n) = 1\}|$ is Euler's totient function. So by the Chinese remainder theorem, if n is a sum of h k-th powers of primes greater than $k+1$, then $n \equiv h \pmod{K(k)}$. Note that if k is odd, then $K(k) = 2$.

k	1	2	3	4	5	6	7	8	9	10
$K(k)$	2	24	2	240	2	504	2	480	2	264

Table 1. First few values of $K(k)$.

The singular series associated to Waring–Goldbach's problem is defined as

$$\mathfrak{S}^*_{k,h}(n) := \sum_{q\geq 1} \sum_{\substack{a=1\\(a,q)=1}}^{q} \frac{S(q,a)^h}{\varphi(q)^h} e\left(-\frac{na}{q}\right), \tag{1.15}$$

where $S(q,a)$ is as in (1.13). For $h \geq 2^k+1$, we have $\mathfrak{S}^*_{k,h}(n) \asymp 1$ for $n \equiv h \pmod{K(k)}$ (see Lemma 5.14). In order to obtain thin subbases of prime powers, we first prove a result similar to Wooley [**43**, Theorem 1.1] for $\mathbb{P}^k$.

Theorem 1.15. *Let $k \geq 1$ be an integer, and*

$$h \geq h^*_k := \begin{cases} 2^k + 1 & \text{if } 1 \leq k \leq 11, \\ \lceil 2k^2(2\log k + \log\log k + 2.5)\rceil & \text{if } k \geq 12. \end{cases} \tag{1.16}$$

For every $\omega \geq 1/h$, we have

$$\sum_{\substack{x_1,\ldots,x_h \in \mathbb{P}^k\\ x_1+\cdots+x_h=n}} (x_1\cdots x_h)^{\omega-\frac{1}{k}}(\log x_1 \cdots \log x_h) = \mathfrak{S}^*_{k,h}(n)\,\frac{\Gamma(\omega)^h}{\Gamma(h\omega)}\,n^{h\omega-1} + O_R\left(\frac{n^{h\omega-1}}{(\log n)^R}\right)$$

for every $R > 1$.

Note that the implied constant also depends on h, k, but we omit this dependency. With this, we will show the following:

Theorem 1.16. *Let $k \geq 1$ be an integer, $h \geq h^*_k$ where h^*_k is as in* (1.16)*, and suppose that $n \equiv h \pmod{K(k)}$.*

(i) *For every $0 < \kappa < h/k - 1$ and $c > 0$, there exists a subset $A \subseteq \mathbb{P}^k$ such that*

$$r_{A,h}(n) \sim \mathfrak{S}^*_{k,h}(n)\, cn^{\kappa},$$

where $\mathfrak{S}^*_{k,h}(n)$ is the singular series for Waring–Goldbach's problem (1.15).

(ii) *Let $0 \leq \kappa \leq h/k-1$, ψ be a measurable positive real function satisfying $\psi(x) \asymp_\lambda \psi(x^\lambda)$ for every $\lambda > 0$, and write $F(x) = x^\kappa\psi(x)$. If $\log x \ll F(x) \ll x^{h/k-1}/(\log x)^h$, then there exists a subset $A \subseteq \mathbb{P}^k$ such that*

$$r_{A,h}(n) \asymp F(n).$$

The hypothesis for ψ in Theorem 1.16 (ii) is more restrictive than slow variation, since we always have $\psi \asymp \phi$ for some ϕ of slow variation (cf. Remark 5.25). Nonetheless, Theorem 1.16 implies, in particular, that there exists $A \subseteq \mathbb{P}$ such that $r_{A,3}(n) \asymp \log n$ for n odd, there exists $B \subseteq \mathbb{P}^2$ such that $r_{B,5}(n) \asymp \log n$ for $n \equiv 5 \pmod{24}$, and so on.

Remark. Wirsing [**41**, Theorem 2] showed that for every $h \geq 3$, there exists a subset $A \subseteq \mathbb{P}$ with $|A \cap [1,x]| \ll (x\log x)^{1/h}$ such that every $n \equiv h \pmod 2$ can be written as a sum of h elements of A. Our result extends this, by showing the existence of $B \subseteq \mathbb{P}$ with $|B \cap [1,x]| \asymp (x \log x)^{1/h}$ (by (1.17)) such that $r_{B,h}(n) \asymp \log n$ for $n \equiv h \pmod 2$.

Assuming the asymptotic version of Goldbach's conjecture, Granville [**12**, Theorem 2] showed that there is a subset $A \subseteq \mathbb{P}$ with $|A \cap [1,x]| \asymp (x \log x)^{1/2}$ such that every large even integer is the sum of two elements of A. Our result, however, does not apply to this case.

1.4.3. General setup

Theorems 1.14 and 1.16 will be derived from the more general Theorem 1.17 below. Let $B \subseteq \mathbb{Z}_{\geq 0}$ be a subset, and write $B(x) := |B \cap [1,x]|$. Let F be a regularly varying function. We make the following assumptions about B and F:

(i) (Regular variation) There is $\beta = \beta(B) > 0$ such that, for every fixed $\lambda \geq 1$,

$$B(\lambda x) \sim \lambda^\beta B(x).$$

(ii) (Low additive energy) There exists $H_{\text{(ii)}} \in \mathbb{Z}_{\geq 1}$ such that, for every $h \geq H_{\text{(ii)}}$,

$$\sum_{n \leq x} r_{B,h}(n)^2 \ll \frac{B(x)^{2h}}{x} x^{o(1)}.$$

(iii) (Counting solutions with weights) There exists $H_{\text{(iii)}} \in \mathbb{Z}_{\geq 1}$ such that the following holds: Let $h \geq H_{\text{(iii)}}$, and suppose $f(x) := (xF(x))^{1/h} = x^\omega \phi(x) \leq (1 + o(1))B(x)$, with $1/h \leq \omega \leq \beta$. Then:

$$\sum_{\substack{x_1,\dots,x_h \in B \\ x_1+\dots+x_h=n}} \frac{f(x_1)}{B(x_1)} \cdots \frac{f(x_h)}{B(x_h)} \sim \mathfrak{S}_{B,h}(n)\, C_{B,h,f}\, \frac{f(n)^h}{n},$$

where $C_{B,h,f} \in \mathbb{R}_{>0}$ is a constant, and $\mathfrak{S}_{B,h}(n)$ is some function of n satisfying

$$\mathfrak{S}_{B,h}(n) \asymp 1 \text{ for } n \in \mathscr{S}, \text{ for some subset } \mathscr{S} \subseteq \mathbb{Z}_{\geq 0}.$$

Condition (ii) asks for hB to have almost as low additive energy as possible, in the sense that $\sum_{n \leq x} r_{B,h}(n)^2 \geq (\sum_{n \leq x} r_{B,h}(n))^2/x \asymp B(x)^{2h}/x$ by Cauchy–Schwarz. It will only be used in the proof of Proposition 5.2. In condition (iii), we roughly ask for the expectation of $r_{\mathscr{A},h}(n)$ for a random subset $\mathscr{A} \subseteq B$ of density $|\mathscr{A} \cap [1,x]| \approx f(x)$ to have a certain asymptotic behaviour, over a subset $\mathscr{S} \subseteq \mathbb{Z}_{\geq 0}$ that is usually an arithmetic progression.

Theorem 1.17. *Let $B \subseteq \mathbb{Z}_{\geq 0}$ be a subset and F be a regularly varying function satisfying conditions (i)–(iii). Let $h \geq \max\{2H_{\text{(ii)}} + 1, H_{\text{(iii)}}\}$ be an integer. If $F(n)/\log n \to \infty$ as $n \to \infty$, then there exists $A \subseteq B$ such that*

$$r_{A,h}(n) \sim \mathfrak{S}_{B,h}(n)F(n) \quad \textit{for} \quad n \in \mathscr{S}.$$

If $F(n) \gg \log n$, *then there exists* $A \subseteq B$ *such that*

$$r_{A,h}(n) \asymp F(n) \quad \textit{for} \quad n \in \mathscr{S}.$$

In combination with Lemma 5.1, the proof of Theorem 1.17 also implies that for a given $F(x) = x^\kappa \psi(x)$, the set A satisfies

$$|A \cap [1,x]| \sim \frac{h\beta}{1+\kappa} C_{B,h,f}^{-1/h} (xF(x))^{1/h}. \tag{1.17}$$

Chapter 2

On the structure of t-representable sumsets

In this chapter, we will prove Theorems 1.1–1.5 from the introduction, which establish bounds for the structure threshold of t-representable sumset $(hA)^{(t)}$ when $A \subseteq \mathbb{Z}$ and $A \subseteq \mathbb{Z}^d$. Our results provide asymptotically optimal bounds on the threshold h in terms of the Frobenius number $\mathrm{Fr}_t(A)$ in $\mathbb{Z}$, and generalize previous theorems in $\mathbb{Z}^d$ for $t = 1$ to arbitrary t.

2.1. Estimating $\mathrm{Fr}_t(A)$

As in Subsection 1.1.2, let $m \geq 2$, $\ell \geq 1$, and

$$A = \{0 = a_0 < a_1 < \cdots < a_\ell < a_{\ell+1} = m\} \subseteq \mathbb{Z}_{\geq 0}$$

be a finite set with $\gcd(A) = 1$. For $h \geq 1$, write

$$R_{A,h}(n) = \{(k_0, \ldots, k_{\ell+1}) \in \mathbb{Z}_{\geq 0}^{\ell+2} \mid k_0 a_0 + \cdots + k_{\ell+1} a_{\ell+1} = n,\ \textstyle\sum_{i=0}^{\ell+1} k_i = h\}$$

for the number of ways to write n as a sum of h elements of A, and

$$R_A(n) := \lim_{h\to\infty} R_{A,h}(n) = \{(k_0, \ldots, k_{\ell+1}) \in \mathbb{Z}_{\geq 0}^{\ell+2} \mid k_0 a_0 + \cdots + k_{\ell+1} a_{\ell+1} = n\}$$

for the *total representation function* of A.

Proposition 2.1. *For every $n \geq 0$, we have*

$$R_A(n) \ \leq\ \frac{1}{\ell!} \frac{(n + a_1 \sum_{j=2}^{\ell+1} a_j)^\ell}{a_1 \cdots a_\ell m}.$$

Moreover, if $n \geq (a_1 - 1) \sum_{j=2}^{\ell+1} a_j$, then

$$R_A(n) \ \geq\ \frac{1}{\ell!} \frac{(n - (a_1 - 1) \sum_{j=2}^{\ell+1} a_j)^\ell}{a_1 \cdots a_\ell m}$$

To prove this, we will need the following standard lattice point counting lemma:

Lemma 2.2. *Let $d \geq 2$ be an integer, and $N_1, N_2, \ldots, N_d \in \mathbb{Z}_{\geq 0}$. For $R \in \mathbb{R}_{\geq 0}$, define the d-simplex*

$$\varDelta_R(N_1, \ldots, N_d) := \{(x_1, \ldots, x_d) \in (\mathbb{R}_{\geq 0})^d \mid x_1N_1 + x_2N_2 + \cdots + x_dN_d \leq R\}.$$

Then,

$$\mathrm{vol}_{\mathbb{R}^d} \varDelta_R(N_1, \ldots, N_d) \leq |\varDelta_R(N_1, \ldots, N_d) \cap \mathbb{Z}^d| \leq \mathrm{vol}_{\mathbb{R}^d} \varDelta_{R+\sum_{i=1}^d N_i}(N_1, \ldots, N_d), \tag{2.1}$$

and

$$\mathrm{vol}_{\mathbb{R}^d} \varDelta_R(N_1, \ldots, N_d) = \frac{1}{d!} \frac{R^d}{N_1 \cdots N_d}. \tag{2.2}$$

Proof. To each point $\mathbf{p} = (p_1, \ldots, p_d) \in \varDelta_R(N_1, \ldots, N_d) \cap \mathbb{Z}^d$ consider the unit hypercube

$$H(\mathbf{p}) := \{(p_1 + y_1, \ldots, p_d + y_d) \mid 0 \leq y_1, \ldots, y_d \leq 1\} = \mathbf{p} + H(\mathbf{0}).$$

The union $\bigcup_{\mathbf{p} \in \varDelta_R(N_1,\ldots,N_d) \cap \mathbb{Z}^d} H(\mathbf{p})$ covers $\varDelta_R(N_1, \ldots, N_d)$. Therefore

$$\begin{aligned} |\varDelta_R(N_1, \ldots, N_d) \cap \mathbb{Z}^d| &= \mathrm{vol}_{\mathbb{R}^d}\Bigg(\bigcup_{\mathbf{p} \in \varDelta_R(N_1,\ldots,N_d) \cap \mathbb{Z}^d} H(\mathbf{p})\Bigg) \\ &\geq \mathrm{vol}_{\mathbb{R}^d} \varDelta_R(N_1, \ldots, N_d). \end{aligned}$$

Moreover,

$$\begin{aligned} &\mathrm{vol}_{\mathbb{R}^d}\Bigg(\bigcup_{\mathbf{p} \in \varDelta_R(N_1,\ldots,N_d) \cap \mathbb{Z}^d} H(\mathbf{p})\Bigg) \\ &\leq \mathrm{vol}_{\mathbb{R}^d}\{(x_1, \ldots, x_d) \in (\mathbb{R}_{\geq 0})^d \mid (x_1 - 1)N_1 + (x_2 - 1)N_2 + \cdots + (x_d - 1)N_d \leq R\} \\ &= \mathrm{vol}_{\mathbb{R}^d}\left\{(x_1, \ldots, x_d) \in (\mathbb{R}_{\geq 0})^d \;\middle|\; x_1N_1 + x_2N_2 + \cdots + x_dN_d \leq R + \sum_{i=1}^d N_i\right\} \\ &= \mathrm{vol}_{\mathbb{R}^d}\Delta_{R+\sum_{i=1}^d N_i}(N_1, \ldots, N_d), \end{aligned}$$

thus proving (2.1). For (2.2), we have

$$\begin{aligned} \mathrm{vol}_{\mathbb{R}^d} \varDelta_R(N_1, \ldots, N_d) &= \int_{\substack{x_1N_1+\ldots+x_dN_d \leq R \\ x_1,\,\ldots,\,x_d \geq 0}} \mathrm{d}x_1 \cdots \mathrm{d}x_d \\ &= \frac{R^d}{N_1 \cdots N_d} \int_{\substack{x_1+\ldots+x_d \leq 1 \\ x_1,\,\ldots,\,x_d \geq 0}} \mathrm{d}x_1 \cdots \mathrm{d}x_d = \frac{1}{d!} \frac{R^d}{N_1 \cdots N_d}. \end{aligned}$$

□

Lemma 2.3. *Let $A = \{0 = a_0 < a_1 < \cdots < a_\ell < a_{\ell+1} =: m\} \subseteq \mathbb{Z}$ be a finite set of integers with $\gcd(A) = 1$. For $n \geq 0$, let*

$$S(n) := \left\{(\mu_2, \ldots, \mu_{\ell+1}) \in \{0, \ldots, a_1 - 1\}^\ell \;\middle|\; \sum_{j=2}^{\ell+1} a_j\mu_j \equiv n \pmod{a_1}\right\}.$$

Then $|S(n)| = a_1^{\ell-1}$.

Proof. If $0 \le b < a_1$ is such that $n \equiv b \pmod{a_1}$ then $|S(n)| = |S(b)|$. Let $g := \gcd(a_2, \ldots, a_\ell, m)$ and $x_2, \ldots, x_{\ell+1} \in \mathbb{Z}$ be such that $\sum_{j=2}^{\ell+1} a_j x_j = g$. For each $(\mu_2, \ldots, \mu_{\ell+1}) \in S(b)$ we have $(\mu_2', \ldots, \mu_{\ell+1}') \in S(b+g)$, where $0 \le \mu_j' < a_1$ is such that $\mu_j' \equiv \mu_j + x_j \pmod{a_1}$. Hence, $|S(b)| = |S(b+g)|$.

By the definition of g, $\gcd(a_1, g) = 1$, so $\{b, b+g, \ldots, b+(a_1-1)g\}$ is a complete set of representatives of residues modulo a_1. Extending the argument above, we get that $|S(b)| = |S(b+g)| = \cdots = |S(b+(a_1-1)g)|$. Therefore, as $\sum_{b=0}^{a_1-1} |S(b)| = \#\{(\mu_2, \ldots, \mu_{\ell+1}) \in \{0, \ldots, a_1-1\}^\ell\} = a_1^\ell$, $|S(n)| = a_1^{\ell-1}$ for every $n \ge 0$. □

Proof of Proposition 2.1. For each representation $k_1 a_1 + \cdots + k_\ell a_\ell + k_{\ell+1} m = n$, we can write $k_j = \mu_j + a_1 q_j$ for some unique $\mu_j \in \{0, \ldots, a_1 - 1\}$ and $q_j \ge 0$, so that

$$k_1 + \sum_{j=2}^{\ell+1} a_j q_j = \frac{n - \sum_{j=2}^{\ell+1} a_j \mu_j}{a_1}.$$

Thus,

$$\begin{aligned} R_A(n) &= \#\Big\{(k_1, \ldots, k_{\ell+1}) \in (\mathbb{Z}_{\ge 0})^{\ell+1} \;\Big|\; k_1 a_1 + \cdots + k_\ell a_\ell + k_{\ell+1} m = n\Big\} \\ &= \sum_{(\mu_2, \ldots, \mu_{\ell+1}) \in S(n)} R_{\{1, a_2, \ldots, a_\ell, m\}}\left(\frac{n - \sum_{j=2}^{\ell+1} a_j \mu_j}{a_1}\right), \end{aligned}$$

where $S(n)$ is as in Lemma 2.3. For each $N \ge 0$, in the notation of Lemma 2.2, we have

$$\begin{aligned} R_{\{1, a_2, \ldots, a_\ell, m\}}(N) &= \#\Big\{(q_2, \ldots, q_{\ell+1}) \in (\mathbb{Z}_{\ge 0})^{\ell} \;\Big|\; q_2 a_2 + \cdots + q_\ell a_\ell + q_{\ell+1} m \le N\Big\} \\ &= |\Delta_N(a_2, \ldots, a_{\ell+1}) \cap \mathbb{Z}^\ell|, \end{aligned}$$

so, by Lemma 2.2,

$$\frac{1}{\ell!} \frac{N^\ell}{a_2 \cdots a_\ell m} \;\le\; R_{\{1, a_2, \ldots, a_\ell, m\}}(N) \;\le\; \frac{1}{\ell!} \frac{(N + \sum_{j=2}^{\ell+1} a_j)^\ell}{a_2 \cdots a_\ell m}.$$

Therefore, since $0 \le n - (a_1 - 1)\sum_{j=2}^{\ell+1} a_j \le n - \sum_{j=2}^{\ell+1} a_j \mu_j \le n$, we have

$$|S(n)| \cdot \frac{1}{\ell!} \frac{(n - (a_1-1)\sum_{j=2}^{\ell+1} a_j)^\ell}{a_1^\ell \, a_2 \cdots a_\ell m} \;\le\; R_A(n) \;\le\; |S(n)| \cdot \frac{1}{\ell!} \frac{(n + a_1 \sum_{j=2}^{\ell+1} a_j)^\ell}{a_1^\ell \, a_2 \cdots a_\ell m}$$

so, by Lemma 2.3:

$$\frac{1}{\ell!} \frac{(n - (a_1-1)\sum_{j=2}^{\ell+1} a_j)^\ell}{a_1 \cdots a_\ell m} \;\le\; R_A(n) \;\le\; \frac{1}{\ell!} \frac{(n + a_1 \sum_{j=2}^{\ell+1} a_j)^\ell}{a_1 \cdots a_\ell m}.$$ □

Remark 2.4. If $\Delta_A := (2a_1 - 1)\sum_{j=2}^{\ell+1} a_j$, then Proposition 2.1 shows, in particular, that $R_A(n + \Delta_A + k) \ge R_A(n)$ for every $k \ge 0$, $n \ge (a_1 - 1)\sum_{j=2}^{\ell+1} a_j$. In fact, if $N = n + \Delta_A + k$, then

$$R_A(N) \ge \frac{1}{\ell!} \frac{(n + a_1 \sum_{j=2}^{\ell+1} a_j + k)^\ell}{a_1 \cdots a_\ell m}$$

$$\geq \left(1 + \frac{k\ell}{n + a_1 \sum_{j=2}^{\ell+1} a_j}\right) \frac{1}{\ell!} \frac{(n + a_1 \sum_{j=2}^{\ell+1} a_j)^\ell}{a_1 \cdots a_\ell m}$$
$$\geq \left(1 + \frac{k\ell}{n + \Delta_A}\right) R_A(n).$$

The generalized Frobenius number is defined, for each $t \geq 1$, as $\mathrm{Fr}_t(A) := \max\{n \in \mathbb{Z}_{\geq 0} \mid R_A(n) < t\}$. The value of $\mathrm{Fr}_t(A)$ can be estimated using Proposition 2.1.

Corollary 2.5 (Estimates for $\mathrm{Fr}_t(A)$)**.** *If*

$$n > (a_1 \cdots a_\ell m)^{1/\ell} (\ell!)^{1/\ell} (t-1)^{1/\ell} + (a_1 - 1) \sum_{j=2}^{\ell+1} a_j,$$

then $R_A(n) \geq t$, *and if*

$$n \leq (a_1 \cdots a_\ell m)^{1/\ell} (\ell!)^{1/\ell} (t-1)^{1/\ell} - a_1 \sum_{j=2}^{\ell+1} a_j - 1,$$

then $R_A(n) < t$. *In particular:*

- $\mathrm{Fr}_t(A) \leq (a_1 \cdots a_\ell m)^{1/\ell} (\ell!)^{1/\ell} (t-1)^{1/\ell} + (a_1 - 1) \sum_{j=2}^{\ell+1} a_j$;
- $\mathrm{Fr}_t(A) > (a_1 \cdots a_\ell m)^{1/\ell} (\ell!)^{1/\ell} (t-1)^{1/\ell} - a_1 \sum_{j=2}^{\ell+1} a_j - 1$.

Proof. Let $N \geq (a_1 - 1) \sum_{j=2}^{\ell+1} a_j$ be the largest integer such that

$$\frac{1}{\ell!} \frac{(N - (a_1 - 1) \sum_{j=2}^{\ell+1} a_j)^\ell}{a_1 \cdots a_\ell m} \leq t - 1.$$

This is equivalent to

$$N \leq (a_1 \cdots a_\ell m)^{1/\ell} (\ell!)^{1/\ell} (t-1)^{1/\ell} + (a_1 - 1) \sum_{j=2}^{\ell+1} a_j.$$

By Proposition 2.1, $R_A(n) \geq t$ for all $n > N$, so $N \geq \mathrm{Fr}_t(A)$, proving the first part. Similarly, let $M \geq 0$ be the largest integer such that

$$\frac{1}{\ell!} \frac{(M + a_1 \sum_{j=2}^{\ell+1} a_j)^\ell}{a_1 \cdots a_\ell m} \leq t - 1.$$

That is given by

$$M = \lfloor (a_1 \cdots a_\ell m)^{1/\ell} (\ell!)^{1/\ell} (t-1)^{1/\ell} \rfloor - a_1 \sum_{j=2}^{\ell+1} a_j$$
$$> (a_1 \cdots a_\ell m)^{1/\ell} (\ell!)^{1/\ell} (t-1)^{1/\ell} - a_1 \sum_{j=2}^{\ell+1} a_j - 1.$$

By Proposition 2.1, $R_A(n) \leq t - 1$ for every $n \leq M$, so $\mathrm{Fr}_t(A) \geq M$. □

2.2. The structure theorem for $(hA)^{(t)}$

In this section, let $A = \{0 = a_0 < a_1 < \cdots < a_\ell < a_{\ell+1} = m\} \subseteq \mathbb{Z}$ be a finite set of integers with $\gcd(A) = 1$, and let $t \geq 1$ be a fixed integer. Recall that for $t \geq 1$, we define the t-representable h-fold sumset of A as $(hA)^{(t)} = \{n \in \mathbb{Z}_{\geq 0} \mid R_{A,h}(n) \geq t\}$, so that

$$\mathcal{P}_t(A) := \bigcup_{h \geq 1} (hA)^{(t)} = \{n \in \mathbb{Z}_{\geq 0} \mid R_A(n) \geq t\}.$$

The t-exceptional set of A is defined as

$$\mathcal{E}_t(A) := \mathbb{Z}_{\geq 0} \setminus \mathcal{P}_t(A) = \{n \in \mathbb{Z}_{\geq 0} \mid R_A(n) < t\}.$$

As in (1.2), the set $(hA)^{(t)}$ is said to be structured if

$$(hA)^{(t)} = [hm] \setminus \Big(\mathcal{E}_t(A) \cup (hm - \mathcal{E}_t(m - A))\Big), \tag{2.3}$$

where $[hm] = \{0,1, \ldots, hm\}$. We start with a lemma about R_A.

Lemma 2.6. *$R_{A,h}(n) = R_A(n)$ for every $h \geq n/a_1$.*

Proof. Since $0 \in A$, we have $R_{A,1}(n) \leq R_{A,2}(n) \leq \cdots \leq R_A(n)$ for every fixed n. Let $c_1 + \cdots + c_u = n$ (with $c_i \in A \setminus \{0\}$) be a generic representation of n. Since $c_i \geq a_1$, we have $n = c_1 + \cdots + c_u \geq ua_1$, and so $u \leq n/a_1$. Thus, if $h \geq n/a_1$, then every representation is counted. □

Lemma 2.7. *For every $k \geq 1$, we have*

$$\{\mathrm{Fr}_t(A) + 1, \ldots, \mathrm{Fr}_t(A) + km\} \subseteq ((H_+ + k - 1)A)^{(t)},$$

where $H_+ := \lceil (\mathrm{Fr}_t(A) + m)/a_1 \rceil$.

Proof. We have $\{\mathrm{Fr}_t(A) + 1, \ldots, \mathrm{Fr}_t(A) + m\} \subseteq \mathcal{P}_t(A)$, so it follows by Lemma 2.6 that $\{\mathrm{Fr}_t(A) + 1, \ldots, \mathrm{Fr}_t(A) + m\} \subseteq (H_+A)^{(t)}$. Then,

$$\begin{aligned}
\{\mathrm{Fr}_t(A) + 1, \ldots, \mathrm{Fr}_t(A) + km\} &= \{\mathrm{Fr}_t(A) + 1, \ldots, \mathrm{Fr}_t(A) + m\} + (k-1)\{0,m\} \\
&\subseteq (H_+A)^{(t)} + (k-1)A \\
&\subseteq ((H_+ + k - 1)A)^{(t)}.
\end{aligned}$$

The last line follows from the fact that $A + (hA)^{(t)} \subseteq ((h+1)A)^{(t)}$ (since $R_{A,h}(n) \leq R_{A,h+1}(n + a)$ for any $a \in A \setminus \{0\}$). □

Throughout the rest of this section, let

$$H_+ := \left\lceil \frac{\mathrm{Fr}_t(A) + m}{a_1} \right\rceil, \qquad H_- := \left\lceil \frac{\mathrm{Fr}_t(m - A) + m}{m - a_\ell} \right\rceil.$$

Lemma 2.8. *For every $h \geq \max\{H_+, H_-\}$, we have*

$$\Big(\{0,1,\ldots,\mathrm{Fr}_t(A)+(h-H_++1)m\}\cup$$
$$\{(H_--1)m-\mathrm{Fr}_t(m-A),\ldots,hm\}\Big)\setminus\Big(\mathcal{E}_t(A)\cup(hm-\mathcal{E}_t(m-A))\Big)\subseteq(hA)^{(t)}.$$

Proof. Applying Lemma 2.7 with $k = h-H_++1$, we have $\{\mathrm{Fr}_t(A)+1,\ldots,\mathrm{Fr}_t(A)+(h-H_++1)m\} \subseteq (hA)^{(t)}$. Since $h \geq \mathrm{Fr}_t(A)/a_1$, by Lemma 2.6 we also have $\{0,1,\ldots,\mathrm{Fr}_t(A)\}\setminus\mathcal{E}_t(A) = \{0,1,\ldots,\mathrm{Fr}_t(A)\}\cap\mathcal{P}_t(A) \subseteq (hA)^{(t)}$. Therefore:

$$\{0,1,\ldots,\mathrm{Fr}_t(A)+(h-H_++1)m\}\setminus\mathcal{E}_t(A)\subseteq(hA)^{(t)}. \tag{2.4}$$

Applying the same argument above for $m-A$, with $k = h-H_-+1$, we get that $\{0,1,\ldots,\mathrm{Fr}_t(m-A)+(h-H_-+1)m\}\setminus\mathcal{E}_t(m-A) \subseteq (h(m-A))^{(t)}$. Since $(hA)^{(t)} = hm-(h(m-A))^{(t)}$, this is equivalent to

$$\{(H_--1)m-\mathrm{Fr}_t(m-A),\ldots,hm\}\setminus(hm-\mathcal{E}_t(m-A))\subseteq(hA)^{(t)}. \tag{2.5}$$

Putting (2.4) and (2.5) together yields the lemma. □

Lemma 2.9. $H_+ + H_- - 2 \geq \max\{H_+,H_-\}$.

Proof. Since $a_1 \leq m-1$, we have $2a_1 - m \leq a_1 - 1$. As $a_1 - 1 \leq \mathrm{Fr}(A)$, it follows that $2 \leq (\mathrm{Fr}(A)+m)/a_1 \leq \lceil(\mathrm{Fr}_t(A)+m)/a_1\rceil = H_+$. Therefore $H_++H_--2 \geq H_-$. Analogously, we deduce that $H_- \geq 2$, and so $H_+ + H_- - 2 \geq H_+$. □

2.2.1. Proof of Theorem 1.1

Theorem 1.1 *If $|A| \geq 4$, then $(hA)^{(t)}$ is structured as in* (2.3) *for all*

$$h \geq \left\lfloor\frac{\mathrm{Fr}_t(A)+m}{a_1}\right\rfloor + \left\lfloor\frac{\mathrm{Fr}_t(m-A)+m}{m-a_\ell}\right\rfloor.$$

Proof. By Lemma 2.8, we have that if $h \geq \max\{H_+, H_-\}$ then $(hA)^{(t)}$ is structured, unless

$$\mathrm{Fr}_t(A)+(h-H_++1)m < (H_--1)m-\mathrm{Fr}_t(m-A),$$

which is equivalent to

$$h < (H_++H_--2)-\frac{\mathrm{Fr}_t(A)}{m}-\frac{\mathrm{Fr}_t(m-A)}{m}. \tag{2.6}$$

However, by our hypothesis, using Lemma 2.9 we have

$$h \geq \left\lfloor\frac{\mathrm{Fr}_t(A)+m}{a_1}\right\rfloor + \left\lfloor\frac{\mathrm{Fr}_t(m-A)+m}{m-a_\ell}\right\rfloor \geq H_++H_--2$$

$$\geq \max\{H_+,H_-\},$$

so the condition of Lemma 2.8 is satisfied and (2.6) never occurs. $\square$

Remark 2.10. Our proof gives something more: For $h \geq \left\lfloor \frac{\mathrm{Fr}_t(A)+m}{a_1} \right\rfloor + \left\lfloor \frac{\mathrm{Fr}_t(m-A)+m}{m-a_\ell} \right\rfloor$, it shows that $(hA)^{(t)} = [hm] \setminus \big(\mathcal{E}_t(A) \cup (hm - \mathcal{E}_t(m-A))\big)$ contains an interval of length at least $2m$. Indeed, we have

$$\{\mathrm{Fr}_t(A)+1, \ldots, hm - \mathrm{Fr}_t(m-A) - 1\} \subseteq (hA)^{(t)},$$

so $(hA)^{(t)}$ contains an interval of length at least

$$\begin{aligned}
(hm- &\mathrm{Fr}_t(m-A)) - \mathrm{Fr}_t(A) - 1 \\
&\geq \left\lfloor \frac{\mathrm{Fr}_t(A)+m}{a_1} \right\rfloor m + \left\lfloor \frac{\mathrm{Fr}_t(m-A)+m}{m-a_\ell} \right\rfloor m - \mathrm{Fr}_t(m-A) - \mathrm{Fr}_t(A) - 1 \\
&> \left(\frac{m}{a_1} - 1\right)(\mathrm{Fr}_t(A)+m) + \left(\frac{m}{m-a_\ell} - 1\right)(\mathrm{Fr}_t(m-A)+m) - 1 \\
&\geq \left(\frac{m}{a_1} + \frac{m}{m-a_\ell} - 2\right) m - 1.
\end{aligned}$$

Since $a_\ell \geq a_1$, we have $\frac{m}{a_1} + \frac{m}{m-a_\ell} \geq \frac{m}{a_1} + \frac{m}{m-a_1} = \frac{m^2}{a_1(m-a_1)} \geq 4$, the last inequality being minimized for $a_1 = m/2$. Thus,

$$(hm - \mathrm{Fr}_t(m-A)) - \mathrm{Fr}_t(A) - 1 > 2m - 1.$$

2.2.2. Proof of Theorem 1.2

Theorem 1.2 *If* $|A| \geq 4$, *then* $(hA)^{(t)}$ *is structured as in* (2.3) *for all*

$$h \geq C_{A,t}\, \frac{1}{e} m\ell t^{1/\ell},$$

where

$$C_{A,t} \leq \left(1 + \frac{4}{\ell}\right)\frac{e}{t^{1/\ell}} + \left(1 + \frac{2}{\ell}\right)\frac{1 + (\log 4\ell)/\ell}{\min\{a_1, m - a_\ell\}}.$$

In particular, $C_{A,t} \leq 3e$ *if* $\ell \geq 4$, *and* $C_{A,t} \leq 1 + o(1)$ *as* $\ell \to \infty$, $t^{1/\ell} \to \infty$.

Proof. Plugging the estimate of Corollary 2.5 into Theorem 1.1 yields that $(hA)^{(t)}$ is structured for every $h \geq h_t(A)$, where

$$\begin{aligned}
h_t(A) &\leq \frac{\mathrm{Fr}_t(A)+m}{a_1} + \frac{\mathrm{Fr}_t(m-A)+m}{m-a_\ell} \\
&\leq \left(\frac{m}{a_1} + \frac{(a_2 \cdots a_\ell m)^{1/\ell}(\ell!)^{1/\ell}(t-1)^{1/\ell}}{a_1^{1-1/\ell}} + \left(1 - \frac{1}{a_1}\right)\sum_{j=2}^{\ell+1} a_j\right) +
\end{aligned}$$

$$+\left(\frac{m}{m-a_\ell}+\frac{(m(m-a_1)\cdots(m-a_{\ell-1}))^{1/\ell}}{(m-a_\ell)^{1-1/\ell}}(\ell!)^{1/\ell}(t-1)^{1/\ell}+\right.$$

$$\left.+\left(1-\frac{1}{m-a_\ell}\right)\sum_{j=0}^{\ell-1}(m-a_j)\right).$$

By the AM-GM inequality,

$$(a_2\cdots a_\ell m)^{1/\ell}\le\frac{1}{\ell}\left(\sum_{j=2}^{\ell+1}a_j\right),\quad (m(m-a_1)\cdots(m-a_{\ell-1}))^{1/\ell}\le\frac{1}{\ell}\left(\sum_{j=0}^{\ell-1}(m-a_j)\right),$$

so for $t\ge 2$,

$$\begin{aligned}
h_t(A)&\le\left(\frac{1}{a_1}+\frac{1}{m-a_\ell}\right)m+\left(\frac{(\ell!)^{1/\ell}}{\ell}\frac{(t-1)^{1/\ell}}{a_1^{1-1/\ell}}+1-\frac{1}{a_1}\right)\sum_{j=2}^{\ell+1}a_j+\\
&\qquad+\left(\frac{(\ell!)^{1/\ell}}{\ell}\frac{(t-1)^{1/\ell}}{(m-a_\ell)^{1-1/\ell}}+1-\frac{1}{m-a_\ell}\right)\sum_{j=0}^{\ell-1}(m-a_j)\\
&<2m+\left(\frac{(\ell!)^{1/\ell}}{\ell}\frac{(t-1)^{1/\ell}}{\min\{a_1,m-a_\ell\}^{1-1/\ell}}+1\right)\left(\sum_{j=2}^{\ell+1}a_j+\sum_{j=0}^{\ell-1}(m-a_j)\right)\\
&<2m+\left(\frac{(\ell!)^{1/\ell}}{\ell}\frac{(t-1)^{1/\ell}}{\min\{a_1,m-a_\ell\}^{1-1/\ell}}+1\right)(\ell+2)m\\
&=\underbrace{\left(\frac{2e}{\ell t^{1/\ell}}+\left(\frac{e(\ell!)^{1/\ell}/\ell}{\min\{a_1,m-a_\ell\}^{1-1/\ell}}\left(1-\frac{1}{t}\right)^{1/\ell}+\frac{e}{t^{1/\ell}}\right)\left(1+\frac{2}{\ell}\right)\right)}_{=:C_{A,t}}\frac{1}{e}m\ell t^{1/\ell}.
\end{aligned}$$

Using that $(\ell!)^{1/\ell}\le\frac{1}{e}(\ell+\log 4\ell)$ for $\ell\ge 2$, we have

$$C_{A,t}\le\left(1+\frac{4}{\ell}\right)\frac{e}{t^{1/\ell}}+\left(1+\frac{2}{\ell}\right)\frac{1+(\log 4\ell)/\ell}{\min\{a_1,m-a_\ell\}},\tag{2.7}$$

completing the proof. ☐

Remark 2.11. Note that if we take $\ell\to\infty$, $t^{1/\ell}\to\infty$ for sets $A\subseteq\mathbb{Z}_{\ge 0}$ with $\min\{a_1,m-a_\ell\}\ge k$ for some fixed $k\ge 1$, then $C_{A,t}\le(1+o(1))k^{-1}$.

Remark 2.12 (Comparison with Yang–Zhou)**.** Suppose that $t\ge 8\ell\ge 32$. Yang–Zhou [**45**] showed that $(hA)^{(t)}$ is structured as in (2.3) if $h\ge\sum_{i=2}^{\ell+1}(ta_i-1)-1$. From the crude lower bound

$$\begin{aligned}
\sum_{i=2}^{\ell+1}(ta_i-1)-1&\ge mt+\left(\frac{\ell(\ell+1)}{2}-1\right)t-\ell-1\\
&=\left(m+\frac{\ell^2+\ell-2}{2}-\frac{\ell}{t}-\frac{1}{t}\right)t>\left(m+\frac{\ell^2}{2}\right)t,
\end{aligned}$$

we would like to show the inequality

$$C_{A,t} \cdot \frac{1}{e} m\ell t^{1/\ell} \leq \left(m + \frac{\ell^2}{2}\right)t, \tag{2.8}$$

or, equivalently,

$$C_{A,t} \cdot \frac{1}{e}\frac{t^{1/\ell}}{t} \leq \frac{1}{\ell} + \frac{\ell}{2m}.$$

The inequality above is true if

$$t^{1-1/\ell} \geq \frac{C_{A,t}}{e}\ell,$$

or $t \geq (C_{A,t}/e)^{1+\frac{1}{\ell-1}}\ell^{1+\frac{1}{\ell-1}}$. For $\ell \geq 4$, from the numerical estimates

$$\ell^{1+\frac{1}{\ell-1}} \leq (4^{\frac{1}{3}})\ell < 1.6\ell \quad \text{and} \quad (C_{A,t}/e)^{1+\frac{1}{\ell-1}} \leq (3e/e)^{1+\frac{1}{\ell-1}} \leq 5,$$

it follows that (2.8) holds true for $t \geq 8\ell$.

2.3. An extremal family of examples

Let $m \geq 5$ be an integer. Take integers $2 \leq \ell \leq m/2$ and $0 \leq T \leq (m-\ell)/(\ell-1)$, and define

$$A = A_{\ell,m} := \{0,1,m-\ell+1,\dots,m\}, \qquad t = t_R := \binom{\ell+T}{T},$$

so that $|A| = \ell + 2$. We are going to show that if $h_t = h_{t_T}(A_{\ell,m})$ is the smallest integer for which $(hA_{m,\ell})^{(t_T)}$ is structured for every $h \geq h_t$, then $h_t \geq (T+1)(m-\ell+1)-1$.

Lemma 2.13. $\mathcal{E}_t(A), \mathcal{E}_t(m-A) \subseteq [mT-1]$.

Proof. Since $1 \in A \cap (m-A)$, it suffices to show that $R_A(mT)$, $R_{m-A}(mT) \geq t$. The representations of mT are of the form

$$mT = k_0 \cdot 1 + k_1(m-\ell+1) + \cdots + k_{\ell-1}(m-1) + k_\ell m$$

in A, and

$$mT = k'_0 \cdot 1 + \cdots + k'_{\ell-2}(\ell-1) + k'_{\ell-1}(m-1) + k'_\ell m$$

in $m-A$, with k_i, $k'_i \geq 0$. For any choice of k_i's ($i \geq 1$) with $\sum_{i=1}^{\ell} k_i \leq T$ (resp. k'_i), we can define $k_0 \geq 0$ (resp. k'_0) by the difference. Thus,

$$R_A(mT) \geq \#\left\{(k_1,\dots,k_\ell) \in \mathbb{Z}_{\geq 0}^{\ell} \;\middle|\; \sum_{i=1}^{\ell} k_i \leq T\right\} = \binom{\ell+T}{T} = t,$$

and similarly $R_{m-A}(mT) \geq t$. $\square$

Throughout the rest of the argument, let

$$g := (T+1)(m-\ell+1) - 1. \tag{2.9}$$

Since $0 < (T+1)(\ell-1)+1 \le m$ for T in our range, we have $\lfloor \frac{g}{m} \rfloor = \lfloor T+1-\frac{(T+1)(\ell-1)+1}{m} \rfloor = T$. We can therefore write $g = x + mT$, for some $x \in [m-1]$.

Lemma 2.14. *$R_A(g) = t$.*

Proof. The representations of g are of the form

$$g = k_0 \cdot 1 + k_1(m-\ell+1) + \cdots + k_{\ell-1}(m-1) + k_\ell m, \tag{2.10}$$

with $k_i \ge 0$. By the definition of g, there cannot be $i \ge 1$ for which $k_i > T$; in particular, we cannot have $\sum_{i=1}^{\ell} k_i > T$. At the same time, since $mT \le g$, for all choices of k_i's ($i \ge 1$) with $\sum_{i=1}^{\ell} k_i \le T$, we can define $k_0 \ge 0$ by the difference. Therefore:

$$R_A(g) = \#\left\{(k_1, \ldots, k_\ell) \in \mathbb{Z}_{\ge 0}^{\ell} \;\middle|\; \sum_{i=1}^{\ell} k_i \le T\right\} = \binom{\ell+T}{T} = t. \qquad \square$$

Corollary 2.15. *$g - m \le \mathrm{Fr}_t(A) \le m\lfloor \frac{g}{m} \rfloor - 1$.*

Proof. Since $\lfloor \frac{g}{m} \rfloor = T$, Lemma 2.13 implies the upper bound. For the lower bound, note that every representation of $g-m$ can be turned into a representation of g by adding the element m; moreover, we have the representation $g = k_0 \cdot 1$ in (2.10), which is not obtained in this fashion. So $R_A(g) \ge R_A(g-m)+1$, which by Lemma 2.14 implies that $R_A(g-m) \le t-1$, and thus $g - m \in \mathcal{E}_t(A)$ (or $g - m \le 0$, in which case the lower bound holds trivially). $\square$

Proposition 2.16.

(i) *$(HA)^{(t)} \neq [Hm] \setminus \Big(\mathcal{E}_t(A) \cup (Hm - \mathcal{E}_t(m-A))\Big)$, for $H := 2T+1$.*

(ii) *If $h > 2T+1$ and $(hA)^{(t)} = [hm] \setminus \Big(\mathcal{E}_t(A) \cup (hm - \mathcal{E}_t(m-A))\Big)$, then we must have $h \ge g = (T+1)(m-\ell+1) - 1$.*

Proof. The representation $g = k_0 \cdot 1$ in (2.10) is the one with the most summands, so $R_{A,h}(g) = t$ if and only if $h \ge g = (T+1)(m-\ell+1)-1$. However, by Lemma 2.13, we know that

$$g \in x + m \cdot \{T, T+1, \ldots, H-1-T\} \subseteq [Hm] \setminus \Big(\mathcal{E}_t(A) \cup (Hm - \mathcal{E}_t(m-A))\Big)$$

(where $g = x + mT$, $x \in [m-1]$) for $H = 2T+1$; so since $2T+1 < (T+1)(m-\ell+1)-1$, it follows that $g \notin (HA)^{(t)}$. We conclude that $(HA)^{(t)}$ cannot be structured, proving part (i). Part (ii) likewise follows from these arguments. $\square$

Remark 2.17. In Proposition 2.16 we showed that $h_t(A) \ge g$. Since $t = \binom{\ell+T}{T}$, we have $\frac{(\ell+T)^\ell}{\ell^\ell} \le t \le \frac{(\ell+T)^\ell}{\ell!}$, so $(\ell!)^{1/\ell} t^{1/\ell} - \ell \le T \le \ell t^{1/\ell} - \ell$ and $t^{1/\ell} \ge 1 + \frac{T}{\ell}$. Letting $m \to \infty$, with

$\ell := \lfloor m^{1/2.01} \rfloor$ and $T = \lfloor m^{1/2} \rfloor$, we get $t^{1/\ell} \to \infty$. Thus (using that $\ell! \geq \ell^\ell / e^\ell$):

$$\begin{aligned} g = (T+1)(m-\ell+1) - 1 &\geq ((\ell!)^{1/\ell} t^{1/\ell} - \ell)(m-\ell) \\ &\geq (1 - o_{m\to\infty}(1)) \frac{1}{e} \ell t^{1/\ell} \cdot (1 - o_{m\to\infty}(1))\, m \\ &= (1 - o_{m\to\infty}(1))\, \frac{1}{e} m \ell t^{1/\ell}. \end{aligned}$$

Applying Theorem 1.2, we get $h_t(A) \sim_{m\to\infty} \frac{1}{e} m \ell t^{1/\ell}$.

2.4. t-representables in $\mathbb{Z}^d$

As in Subsection 1.1.3, let $A \subseteq \mathbb{Z}^d$ be a finite set. For $h \geq 1$, the *representation function* of A is defined by

$$R_{A,h}(\mathbf{p}) = \# \left\{ (k_{\mathbf{a}})_{\mathbf{a}\in A} \in \mathbb{Z}_{\geq 0}^{|A|} \;\middle|\; \sum_{\mathbf{a}\in A} k_{\mathbf{a}} \mathbf{a} = \mathbf{p},\ \sum_{\mathbf{a}\in A} k_{\mathbf{a}} = h \right\},$$

which counts the number of ways to express $\mathbf{p} \in \mathbb{Z}^d$ as a sum of h elements from A. Define the *h-fold t-representable sumset* of A as

$$(hA)^{(t)} := \left\{ \mathbf{p} \in \mathbb{Z}^d \;\middle|\; R_{A,h}(\mathbf{p}) \geq t \right\}.$$

The *convex hull* of A is the set

$$\mathcal{H}(A) := \left\{ \sum_{\mathbf{a}\in A} c_{\mathbf{a}} \mathbf{a} \;\middle|\; c_{\mathbf{a}} \in \mathbb{R}_{\geq 0},\ \sum_{\mathbf{a}\in A} c_{\mathbf{a}} = 1 \right\}.$$

Let $\mathrm{ex}(\mathcal{H}(A))$ denote the set of *extremal points* (or "corners") of $\mathcal{H}(A)$, i.e., those points in $\mathcal{H}(A)$ that are not convex combinations of other points in $\mathcal{H}(A)$. After an affine transformation if necessary, we may assume that $\mathbf{0} \in \mathrm{ex}(\mathcal{H}(A))$. We define the *cone generated by A* as

$$\mathcal{C}_A := \left\{ \sum_{\mathbf{a}\in A} c_{\mathbf{a}} \mathbf{a} \;\middle|\; c_{\mathbf{a}} \in \mathbb{R}_{\geq 0} \right\},$$

and the *integral span* of A as

$$\Lambda_A := \mathrm{span}_{\mathbb{Z}}(A) = \left\{ \sum_{\mathbf{a}\in A} c_{\mathbf{a}} \mathbf{a} \;\middle|\; c_{\mathbf{a}} \in \mathbb{Z} \right\}.$$

The *t-exceptional set* of A is given by

$$\mathcal{E}_t(A) := (\mathcal{C}_A \cap \Lambda_A) \setminus \mathcal{P}_t(A),$$

where

$$\mathcal{P}_t(A) := \bigcup_{h\geq 1} (hA)^{(t)}$$

is the set of all points that are t-representable by A in some number of summands. As in (1.3), we say that the set $(hA)^{(t)}$ is *structured* if

$$(hA)^{(t)} = (h\mathcal{H}(A) \cap \Lambda_A) \setminus \left(\bigcup_{\mathbf{v} \in \operatorname{ex}(\mathcal{H}(A))} (h\mathbf{v} - \mathcal{E}_t(\mathbf{v} - A)) \right). \tag{2.11}$$

Let $\mathfrak{n} \in \mathbb{R}^d$ be a unit vector such that

$$\langle \mathfrak{n}, \mathbf{v} \rangle > 0 \quad \text{for all } \mathbf{v} \in \mathcal{C}_A \setminus \{\mathbf{0}\},$$

so that the entire cone $\mathcal{C}_A \setminus \{\mathbf{0}\}$ lies on one side of the hyperplane orthogonal to $\mathfrak{n}$. We then define

$$\delta_A := \min_{\mathbf{a} \in A \setminus \{\mathbf{0}\}} \langle \mathbf{a}, \mathfrak{n} \rangle, \qquad \Delta_A := \max_{\mathbf{a} \in A \setminus \{\mathbf{0}\}} \langle \mathbf{a}, \mathfrak{n} \rangle.$$

That is, we project the nonzero elements of A onto the ray $\mathbb{R}_{\geq 0}\mathfrak{n}$, and define δ_A and Δ_A as the minimal and maximal nonzero projection lengths, respectively. In this section, we will prove the following two results:

Lemma 1.3 *There exists a minimum $\varphi = \varphi_{A,t} \in \mathbb{R}_{\geq 1}$ such that, for every real $\lambda \geq \varphi$, we have*

$$\Big((\lambda \mathcal{H}(A) \cap \Lambda_A) \setminus \mathcal{E}_t(A) \Big) + A = \Big((\lambda + 1)\mathcal{H}(A) \cap \Lambda_A \Big) \setminus \mathcal{E}_t(A).$$

Theorem 1.4 *The set $(hA)^{(t)} \subseteq \mathbb{Z}^d$ is structured as in* (2.11) *for every*

$$h \geq \max_{\substack{\mathbf{0} \in B \subseteq \operatorname{ex}(\mathcal{H}(A)) \\ |B| = d+1 \\ \operatorname{span}_{\mathbb{R}}(B) = \mathbb{R}^d}} \left(\sum_{\mathbf{b} \in B} \left\lceil \frac{\Delta_{\mathbf{b}-A}}{\delta_{\mathbf{b}-A}} \, \varphi_{\mathbf{b}-A,t} \right\rceil \right),$$

where $\varphi_{\mathbf{b}-A,t}$ is the constant from Lemma 1.3 for the set $\mathbf{b} - A$.

2.4.1. Deduction of Theorem 1.4 from Lemma 1.3

Write

$$R_A(\mathbf{p}) := \lim_{h \to \infty} R_{A,h}(\mathbf{p}) = \#\left\{ (k_{\mathbf{a}})_{\mathbf{a} \in A} \in \mathbb{Z}_{\geq 0}^{|A|} \;\middle|\; \sum_{\mathbf{a} \in A} k_{\mathbf{a}} \mathbf{a} = \mathbf{p} \right\}$$

for the *total representation function* of A, so that $\mathcal{P}_t(A) = \{\mathbf{p} \in \mathcal{C}_A \cap \Lambda_A \mid R_A(\mathbf{p}) \geq t\}$, and $\mathcal{E}_t(A) = \{\mathbf{p} \in \mathcal{C}_A \cap \Lambda_A \mid R_A(\mathbf{p}) < t\}$. Letting $\mathfrak{n}$, δ_A, and Δ_A be as defined above, we start with a $\mathbb{Z}^d$ version of Lemma 2.6.

Lemma 2.18. *If $\mathbf{p} \in \mathcal{C}_A \cap \Lambda_A$, then $R_{A,h}(\mathbf{p}) = R_A(\mathbf{p})$ for every $h \geq \langle \mathbf{p}, \mathfrak{n} \rangle / \delta_A$.*

Proof. Since $\mathbf{0} \in A$, we have $R_{A,1}(\mathbf{p}) \leq R_{A,2}(\mathbf{p}) \leq \cdots \leq R_A(\mathbf{p})$ for every fixed $\mathbf{p} \in \mathcal{C}_A \cap \Lambda_A$. Let $\mathbf{p} = \sum_{\mathbf{a} \in A \setminus \{0\}} k_{\mathbf{a}} \mathbf{a}$ (with $k_{\mathbf{a}} \in \mathbb{Z}_{\geq 0}$) be an arbitrary representation of $\mathbf{p}$ by A. Since $\langle \cdot, \mathfrak{n} \rangle$

is linear, we have

$$\langle \mathbf{p}, \mathfrak{n} \rangle = \sum_{\mathbf{a} \in A \setminus \{0\}} k_{\mathbf{a}} \langle \mathbf{a}, \mathfrak{n} \rangle \geq \delta_A \sum_{\mathbf{a} \in A \setminus \{0\}} k_{\mathbf{a}},$$

and thus $\sum_{\mathbf{a} \in A \setminus \{0\}} k_{\mathbf{a}} \leq \langle \mathbf{p}, \mathfrak{n} \rangle / \delta_A$. So every possible representation of $\mathbf{p}$ by A is taken into account once $h \geq \langle \mathbf{p}, \mathfrak{n} \rangle / \delta_A$. □

Fix $t \geq 1$, and define

$$H_A = H_{A,t} := \left\lceil \frac{\Delta_A}{\delta_A} \varphi_{A,t} \right\rceil \quad \left(\text{resp. } H_{\mathbf{v}-A} := \left\lceil \frac{\Delta_{\mathbf{v}-A}}{\delta_{\mathbf{v}-A}} \varphi_{\mathbf{v}-A,t} \right\rceil, \text{ for } \mathbf{v} \in \operatorname{ex}(\mathcal{H}(A)) \right),$$

where $\varphi_{A,t}$ (resp. $\varphi_{\mathbf{v}-A}$) is the constant from Lemma 1.3. Thus, by Lemma 2.18,

$$(\varphi_{A,t} \mathcal{H}(A) \cap \Lambda_A) \setminus \mathcal{E}_t(A) \subseteq (H_A A)^{(t)} \tag{2.12}$$

(resp. $(\varphi_{\mathbf{v}-A,t} \mathcal{H}(\mathbf{v}-A) \cap \Lambda_A) \setminus \mathcal{E}_t(\mathbf{v}-A) \subseteq (H_{\mathbf{v}-A}(\mathbf{v}-A))^{(t)}$). More generally:

Lemma 2.19. *For each* $\mathbf{v} \in \operatorname{ex}(\mathcal{H}(A))$ *and* $h \geq H_{\mathbf{v}-A}$, *we have*

$$\Big(G_{\mathbf{v}} \, \mathbf{v} + (h - G_{\mathbf{v}}) \mathcal{H}(A) \Big) \cap \Lambda_A \setminus \Big(h\mathbf{v} - \mathcal{E}_t(\mathbf{v} - A) \Big) \subseteq (hA)^{(t)},$$

where $G_{\mathbf{v}} = G_{\mathbf{v},t} := H_{\mathbf{v}-A} - \varphi_{\mathbf{v}-A,t}$.

Proof. Applying Lemma 1.3 to $\lambda = \varphi_{\mathbf{v}-A,t} + k$ together with (2.12), we get

$$\begin{aligned}
&\Big((\varphi_{\mathbf{v}-A,t} + k) \mathcal{H}(\mathbf{v} - A) \cap \Lambda_A \Big) \setminus \mathcal{E}_t(\mathbf{v} - A) \\
&\qquad\qquad = \Big(\varphi_{\mathbf{v}-A,t} \mathcal{H}(\mathbf{v} - A) \cap \Lambda_A \Big) \setminus \mathcal{E}_t(\mathbf{v} - A) + k(\mathbf{v} - A) \\
&\qquad\qquad \subseteq (H_{\mathbf{v}-A}(\mathbf{v} - A))^{(t)} + k(\mathbf{v} - A) \\
&\qquad\qquad \subseteq ((H_{\mathbf{v}-A} + k)(\mathbf{v} - A))^{(t)}
\end{aligned}$$

for every integer $k \geq 0$. Taking $k := h - H_{\mathbf{v}-A}$, it follows that

$$\begin{aligned}
\Big((h - (H_{\mathbf{v}-A} - \varphi_{\mathbf{v}-A,t})) \mathcal{H}(\mathbf{v} - A) \Big) \cap \Lambda_A \setminus \mathcal{E}_t(\mathbf{v} - A) &\subseteq (h(\mathbf{v} - A))^{(t)} \\
&= h\mathbf{v} - (hA)^{(t)}.
\end{aligned}$$

Using that $\mathcal{H}(\mathbf{v} - A) = \mathbf{v} - \mathcal{H}(A)$, we have

$$\Big(h\mathbf{v} - G_{\mathbf{v}} \mathbf{v} - (h - G_{\mathbf{v}}) \mathcal{H}(A) \Big) \cap \Lambda_A \setminus \mathcal{E}_t(\mathbf{v} - A) \subseteq h\mathbf{v} - (hA)^{(t)}.$$

Subtracting both sides from $h\mathbf{v}$ proves the lemma. □

Using this, we can show that certain parts of the structured set in (2.11) do belong to $(hA)^{(t)}$.

Lemma 2.20. *Let $\mathbf{0} \in B \subseteq \mathrm{ex}(\mathcal{H}(A))$ be a subset such that $B \setminus \{\mathbf{0}\}$ is linearly independent and $|B| = d+1$. Then,*

$$(h\mathcal{H}(B) \cap \Lambda_A) \setminus \left(\mathcal{E}_t(A) \cup \bigcup_{\mathbf{b}\in B\setminus\{\mathbf{0}\}} (h\mathbf{b} - \mathcal{E}_t(\mathbf{b} - A))\right) \subseteq (hA)^{(t)}$$

for every $h \geq H_A + \sum_{\mathbf{b}\in B\setminus\{\mathbf{0}\}} H_{\mathbf{b}-A}$.

Proof. Write $B = \{\mathbf{0},\mathbf{b}_1, \dots, \mathbf{b}_d\}$, and $(x_1, \dots ,x_d)_B := \sum_{i=1}^d x_i\mathbf{b}_i$. Take

$$\mathbf{p} \in (h\mathcal{H}(B) \cap \Lambda_A) \setminus \left(\mathcal{E}_t(A) \cup \bigcup_{i=1}^{d} (h\mathbf{b}_i - \mathcal{E}_t(\mathbf{b}_i - A))\right) \tag{2.13}$$

so that $\mathbf{p} = (p_1, \dots ,p_d)_B$ for some $p_i \in \mathbb{R}_{\geq 0}$.

Let $h \geq \max_{\mathbf{b}\in B\setminus\{\mathbf{0}\}} H_{\mathbf{b}-A}$. If there is $1 \leq i \leq d$ such that $p_i \geq H_{\mathbf{b}_i-A} - \varphi_{\mathbf{b}_i-A,t}$, then

$$\mathbf{p} \in (H_{\mathbf{b}_i-A} - \varphi_{\mathbf{b}_i-A,t})\,\mathbf{b}_i + (h - (H_{\mathbf{b}_i-A} - \varphi_{\mathbf{b}_i-A,t}))\mathcal{H}(B),$$

which by Lemma 2.19 implies that $\mathbf{p} \in (hA)^{(t)}$.

Otherwise, $\mathbf{p}$ is such that $0 \leq p_i \leq H_{\mathbf{b}_i-A} - \varphi_{\mathbf{b}_i-A,t}$ for every $1 \leq i \leq d$. For each i, if $h \geq H_{\mathbf{b}_i-A} - \varphi_{\mathbf{b}_i-A,t}$ then $j\mathbf{b}_i \in h\mathcal{H}(B)$ for every $0 \leq j \leq H_{\mathbf{b}_i-A} - \varphi_{\mathbf{b}_i-A,t}$. Therefore, if $h \geq \sum_{i=1}^d (H_{\mathbf{b}_i-A} - \varphi_{\mathbf{b}_i-A,t})$, then

$$\mathbf{p} \in \{(x_1, \dots , x_d)_B \mid 0 \leq x_i \leq H_{\mathbf{b}_i-A} - \varphi_{\mathbf{b}_i-A,t}, x_i \in \mathbb{R}\} \cap \Lambda_A \subseteq h\mathcal{H}(B) \cap \Lambda_A.$$

Thus, for $h \geq H_A + \sum_{i=1}^d H_{\mathbf{b}_i-A}$, Lemma 2.19 (applied with $\mathbf{v} = 0$) guarantees that every $\mathbf{p}$ in (2.13) is in $(hA)^{(t)}$. □

Finally, to glue together all the parts of the structured set as they appear in Lemma 2.20, we use the following version of a classical result in convex geometry:

Lemma 2.21 (Carathéodory's theorem)**.** *We have*

$$\mathcal{H}(A) = \bigcup_{\substack{\mathbf{0}\in B\subseteq \mathrm{ex}(\mathcal{H}(A))\\ |B|=d+1\\ \mathrm{span}_{\mathbb{R}}(B)=\mathbb{R}^d}} \mathcal{H}(B).$$

Proof. We adapt the proof of Granville–Shakan [**13**, Lemma 4]. Since $\mathcal{H}(\mathrm{ex}(\mathcal{H}(A))) = \mathcal{H}(A)$,[1] we can suppose without loss of generality that $A = \mathrm{ex}(\mathcal{H}(A))$. For any $\mathbf{v} \in \mathcal{H}(A)$, we can represent it as $\mathbf{v} = \sum_{\mathbf{a}\in A} c_{\mathbf{a}}\mathbf{a}$ for some real $c_{\mathbf{a}} \geq 0$ such that

$$0 \leq \sum_{\mathbf{a}\in A} c_{\mathbf{a}} \leq 1.$$

Define $B := \{\mathbf{a} \in A \mid c_{\mathbf{a}} > 0\}$, and select a representation $(c_{\mathbf{a}})_{\mathbf{a}\in A}$ that minimizes $|B|$. We claim that B is a set of linearly independent elements.

[1] cf. Brøndsted [**4**, Theorem 7.2].

Indeed, suppose the contrary; i.e., that $\sum_{\mathbf{b}\in B} e_{\mathbf{b}}\mathbf{b} = 0$ for some set of $e_{\mathbf{b}} \in \mathbb{R}$ with not all $e_{\mathbf{b}} = 0$. Without loss of generality, suppose that $\sum_{\mathbf{b}\in B} e_{\mathbf{b}} \geq 0$ (otherwise, change the sign of each $e_{\mathbf{b}}$). Hence, there exists at least one element of $\mathbf{b} \in B$ such that $e_{\mathbf{b}} > 0$. Define

$$m := \min_{\substack{\mathbf{b}\in B\\ e_{\mathbf{b}}>0}} c_{\mathbf{b}}/e_{\mathbf{b}},$$

so that $c_{\mathbf{b}^*} = me_{\mathbf{b}^*}$ for some $\mathbf{b}^* \in B$, and $0 \leq \sum_{\mathbf{b}\in B} me_{\mathbf{b}} \leq \sum_{\mathbf{b}\in B} c_{\mathbf{b}}$. But then $\mathbf{v} = \sum_{\mathbf{b}\in B}(c_{\mathbf{b}} - me_{\mathbf{b}})\mathbf{b}$, where $c_{\mathbf{b}} - me_{\mathbf{b}} \geq 0$ for every $\mathbf{b} \in B$, $0 \leq \sum_{\mathbf{b}\in B}(c_{\mathbf{b}} - me_{\mathbf{b}}) \leq 1$, and $c_{\mathbf{b}^*} - me_{\mathbf{b}^*} = 0$. This contradicts the minimality of $|B|$.

Since we can then adjoin elements from A to B until we have d independent non-zero elements, this concludes the proof. □

Proof of Theorem 1.4. By Lemma 2.21, we have $h\mathcal{H}(A) = \bigcup_B h\mathcal{H}(B)$. Thus, taking $h \geq H_A + \max_B \sum_{\mathbf{b}\in B\setminus\{\mathbf{0}\}} H_{\mathbf{b}-A}$ we may apply Lemma 2.20 to each B, obtaining the inclusion "$\supseteq$" in (2.11). The inclusion "$\subseteq$" follows by definition. □

Remark 2.22 (Analogy to the case $d = 1$)**.** Let

$$A = \{0 = a_0 < a_1 < \cdots < a_\ell < a_{\ell+1} = m\} \subseteq \mathbb{Z}$$

be a set with $\gcd(A) = 1$. In this case, $\Lambda_A = \mathbb{Z}$, $\delta_A = a_1$, $\Delta_A = m$, $\mathcal{H}(A) = [0,m]$, and $\mathrm{ex}(\mathcal{H}(A)) = \{0,m\}$. By the definition of $\mathrm{Fr}_t(A)$, writing $F := (\mathrm{Fr}_t(A) + m)/m$, we have $\mathcal{E}_t(A) \subseteq \{0, \ldots, (F-1)m\}$, and so

$$\{\mathrm{Fr}_t(A) + 1, \ldots, \mathrm{Fr}_t(A) + m\} \subseteq (F\mathcal{H}(A) \cap \Lambda_A) \setminus \mathcal{E}_t(A).$$

Thus, for every real $\lambda \geq F$, we have

$$\begin{aligned}(\lambda\mathcal{H}(A) \cap \Lambda_A) \setminus \mathcal{E}_t(A) + A &= \{0, \ldots, \lfloor\lambda m\rfloor\} \cap \mathcal{P}_t(A) + A\\ &= \{0, \ldots, \lfloor\lambda m\rfloor + m\} \cap \mathcal{P}_t(A)\\ &= ((\lambda+1)\mathcal{H}(A) \cap \Lambda_A) \setminus \mathcal{E}_t(A),\end{aligned}$$

which implies $\varphi_{A,t} \leq F$ as in Lemma 1.3. Applying Theorem 1.4, we obtain that $(hA)^{(t)}$ is structured for every $h \geq h_t(A)$, with

$$h_t(A) \leq \left\lceil \frac{\Delta_A}{\delta_A}\varphi_{A,t} \right\rceil + \left\lceil \frac{\Delta_{m-A}}{\delta_{m-A}}\varphi_{m-A,t} \right\rceil = \left\lceil \frac{\mathrm{Fr}_t(A) + m}{a_1} \right\rceil + \left\lceil \frac{\mathrm{Fr}_t(m-A) + m}{m - a_\ell} \right\rceil.$$

2.4.2. Proof of Lemma 1.3

Given $\mathbf{u} = (u_1, \ldots, u_d)$, $\mathbf{v} = (v_1, \ldots, v_d) \in \mathbb{Z}^d_{\geq 0}$, write $\mathbf{u} \leq \mathbf{v}$ is $u_i \leq v_i$ for every $1 \leq i \leq d$. We will use the following classical lemma.

Lemma 2.23 (Dickson's lemma)**.** *Let $S \subseteq \mathbb{Z}^d_{\geq 0}$. There is a finite subset $T \subseteq S$ such that for all $\mathbf{s} \in S$, there exists $\mathbf{t} \in T$ such that $\mathbf{t} \leq \mathbf{s}$.*

Proof. See Lemma 5 in Granville–Shakan [**13**]. ☐

The next lemma is based on Proposition 4 of Granville–Shakan [**13**].

Lemma 2.24. *Let $\mathbf{0} \in B \subseteq \mathrm{ex}(\mathcal{H}(A))$ be a subset such that $B \setminus \{\mathbf{0}\}$ is linearly independent and $|B| = d+1$. Then, there exists a finite set $F_B = F_{B,t}(A) \subseteq \mathcal{P}_t(A)$ such that*

$$\mathcal{P}_t(A) \cap \mathcal{C}_B = F_B + \mathcal{P}(B)$$

Proof. The fundamental domain for Λ_B is

$$\mathbb{R}^d/\Lambda_B \simeq \mathcal{F} := \left\{ \sum_{\mathbf{b} \in B} s_{\mathbf{b}} \mathbf{b} \;\middle|\; s_{\mathbf{b}} \in [0,1), \, \forall \mathbf{b} \in B \right\}.$$

Since $\mathcal{F}$ is bounded, the set $\mathcal{F} \cap \Lambda_A$ is finite. Thus, we can partition $\mathcal{P}_t(A) \cap \mathcal{C}_B$ as

$$\mathcal{P}_t(A) \cap \mathcal{C}_B = \bigsqcup_{\mathbf{v} \in \mathcal{F} \cap \Lambda_A} (\mathbf{v} + \Lambda_B) \cap \mathcal{P}_t(A).$$

For each $\mathbf{v} \in \mathcal{F} \cap \Lambda_A$, define

$$S_{\mathbf{v}} := \left\{ \mathbf{s} = (s_{\mathbf{b}})_{\mathbf{b} \in B \setminus \{\mathbf{0}\}} \in \mathbb{Z}^{|B|-1}_{\geq 0} \;\middle|\; \mathbf{v} + \sum_{\mathbf{b} \in B \setminus \{\mathbf{0}\}} s_{\mathbf{b}} \mathbf{b} \in (\mathbf{v} + \Lambda_B) \cap \mathcal{P}_t(A) \right\}.$$

By Dickson's Lemma 2.23, there is a finite subset $T_{\mathbf{v}} \subseteq S_{\mathbf{v}}$ such that for every $\mathbf{s} \in S_{\mathbf{v}}$, there is $\mathbf{t} \in T_{\mathbf{v}}$ such that $\mathbf{t} \leq \mathbf{s}$. Define the finite set

$$F_{\mathbf{v}} := \left\{ \mathbf{v} + \sum_{\mathbf{b} \in B \setminus \{\mathbf{0}\}} t_{\mathbf{b}} \mathbf{b} \;\middle|\; \mathbf{t} = (t_{\mathbf{b}})_{\mathbf{b} \in B \setminus \{\mathbf{0}\}} \in T_{\mathbf{v}} \right\}.$$

By definition, for every $\mathbf{p} \in (\mathbf{v} + \Lambda_B) \cap \mathcal{P}_t(A)$ there is $\mathbf{q} \in F_{\mathbf{v}}$ such that $\mathbf{p} - \mathbf{q} \in \mathcal{P}(B)$. Hence, $(\mathbf{v} + \Lambda_B) \cap \mathcal{P}_t(A) = F_{\mathbf{v}} + \mathcal{P}(B)$. Taking the union over $\mathbf{v}$'s, we conclude that

$$\mathcal{P}_t(A) \cap \mathcal{C}_B = \bigsqcup_{\mathbf{v} \in \mathcal{F} \cap \Lambda_A} \Big(F_{\mathbf{v}} + \mathcal{P}(B) \Big) = F_B + \mathcal{P}(B),$$

where $F_B := \bigsqcup_{\mathbf{v} \in \mathcal{F} \cap \Lambda_A} F_{\mathbf{v}}$. ☐

Corollary 2.25. *Let $\mathbf{0} \in B \subseteq \mathrm{ex}(\mathcal{H}(A))$ be a subset such that $B \setminus \{\mathbf{0}\}$ is linearly independent and $|B| = d+1$, and let $\mu_B := \min\{\mu \in \mathbb{R}_{\geq 1} \mid F_B \subseteq \mu \mathcal{H}(B)\}$, where F_B is as in Lemma 2.24. Then, for real $\lambda \geq \mu_B$, we have*

$$\mathcal{P}_t(A) \cap (\lambda + 1)\mathcal{H}(B) = (\mathcal{P}_t(A) \cap \lambda \mathcal{H}(B)) + B.$$

Proof. The inclusion "$\supseteq$" is clear. Since $\mathbf{0} \in B$, it suffices to show that for

$$\mathbf{p} \in \mathcal{P}_t(A) \cap (\lambda + 1)\mathcal{H}(B) \setminus \lambda \mathcal{H}(B)$$

there exists $\mathbf{b} \in B$ such that $\mathbf{p} - \mathbf{b} \in \mathcal{P}_t(A) \cap \lambda\mathcal{H}(B)$.

By Lemma 2.24 we have $\mathcal{P}_t(A) \cap \lambda\mathcal{H}(B) = (\mathcal{P}_t(A) \cap \mathcal{C}_B) \cap \lambda\mathcal{H}(B) = (F_B + \mathcal{P}(B)) \cap \lambda\mathcal{H}(B)$, so we can write $\mathbf{p} = \mathbf{f} + \sum_{\mathbf{b} \in B \setminus \{\mathbf{0}\}} c_\mathbf{b}\mathbf{b}$ for some $\mathbf{f} \in F_B$ and some integers $c_\mathbf{b} \in \mathbb{Z}_{\geq 0}$, with at least one (say, $\mathbf{b}^* \in B$) $c_{\mathbf{b}^*} \geq 1$, because $\lambda \geq \mu_B$. Thus

$$\mathbf{p} - \mathbf{b}^* = \mathbf{f} + \sum_{\mathbf{b} \in B \setminus \{\mathbf{0}\}} c_\mathbf{b}\mathbf{b} - \mathbf{b}^* \in F_B + \mathcal{P}(B) = \mathcal{P}_t(A) \cap \mathcal{C}_B,$$

so it suffices to show that $\mathbf{p} - \mathbf{b}^* \in \lambda\mathcal{H}(B)$.

Since $B \setminus \{\mathbf{0}\}$ is a basis for $\mathbb{R}^d$ and $\mathbf{p} \in (\lambda+1)\mathcal{H}(B) \setminus \lambda\mathcal{H}(B) \subseteq \mathcal{C}_B$, there exist unique $x_\mathbf{b} \in \mathbb{R}$, necessarily non-negative, such that $\mathbf{p} = \sum_{\mathbf{b} \in B \setminus \{0\}} x_\mathbf{b}\mathbf{b}$ and $\lambda < \sum_{\mathbf{b} \in B \setminus \{0\}} x_\mathbf{b} \leq \lambda + 1$. Since $\mathbf{p} - \mathbf{b}^* \in \mathcal{C}_B$, there exist unique $y_\mathbf{b} \in \mathbb{R}$, necessarily non-negative, such that $\sum_{\mathbf{b} \in B \setminus \{0\}} y_\mathbf{b}\mathbf{b} = \mathbf{p} - \mathbf{b}^*$. By uniqueness, $y_\mathbf{b} = x_\mathbf{b}$ for $\mathbf{b} \in B \setminus \{\mathbf{b}^*\}$, and $y_{\mathbf{b}^*} = x_{\mathbf{b}^*} - 1$. Therefore, $\sum_{\mathbf{b} \in B \setminus \{0\}} y_\mathbf{b} \leq \lambda$, implying that $\mathbf{p} - \mathbf{b}^* \in \lambda\mathcal{H}(B)$. ☐

Proof of Lemma 1.3. Applying Lemma 2.21 together with Corollary 2.25, we obtain, for $\lambda \geq \max_B \mu_B$,

$$\begin{aligned}\mathcal{P}_t(A) \cap (\lambda+1)\mathcal{H}(A) &= \bigcup_B \mathcal{P}_t(A) \cap (\lambda+1)\mathcal{H}(B)\\ &= \bigcup_B B + (\mathcal{P}_t(A) \cap \lambda\mathcal{H}(B))\\ &\subseteq A + \bigcup_B \mathcal{P}_t(A) \cap \lambda\mathcal{H}(B) = A + (\mathcal{P}_t(A) \cap \lambda\mathcal{H}(A)),\end{aligned}$$

where $\mathbf{0} \in B \subseteq \mathrm{ex}(\mathcal{H}(A))$ runs through subsets such that $B \setminus \{\mathbf{0}\}$ is linearly independent and $|B| = d+1$. Since the reverse inclusion is trivial, writing $\mathcal{P}_t(A) \cap \lambda\mathcal{H}(A) = (\lambda\mathcal{H}(A) \cap \Lambda_A) \setminus \mathcal{E}_t(A)$ finishes the proof. ☐

2.4.3. Proof of Theorem 1.5

Theorem 1.5 *If $A \subseteq \mathbb{Z}^d$ is finite, then for every $t \geq 1$ there is $h_t^{\mathrm{Kh}}(A) \in \mathbb{Z}_{\geq 1}$ such that, for every $h \geq h_t^{\mathrm{Kh}}(A)$, we have*

$$|(hA)^{(t)}| = P_{A,t}(h),$$

where $P_{A,t}(x) \in \mathbb{Q}[x]$ is a polynomial of degree $\leq d$.

Proof. We generalize the method of Nathanson–Rusza [**31**]. Let $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_\ell\} \subseteq \mathbb{Z}^d$ be a finite subset of $\mathbb{Z}^d$. Define the set $\widetilde{A} = \{\alpha_1, \ldots, \alpha_\ell\} \subseteq \mathbb{Z}^{d+1}$ where each $\alpha_j := (\mathbf{a}_j, 1)$. Define the projection

$$\begin{aligned}\pi = \pi_{\widetilde{A}} : \mathbb{Z}^\ell &\longrightarrow \mathbb{Z}^{d+1}\\ \mathbf{u} &\longmapsto \sum_{i=1}^{\ell} u_i\alpha_i,\end{aligned}$$

so that

$$(hA)^{(t)} = \{\mathbf{p} \in \mathbb{Z}^d \mid |\pi^{-1}(\mathbf{p},h)| \geq t\}.$$

We define two orders in $\mathbb{Z}^\ell$:

- $\mathbf{u} \leq \mathbf{v}$ if $\mathbf{v} - \mathbf{u} \in \mathbb{Z}^\ell_{\geq 0}$.
- $\mathbf{u} \leq_{\text{lex}} \mathbf{v}$ if there is $1 \leq j \leq \ell$ such that $u_1 = v_1, \ldots, u_{j-1} = v_{j-1}, u_j \leq v_j$. Note that this is a total ordering, and $\mathbf{u} \leq \mathbf{v}$ implies $\mathbf{u} \leq_{\text{lex}} \mathbf{v}$ but not vice versa.

For each $t \geq 1$, write

$$\mathcal{U}^{(t)} = \mathcal{U}^{(t)}_{\widetilde{A}} := \{\mathbf{z} \in \mathbb{Z}^\ell_{\geq 0} \mid \exists \mathbf{w}_1, \ldots, \mathbf{w}_t \neq \mathbf{z} \text{ s.t. } \mathbf{w}_i <_{\text{lex}} \mathbf{z},\, \mathbf{z} - \mathbf{w}_i \in \ker \pi\}, \tag{2.14}$$

for the set of *t-useless elements*, so that

$$\begin{aligned} |(hA)^{(t)}| = \#\{\mathbf{u} \in \mathbb{Z}^\ell_{\geq 0} \mid \mathbf{u} \notin \mathcal{U}^{(t)} \text{ and } (\pi(\mathbf{u}))_{d+1} = h\} \,-& \\ \#\{\mathbf{u} \in \mathbb{Z}^\ell_{\geq 0} \mid \mathbf{u} \notin \mathcal{U}^{(t-1)} \text{ and } (\pi(\mathbf{u}))_{d+1} = h\}.& \end{aligned} \tag{2.15}$$

Indeed, this counts those $\mathbf{u} \in \mathbb{Z}^\ell_{\geq 0}$ with $(\pi(\mathbf{u}))_{d+1} = h$ that have exactly $t-1$ elements $\mathbf{0} \leq \mathbf{v} <_{\text{lex}} \mathbf{u}$ with $\pi(\mathbf{v}) = \pi(\mathbf{u})$. The set of $\leq$-minimal elements of $\mathcal{U}^{(t)}$

$$\mathcal{M}^{(t)} = \mathcal{M}^{(t)}_{\widetilde{A}} := \{\mathbf{z} \in \mathcal{U}^{(t)} \mid \nexists \mathbf{w} \in \mathcal{U}^{(t)} \text{ s.t. } \mathbf{w} < \mathbf{z}\},$$

is, by Dickson's Lemma 2.23, a finite set. Note that $\mathbf{u} \in \mathcal{U}^{(t)}$ if and only if there exists $\mathbf{t} \in \mathcal{M}^{(t)}$ such that $\mathbf{u} \geq \mathbf{t}$.

We claim that

$$\begin{aligned} &\#\{\mathbf{u} \in \mathbb{Z}^\ell_{\geq 0} \mid \mathbf{u} \notin \mathcal{U}^{(t)} \text{ and } (\pi(\mathbf{u}))_{d+1} = h\} \\ &\qquad = \#\{\mathbf{u} \in \mathbb{Z}^\ell_{\geq 0} \mid (\pi(\mathbf{u}))_{d+1} = h\} - \#\{\mathbf{u} \in \mathcal{U}^{(t)} \mid (\pi(\mathbf{u}))_{d+1} = h\} \\ &\qquad = \sum_{T \subseteq \mathcal{M}^{(t)}} (-1)^{|T|}\, \#\{\mathbf{u} \in \mathbb{Z}^\ell_{\geq 0} \mid (\pi(\mathbf{u}))_{d+1} = h \text{ and } \mathbf{t}_T \leq \mathbf{u}\}, \end{aligned} \tag{2.16}$$

where the sum runs over all subsets T of $\mathcal{M}^{(t)}$, and $(\mathbf{t}_T)_i := \max_{\mathbf{t} \in T} (\mathbf{t})_i$. To prove the last line, note that for each $\mathbf{u} \in \mathbb{Z}^\ell_{\geq 0}$ with $(\pi(\mathbf{u}))_{d+1} = h$, there exists a maximal $T = T_{\mathbf{u}} \subseteq \mathcal{M}^{(t)}$ such that $\mathbf{u} \geq \mathbf{t}_T$. The term $\#\{\mathbf{u} \in \mathbb{Z}^\ell_{\geq 0} \mid (\pi(\mathbf{u}))_{d+1} = h\}$ corresponds to those $\mathbf{u}$ with $T_{\mathbf{u}} = \varnothing$. The remaining $\mathbf{u}$ with $T_{\mathbf{u}} \neq \varnothing$ (which are exactly the elements of $\mathcal{U}^{(t)}$) are counted $\sum_{U \subseteq T, U \neq \varnothing} (-1)^{|U|} = (1-1)^k - 1 = -1$ times, yielding the term $\#\{\mathbf{u} \in \mathcal{U}^{(t)} \mid (\pi(\mathbf{u}))_{d+1} = h\}$.

Thus, by the standard "stars and bars" argument, we obtain from (2.16) that

$$\#\{\mathbf{u} \in \mathbb{Z}^\ell_{\geq 0} \mid \mathbf{u} \notin \mathcal{U}^{(t)} \text{ and } (\pi(\mathbf{u}))_{d+1} = h\} = \sum_{T \subseteq \mathcal{M}^{(t)}} (-1)^{|T|} \binom{h - \sigma(\mathbf{t}_T) + \ell - 1}{\ell - 1},$$

where $\sigma(\mathbf{t}_T) := \sum_i (\mathbf{t}_T)_i$, provided $h \geq \sigma(\mathbf{t}_T)$ for every $T \subseteq \mathcal{M}^{(t)}$. Similarly,

$$\#\{\mathbf{u} \in \mathbb{Z}^\ell_{\geq 0} \mid \mathbf{u} \notin \mathcal{U}^{(t-1)} \text{ and } (\pi(\mathbf{u}))_{d+1} = h\} = \sum_{S \subseteq \mathcal{M}^{(t-1)}} (-1)^{|S|} \binom{h - \sigma(\mathbf{t}_S) + \ell - 1}{\ell - 1},$$

therefore (2.15) is polynomial in h for $h \geq h_t^{\mathrm{Kh}}(A)$, where

$$h_t^{\mathrm{Kh}}(A) \leq \max\left\{ \sum_i \max_{\mathbf{t}\in\mathcal{M}^{(t)}} (\mathbf{t})_i,\ \sum_i \max_{\mathbf{t}\in\mathcal{M}^{(t-1)}} (\mathbf{t})_i \right\} < \infty$$

(since $\mathcal{M}^{(t)}$, $\mathcal{M}^{(t-1)}$ are finite), completing the proof. □

Chapter 3

Knights are 24/13 times faster than the king

In this chapter, we determine the average speed advantage of the (a,b)-knight over the king on an infinite chessboard, proving Theorem 1.7 of Section 1.2. This is achieved by comparing the minimal number of moves required to reach a point $\mathbf{p} \in \mathbb{Z}^2$ using sumsets $h\mathrm{N}_{a,b}$ and $h\mathrm{K}$. Using Theorem 1.6, we show that the inverse of the average ratio between these quantities is given by $\frac{2(a+b)b^2}{a^2+3b^2}$, confirming that the knight is $24/13 \approx 1.85$ times faster than the king (when $a = 1$ and $b = 2$).

3.1. Knights in $\mathbb{Z}^2$

For a set $A \subset \mathbb{Z}^2$, we write $A(x,y) = \min\{h \geq 1 \mid (x,y) \in hA\}$ for the minimum number of moves it takes A to get to the point (x,y) starting from $(0,0)$. The king is characterized by the set of moves

$$\mathrm{K} = \{(1,0), (1,1), (0,1), (-1,1), (-1,0), (-1,-1), (0,-1), (1,-1)\},$$

and the (a,b)-knight by

$$\mathrm{N}_{a,b} = \{(b,a), (a,b), (-a,b), (-b,a), (-b,-a), (-a,-b), (a,-b), (b,-a)\}.$$

We start with a lemma estimating how long the (a,b)-knight takes to access a point in $\mathcal{B}_{a+b}$, where

$$\mathcal{B}_h = \{(x,y) \in \mathbb{Z}^2 \mid \max\{|x|,|y|\} \leq h\} = h\mathrm{K}$$

is the ball of radius h with respect to the max norm.

Lemma 3.1. *Let $b > a \geq 1$ be integers with $\gcd(a,b) = 1$ and $a + b$ odd. For every $(x,y) \in \mathcal{B}_{a+b}$, we have $\mathrm{N}_{a,b}(x,y) = O(b)$ uniformly for a,b.*

Proof. Since $\gcd(a,b) = 1$, for every $1 \leq k \leq b$ there are $x,y \in \mathbb{Z}$ with $ax + by = k$, and we can select x,y such that $|x| \leq b$, $|y| \leq a$. Hence, since $\mathrm{N}_{a,b}$ is symmetric,

$$(2k,0) = x\Big((a,b) + (a,-b)\Big) + y\Big((b,a) + (b,-a)\Big)$$

is accessible in $2(|x| + |y|) \leq 2(a + b) < 4b$ moves, and so are the points $(-2k,0)$, $(0,2k)$, $(0,-2k)$. This implies that every point in $\mathcal{B}_{a+b}$ with even coordinates is accessible in $O(b)$ moves. By symmetry, it then suffices to show $\mathrm{N}_{a,b}(1,0) = O(b)$.

Suppose that a is even (so b is odd). Then, the point $(1-a,-b) \in \mathcal{B}_{a+b}$ has even coordinates, and so is accessible in $O(b)$ moves. Therefore, so is $(1,0) = (1-a,-b)+(a+b)$. The case when a is odd (so b is even) is similar. □

3.1.1. Proof of Theorem 1.6

Theorem 1.6 *Let* $b > a \geq 1$ *be integers with* $\gcd(a,b) = 1$ *and* $a+b$ *odd, and let* $x \geq y \in \mathbb{Z}_{\geq 0}$.

(i) *If* $y \leq \dfrac{a}{b}x$, *then* $\mathrm{N}_{a,b}(x,y) = \dfrac{x}{b} + O(b)$.

(ii) *If* $y > \dfrac{a}{b}x$, *then* $\mathrm{N}_{a,b}(x,y) = \dfrac{x+y}{a+b} + O(b)$.

Proof. We prove the parts separately.

• Part (i): Let $\ell := \lfloor x/b \rfloor$, so that $\ell b \leq x < (\ell+1)b$ and $0 \leq y < (\ell+1)a$. Because $x \geq \ell b$, we have $\mathrm{N}_{a,b}(x,y) \geq \ell$. On the other hand, for each integer $0 \leq k \leq \ell/2$,

$$\Big(\ell - k\Big)(b,a) + k(b,-a) = (\ell b, (\ell - 2k)a),$$

so all the points in $\mathcal{S}_{(\ell b,\ell a)} := \{(\ell b, (\ell - 2t)a) \mid 0 \leq k \leq \ell/2\}$ are accessible in ℓ moves or less. All the points (x,y) with $\ell b \leq x < (\ell+1)b$ and $0 \leq y < (\ell+1)a$ are at distance[1] at most $a+b$ from $\mathcal{S}_{(\ell b,\ell a)}$. Since, by Lemma 3.1, $\mathrm{N}_{a,b}$ accesses all the points of $\mathcal{B}_{a+b}$ in $O(b)$ moves, it follows that $\mathrm{N}_{a,b}(x,y) \leq \ell + O(b)$.

• Part (ii): Let $t,u \in \mathbb{R}_{\geq 0}$ be such that $(x,y) = t(a,b) + u(b,a)$, so that $\mathrm{N}_{a,b}(x,y) \geq t + u$. Since

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}\begin{pmatrix} t \\ u \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \iff \frac{1}{b^2 - a^2}\begin{pmatrix} -a & b \\ b & -a \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} t \\ u \end{pmatrix},$$

we have $t = (by - ax)/(b^2 - a^2)$, $u = (bx - ay)/(b^2 - a^2)$ (both strictly positive, because $y/x > a/b$), and hence

$$\mathrm{N}_{a,b}(x,y) \geq \frac{(b-a)(x+y)}{b^2 - a^2} = \frac{x+y}{a+b}.$$

On the other hand, $\lfloor t \rfloor(a,b) + \lfloor u \rfloor(b,a) = (x,y) + \mathbf{r}$, where $\mathbf{r} \in \mathcal{B}_{a+b}$. Since, by Lemma 3.1, $\mathrm{N}_{a,b}$ accesses all the points of $\mathcal{B}_{a+b}$ in $O(b)$ moves, it follows that $\mathrm{N}_{a,b}(x,y) \leq \lfloor t \rfloor + \lfloor u \rfloor + O(b) = \frac{x+y}{a+b} + O(b)$. □

[1] With respect to the max norm.

3.1.2. Distribution of N/K

It follows from Theorem 1.6 that, for $x \geq y \in \mathbb{Z}_{\geq 0}$, the ratio $\frac{\mathrm{N}_{a,b}(x,y)}{\mathrm{K}(x,y)}$ lies essentially in between $\frac{1}{b}$ and $\frac{2}{a+b}$:

$$\frac{\mathrm{N}_{a,b}(x,y)}{\mathrm{K}(x,y)} = \begin{cases} \frac{1}{b} + O\left(\frac{b}{x}\right) & \text{if } \frac{y}{x} \leq \frac{a}{b}, \\ \frac{1}{a+b}\left(1 + \frac{y}{x}\right) + O\left(\frac{b}{x}\right) & \text{if } \frac{y}{x} > \frac{a}{b}. \end{cases}$$

Analysing this ratio in the box $\mathcal{B}_h$, one can study the *distribution* of $\mathrm{N}_{a,b}/\mathrm{K}$ via the real function

$$D_{a,b}(t) := \lim_{h\to+\infty} \frac{\#\{(x,y) \in \mathcal{B}_h \mid \frac{\mathrm{N}_{a,b}(x,y)}{\mathrm{K}(x,y)} \leq t\}}{|\mathcal{B}_h|}.$$

Both $\mathrm{N}_{a,b}$ and K are symmetric. Therefore, since $\frac{1}{a+b}(1+\frac{y}{x}) \leq t$ if and only if $\frac{y}{x} \leq (a+b)t - 1$, and the proportion of points in $\mathcal{B}_h \cap \{(x,y) \in \mathbb{Z}_{\geq 0} \mid x \geq y\}$ with $\frac{y}{x} \leq u$ equals $\frac{2}{h(h+1)} \sum_{x=1}^{h} \sum_{y=1}^{\lfloor ux \rfloor} 1 = u + O(1/h)$, we have

$$D_{a,b}(t) = \begin{cases} 0 & \text{if } t < \frac{1}{b}, \\ (a+b)t - 1 & \text{if } \frac{1}{b} \leq t \leq \frac{2}{a+b}, \\ 1 & \text{if } t > \frac{2}{a+b}. \end{cases} \tag{3.1}$$

3.1.3. Proof of Theorem 1.7

Recall that the velocity of a piece $A \subseteq \mathbb{Z}^2$ with respect to the king K is defined as

$$v(A) := \lim_{h\to\infty} \frac{2h}{3} \left(\frac{1}{|\mathcal{B}_h|} \sum_{\mathbf{p}\in\mathcal{B}_h} A(\mathbf{p}) \right)^{-1}.$$

Theorem 1.7 *Let $b > a \geq 1$ be integers with $\gcd(a,b) = 1$ and $a+b$ odd. Then:*

$$v(\mathrm{N}_{a,b}) = \frac{2(a+b)b^2}{a^2+3b^2}.$$

Proof. By the symmetries of $\mathrm{N}_{a,b}(x,y)$, we have

$$\lim_{h\to+\infty} \frac{3}{2h} \left(\frac{1}{|\mathcal{B}_h|} \sum_{\mathbf{p}\in\mathcal{B}_h} \mathrm{N}_{a,b}(\mathbf{p}) \right) = \lim_{h\to+\infty} \frac{3}{2h} \left(\frac{2}{h(h+1)} \sum_{\substack{x,y\in\mathbb{Z}_{\geq 0} \\ 1\leq y\leq x\leq h}} \mathrm{N}_{a,b}(x,y) \right), \tag{3.2}$$

so it suffices to prove the existence and calculate the right-hand side.

By Theorem 1.6, we have

$$\sum_{\substack{x,y\in\mathbb{Z}_{\geq 0}\\ 1\leq y\leq x\leq h}} \mathrm{N}_{a,b}(x,y) = \sum_{x=1}^{h} \left\lfloor \frac{a}{b}\,x \right\rfloor \frac{x}{b} + \sum_{x=1}^{h} \sum_{\substack{y=1\\ y/x>a/b}}^{x} \frac{x+y}{a+b} + O((a+b)h^2)$$
$$= \sum_{x=1}^{h} \left(\frac{a}{b^2} + \frac{1}{a+b} \sum_{\substack{y=1\\ y/x>a/b}}^{x} \left(1+\frac{y}{x}\right)\frac{1}{x} \right) x^2 + O((a+b)h^2).$$

Since

$$\sum_{\substack{y=1\\ y/x>a/b}}^{x} \left(1+\frac{y}{x}\right)\frac{1}{x} = \frac{1}{x}\left(\sum_{\substack{y=1\\ y/x>a/b}}^{x} 1 \right) + \frac{1}{x^2}\left(\sum_{\substack{y=1\\ y/x>a/b}}^{x} y \right)$$
$$= \left(1-\frac{a}{b}\right) + \frac{1}{2}\left(1-\frac{a^2}{b^2}\right) + O\left(\frac{1}{x}\right),$$

it follows that:

$$\sum_{\substack{x,y\in\mathbb{Z}_{\geq 0}\\ 1\leq y\leq x\leq h}} \mathrm{N}_{a,b}(x,y) = \left(\frac{a}{b^2} + \frac{1}{a+b}\left(\left(1-\frac{a}{b}\right) + \frac{1}{2}\left(1-\frac{a^2}{b^2}\right) \right) \right) \frac{h(h+1)(2h+1)}{6}$$
$$+ O((a+b)h^2).$$

Plugging this into the limit $v(\mathrm{N}_{a,b})$, we obtain

$$v(\mathrm{N}_{a,b}) = \lim_{h\to+\infty} \frac{2h}{3} \left(\frac{2}{h(h+1)} \sum_{\substack{x,y\in\mathbb{Z}_{\geq 0}\\ 1\leq y\leq x\leq h}} \mathrm{N}_{a,b}(x,y) \right)^{-1}$$
$$= \left(\frac{a}{b^2} + \frac{1}{a+b}\left(\left(1-\frac{a}{b}\right) + \frac{1}{2}\left(1-\frac{a^2}{b^2}\right) \right) \right)^{-1}$$
$$= \frac{2}{3}\left(\frac{2a^2+2ab}{3b^2} + \left(1-\frac{a}{b}\right)\left(1+\frac{a}{3b}\right) \right)^{-1} (a+b)$$
$$= \frac{2}{3}\left(1+\frac{1}{3}\,\frac{a^2}{b^2}\right)^{-1}(a+b) = \frac{2(a+b)b^2}{a^2+3b^2},$$

concluding the proof. □

3.2. Remarks

Remark 3.2. One checks that calculating the average using (3.1) agrees, in fact, with (the inverse of) Theorem 1.7:

$$\mathbb{E}\left(\frac{\mathrm{N}_{a,b}}{\mathrm{K}}\right) := \int_0^{+\infty} (1-D_{a,b}(t))\,\mathrm{d}t = \frac{1}{b} + \int_{1/b}^{2/(a+b)} (2-(a+b)t)\,\mathrm{d}t$$

$$= \frac{1}{b} + \frac{2(b-a)}{(b+a)b} - \frac{(b-a)(a+3b)}{2(a+b)b^2} = \frac{a^2+3b^2}{2(a+b)b^2}.$$

Remark 3.3 (On generality)**.** The choice of the box $\mathcal{B}_h$ in the definition of (1.6) is not generic, and different expanding regimes will give different answers for the ratio. In general, let $d \geq 2$ and $A \subseteq \mathbb{Z}^2$ be primitive set, and suppose that the origin $\mathbf{0}$ lies inside the convex hull $\mathcal{H}(A)$ of A. Write $A_{\mathbf{0}} = A \cup \{\mathbf{0}\}$. By Khovanskii's theorem [**20**, Corollary 1], we have $|hA_{\mathbf{0}}| = \mathrm{vol}(\mathcal{H}(A))\, h^d + O(h^{d-1})$ and

$$|hA_{\mathbf{0}} \setminus (h-1)A_{\mathbf{0}}| = d\,\mathrm{vol}(\mathcal{H}(A))\, h^{d-1} + O(h^{d-2}),$$

where $\mathrm{vol}(\mathcal{H}(A))$ denotes the d-volume of the convex hull of A. Thus,

$$\frac{1}{|hA_{\mathbf{0}}|} \sum_{\mathbf{p} \in hA_{\mathbf{0}}} A(\mathbf{p}) = \frac{1}{|hA_{\mathbf{0}}|} \sum_{\ell=1}^{h} \sum_{\mathbf{p} \in \ell A_{\mathbf{0}} \setminus (\ell-1)A_{\mathbf{0}}} A(\mathbf{p}) = \frac{dh}{d+1} + O(1).$$

Given a finite primitive set $B \subseteq \mathbb{Z}^d$, we define the velocity of B *relative to* A as

$$v_A(B) := \lim_{h \to +\infty} \left(1 + \frac{1}{d}\right) h \left(\frac{1}{|hA_{\mathbf{0}}|} \sum_{\mathbf{p} \in hA_{\mathbf{0}}} B(\mathbf{p}) \right)^{-1}.$$

It would be interesting to calculate the velocity of generalized knights with respect to the generalized king $\mathrm{K}^d = \{\mathbf{p} \in \mathbb{Z}^d \mid \|p\|_\infty = 1\}$, or velocities with respect to other pieces such as the *taxicab* $\mathrm{T} := \{\mathbf{p} = (x,y) \in \mathbb{Z}^2 \mid \|\mathbf{p}\|_1 := |x| + |y| = 1\} = \{(1,0), (0,1), (-1,0), (0,-1)\}$.

Remark 3.4 (Fiboknights)**.** Fibonacci numbers $F_0 = 1$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ (for $n \geq 2$) satisfy the property that F_{3n} is even, F_{3n+1}, F_{3n+2} are odd, and $\gcd(F_n, F_{n+1}) = 1$. Define the *n-th Fiboknight* as

$$\mathrm{FN}_n = \mathrm{N}_{F_{n+1}, F_{n+2}},$$

so that the usual knight is the first Fiboknight. By the properties of Fibonacci numbers, FN_n is only primitive for n such that $3 \nmid n$.

Let $k \geq 1$, and let $n \to \infty$ through $n \in \mathbb{Z}_{\geq 1}$ for which FN_n, FN_{n+k} are primitive. Then, by Theorem 1.7, writing $\phi = \frac{1+\sqrt{5}}{2}$ for the golden ratio, we have

$$\begin{aligned}
\lim_{\substack{n\to\infty \\ 3\nmid n,\, n+k}} \frac{v(\mathrm{FN}_{n+k})}{v(\mathrm{FN}_n)} &= \lim_{\substack{n\to\infty \\ 3\nmid n,\, n+k}} \frac{\dfrac{2(F_{n+k+1} + F_{n+k+2})F_{n+k+2}^2}{F_{n+k+1}^2 + 3F_{n+k+2}^2}}{\dfrac{2(F_{n+1} + F_{n+2})F_{n+2}^2}{F_{n+1}^2 + 3F_{n+2}^2}} \\
&= \lim_{\substack{n\to\infty \\ 3\nmid n,\, n+k}} \frac{F_{n+k+3}}{F_{n+3}} \frac{F_{n+k+2}^2}{F_{n+2}^2} \frac{(F_{n+1}^2 + 3F_{n+2}^2)}{(F_{n+k+1}^2 + 3F_{n+k+2}^2)} \\
&= \phi^k\, \phi^{2k} \frac{1 + 3\phi^2}{\phi^{2k} + 3\phi^{2k+2}} \\
&= \phi^k.
\end{aligned}$$

In particular, the ratio of the velocity of consecutive Fiboknights (which can only be of the form FN_{3n+1}, FN_{3n+2}) converges to ϕ. In general, for fixed m,$k \geq 1$,

$$\lim_{\substack{n\to\infty \\ \text{primitive}}} \frac{v(\mathrm{N}_{F_{n+k},F_{n+m+k}})}{v(\mathrm{N}_{F_n,F_{n+m}})} = \frac{\dfrac{2(\phi^k+\phi^{m+k})\phi^{2(m+k)}}{\phi^{2k}+3\phi^{2(m+k)}}}{\dfrac{2(1+\phi^m)\phi^{2m}}{1+3\phi^{2m}}} = \phi^k.$$

Chapter 4

Representation functions with prescribed rates of growth

In this chapter, we will prove several theorems related to the representation functions $r_{A,h}(n)$ of subsets $A \subseteq \mathbb{Z}_{\geq 0}$ with specified growth rates. We will establish Theorem 1.8, which shows the existence of a set A with $r_{A,h}(n) \sim F(n)$ for regularly varying functions F satisfying $\frac{F(x)}{\log x} \to \infty$. We will also prove Theorems 1.10 and 1.11, which extends the range of permissible functions F by relaxing regularity conditions, allowing us to find A satisfying $r_{A,h}(n) \asymp F(n)$. Finally, we examine a probabilistic heuristic that predicts $r_{A,h}(n)$ vanishes infinitely often if $r_{A,h}(n) = o(\log n)$, providing insights into a conjecture of Erdős and Turán.

4.1. Probabilistic setup

Given a locally integrable, positive real function $f(x) \ll x$ satisfying

$$\int_1^x \frac{f(t)}{t}\,\mathrm{d}t \asymp f(x), \tag{4.1}$$

consider the probability space whose elements are subsets $0 \in \mathscr{A} \subseteq \mathbb{Z}_{\geq 0}$ and

$$\Pr(\mathbf{1}_{\mathscr{A}}(n) = 1) = \mathbb{E}(\mathbf{1}_{\mathscr{A}}(n)) := \min\left\{c\,\frac{f(n)}{n},\, 1\right\} \qquad (\forall n \in \mathbb{Z}_{\geq 1}) \tag{4.2}$$

for some constant $c > 0$ to be chosen later, where the $\mathbf{1}_{\mathscr{A}}(n)$'s are mutually independent boolean random variables.[1] The purpose of this space is to have the counting function of $\mathscr{A}$ be of the same order of magnitude as f: by the strong law of large numbers, we have $|\mathscr{A} \cap [1,x]| \overset{\text{a.s}}{\sim} c\sum_{n\leq x} \frac{\min\{f(n),n/c\}}{n} \asymp_c f(x)$.

We work under stronger hypotheses to prove Theorems 1.8–1.10, but functions satisfying (4.1) capture the "minimal assumptions" necessary to prescribe an order of growth using (4.2), and will be used in Theorem 1.11.

[1] cf. Chapter III of Halberstam–Roth [**17**] for a construction of the product measure.

Lemma 4.1 (Characterization)**.** *A positive, locally integrable real function f satisfies $\int_1^x \frac{f(t)}{t}\,\mathrm{d}t \asymp f(x)$ if and only if:*

(i) *For any $\lambda > 0$, we have $f(\lambda x) \asymp_\lambda f(x)$; and*

(ii) *There is $\vartheta = \vartheta_f > 0$ for which the following holds: there exists $x_0 \in \mathbb{R}_{>0}$ and $M > 0$ such that, for every $y > x \geq x_0$, we have $\dfrac{f(x)}{x^\vartheta} \leq M \dfrac{f(y)}{y^\vartheta}$.*

Proof. This is Corollary 2.6.2 of Bingham–Goldie–Teugels [**2**], to which we give a short proof for the sake of completeness.

($\Longrightarrow$) Let $g(x) := \int_1^x \frac{f(t)}{t}\,\mathrm{d}t$. Then, $g(x) \asymp f(x)$, and $g'(x) = f(x)/x$, so

$$\frac{g'(x)}{g(x)} \asymp \frac{1}{x}.$$

Taking $\lambda > 1$, integrating from x to λx yields $\log(g(\lambda x)/g(x)) \asymp \log \lambda$, so there are $\vartheta, \eta > 0$ such that $\lambda^\theta g(x) \leq g(\lambda x) \leq \lambda^\eta g(x)$. Hence,

$$r\lambda^\theta f(x) \leq f(\lambda x) \leq s\lambda^\eta f(x) \tag{4.3}$$

for some r,$s > 0$. For $0 < \lambda < 1$, simply take $x = \lambda^{-1} y$ in (4.3), concluding (i).

For (ii), taking $\lambda = y/x$ in (4.3) yields $r(y/x)^\theta f(x) \leq f(y)$, and so

$$\frac{f(x)}{x^\vartheta} \leq M \frac{f(y)}{y^\vartheta}$$

for $M = 1/r$.

($\Longleftarrow$) Given $x \in \mathbb{R}_{>1}$, let $J \geq 1$ be the smallest integer such that $2^J \geq x$. Since $f(2x) \asymp f(x)$, by (i) we have $f(2^{J-1}) \asymp f(x) \asymp f(2^J)$ (cf. Remark 4.2). Moreover,

$$\int_1^x \frac{f(t)}{t}\,\mathrm{d}t = \sum_{j=0}^{J-2} \int_{2^j}^{2^{j+1}} \frac{f(t)}{t}\,\mathrm{d}t + \int_{2^{J-1}}^{x} \frac{f(t)}{t}\,\mathrm{d}t \asymp \sum_{j=1}^{J} f(2^j).$$

By (ii), $f(2^\ell) \leq M 2^{-(J-\ell)} f(2^J)$ for $\ell \geq \ell_0$, where ℓ_0 is such that $2^{\ell_0} > x_0$. Thus,

$$f(2^J) \leq \sum_{\ell=\ell_0}^{J} f(2^\ell) \leq M\, f(2^J) \sum_{\ell=\ell_0}^{J} \frac{1}{2^{J-\ell}} \ll f(2^J),$$

so $\int_1^x \frac{f(t)}{t}\,\mathrm{d}t \asymp f(2^J) \asymp f(x)$. □

Remark 4.2 (Uniform convergence)**.** Let $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ be a measurable function satisfying $f(\lambda x) \asymp_\lambda f(x)$ for every $\lambda > 0$. Then, for every real $\Lambda > 1$ we have

$$0 < \liminf_{x\to\infty} \inf_{\lambda\in[1,\Lambda]} \frac{f(\lambda x)}{f(x)} \leq \limsup_{x\to\infty} \sup_{\lambda\in[1,\Lambda]} \frac{f(\lambda x)}{f(x)} < \infty$$

(cf. BGT [**2**, Theorem 2.0.8]). This implies, for instance, that for every fixed $\varepsilon > 0$, $f(k) \asymp_\varepsilon f(n)$ uniformly for $n \geq 1$ and $\varepsilon n \leq k \leq \varepsilon^{-1} n$ (i.e., the implied constant depends only on ε).

4.1.1. Exact solutions

We say that a solution to $b_1x_1 + \cdots + b_\ell x_\ell = n$ is *exact* if the x_i's are pairwise distinct. Define the *exact representation function*

$$\rho_{\mathscr{A},\ell}(n) = \rho_{\mathscr{A},\ell}^{(b_1,\ldots,b_h)}(n) := \sum_{\substack{x_1,\ldots,x_\ell \in \mathbb{Z}_{\geq 0} \\ b_1x_1+\cdots+b_\ell x_\ell = n \\ x_i\text{'s distinct}}} \mathbf{1}_{\mathscr{A}}(x_1)\cdots\mathbf{1}_{\mathscr{A}}(x_\ell). \tag{4.4}$$

This function is more amenable to probabilistic methods, since it is a sum of products of ℓ independent variables. If $(x_1,\ldots,x_\ell)$ is a solution to $b_1x_1 + \cdots + b_\ell x_\ell = n$ with $x_1 = x_2$, but $x_2 \neq \cdots \neq x_\ell$, then $(x_2,\ldots,x_\ell)$ is an exact solution to the equation

$$(b_1 + b_2)x_2 + b_3x_3 + \cdots + b_\ell x_\ell = n.$$

Similarly, every non-exact solution of length ℓ yields an exact solution to an equation of smaller length. More precisely, we have

$$r_{\mathscr{A},\ell}(n) = \rho_{\mathscr{A},\ell}(n) + \sum_{(c_1,\ldots,c_t)} \rho_{\mathscr{A},t}^{(c_1,\ldots,c_t)}(n), \tag{4.5}$$

where the sum runs through the $(c_1,\ldots,c_t)$, $t < \ell$ that generate equations $c_1x_1 + \cdots + c_tx_t = n$ which are produced by non-exact solutions to $b_1x_1 + \cdots + b_\ell x_\ell$. Note that $\max_{(c_1,\ldots,c_t)} \max\{c_i\} \leq b_1 + \cdots + b_\ell$.

Lemma 4.4 uses the strategy of dividing the sum over solutions to $b_1x_1 + \cdots + b_\ell x_\ell$ into dyadic intervals by Vu [**39**, Lemma 3.3].

Lemma 4.3. *Let $\ell \geq 1$. For every $P_1,\ldots,P_\ell > 0$, the number of integer solutions $(x_1,\ldots,x_\ell) \in \mathbb{Z}_{\geq 0}^\ell$ to*

$$b_1x_1 + \cdots + b_\ell x_\ell = n,$$

with each $x_j \leq P_j$, is $O_{\ell,b_1,\ldots,b_\ell}(\frac{1}{n}P_1\cdots P_\ell)$.

Proof. If $P_i < n/(\max_{i\leq\ell} b_i)\ell$ for every i, then there are no solutions $(x_1,\ldots,x_\ell) \in [1,P_1] \times \cdots \times [1,P_\ell]$, since the sum is $< n$, and the statement is true. So suppose there is some $1 \leq j \leq \ell$ for which $P_j \geq n/(\max_{i\leq\ell} b_i)\ell$.

There are at most $P_1\cdots P_{j-1}P_{j-1}\cdots P_\ell$ possible values $b_1x_1 + \cdots + b_{j-1}x_{j-1} + b_{j+1}x_{j+1} + \cdots + b_\ell x_\ell$ can assume, and for each, there is at most one value of x_j that makes $b_1x_1 + \cdots + b_\ell x_\ell = n$. Thus, the number of solutions is $O(P_1 \ldots P_{j-1}P_{j+1}\cdots P_\ell)$, and since $P_j/n \geq 1/(\max_{i\leq\ell} b_i)\ell$, this is $O_{\ell,b_1,\ldots,b_\ell}(\frac{1}{n}P_1\cdots P_\ell)$. ☐

Lemma 4.4 (Main lemma)**.** *For every $1 \leq \ell \leq h$,*

$$\frac{\min\{cf(n),n\}^\ell}{n}\mathbf{1}_{\gcd(b_1,\ldots,b_\ell)|n} \ll \mathbb{E}(r_{\mathscr{A},\ell}(n)) \ll c^\ell\frac{f(n)^\ell}{n}\mathbf{1}_{\gcd(b_1,\ldots,b_\ell)|n},$$

where the implied constants do not depend on c.

Proof. Write $f_c(x) := \min\{cf(x),x\}$. Since there is only a finite number of equations of smaller length that can be obtained from $b_1x_1 + \cdots + b_\ell x_\ell$ as in (4.5), in order to show the statement of the theorem, it suffices to show that

$$\frac{f_c(n)^t}{n}\mathbf{1}_{\gcd(c_1,\ldots,c_\ell)|n} \ll \mathbb{E}(\rho_{\mathscr{A},\ell}^{(c_1,\ldots,c_t)}(n)) \ll c^t\frac{f(n)^t}{n}\mathbf{1}_{\gcd(c_1,\ldots,c_\ell)|n}$$

for every $1 \le t \le \ell$ and $(c_1,\ldots,c_t) \in \{1,\ldots,b_1+\cdots+b_\ell\}^t$.

We start with the lower bound. If $\gcd(c_1,\ldots,c_t) \mid n$, then the total number of exact solutions to $c_1x_1 + \cdots + c_tx_t = n$ is $\ge \delta n^{t-1}$ for some $\delta > 0$ — this is the case because non-exact solutions can be counted as solutions to equations of order $\le t$, and hence are bounded by $O(n^{t-2})$. By Lemma 4.3, there is $C > 0$ such that for any small $\varepsilon > 0$, the number of solution with $x_j \le \varepsilon n$ is $\le C\frac{1}{n}(\varepsilon n)^t = C\varepsilon^t n^{t-1}$. Take $\varepsilon > 0$ so that $C\varepsilon^t < \delta/2$.

By Remark 4.2, since $f(k) \ge Mf(n)$ for $\varepsilon n \le k \le n$ and some $M = M_\varepsilon > 0$, we have $cf(k)/k \ge Mf_c(n)/n$. Similarly, $k \ge \varepsilon n$, so $1 \ge \varepsilon f_c(n)/n$, and hence $f_c(k)/k \ge Mf_c(n)/n$, where M does not depend on c. It follows that

$$\begin{aligned}\mathbb{E}(\rho_{\mathscr{A},t}^{(c_1,\ldots,c_t)}(n)) &\ge \sum_{\substack{x_1,\ldots,x_t\in\mathbb{Z}_{\ge 0}\\ c_1x_1+\cdots+c_tx_t=n\\ x_i\text{'s distinct}\\ x_j>\varepsilon n,\ \forall j}} \frac{f_c(x_1)}{x_1}\cdots\frac{f_c(x_t)}{x_t}\\ &\gg n^{t-1}\left(\frac{f_c(n)}{n}\right)^t\mathbf{1}_{\gcd(c_1,\ldots,c_t)|n} = \frac{f_c(n)^t}{n}\mathbf{1}_{\gcd(c_1,\ldots,c_t)|n}.\end{aligned}$$

For the upper bound, let $\mathcal{P}$ be the set of all t-tuples $\mathbf{p} = (P_1,\ldots,P_t)$ with $P_j \in \{1,2,4,\ldots,2^J\}$, where J is the smallest integer for which $2^J \ge n$, and write

$$\sigma_{\mathbf{p}} := \sum_{\substack{(x_1,\ldots,x_t)\subseteq\mathbb{Z}_{\ge 0}^t\\ c_1x_1+\cdots+c_tx_t=n\\ x_i\text{'s distinct}\\ \frac{P_j}{2}-\frac{1}{2}\le x_j<P_j,\ \forall j}} \frac{f(x_1)}{x_1}\cdots\frac{f(x_t)}{x_t}$$

(where "$f(0)/0 = 1$"). We have $\mathbb{E}(\rho_{\mathscr{A},t}^{(c_1,\ldots,c_t)}(n)) \le c^t\sum_{\mathbf{p}\in\mathcal{P}}\sigma_{\mathbf{p}}$. Since the number of terms in $\sigma_{\mathbf{p}}$ is, by Lemma 4.3, $O(\frac{1}{n}P_1\cdots P_h)$, we have:

$$\begin{aligned}\mathbb{E}(\rho_{\mathscr{A},t}^{(c_1,\ldots,c_t)}(n)) &\le c^t\sum_{\mathbf{p}\in\mathcal{P}}\sigma_{\mathbf{p}}\\ &\ll c^t\sum_{\mathbf{p}\in\mathcal{P}}\frac{1}{n}P_1\cdots P_t\frac{f(P_1)}{P_1}\cdots\frac{f(P_t)}{P_t}\mathbf{1}_{\gcd(c_1,\ldots,c_t)|n}\\ &\ll c^t\frac{1}{n}\Big(f(1)+f(2)+f(4)+\cdots+f(2^J)\Big)^t\mathbf{1}_{\gcd(c_1,\ldots,c_t)|n}\\ &\ll c^t\frac{1}{n}f(2^J)^t\mathbf{1}_{\gcd(c_1,\ldots,c_t)|n} \asymp c^t\frac{f(n)^t}{n}\mathbf{1}_{\gcd(c_1,\ldots,c_t)|n},\end{aligned}$$

concluding the proof. ☐

Remark (Equations of smaller length)**.** For $2 \le \ell \le h$, write

$$r^*_{\mathscr{A},\ell}(n) := \max_{1\le i_1<\ldots<i_\ell\le h} \#\{(x_1,\ldots,x_\ell) \in \mathscr{A}^\ell \mid b_{i_1}x_1 + \cdots + b_{i_\ell}x_\ell = n\} \tag{4.6}$$

for the maximum among a choice of $b_{i_1},\ldots,b_{i_\ell}$ of the number of solutions to $b_{i_1}x_1+\cdots+b_{i_\ell}x_\ell = n$. Since there is only a finite number of choices of $b_{i_1},\ldots,b_{i_\ell}$, Lemma 4.4 implies that $\mathbb{E}(r^*_{\mathscr{A},\ell}(n)) \ll c^\ell f(n)^\ell/n$.

4.1.2. Theorem 1.11: Case $h = 2$

Theorem 1.11 (Case $h = 2$)**.** *If*

(i) (Range) $(x \log x)^{1/2} \ll f(x) \ll x$,

(ii) (Regularity) $\displaystyle\int_1^x \frac{f(t)}{t}\,\mathrm{d}t \asymp f(x)$;

then there exists $A \subseteq \mathbb{Z}_{\ge 0}$ *such that* $|A \cap [1,x]| \asymp f(x)$ *and* $r_{A,2}(n) \asymp \dfrac{f(n)^2}{n}$.

Proof. Suppose that $(x \log x)^{1/2} \ll f(x) \ll x$. Let $\widehat{r}_{\mathscr{A},2}(n)$ be the size of a maximal set of disjoint solutions $\{x_1,x_2\}$ to $b_1x_1 + b_2x_2 = n$, i.e. not sharing a x_j, so that

$$\widehat{r}_{\mathscr{A},2}(n) \le r_{\mathscr{A},2}(n) \le 2\,\widehat{r}_{\mathscr{A},2}(n).$$

In particular, $\mathbb{E}(\widehat{r}_{\mathscr{A},2}(n)) \gg \min\{cf(n), n\}^2/n \ge c^2\, d \log n$ for some $d > 0$, by Lemma 4.4. Since $\widehat{r}_{\mathscr{A},2}(n)$ is a sum of independent boolean random variables of the type $\mathbf{1}_{\mathscr{A}}(x)\mathbf{1}_{\mathscr{A}}(\frac{n-b_2x}{b_1})$, we may apply Chernoff's inequality [**37**, Theorem 1.8], obtaining

$$\begin{aligned}\Pr\left(|\widehat{r}_{\mathscr{A},2}(n) - \mathbb{E}(\widehat{r}_{\mathscr{A},2}(n))| \ge \tfrac{1}{2}\mathbb{E}(\widehat{r}_{\mathscr{A},2}(n))\right) &\le 2e^{-\frac{1}{16}\mathbb{E}(\widehat{r}_{\mathscr{A},2}(n))} \\ &\le 2e^{-\frac{1}{16}c^2 d\,\log n} \le n^{-2}\end{aligned}$$

for large enough c. By the Borel–Cantelli lemma, we conclude that $r_{\mathscr{A},2}(n) \asymp \widehat{r}_{\mathscr{A},2}(n) \overset{\text{a.s.}}{\asymp} f(n)^2/n$, completing the proof. ☐

4.1.3. δ-small and δ-normal solutions

As in Vu [**39**], in order to estimate $r_{\mathscr{A},h}(n)$, we separate the solutions being counted into *small* and *normal*, depending on a parameter δ, as follows: For $0 < \delta < 1$, define

$$\begin{aligned} r^{(\delta\text{-small})}_{\mathscr{A},\ell}(n) &:= \sum_{\substack{x_1,\dots,x_\ell \in \mathbb{Z}_{\geq 0} \\ b_1x_1+\cdots+b_\ell x_\ell = n \\ \exists j \;|\; x_j < n^\delta}} \mathbf{1}_{\mathscr{A}}(x_1)\cdots\mathbf{1}_{\mathscr{A}}(x_\ell), \\ r^{(\delta\text{-normal})}_{\mathscr{A},\ell}(n) &:= \sum_{\substack{x_1,\dots,x_\ell \in \mathbb{Z}_{\geq 0} \\ b_1x_1+\cdots+b_\ell x_\ell = n \\ x_1,\dots,x_\ell \geq n^\delta}} \mathbf{1}_{\mathscr{A}}(x_1)\cdots\mathbf{1}_{\mathscr{A}}(x_\ell), \end{aligned} \tag{4.7}$$

so that $r_{\mathscr{A},\ell}(n) = r^{(\delta\text{-small})}_{\mathscr{A},\ell}(n) + r^{(\delta\text{-normal})}_{\mathscr{A},\ell}(n)$. Both $\rho^{(\delta\text{-small})}_{\mathscr{A},\ell}(n)$ and $\rho^{(\delta\text{-normal})}_{\mathscr{A},\ell}(n)$ are defined similarly. We show that δ-small solution are, in average, few.

Lemma 4.5. *Let $\vartheta = \vartheta_f$ be as in item* (ii) *of Lemma 4.1. Then, for every $0 < \delta < 1$, we have*

$$\mathbb{E}\Big(r^{(\delta\text{-small})}_{\mathscr{A},h}(n)\Big) \ll c^h\, n^{-(1-\delta)\vartheta}\,\frac{f(n)^h}{n}.$$

Proof. Let r^* be as in (4.6). We have

$$\begin{aligned} \mathbb{E}(r^{(\delta\text{-small})}_{\mathscr{A},h}(n)) &\leq \sum_{j=1}^{h}\sum_{x_j \leq n^\delta} \mathbb{E}\Big(r^*_{\mathscr{A},h-1}(n-b_jx_j)\mathbf{1}_{\mathscr{A}}(x_j)\Big) \\ &\leq c\sum_{j=1}^{h}\sum_{x_j \leq n^\delta} \frac{f(x_j)}{x_j}\,\mathbb{E}\Big(r^*_{\mathscr{A},h-1}(n-b_jx_j) \mid \mathbf{1}_{\mathscr{A}}(x_j)=1\Big). \end{aligned}$$

Using that

$$\mathbb{E}\Big(r^*_{\mathscr{A},h-1}(n-b_jx_j) \mid \mathbf{1}_{\mathscr{A}}(x_j)=1\Big) \leq \sum_{\ell=1}^{h-1}\sum_{b=1}^{h(\max b_i)} \mathbb{E}\Big(r^*_{\mathscr{A},h-\ell}(n-bx_j)\Big)$$

we obtain by Lemma 4.4 that

$$\begin{aligned} \mathbb{E}(r^{(\delta\text{-small})}_{\mathscr{A},h}(n)) &\ll c^h\frac{f(n)^{h-1}}{n}\sum_{k\leq n^\delta}\frac{f(k)}{k} \\ &\asymp c^h f(n^\delta)\frac{f(n)^{h-1}}{n}. \end{aligned}$$

Since there is $\vartheta = \vartheta_f > 0$ for which $f(n^\delta) = f(n^{-(1-\delta)}\,n) \ll n^{-(1-\delta)\vartheta}f(n)$ by Lemma 4.1, the lemma follows. □

4.1.4. Disjoint families of representations

Let $\widehat{r}_{\mathscr{A},\ell}(n)$ denote the maximum size of a disjoint family (abbreviated *disfam*) of solutions $R = (x_1,\dots,x_\ell) \in \mathscr{A}$ of n. Thus, $\widehat{r}_{\mathscr{A},\ell}(n) = |\mathcal{M}|$ for some maximal disjoint family (abbreviated *maxdisfam*) of representations. This means that for every solution R, there is a solution $S \in \mathcal{M}$ such that $S \cap R \neq \varnothing$. Hence, for r^* as in (4.6),

$$r_{\mathscr{A},\ell}(n) \leq \sum_{j=1}^{\ell} \sum_{\substack{k \in S \\ S \in \mathcal{M}}} r^*_{\mathscr{A},\ell-1}(n - b_j k) \leq \ell \cdot \ell! \, \widehat{r}_{\mathscr{A},\ell}(n) \cdot \left(\max_{k \leq n} r^*_{\mathscr{A},\ell-1}(k) \right). \tag{4.8}$$

Whenever we add a " $\widehat{\ }$ " to a representation function, we are taking the size a maximum disfam of representations counted by that function: e.g., $\widehat{r}^*_{\mathscr{A},\ell}$, $\widehat{\rho}_{\mathscr{A},\ell}$, $\widehat{\rho}^{(\delta\text{-small})}_{\mathscr{A},\ell}$. We state the next lemma in sufficient generality to cover most use cases.

Lemma 4.6. *For every $2 \leq \ell \leq h$, we have*

$$\mathrm{R}_{\mathscr{A},\ell}(n) \ll \widehat{\mathrm{R}}_{\mathscr{A},\ell}(n) \left(\max_{k \leq n} \widehat{r}^*_{\mathscr{A},\ell-1}(k) \right) \cdots \left(\max_{k \leq n} \widehat{r}^*_{\mathscr{A},2}(k) \right),$$

where $\mathrm{R} = r,\ r^*,\ \rho,\ \rho^{(\delta\text{-small})}$.

Proof. Given that (4.8) applies to R, we keep applying the same bound to $r^*_{\mathscr{A},\ell-t}$ $(1 \leq t \leq \ell - 2)$, obtaining

$$\mathrm{R}_{\mathscr{A},\ell}(n) \ll \widehat{\mathrm{R}}_{\mathscr{A},\ell}(n) \left(\max_{k \leq n} \widehat{r}^*_{\mathscr{A},\ell-1}(k) \right) \cdots \left(\max_{k \leq n} \widehat{r}^*_{\mathscr{A},3}(k) \right) \left(\max_{k \leq n} r^*_{\mathscr{A},2}(k) \right).$$

Since $r^*_{\mathscr{A},2}(k) \leq 2\widehat{r}^*_{\mathscr{A},2}(k)$, the conclusion follows. □

Lemma 4.6 will be used together with the following lemma [**10**, Lemma 1]:

Lemma 4.7 (Disjointness lemma)**.** *Let $\mathscr{E} = \{E_1, E_2, \ldots\}$ be a family of events, and define $S := \sum_{E \in \mathscr{E}} \mathbf{1}_E$. If $\mathbb{E}(S) < \infty$, then for every $k \in \mathbb{Z}_{\geq 1}$ we have*

$$\Pr(\exists \mathcal{D} \subseteq \mathscr{E} \text{ disfam } |\mathcal{D}| = k) \leq \sum_{\substack{\mathcal{J} \subseteq \mathscr{E} \text{ disfam} \\ |\mathcal{J}| = k}} \Pr\left(\bigwedge_{E \in \mathcal{J}} E \right) \leq \frac{\mathbb{E}(S)^k}{k!}.$$

Proof.

$$\sum_{\substack{\mathcal{J} \subseteq \mathscr{E} \text{ disfam} \\ |\mathcal{J}| = k}} \Pr\left(\bigwedge_{E \in \mathcal{J}} E \right) = \sum_{\substack{\mathcal{J} \subseteq \mathscr{E} \text{ disfam} \\ |\mathcal{J}| = k}} \prod_{E \in \mathcal{J}} \Pr(E) \leq \frac{1}{k!} \left(\sum_{E \in \mathscr{E}} \Pr(E) \right)^k = \frac{\mathbb{E}(S)^k}{k!}. \qquad \square$$

Remark. If there exists a maxdisfam of size greater than k, then in particular there exists a disfam of size k. Thus, the form we will apply this lemma is as follows: Since $k! \geq k^k e^{-k}$,

$$\Pr(\exists \text{maxdisfam of size} \geq x) \leq \left(\frac{e\,\mathbb{E}}{\lceil x \rceil} \right)^{\lceil x \rceil} \qquad (\text{for real } x \geq 1)$$

$$\leq \left(\frac{e\,\mathbb{E}}{x} \right)^{x} \qquad (\text{for real } x \geq 1 + \mathbb{E}).$$

4.2. Asymptotic case

Recall that a real-valued function $F : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ is called *regularly varying* if it is measurable and $\lim_{x\to\infty} F(\lambda x)/F(x)$ exists for every $\lambda > 0$. Regularly varying functions are of the form $F(x) = x^\kappa \phi(x)$, where $\kappa \in \mathbb{R}$ and $\phi(x)$ is *slowly varying*, meaning $\lim_{x\to\infty} \phi(\lambda x)/\phi(x) = 1$ for every $\lambda > 0$.

For this section, fix $h \geq 2$, let $F(x) = x^\kappa \phi(x)$ for some slowly varying function ϕ and some real $0 \leq \kappa \leq h-1$, and define

$$f(x) := (xF(x))^{1/h} = x^{(1+\kappa)/h}\phi(x)^{1/h}. \tag{4.9}$$

We choose and fix a constant $c > 0$, and work with f satisfying

$$f(x) \gg (x \log x)^{1/h} \quad \text{and} \quad cf(x) \leq x.$$

4.2.1. Concentration of boolean polynomials

We will prove that $r_{\mathscr{A},h}$ strongly concentrates around its mean using the strategy of Vu [**39, 40**]. Precisely, let $n \in \mathbb{Z}_{\geq 1}$, and take $v_1, \ldots, v_n$ to be independent, not necessarily identically distributed, {0,1}-random variables. A *boolean polynomial* is a multivariate polynomial

$$Y(v_1, \ldots, v_n) = \sum_i c_i I_i \in \mathbb{R}[v_1, \ldots, v_n],$$

where the I_is are monomials: products of some of the v_ks. We say that f is

- *positive* if $c_i \in \mathbb{R}_{>0}$ for every i;
- *simple* if the largest exponent of v_i in a monomial is 1 for every i;
- *homogeneous* if every monomial has the same degree;
- *normal* if $0 \leq c_i \leq 1$ for every i, and the free coefficient of Y is 0.

For a non-empty multiset $S \subseteq \{v_1, \ldots, v_n\}$, define $\partial_S := \prod_{v\in S} \partial_v$, where ∂_v is the partial derivative in v. For example: if $S = \{1,1,2\}$, then $\partial_S(v_1^3 v_2 v_3 + 3v_1^5) = 6v_1v_3$. Define

$$\mathbb{E}_j(Y) := \max_{\substack{S\subseteq\{v_1,\ldots,v_n\}\\ \text{multiset}, |S|=j}} \mathbb{E}(\partial_S Y), \qquad \mathbb{E}'(Y) = \max_{j\geq 1} \mathbb{E}_j(Y).$$

We will need two concentration results:

Theorem 4.8 (Kim–Vu [**21**], 2000)**.** *Let $d \geq 1$, and $Y(v_1, \ldots, v_n)$ is a positive, simple boolean polynomial of degree d. Write $E' := \mathbb{E}'(Y)$ and $E := \max\{\mathbb{E}(Y), E'\}$. Then, for any real $\lambda \geq 1$, we have*

$$\Pr\left(|Y - \mathbb{E}(Y)| > 8^d\sqrt{d!}\,\lambda^d\,(E'E)^{1/2}\right) \ll_d n^{d-1}e^{-\lambda}$$

In applications, we will always take $\lambda = (d+1)\log n$, so Kim–Vu's inequality will be useful when $1 \ll \mathbb{E}' \ll \mathbb{E}/(\log n)^{2d}$. To deal with the cases with small expectation, we will use a corollary of another theorem of Vu [**40**, Theorem 1.4]:

Theorem 4.9 (Vu, 2000)**.** *Let $d \geq 2$, and $Y(v_1,\dots,v_n) = \sum_i c_i I_i$ be a simple, homogeneous, normal boolean polynomial of degree d. Then, for any $\alpha,\beta \in \mathbb{R}_{>0}$, there exists a constant $K = K(d,\alpha,\beta)$ such that: If $\mathbb{E}_1(Y)$, ..., $\mathbb{E}_{d-1}(Y) \leq n^{-\alpha}$, then for any real $0 < \lambda \leq \mathbb{E}(Y)$ we have*

$$\Pr(|Y - \mathbb{E}(Y)| \geq (\lambda \mathbb{E}(Y))^{1/2}) \leq 2d\, e^{-\lambda/16dK} + n^{-\beta}.$$

Remark. The random variable $r_{\mathscr{A},\ell}(n)$ can be seen as a boolean polynomial

$$r_{\mathscr{A},\ell}(n) = Y(v_1,\dots,v_n),$$

where the v_i's are independent $\{0,1\}$-random variables with $\Pr(v_i = 1) = \mathbb{E}(\mathbf{1}_{\mathscr{A}}(i))$. The expectations of derivatives of $r_{\mathscr{A},\ell}(n)$, thus, are bounded from above by

$$\mathbb{E}(r^*_{\mathscr{A},h-t}(n-k)), \qquad 1 \leq k \leq n.$$

for $1 \leq t \leq h$.

4.2.2. Expectation of $r_{\mathscr{A},h}(n)$

In the space (4.2) defined by f as in (4.9), we can get more precise estimates for $\mathbb{E}(r_{\mathscr{A},\ell}(n))$. Note that by the strong law of large numbers,

$$\begin{aligned}
|\mathscr{A} \cap [1,x]| \overset{\text{a.s.}}{\sim} c\int_1^x \frac{f(t)}{t}\,\mathrm{d}t &= c\int_1^x t^{\frac{1+\kappa}{h}-1}\phi(t)^{1/h}\,\mathrm{d}t \\
&= c\left(\int_{1/x}^1 u^{\frac{1+\kappa}{h}-1}\left(\frac{\phi(ux)}{\phi(x)}\right)^{1/h}\mathrm{d}u\right)x^{(1+\kappa)/h}\phi(x)^{1/h} \\
&\sim c\frac{h}{1+\kappa}x^{(1+\kappa)/h}\phi(x)^{1/h} = c\frac{h}{1+\kappa}f(x).
\end{aligned} \tag{4.10}$$

The last line is obtained as follows: by Potter bounds (cf. BGT [**2**, Theorem 1.5.6 (i)]), for every $\delta > 0$ there is $C = C_\delta$ such that, for large $x \geq x_\delta$ and $C/x \leq u \leq 1$, we have $\phi(ux)/\phi(x) \leq 2u^{-\delta}$. Choosing $\delta < \frac{1+\kappa}{2}$, we split the integral $\int_{1/x}^1 = \int_{1/x}^{C/x} + \int_{C/x}^1$. Since the definition of slowly varying implies that

$$u^{\frac{1+\kappa}{h}-1}\left(\frac{\phi(ux)}{\phi(x)}\right)^{1/h}\mathbf{1}_{(C/x,1]} \xrightarrow{x\to\infty} u^{\frac{1+\kappa}{h}-1}\mathbf{1}_{(0,1]},$$

the dominated convergence theorem yields that $\int_{C/x}^1 u^{\frac{1+\kappa}{h}-1}(\frac{\phi(ux)}{\phi(x)})^{1/h}\,\mathrm{d}u \to \int_0^1 u^{\frac{1+\kappa}{h}-1}$ as $x \to \infty$. On the other hand, since $\phi(x) = x^{o(1)}$, the term $\int_{1/x}^{C/x}$ vanishes.

We are going to show that:

Lemma 4.10. *We have*

$$\mathbb{E}(r_{\mathscr{A},h}(n)) \sim c^h \frac{\Gamma(\frac{1+\kappa}{h})^h}{\Gamma(1+\kappa)} \frac{F(n)}{(b_1 \cdots b_h)^{\frac{1+\kappa}{h}}}.$$

The proof also works for $F = \log$, a fact which will be used in Section 4.5 (in fact, we only use that $F(x) \to \infty$ as $x \to \infty$). We start with the following lemma:

Lemma 4.11. *Let $L \geq 1$ and $0 \leq r < L$ be integers. For any real numbers $\alpha \geq \beta > 0$ with $\beta \leq 1$, we have*

$$S(n) := \sum_{\substack{m=1 \\ m \equiv r \pmod{L}}}^{n-1} m^{\alpha-1}(n-m)^{\beta-1} = \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)} \cdot \frac{n^{\alpha+\beta-1}}{L} + O_{\alpha,\beta,L}(n^{\alpha-1}).$$

Proof. Define

$$\gamma_n(t) := (Lt+r)^{\alpha-1}(n-r-Lt)^{\beta-1}, \quad \text{for } t \in \left[0, \frac{n-r}{L}\right],$$

so that

$$S(n) = \sum_{k=0}^{K} \gamma_n(k), \quad \text{where } K := \left\lfloor \frac{n-r-1}{L} \right\rfloor.$$

The function $x \mapsto x^{\alpha-1}(n-x)^{\beta-1}$ has at most one critical point in $(0, n)$, since its logarithmic derivative

$$\frac{\mathrm{d}}{\mathrm{d}x} \log\left(x^{\alpha-1}(n-x)^{\beta-1}\right) = \frac{\alpha-1}{x} - \frac{\beta-1}{n-x}$$

changes sign at most once. Thus, $\gamma_n(t)$ is unimodal in $(0,K)$, and can be well approximated by the integral:

$$S(n) = \sum_{k=0}^{K} \gamma_n(k) = \int_0^K \gamma_n(t)\,\mathrm{d}t + O\left(\sup_{t\in[0,K]} \gamma_n(t)\right).$$

The maximum of $\gamma_n(t)$ is either attained at the critical point (which can be shown to be of the form $t^* \sim cn$ for some constant $c \in (0,1)$) or at the extremes of the $[0,K]$, and so can be bounded by $O_{\alpha,\beta,L}(n^{\alpha-1} + n^{\alpha+\beta-2}) = O_{\alpha,\beta,L}(n^{\alpha-1})$, since $\beta \leq 1$.

To compute the integral, we first change variables: let $x = Lt + r$, so that $t = \frac{x-r}{L}$ and $\mathrm{d}t = \frac{\mathrm{d}x}{L}$. Then

$$S(n) = \frac{1}{L} \int_r^{r+LK} x^{\alpha-1}(n-x)^{\beta-1}\,\mathrm{d}x + O_{\alpha,\beta,L}(n^{\alpha-1})$$

The integral $\int_r^{r+LK} \cdots$ differs from the full interval $[0, n]$ only near the endpoints, where the integral is bounded by

$$\left(\int_0^r + \int_{r+LK}^n\right) x^{\alpha-1}(n-x)^{\beta-1}\,\mathrm{d}x \ll n^{\alpha-1} \max\left\{\frac{L^\alpha}{\alpha}, \frac{L^\beta}{\beta}\right\}.$$

Therefore:

$$\begin{aligned}S(n) &= \frac{1}{L}\int_0^n x^{\alpha-1}(n-x)^{\beta-1}\,\mathrm{d}x + O_{\alpha,\beta,L}(n^{\alpha-1}) \\ &= \frac{n^{\alpha+\beta-1}}{L}\int_0^1 u^{\alpha-1}(1-u)^{\beta-1}\,\mathrm{d}u + O_{\alpha,\beta,L}(n^{\alpha-1}) \\ &= \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}\frac{n^{\alpha+\beta-1}}{L} + O_{\alpha,\beta,L}(n^{\alpha-1}),\end{aligned}$$

as claimed. □

Lemma 4.12. *For any real $1/h \le \omega \le 1$, we have*

$$\sum_{\substack{(k_1,\ldots,k_h)\in\mathbb{Z}_{\ge1}^h \\ b_1k_1+\cdots+b_hk_h=n}} (k_1\cdots k_h)^{\omega-1} = \frac{\Gamma(\omega)^h}{\Gamma(h\omega)}\frac{n^{h\omega-1}}{(b_1\cdots b_h)^{\omega}} + O(n^{(h-1)\omega-1})$$

Proof. We will show by induction that for $2 \le \ell \le h$, we have

$$\begin{aligned}S_\ell(n) &:= \sum_{\substack{(k_1,\ldots,k_\ell)\in\mathbb{Z}_{\ge1}^\ell \\ b_1k_1+\cdots+b_\ell k_\ell=n}} (k_1\cdots k_\ell)^{\omega-1} \\ &= \frac{\Gamma(\omega)^\ell}{\Gamma(\ell\omega)}\frac{\gcd(b_1,\ldots b_\ell)}{(b_1\cdots b_\ell)^{\omega}} n^{\ell\omega-1}\,\mathbf{1}_{\gcd(b_1,\ldots b_\ell)\mid n} + O(n^{(\ell-1)\omega-1}),\end{aligned} \tag{4.11}$$

For the case $\ell = 2$, we have

$$\begin{aligned}S_2(n) = \sum_{\substack{(k_1,k_2)\in\mathbb{Z}_{\ge1}^2 \\ b_1k_1+b_2k_2=n}} (k_1k_2)^{\omega-1} &= \sum_{\substack{k=1 \\ b_1k\equiv n \pmod{b_2}}}^{n/b_1-1} k^{\omega-1}\left(\frac{n-b_1k}{b_2}\right)^{\omega-1} \\ &= \frac{1}{(b_1b_2)^{\omega-1}} \sum_{\substack{m=1 \\ m\equiv 0 \pmod{b_1} \\ m\equiv n \pmod{b_2}}}^{n-1} m^{\omega-1}(n-m)^{\omega-1}\end{aligned}$$

The system of congruences $m \equiv 0 \pmod{b_1}$, $m \equiv n \pmod{b_2}$ has a solution $m \equiv r \pmod{\operatorname{lcm}(b_1,b_2)}$ if and only if $\gcd(b_1,b_2) \mid n$. Therefore, by Lemma 4.11,

$$S_2(n) = \frac{\Gamma(\omega)^2}{\Gamma(2\omega)}\frac{\gcd(b_1,b_2)}{(b_1b_2)^{\omega}} n^{2\omega-1}\,\mathbf{1}_{\gcd(b_1,b_2)\mid n} + O(n^{\omega-1}).$$

Assume by induction that (4.11) holds for some $\ell \ge 2$. Write $G = \gcd(b_1,\ldots,b_\ell)$. From Lemma 4.11, we get

$$S_{\ell+1}(n) = \sum_{\substack{(k_1,\ldots,k_\ell)\in\mathbb{Z}_{\ge1}^\ell \\ b_1k_1+\cdots+b_\ell k_\ell\le n \\ b_1k_1+\cdots+b_\ell k_\ell\equiv n \pmod{b_{\ell+1}}}} (k_1\cdots k_\ell)^{\omega-1}\left(\frac{n-(b_1k_1+\cdots+b_\ell k_\ell)}{b_{\ell+1}}\right)^{\omega-1}$$

$$= \sum_{\substack{m=1 \\ m\equiv n \pmod{b_{\ell+1}}}}^{n-1} S_\ell(m) \left(\frac{n-m}{b_{\ell+1}}\right)^{\omega-1}$$

$$= \frac{\Gamma(\omega)^\ell}{\Gamma(\ell\omega)} \frac{G}{(b_1\cdots b_\ell)^\omega b_{\ell+1}^{\omega-1}} \sum_{\substack{m=1 \\ m\equiv 0 \pmod{G} \\ m\equiv n \pmod{b_{\ell+1}}}}^{n-1} m^{\ell\omega-1}(n-m)^{\omega-1} + $$

$$+ O\left(\sum_{m=1}^{n-1} m^{(\ell-1)\omega-1}(n-m)^{\omega-1}\right)$$

$$= \frac{\Gamma(\omega)^{\ell+1}}{\Gamma((\ell+1)\omega)} \frac{Gb_{\ell+1}}{(b_1\cdots b_{\ell+1})^\omega} \frac{n^{(\ell+1)\omega-1}}{\operatorname{lcm}(G,b_{\ell+1})} \mathbf{1}_{\gcd(G,b_{\ell+1})|n} + O(n^{\ell\omega-1}).$$

Since $\frac{Gb_{\ell+1}}{\operatorname{lcm}(G,b_{\ell+1})} = \gcd(G,b_{\ell+1}) = \gcd(b_1,\dots,b_{\ell+1})$, this concludes the proof. □

Let ϕ be a slowly varying function. By uniform convergence (cf. BGT [**2**, Theorem 1.2.1]), given $0<\mu<1$, for every $\varepsilon>0$ there exists $x_{\mu,\varepsilon}\in\mathbb{R}$ such that, for every $x\geq x_{\mu,\varepsilon}$,

$$\left|\frac{\phi(\lambda x)}{\phi(x)} - 1\right| < \varepsilon, \qquad \forall\lambda\in[\mu,1].$$

Taking $\mu=1/j$, $j\in\mathbb{Z}_{\geq 1}$, for large x we define $\epsilon(x) := j$ for $x\in[x_{\frac{1}{j},\frac{1}{j}}, x_{\frac{1}{j+1},\frac{1}{j+1}})$. This defines a non-decreasing function $\epsilon(x)\to\infty$ such that

$$\frac{\phi(y)}{\phi(x)} \to 1 \text{ uniformly for } y\in\left[\frac{x}{\epsilon(x)}, x\right). \tag{4.12}$$

We are now ready to prove Lemma 4.10.

Proof of Lemma 4.10. By Lemma 4.4, non-exact solutions and solutions containing some $k_i=0$ do not contribute more than $O_c(\frac{f(n)^{h-1}}{n})$, therefore

$$\mathbb{E}(r_{\mathscr{A},h}(n)) = c^h \sum_{\substack{(k_1,\dots,k_h)\in\mathbb{Z}^h_{\geq 1} \\ b_1k_1+\cdots+b_hk_h=n}} \frac{f(k_1)}{k_1}\cdots\frac{f(k_h)}{k_h} + O_c\left(\frac{f(n)^{h-1}}{n}\right).$$

Let $\epsilon(x)$ be as in (4.12). Start by separating the sum into

$$S_1 := \sum_{\substack{(k_1,\dots,k_h)\in\mathbb{Z}^h_{\geq 1} \\ b_1k_1+\cdots+b_1k_h=n \\ \exists j\,|\,k_j<n/\epsilon(n)}} \frac{f(k_1)}{k_1}\cdots\frac{f(k_h)}{k_h}, \qquad S_2 := \sum_{\substack{(k_1,\dots,k_h)\in\mathbb{Z}^h_{\geq 1} \\ b_1k_1+\cdots+b_1k_h=n \\ \forall j,\, k_j\geq n/\epsilon(n)}} \frac{f(k_1)}{k_1}\cdots\frac{f(k_h)}{k_h}.$$

We start with S_1. We have $S_1\leq\sum_{\ell=1}^h S_{1,\ell}$, where

$$S_{1,j} := \sum_{\substack{(k_1,\dots,k_h)\in\mathbb{Z}^h_{\geq 1} \\ b_1k_1+\cdots+b_1k_h=n \\ k_j<n/\epsilon(n)}} \frac{f(k_1)}{k_1}\cdots\frac{f(k_h)}{k_h}.$$

Let $\mathcal{P}$ be the set of all h-tuples $\mathbf{p} = (P_1, \dots, P_h)$ with $P_1 \in \{1,2,4\dots, 2^L\}$, and $P_j \in \{1,2,4,\dots,2^J\}$ $(2 \le j \le h)$, where L (resp. J) is the smallest integer for which $2^L \ge n/\varepsilon(n)$ (resp. $2^J \ge n$), and write

$$\sigma_{\mathbf{p}} := \sum_{\substack{(k_1,\dots,k_h)\in\mathbb{Z}_{\ge 1}^h \\ b_1k_1+\cdots+b_1k_h=n \\ \frac{P_j}{2}\le k_j<P_j,\ \forall j}} \frac{f(k_1)}{k_1}\cdots\frac{f(k_h)}{k_h}.$$

We have $S_{1,1} \le \sum_{\mathbf{p}\in\mathcal{P}} \sigma_{\mathbf{p}}$. The number of terms in $\sigma_{\mathbf{p}}$ is $O(\frac{1}{n}P_1\cdots P_h)$ by Lemma 4.3. Moreover, since $f(x) = x^{\frac{1+\kappa}{h}}\phi(x)^{1/h}$ is regularly varying, we have $\sum_{j=0}^J f(2^j) \ll_\varepsilon f(n)\sum_{j=0}^J 2^{-j(\frac{1+\kappa}{h}-\varepsilon)} \ll f(n)$. Hence:

$$\begin{aligned} S_{1,1} \le \sum_{\mathbf{p}\in\mathcal{P}} \sigma_{\mathbf{p}} &\ll \sum_{\mathbf{p}\in\mathcal{P}} \frac{1}{n}(P_1\cdots P_h)\,\frac{f(P_1)}{P_1}\cdots\frac{f(P_h)}{P_h} \\ &= \frac{1}{n}\sum_{\mathbf{p}\in\mathcal{P}} f(P_1)\cdots f(P_h) \\ &\ll \frac{1}{n}\left(\sum_{j=0}^{L} f(2^j)\right)\left(\sum_{j=0}^{J} f(2^j)\right)^{h-1} \\ &\ll \frac{f(n/\epsilon(n))f(n)^{h-1}}{n} = o\left(\frac{f(n)^h}{n}\right). \end{aligned}$$

The terms $S_{1,\ell}$ can be bounded similarly, so it follows that $S_1 = o(f(n)^h/n)$.

For S_2, since $f(x) = x^{\frac{1+\kappa}{h}}\phi(x)^{1/h}$, by the definition of $\epsilon(x)$ we have

$$\begin{aligned} S_2 &= \phi(n) \sum_{\substack{(k_1,\dots,k_h)\in\mathbb{Z}_{\ge 1}^h \\ b_1k_1+\cdots+b_hk_h=n \\ k_j\ge n/\epsilon(n),\forall j}} (k_1\cdots k_h)^{\frac{1+\kappa}{h}-1}\frac{\phi(x_1)^{1/h}}{\phi(n)^{1/h}}\cdots\frac{\phi(x_h)^{1/h}}{\phi(n)^{1/h}} \\ &\sim \phi(n) \sum_{\substack{(k_1,\dots,k_h)\in\mathbb{Z}_{\ge 1}^h \\ b_1k_1+\cdots+b_hk_h=n \\ k_j\ge n/\epsilon(n),\forall j}} (k_1\cdots k_h)^{\frac{1+\kappa}{h}-1} \end{aligned} \tag{4.13}$$

Using the same methods used to calculate S_1, one can show that

$$S_3 := \phi(n) \sum_{\substack{(k_1,\dots,k_h)\in\mathbb{Z}_{\ge 1}^h \\ b_1k_1+\cdots+b_hk_h=n \\ \exists j\,|\,k_j<n/\epsilon(n)}} (k_1\cdots k_h)^{\frac{1+\kappa}{h}-1} = o\left(\frac{f(n)^h}{n}\right).$$

Thus, since $1/h \le \frac{1+\kappa}{h} \le 1$, we may apply Lemma 4.12, so (4.13) implies that

$$S_2 \sim \frac{\Gamma(\frac{1+\kappa}{h})^h}{\Gamma(1+\kappa)}\frac{n^\kappa\phi(n)}{(b_1\cdots b_h)^{\frac{1+\kappa}{h}}}$$

concluding the proof. $\square$

Remark 4.13 (Case $\phi \equiv 1$)**.** In this case, $F(x) = x^{\kappa}$ for some $\kappa > 0$. We have $\mathbb{E}(|\mathscr{A} \cap [1,x]|) = c\int_1^x t^{\frac{1+\kappa}{h}-1}\,\mathrm{d}t + O_c(1) = c\frac{h}{1+\kappa}x^{(1+\kappa)/h} + O_c(1)$, and $|\mathscr{A} \cap [1,n]|$ is a boolean polynomial of degree 1. For $d = 1$, applying Theorem 4.8 taking $\lambda = 2\log n$ then yields

$$\Pr\Big(\Big||\mathscr{A} \cap [1,n]| - \mathbb{E}(|\mathscr{A} \cap [1,n]|)\Big| \geq 16\log n\, \mathbb{E}(|\mathscr{A} \cap [1,n]|)^{1/2}\Big) \ll n^{-2}.$$

By the Borel–Cantelli lemma, $|\mathscr{A} \cap [1,x]| \overset{\text{a.s.}}{=} c\frac{h}{1+\kappa}x^{(1+\kappa)/h} + O(x^{(1+\kappa)/2h}\log x)$.

Furthermore, redoing the calculations at the beginning of Lemma 4.10, using Lemma 4.12 we obtain

$$\mathbb{E}(r_{\mathscr{A},h}(n)) = c^h \frac{\Gamma(\frac{1+\kappa}{h})^h}{\Gamma(1+\kappa)} \frac{n^{\kappa}}{(b_1 \cdots b_h)^{\frac{1+\kappa}{h}}} + O_c\Big(n^{\frac{(h-1)(1+\kappa)}{h}-1}\Big).$$

4.2.3. Proof of Theorem 1.8

Theorem 1.8 *Let $h \geq 2$ be a given integer. Let F be a regularly varying function for which*

$$\frac{F(x)}{\log x} \xrightarrow{x\to\infty} \infty \quad \textit{and} \quad F(x) \leq (1+o(1))\frac{1}{(h-1)!}\frac{x^{h-1}}{b_1\cdots b_h}.$$

Then, there exists $A \subseteq \mathbb{Z}_{\geq 0}$ such that $r_{A,h}(n) \sim F(n)$.

Proof. From (4.5) and Lemma 4.4, we have $\mathbb{E}(r_{\mathscr{A},h}(n)) = \mathbb{E}(\rho_{\mathscr{A},h}(n)) + O_c(\frac{f(n)^{h-1}}{n})$, so $\mathbb{E}(r^*_{\mathscr{A},\ell}(k)) \ll k^{\frac{\ell(1+\kappa)}{h}-1+o(1)}$ $(1 \leq \ell \leq h-1)$ where r^* is as in (4.6), and by Lemma 4.10, $\mathbb{E}(\rho_{\mathscr{A},h}(n)) \sim c^h d_{h,\kappa} F(n)$ for a certain $d_{h,\kappa}$. So choose $c := d_{h,\kappa}^{-1/h}$. Recall that

$$\mathbb{E}_j(Y) = \max_{\substack{S\subseteq\{v_1,\dots,v_n\}\\ \text{multiset}, |S|=j}} \mathbb{E}(\partial_S Y), \qquad \mathbb{E}'(Y) = \max_{j\geq 1} \mathbb{E}_j(Y).$$

• <u>Case $\kappa > 0$</u>: We have

$$\mathbb{E}'(r_{\mathscr{A},h}(n)) \leq 1 + \max_{1\leq \ell\leq h-1}\max_{k\leq n} \mathbb{E}(r^*_{\mathscr{A},\ell}(k)) \ll n^{\max\{0,\frac{(h-1)\kappa}{h}-1\}+o(1)},$$

therefore $E = \mathbb{E}(r_{\mathscr{A},h}(n))$ and $E' = \mathbb{E}'(r_{\mathscr{A},h}(n))$ for large n. Taking $\lambda = (h+1)\log n$ in Theorem 4.8, we have[2]

$$\lambda^h\left(\frac{E'}{E}\right)^{1/2} \leq (h+1)^h(\log n)^h\left(\frac{1+\max_{1\leq\ell\leq h-1}\max_{k\leq n}\mathbb{E}(r^*_{\mathscr{A},\ell}(k))}{\mathbb{E}(\rho_{\mathscr{A},h}(n))}\right)^{1/2}$$

$$\ll \left(\frac{n^{\max\{0,\frac{(h-1)\kappa}{h}-1\}+o(1)}}{n^{\kappa+o(1)}}\right)^{1/2} = n^{-\frac{\kappa}{2}+\max\{0,\frac{(h-1)\kappa}{2h}-\frac{1}{2}\}+o(1)} \qquad (= o(1)).$$

[2]The $o(1)$ term in the exponent of the error term comes from the fact that, unless we assume ϕ increasing, the best general estimate for $\max_{k\leq n}\phi(k)$ is $n^{o(1)}$.

Thus,

$$\Pr\left(\left|\rho_{\mathscr{A},h}(n)-\mathbb{E}(\rho_{\mathscr{A},h}(n))\right| \geq \frac{8^h\sqrt{h!}}{n^{\frac{\kappa}{2}-\max\{0,\frac{(h-1)\kappa}{2h}-\frac{1}{2}\}+o(1)}}\,\mathbb{E}(\rho_{\mathscr{A},h}(n))\right) \ll n^{-2} \tag{4.14}$$

which by the Borel–Cantelli lemma implies that $\rho_{\mathscr{A},h}(n) \overset{\text{a.s.}}{\sim} \mathbb{E}(\rho_{\mathscr{A},h}(n))$.

To bound the non-exact solutions, note that by (4.5), $r_{\mathscr{A},h}(n) - \rho_{\mathscr{A},h}(n)$ equals the number of exact solutions to a finite number of linear equations of smaller length, with coefficients bounded by $\max_i b_i$. So it suffices to show that $\rho_{\mathscr{A},t}(n) = \rho_{\mathscr{A},t}^{(c_1,\dots,c_t)}(n) \overset{\text{a.s.}}{=} O(n^{\max\{0,(1-\frac{1}{h})\kappa-1\}+o(1)})$ for every equation $c_1x_1+\cdots+c_tx_t$ produced by non-exact solutions to $b_1x_1+\cdots+b_hx_h$, as in (4.5). Since $t \leq h-1$, for $\rho_{\mathscr{A},t}$ we have, in the notation of Lemma 4.8,

$$E' \ll n^{\max\{0,\frac{(h-2)\kappa}{h}-1\}+o(1)}, \quad E = \max\{E', n^{(1-\frac{1}{h})\kappa-1+o(1)}\},$$

so it follows that

$$\Pr\left(|\rho_{\mathscr{A},t}(n)-\mathbb{E}(\rho_{\mathscr{A},t}(n))| \geq 8^h\sqrt{h!}\,(\log n)^h\, n^{\max\{0,(1-\frac{1}{h})\kappa-1\}+o(1)}\right) \ll n^{-2},$$

which by the Borel–Cantelli lemma implies that $\rho_{\mathscr{A},t}(n) \overset{\text{a.s.}}{\ll} n^{\max\{0,(1-\frac{1}{h})\kappa-1\}+o(1)}$.

• <u>Case $\kappa = 0$</u>: For $\kappa = 0$, we apply Theorem 4.9 to $\rho_{\mathscr{A},h}^{(\delta\text{-normal})}(n)$ — after this, it will suffice to show that $\rho_{\mathscr{A},h}^{(\delta\text{-small})}(n)$ and $r_{\mathscr{A},h}(n)-\rho_{\mathscr{A},h}(n)$ are almost surely $O(1)$. The function $\rho_{\mathscr{A},h}^{(\delta\text{-normal})}(n)$ is a homogeneous, simple boolean polynomial of degree h, with partial derivatives bounded by, for $1 \leq j \leq h-1$,

$$\mathbb{E}_j(\rho_{\mathscr{A},h}^{(\delta\text{-normal})}(n)) \leq \max_{n^\delta \leq k \leq n} \mathbb{E}(r^*_{\mathscr{A},h-j}(k)) \ll_c \max_{n^\delta \leq k \leq n} \frac{f(k)^{h-j}}{k} \ll n^{-\delta\frac{j}{h}+o(1)}$$

by Lemma 4.4. Each monomial of $\rho_{\mathscr{A},h}(n)$ appears at most $h!$ times, so $\frac{1}{h!}\rho_{\mathscr{A},h}^{(\delta\text{-normal})}(n)$ is a normal polynomial. Thus, taking $0 < \alpha < \frac{\delta}{h}$, $\beta = 2$, $K = K(\alpha,\beta,h)$ in Theorem 4.9, since $\mathbb{E}(\rho_{\mathscr{A},h}^{(\delta\text{-normal})}(n))/\log n \to \infty$ as $x \to \infty$ (by Lemmas 4.4, 4.5 and our assumptions), we have

$$\Pr\left(|\rho_{\mathscr{A},h}^{(\delta\text{-normal})}(n)-\mathbb{E}(\rho_{\mathscr{A},h}^{(\delta\text{-normal})}(n))| \geq (h!\lambda\,\mathbb{E}(\rho_{\mathscr{A},h}^{(\delta\text{-normal})}(n)))^{1/2}\right) \ll n^{-2}$$

by taking $\lambda = 32hK\log n$. Since $(\lambda\mathbb{E}(\rho_{\mathscr{A},h}^{(\delta\text{-normal})}(n)))^{1/2} = o(\mathbb{E}(\rho_{\mathscr{A},h}^{(\delta\text{-normal})}(n)))$, the Borel–Cantelli lemma implies that $\rho_{\mathscr{A},h}^{(\delta\text{-normal})}(n) \overset{\text{a.s.}}{\sim} \mathbb{E}(\rho_{\mathscr{A},h}^{(\delta\text{-normal})}(n))$.

To bound $\rho_{\mathscr{A},h}^{(\delta\text{-small})}(n)$, we use Lemma 4.6. By Lemma 4.4, we have $\mathbb{E}(r^*_{\mathscr{A},\ell}(n)) \ll n^{-\frac{1}{h}+o(1)}$ for $1 \leq \ell \leq h-1$, and by Lemma 4.5 we have $\mathbb{E}(\rho_{\mathscr{A},h}^{(\delta\text{-small})}(n)) \ll n^{-\frac{1-\delta}{2h}+o(1)}$ (since we can take $\vartheta = \frac{1}{2h}$ in Lemma 4.1 (ii)). By the disjointness lemma 4.7,

$$\Pr(\widehat{r}^*_{\mathscr{A},\ell}(n) \geq T) \leq \left(\frac{e}{T}\right)^T n^{-T/h+o(1)} \ll n^{-3}$$

for large $T \in \mathbb{R}_{>0}$ — and similarly for $\widehat{\rho}^{(\delta\text{-small})}_{\mathscr{A},h}(n)$. Therefore, $\widehat{r}^{*}_{\mathscr{A},\ell}(n) \overset{\text{a.s.}}{\ll} 1$ for $1 \le \ell \le h-1$ and $\widehat{\rho}^{(\delta\text{-small})}_{\mathscr{A},h}(n) \overset{\text{a.s.}}{\ll} 1$ by the Borel–Cantelli lemma. For each $2 \le \ell \le h-1$ it follows from the union bound that

$$\sum_{k \le n} \Pr(\widehat{r}^{*}_{\mathscr{A},\ell}(n) \ge T) \ll n^{-2},$$

so again by Borel–Cantelli we have $\max_{k \le n} \widehat{r}^{*}_{\mathscr{A},\ell}(k) \overset{\text{a.s.}}{\ll} 1$. Plugging this into Lemma 4.6 yields $\rho^{(\delta\text{-small})}_{\mathscr{A},h}(n) \overset{\text{a.s.}}{\ll} \widehat{\rho}^{(\delta\text{-small})}_{\mathscr{A},h}(n) \overset{\text{a.s.}}{\ll} 1$, as desired.

To bound $r_{\mathscr{A},h}(n) - \rho_{\mathscr{A},h}(n)$, by (4.5) it suffices to bound $\rho_{\mathscr{A},t}(n) := \rho^{(c_1,\ldots,c_t)}_{\mathscr{A},t}(n)$ for $t \le h-1$. If $t = 2$ then $\rho_{\mathscr{A},t}(n) \le 1$ trivially. For $t \ge 2$, we apply Lemma 4.6 again, obtaining $\rho_{\mathscr{A},t}(n) \overset{\text{a.s.}}{\ll} \widehat{\rho}_{\mathscr{A},t}(n) \overset{\text{a.s.}}{\ll} 1$, concluding the proof. □

4.2.4. Proof of Corollary 1.9

Corollary 1.9 *Let $h \ge 2$ be a given integer, and $0 < \kappa \le h-1$ a real number. Then, for any $C \in \mathbb{R}_{>0}$, there exists $A \subseteq \mathbb{Z}_{\ge 0}$ such that $|A \cap [1,x]| = Cx^{(1+\kappa)/h} + O(x^{(1+\kappa)/2h} \log x)$ and*

$$r_{A,h}(n) = C^h \frac{(1+\kappa)^h}{h^h} \frac{\Gamma(\frac{1+\kappa}{h})^h}{\Gamma(1+\kappa)} \frac{n^\kappa}{(b_1 \cdots b_h)^{\frac{1+\kappa}{h}}} + O(E_{h,\kappa}),$$

where $E_{2,\kappa} := n^{\frac{\kappa}{2}}(\log n)^2$, $E_{3,\kappa} := n^{\frac{\kappa}{2} + \max\{0, \frac{\kappa}{3} - \frac{1}{2}\}}(\log n)^3$, and for $h \ge 4$,

$$E_{h,\kappa} := \begin{cases} n^{\frac{\kappa}{2}}(\log n)^h & \text{if } 0 \le \kappa \le \frac{2}{h-2}, \\ n^{(1-\frac{1}{h})\kappa - \frac{1}{h}} & \text{if } \frac{2}{h-2} < \kappa < h-2, \\ n^{(1-\frac{1}{2h})\kappa - \frac{1}{2}}(\log n)^h & \text{if } h-2 \le \kappa \le h-1. \end{cases}$$

Proof. With Remark 4.13, we can redo the calculation in the case $\kappa > 0$ of the proof of Theorem 1.8, obtaining $\lambda^h \left(\frac{E'}{E}\right)^{1/2} \ll (\log n)^h n^{-\frac{(1+\kappa)}{2h}}$. The equivalent to inequality (4.14) together with the Borel–Cantelli lemma provides the almost sure estimate

$$\rho_{\mathscr{A},h}(n) \overset{\text{a.s.}}{=} \mathbb{E}(\rho_{\mathscr{A},h}(n)) + O\Big(n^{\frac{\kappa}{2} + \max\{0, \frac{(h-1)\kappa}{2h} - \frac{1}{2}\}}(\log n)^h\Big).$$

Since $\rho^{(c_1,\ldots,c_t)}_{\mathscr{A},t}(n) \overset{\text{a.s.}}{\ll} n^{\max\{0,(1-\frac{1}{h})\kappa - 1\} + o(1)}$ for $t \le h-1$, as shown in the proof of Theorem 1.8, it follows from (4.5) and

$$\frac{\kappa}{2} + \max\left\{0, \frac{(h-1)\kappa}{2h} - \frac{1}{2}\right\} > \max\left\{0, \left(1 - \frac{1}{h}\right)\kappa - 1\right\}$$

that

$$r_{\mathscr{A},h}(n) \overset{\text{a.s.}}{=} \mathbb{E}(r_{\mathscr{A},h}(n)) + O\Big(n^{\frac{\kappa}{2} + \max\{0, \frac{(h-1)\kappa}{2h} - \frac{1}{2}\}}(\log n)^h\Big).$$

The result then follows from Remark 4.13, by simplifying the expression

$$O\Big(n^{\frac{(h-1)(1+\kappa)}{h}-1}\Big)+O\Big(n^{\frac{\kappa}{2}+\max\{0,\frac{(h-1)\kappa}{2h}-\frac{1}{2}\}}(\log n)^h\Big)$$

depending on κ and h. □

4.3. Order of magnitude case: Theorem 1.10

Since the case $h=2$ of Theorem 1.11 contains the cases $h=2$ and (4.15) of Theorem 1.10, assume $h\geq 3$. In this section, we will prove the following:

Theorem 1.10 *Let $h\geq 2$ be a fixed integer, and let F be a positive, increasing, locally integrable real function satisfying $F(2x)\ll F(x)$. Suppose further that either*

$$\log x \ll F(x) \ll x^{\frac{1}{h-1}} \tag{4.15}$$

or

$$(\log x)^{2h^2} \ll F(x) \ll x^{h-1} \tag{4.16}$$

Then, there exists $A\subseteq \mathbb{Z}_{\geq 0}$ such that $|A\cap[1,x]|\asymp (xF(x))^{1/h}$ and $r_{A,h}(n)\asymp F(n)$.

Let F be a locally integrable increasing function that satisfies $F(2x)\ll F(x)$ and lies in the range

$$(\log x)^{2h^2} \ll F(x) \ll x^{h-1}.$$

Take $f(x):=(xF(x))^{1/h}$. Note that f satisfies the conditions of Lemma 4.1, for $\vartheta=1/h$. Since $F(x)^{1/h}=f(x)/x^{1/h}$ is increasing, for $1\leq k\leq n$ and $1\leq \ell\leq h-1$ we have

$$f(k)^{h-\ell}\leq k^{1-\ell/h}\left(\frac{f(n)}{n^{1/h}}\right)^{h-\ell}.$$

Hence, by Lemma 4.4,

$$\begin{aligned}\mathbb{E}(r^*_{\mathscr{A},h-\ell}(k)) \ll_c \frac{f(k)^{h-\ell}}{k} &\leq \frac{1}{k^{\frac{\ell}{h}}}\left(\frac{f(n)}{n^{1/h}}\right)^{h-\ell}\\ &= \frac{1}{k^{\frac{\ell}{h}}}\frac{1}{(\frac{f(n)}{n^{1/h}})^{\ell}}\frac{f(n)^h}{n}.\end{aligned} \tag{4.17}$$

Proof of case* (4.16) *of Theorem 1.10. Taking $\lambda=(h+1)\log n$ in Theorem 4.8, by Lemma 4.4 and (4.17) we have

$$\begin{aligned}\lambda^h\left(\frac{E'}{E}\right)^{1/2} &\ll (\log n)^h\left(\frac{1+\max\limits_{1\leq\ell\leq h-1}\max\limits_{k\leq n}\mathbb{E}(r^*_{\mathscr{A},\ell}(k))}{\mathbb{E}(\rho_{\mathscr{A},h}(n))}\right)^{1/2}\\ &\ll_c (\log n)^h\left(\frac{\frac{1}{(\log n)^{2h}}\frac{f(n)^h}{n}}{f(n)^h/n}\right)^{1/2}\\ &\ll 1,\end{aligned}$$

so

$$\Pr\left(|\rho_{\mathscr{A},h}(n)-\mathbb{E}(\rho_{\mathscr{A},h}(n))|\geq C\,\mathbb{E}(\rho_{\mathscr{A},h}(n))\right)\ll n^{-2}$$

for some $C=C_c$. By Lemma 4.4 and the Borel–Cantelli lemma, $\rho_{\mathscr{A},h}(n)\overset{\text{a.s.}}{\asymp}F(n)$.

As in the proof of Theorem 1.8, by (4.5), $r_{\mathscr{A},h}(n)-\rho_{\mathscr{A},h}(n)$ equals the number of exact solutions to a finite number of equations of smaller length. Thus, in order to show that $r_{\mathscr{A},h}(n)\overset{\text{a.s.}}{\asymp}F(n)$, it suffices to show that $\rho_{\mathscr{A},t}(n)\overset{\text{a.s.}}{\ll}F(n)$ for $t\leq h-1$. By Lemma 4.4 and (4.17), since $t\leq h-1$ we have

$$\mathbb{E}(\rho_{\mathscr{A},t}(n))\ll_c\frac{1}{(\log n)^{2h}}\frac{f(n)^h}{n},\quad \max_{1\leq\ell\leq t}\max_{k\leq n}\mathbb{E}(r^*_{\mathscr{A},\ell}(k))\ll_c\frac{1}{(\log n)^{2h}}\frac{f(n)^h}{n},$$

so again by Theorem 4.8, for $\lambda=(h+1)\log n$

$$\Pr\left(|\rho_{\mathscr{A},t}(n)-\mathbb{E}(\rho_{\mathscr{A},t}(n))|\geq D\,\frac{1}{(\log n)^h}\frac{f(n)^h}{n}\right)\ll n^{-2}$$

for some $D=D_c$, which by the Borel–Cantelli lemma concludes the proof. □

4.4. Order of magnitude case: Theorem 1.11

The case $h=2$ was already considered in Subsection 4.1.2, so suppose $h\geq 3$. We will prove the following:

Theorem 1.11 (Case $h\geq 3$) *Let $h\geq 3$ be a given integer, and let $\psi(x)\gg\log x$ be an increasing slowly varying function. If*

(i) (Range) $(x\,\psi(x))^{1/h}\ll f(x)\ll(x\,\psi(x))^{1/(h-1)}$,

(ii) (Regularity) $\int_1^x\frac{f(t)}{t}\,\mathrm{d}t\asymp f(x)$;

then there exists $A\subseteq\mathbb{Z}_{\geq 0}$ such that $|A\cap[1,x]|\asymp f(x)$ and $r_{A,h}(n)\asymp\frac{f(n)^h}{n}$.

Let f be a positive locally integrable real function satisfying $\int_1^x\frac{f(t)}{t}\,\mathrm{d}t\asymp f(x)$ in the range

$$(n\,\psi(n))^{1/h}\ll f(n)\ll(n\,\psi(n))^{1/(h-1)},\tag{4.18}$$

where $\psi(x)\gg\log x$ is some increasing slowly varying function, and choose some

$$1-\frac{1}{4h(1-(h-1)\min\{\vartheta_f,\frac{1}{h}\})}<\delta<1,\tag{4.19}$$

where ϑ_f is as in Lemma 4.1 (ii).

Lemma 4.14. *For $\delta>0$ as in (4.19), and for $c>1$ sufficiently large, we have*

$$\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)\overset{\text{a.s.}}{\asymp}\frac{f(n)^h}{n}.$$

Proof. Partition $\mathbb{N} = \mathbb{Z}_{\geq 0}$ this time into

$$\mathbb{N}^{(1)} := \left\{ n \in \mathbb{N} \;\middle|\; \log n \leq \mathbb{E}(\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)) \leq n^{1/2h} \right\},$$
$$\mathbb{N}^{(2)} := \left\{ n \in \mathbb{N} \;\middle|\; \mathbb{E}(\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)) > n^{1/2h} \right\}.$$

Note that these partitions depend on c. By Lemmas 4.4, 4.5, we have

$$\frac{\min\{cf(n),n\}^h}{n} \ll \mathbb{E}(\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)) \ll c^h \frac{f(n)^h}{n}.$$

We can bound the derivatives of $\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)$ by

$$\begin{aligned}\mathbb{E}(r^{*(\delta\text{-normal})}_{\mathscr{A},\ell}(k)) \ll_c \max_{n^\delta \leq k \leq n} \frac{f(k)^{h-1}}{k} &\ll n^{(1-\delta)(1-(h-1)\vartheta)} \frac{f(n)^{h-1}}{n} \\ &< n^{-1/4h} \frac{f(n)^{h-1}}{n} \end{aligned} \tag{4.20}$$

for $1 \leq \ell \leq h-1$, where $\vartheta = \vartheta_f$ is as in Lemma 4.5. We study the partitions $\mathbb{N}^{(1)}$ and $\mathbb{N}^{(2)}$ separately.

• $\underline{\mathbb{N}^{(1)}}$: For $n \in \mathbb{N}^{(1)}$, by (4.20) we have

$$\begin{aligned}\max_{n^\delta \leq k \leq n} \mathbb{E}(r^{*(\delta\text{-normal})}_{\mathscr{A},h-1}(k)) &< n^{(1-\delta)(1-(h-1)\vartheta)-1/2h+o(1)} \\ &< n^{-1/4h+o(1)} \quad \text{for} \quad k \in [n^\delta,n],\ n \in \mathbb{N}^{(1)}.\end{aligned}$$

Since the expected values of the derivatives of $\frac{1}{h!}\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)$ are all bounded from above by $O_c(n^{-\alpha})$ in $\mathbb{N}^{(1)}$ for some $\alpha > 0$, we apply Theorem 4.9 choosing $\beta = 2$. In the notation of Theorem 4.9, for $c > 1$ large enough we can guarantee that $\mathbb{E}(\frac{1}{h!}\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)) \gg \min\{cf(n),n\}^h/n \geq 32hK\log n$, therefore

$$\Pr\left(|\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n) - \mathbb{E}(\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n))| \geq (h!\lambda\,\mathbb{E}(\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)))^{1/2}\right) \ll n^{-2}$$

taking $\lambda = 32hK\log n$. By the Borel–Cantelli lemma, $\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n) \overset{\text{a.s.}}{\asymp} \frac{f(n)^h}{n}$ in $\mathbb{N}^{(1)}$.

• $\underline{\mathbb{N}^{(2)}}$: Taking $\lambda = (h+1)\log n$ in Theorem 4.8, by Lemma 4.4 and (4.20) we have

$$(\log n)^h \left(\frac{1 + \max_{1\leq \ell \leq h-1} \max_{n^\delta \leq k \leq n} \mathbb{E}(r^*_{\mathscr{A},\ell}(k))}{\mathbb{E}(\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n))} \right)^{1/2} \ll_c n^{-\alpha} \qquad \text{for } n \in \mathbb{N}^{(2)}$$

for some $\alpha > 0$. Thus,

$$\Pr\left(\left|\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n) - \mathbb{E}(\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n))\right| \geq Dn^{-\alpha}\mathbb{E}(\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n))\right) \leq n^{-2}$$

for some $D = D_c$, which by the Borel–Cantelli lemma implies the lemma. □

Proof of Theorem 1.11. It remains to bound $\rho^{(\delta\text{-small})}_{\mathscr{A},h}(n)$ and, by (4.5), $\rho_{\mathscr{A},t}(n)$ for $t \le h-1$. By the range of f and Lemma 4.4, we have $\mathbb{E}(r^*_{\mathscr{A},\ell}(k)) \ll_c k^{-\alpha}$ for some $\alpha > 0$ for all $1 \le \ell \le h-2$, and $\mathbb{E}(r^*_{\mathscr{A},h-1}(k)) \ll_c \psi(k)$. By the disjointness lemma 4.7, we have

$$\Pr(\widehat{r}^*_{\mathscr{A},\ell}(k) \ge T) \le \left(\frac{e}{T}\right)^T k^{-\alpha T} \le k^{-2} \qquad (1 \le \ell \le h-2),$$

and

$$\Pr\left(\widehat{r}^*_{\mathscr{A},h-1}(k) \ge T\psi(k)\right) \le \left(\frac{e}{T}\right)^{-T\psi(k)} \ll k^{-2},$$

both for large real $T = T_c > 0$. By Lemma 4.5, choosing T large enough yields

$$\begin{aligned}\Pr\left(\widehat{\rho}^{(\delta\text{-small})}_{\mathscr{A},h}(n) \ge c^{h-1}\frac{T}{\psi(n)}\frac{f(n)^h}{n}\right) &\le \left(\frac{e\,\mathbb{E}(r^{(\delta\text{-small})}_{\mathscr{A},h}(n))}{c^{h-1}\frac{T}{\psi(n)}\frac{f(n)^h}{n}}\right)^{c^{h-1}\frac{T}{\psi(n)}\frac{f(n)^h}{n}} \\ &\le (n^{-(1-\delta)\vartheta+o(1)})^{c^{h-1}\frac{T}{\psi(n)}\frac{f(n)^h}{n}} \\ &\le n^{-2+o(1)}.\end{aligned}$$

Thus, by the Borel–Cantelli lemma, we have for $k \le n$:

$$\widehat{r}^*_{\mathscr{A},\ell}(k) \overset{\text{a.s.}}{\ll} 1 \quad (1 \le \ell \le h-2), \qquad \widehat{r}^*_{\mathscr{A},h-1}(k) \overset{\text{a.s.}}{\ll} \psi(k) \le \psi(n),$$
$$\widehat{\rho}^{(\delta\text{-small})}_{\mathscr{A},h}(n) \overset{\text{a.s.}}{\ll} \frac{1}{\psi(n)}\frac{f(n)^h}{n}.$$

By Lemma 4.6, it follows that $\rho^{(\delta\text{-small})}_{\mathscr{A},h}(n) \overset{\text{a.s.}}{\ll} \frac{f(n)^h}{n}$ and $\rho_{\mathscr{A},t}(n) \overset{\text{a.s.}}{\ll} \psi(n)$. □

4.5. What if $F(x) \ll \log x$?

In this section, we will prove the following:

Theorem 1.12 *Fix $0 < \varepsilon < \frac{1}{2}$. Define the random set $\mathscr{A} \subseteq \mathbb{Z}_{\ge 0}$ by taking $0 \in \mathscr{A}$ and*

$$\Pr(n \in \mathscr{A}) = \min\left\{c\frac{(n\log(n))^{1/h}}{n}, 1\right\} \qquad (n \ge 1),$$

for $c = (1-\varepsilon)^{1/h}(b_1 \cdots b_h)^{1/h^2}/\Gamma(\frac{1}{h})$. Then $\mathbb{E}(r_{\mathscr{A},h}(n)) \sim (1-\varepsilon)\log n$ as $n \to \infty$, but

$$\Pr(r_{\mathscr{A},h}(n) = 0 \text{ infinitely often}) = 1.$$

Let $0 < \varepsilon < 1$, and define

$$\Pr(n \in \mathscr{A}) := \min\left\{c\frac{f(n)}{n}, 1\right\}$$

for each $n \in \mathbb{Z}_{\geq 1}$, where $f(x) = (x\log(x))^{1/h}$ and

$$c := (1-\varepsilon)^{1/h}\frac{(b_1\cdots b_h)^{1/h^2}}{\Gamma(1/h)},$$

so that, by (4.10), $|\mathscr{A}\cap[1,x]| \sim hc(x\log x)^{1/h}$. By Lemma 4.10, we have

$$\mathbb{E}(r_{\mathscr{A},h}(n)) \sim c^h\Gamma(1/h)^h\frac{\log n}{(b_1\cdots b_h)^{1/h}} \leq (1-\tfrac{\varepsilon}{2})\log n \tag{4.21}$$

for large n. To show that $\{r_{\mathscr{A},h}(n) = 0\}$ has high probability, the following inequality will be used:

Lemma 4.15 (Correlation inequality)**.** *Let Ω be a finite set, and $\mathcal{R}$ be a random subset where the events $\{\omega_1 \in \mathcal{R}\}$, $\{\omega_2 \in \mathcal{R}\}$ are independent for every $\omega_1 \neq \omega_2 \in \Omega$. Let $S_1, \ldots, S_n \subseteq \Omega$ be distinct subsets, and suppose that the events $E_i = \{S_i \subseteq \mathcal{R}\}$ satisfy* $\Pr(E_i) \leq 1/2$. *Then:*

$$\prod_{i=1}^{n}\Pr(\overline{E}_i) \leq \Pr\left(\bigwedge_{i=1}^{n}\overline{E}_i\right) \leq \left(\prod_{i=1}^{n}\Pr(\overline{E}_i)\right)e^{2\Delta},$$

where

$$\Delta = \sum_{\substack{1\leq i<j\leq n\\ E_i\cap E_j\neq\varnothing}}\Pr(E_i\wedge E_j)$$

and $\overline{E}_i$ is the complement of E_i.

Proof. Boppana–Spencer [**3**]. □

Lemma 4.16. $\sum_{n\geq 1}\Pr(r_{\mathscr{A},h}(n) = 0) = \infty.$

Proof. Let

$$\mathcal{S}[n] = \Big\{(x_1,\ldots,k_h) \in \mathbb{Z}_{\geq 0}^h \mid b_1x_1 + \cdots + b_hk_h = n\Big\}. \tag{4.22}$$

Since for every solution $R = (x_1,\ldots,k_h)$ in $\mathcal{S}[n]$ there is some j for which $k_j \geq n/h(\max_i b_i)$, for large n we have $\Pr(R) \leq \varepsilon/2$, and hence

$$1 - \Pr(R) \geq e^{-\frac{\Pr(R)}{1-\Pr(R)}} \geq e^{-\frac{2}{2-\varepsilon}\Pr(R)}.$$

It follows from Lemma 4.15 and (4.21) that, for large n,

$$\begin{aligned}\Pr(r_{\mathscr{A},h}(n) = 0) = \Pr\left(\bigwedge_{R\in\mathcal{S}[n]}\overline{R}\right) &\geq \prod_{R\in\mathcal{S}[n]}(1-\Pr(R))\\ &\geq e^{-\frac{2}{2-\varepsilon}\sum_{R\in\mathcal{S}[n]}\Pr(R)}\\ &= e^{-\frac{2}{2-\varepsilon}\mathbb{E}(r_{\mathscr{A},h}(n))} \geq \frac{1}{n},\end{aligned}$$

so $\sum_{n\geq 1}\Pr(r_{\mathscr{A},h}(n) = 0)$ diverges. □

To prove Theorem 1.12, we will use Lemma 4.16 together with the fact that the random variables $r_{\mathscr{A},h}(n)$ $(n \geq 1)$ have low correlation. To this end, we apply a generalization of the second Borel–Cantelli lemma due to Kochen and Stone:

Lemma 4.17 (Kochen–Stone)**.** *Let $\{E_n\}_{n\geq 1}$ be a family of events in some probability space, and suppose that $\sum_{n\geq 1} \Pr(E_n) = \infty$. Then,*

$$\Pr(E_n, \text{infinitely often}) \geq \limsup_{N\to\infty} \frac{\sum_{1\leq n,m\leq N} \Pr(E_n)\Pr(E_m)}{\sum_{1\leq n,m\leq N} \Pr(E_n \wedge E_m)}.$$

Proof. Cf. Lemma 2 of Yan [**44**]. □

In the notation of (4.22), our events of interest E_n are of the form

$$\{r_{\mathscr{A},h}(n) = 0\} = \bigwedge_{R\in\mathcal{S}[n]} \overline{R}.$$

By Lemma 4.15, we have, for any $m > n \geq 1$,

$$\Pr(r_{\mathscr{A},h}(n) = 0) \geq \prod_{R\in\mathcal{S}[n]} \Pr(\overline{R}) \tag{4.23}$$

and

$$\Pr(r_{\mathscr{A},h}(n) = 0 \text{ and } r_{\mathscr{A},h}(m) = 0) \leq \Bigg(\prod_{R\in\mathcal{S}[n]} \Pr(\overline{R})\Bigg)\Bigg(\prod_{S\in\mathcal{S}[m]} \Pr(\overline{S})\Bigg) e^{\Delta(n,m)}, \tag{4.24}$$

where

$$\Delta(n,m) := \Bigg(\sum_{\substack{R,S\in\mathcal{S}[n]\\ R\cap S\neq\varnothing}} + 2\sum_{\substack{R\in\mathcal{S}[n],\, S\in\mathcal{S}[m]\\ R\cap S\neq\varnothing}} + \sum_{\substack{R,S\in\mathcal{S}[m]\\ R\cap S\neq\varnothing}}\Bigg) \Pr(R\wedge S).$$

Lemma 4.18. $\Delta(n,m) \ll \left(1 + \frac{1}{(m-n)^{\frac{1}{h}+o(1)}}\right)\frac{1}{n^{\frac{1}{h}+o(1)}} + \frac{1}{m^{\frac{1}{h}+o(1)}}$

Proof. We start by estimating the sum over $R,S \in \mathcal{S}[m]$ (the $\mathcal{S}[n]$ case is analogous). If $R\cap S =: I \neq \varnothing$, we have $\Pr(R\wedge S) = \Pr(I)\Pr(R\setminus I)\Pr(S\setminus I)$. Thus, from Lemma 4.4, as $f(n) = (n\log(n))^{1/h}$, we have

$$\begin{aligned}
\sum_{\substack{R,S\in\mathcal{S}[m]\\ R\cap S\neq\varnothing}} \Pr(R\wedge S) &= \sum_{\ell=1}^{h-1} \sum_{\substack{I\subseteq\{0,\dots,m\}\\ |I|=\ell}} \Pr(I)\Bigg(\sum_{\substack{R,S\in\mathcal{S}[m]\\ R\cap S=I}} \Pr(R\setminus I)\Pr(S\setminus I)\Bigg)\\
&\leq \sum_{\ell=1}^{h-1}\sum_{k\leq m} \mathbb{E}(r^*_{\mathscr{A},\ell}(k))\mathbb{E}(r^*_{\mathscr{A},h-\ell}(m-k))^2\\
&\ll \sum_{\ell=1}^{h-1}\sum_{k\leq m} \frac{f(k)^\ell}{k}\left(\frac{f(m-k)^{h-\ell}}{m-k}\right)^2
\end{aligned}$$

$$\ll \sum_{k\le m} \frac{f(k)}{k}\left(\frac{f(m-k)^{h-1}}{m-k}\right)^2 \ll m^{-\frac{1}{h}+o(1)}.$$

Similarly, for $R \in \mathcal{S}[n]$, $S \in \mathcal{S}[m]$ with $m > n$, we have

$$\sum_{\substack{R\in\mathcal{S}[n],\, S\in\mathcal{S}[m]\\ R\cap S\neq\varnothing}} \Pr(R\wedge S) = \sum_{\ell=1}^{h-1} \sum_{\substack{I\subseteq\{0,\ldots,m\}\\ |I|=\ell}} \Pr(I)\left(\sum_{\substack{R\in\mathcal{S}[n],\, S\in\mathcal{S}[m]\\ R\cap S=I}} \Pr(R\setminus I)\Pr(S\setminus I)\right)$$

$$\ll \sum_{k\le n} \frac{f(k)}{k}\left(\frac{f(n-k)^{h-1}}{n-k}\right)\left(\frac{f(m-k)^{h-1}}{m-k}\right)$$

$$\ll (m-n)^{-\frac{1}{h}+o(1)} \sum_{k\le n} \frac{f(k)}{k}\left(\frac{f(n-k)^{h-1}}{n-k}\right)$$

$$\ll (n(m-n))^{-\frac{1}{h}+o(1)},$$

completing the proof. □

By Lemma 4.18, for every $\delta > 0$ there is $K \ge 1$ such that $\Delta(n,m) < \delta$ if $m > n \ge K$. Write $E_n := \{r_{\mathscr{A},h}(n) = 0\}$. By (4.23), (4.24) we have

$$\sum_{\substack{1\le n<m\le N\\ n\le K}} \Pr(E_n\wedge E_m) \le e^{\max\Delta(m,n)}\left(\sum_{n=1}^{K}\prod_{R\in\mathcal{S}[n]}\Pr(\overline{R})\right)\left(\sum_{m\le N}\prod_{S\in\mathcal{S}[m]}\Pr(\overline{S})\right)$$

$$\ll K\sum_{m\le N}\Pr(E_m) = o\left(\left(\sum_{m\le N}\Pr(E_m)\right)^2\right).$$

Thus, we have by Lemma 4.17 that

$$\Pr(E_n,\text{ infinitely often}) \ge \limsup_{N\to\infty} \frac{\sum_{K\le n<m\le N}\Pr(E_n)\Pr(E_m)}{\sum_{K\le n<m\le N}\Pr(E_n\wedge E_m)}$$

$$\ge \limsup_{N\to\infty} \frac{\sum_{K\le n<m\le N}\left(\prod_{R\in\mathcal{S}[n]}\Pr(\overline{R})\right)\left(\prod_{S\in\mathcal{S}[m]}\Pr(\overline{S})\right)}{\sum_{K\le n<m\le N}\left(\prod_{R\in\mathcal{S}[n]}\Pr(\overline{R})\right)\left(\prod_{S\in\mathcal{S}[m]}\Pr(\overline{S})\right)e^{\Delta(n,m)}}$$

$$\ge e^{-\delta}$$

for every $\delta > 0$. This concludes the proof of Theorem 1.12.

Chapter 5

Waring and Waring–Goldbach subbases with prescribed representation function

In this chapter, we explore the probabilistic construction of additive subbases for sets of k-th powers $\mathbb{N}^k$ and k-th powers of primes $\mathbb{P}^k$, focusing on their representation functions and precise growth conditions they must satisfy. We begin by formulating general conditions for sets $B \subseteq \mathbb{N}$ to have subbases with prescribed representation function, culminating in Theorem 1.17. We then show that $\mathbb{N}^k$ and $\mathbb{P}^k$ satisfy these conditions in certain cases, proving Theorems 1.14 and 1.16.

5.1. Random subsets

Recall that a real-valued function $F : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ is called *regularly varying* if it is measurable and $\lim_{x\to\infty} F(\lambda x)/F(x)$ exists for every $\lambda > 0$. Regularly varying functions are of the form $F(x) = x^\kappa \psi(x)$, where $\kappa \in \mathbb{R}$ and $\psi(x)$ is *slowly varying*, meaning $\lim_{x\to\infty} \psi(\lambda x)/\psi(x) = 1$ for every $\lambda > 0$.

Let $B \subseteq \mathbb{N}$ be a subset and F be a regularly varying function satisfying the following three conditions, as in Subsection 1.4.3:

(i) (Regular variation) There is $\beta = \beta(B) > 0$ such that, for every fixed $\lambda \geq 1$,

$$B(\lambda x) \sim \lambda^\beta B(x).$$

(ii) (Low additive energy) There exists $H_{\text{(ii)}} \in \mathbb{Z}_{\geq 1}$ such that, for every $h \geq H_{\text{(ii)}}$,

$$\sum_{n \leq x} r_{B,h}(n)^2 \ll \frac{B(x)^{2h}}{x} x^{o(1)}.$$

(iii) (Counting solutions with weights) There exists $H_{\text{(iii)}} \in \mathbb{Z}_{\geq 1}$ such that the following holds: Let $h \geq H_{\text{(iii)}}$, and suppose $f(x) := (xF(x))^{1/h} = x^\omega \phi(x) \leq (1 + o(1))B(x)$, with $1/h \leq \omega \leq \beta$. Then:

$$\sum_{\substack{x_1,\dots,x_h \in B \\ x_1+\cdots+x_h=n}} \frac{f(x_1)}{B(x_1)} \cdots \frac{f(x_h)}{B(x_h)} \sim \mathfrak{S}_{B,h}(n)\, C_{B,h,f}\, \frac{f(n)^h}{n},$$

where $C_{B,h,f} \in \mathbb{R}_{>0}$ is a constant, and $\mathfrak{S}_{B,h}(n)$ is some function of n satisfying

$$\mathfrak{S}_{B,h}(n) \asymp 1 \text{ for } n \in \mathscr{S}, \text{ for some subset } \mathscr{S} \subseteq \mathbb{Z}_{\geq 0}.$$

Let $h \geq \max\{2H_{(\mathrm{ii})}+1, H_{(\mathrm{iii})}\}$ be an integer. We introduce a constant $c > 0$, to be chosen later, and suppose that for the regularly varying function

$$f(x) = x^{\omega}\phi(x) = (xF(x))^{1/h},$$

we have $cf(x) \leq B(x)$. Now consider a probability space whose elements are subsets $0 \in \mathscr{A} \subseteq B$, where

$$\Pr(\mathbf{1}_{\mathscr{A}}(n) = 1) = \mathbb{E}(\mathbf{1}_{\mathscr{A}}(n)) := c\frac{f(n)}{B(n)}\mathbf{1}_B(n) \qquad (\forall n \in \mathbb{Z}_{\geq 1}), \tag{5.1}$$

and where the variables $\mathbf{1}_{\mathscr{A}}(n)$ are mutually independent {0,1}-random variables. This probability space has the feature that the counting function of $\mathscr{A} \subseteq B$ asymptotically matches f with probability 1:

Lemma 5.1. $|\mathscr{A} \cap [1,x]| \overset{\text{a.s.}}{\sim} c\dfrac{\beta}{\omega}f(x)$.

Proof. Since $B(x)$ is regularly varying, the function $b_{\lfloor x \rfloor} := \inf\{y \in \mathbb{R}_{\geq 0} \mid B(y) \geq \lfloor x \rfloor\}$ is also regularly varying, with $b_{B(x)} \sim x$. Using the fact that compositions of regularly varying functions are also regularly varying, we can express $f(b_{\lfloor x \rfloor}) = x^{\omega/\beta}\vartheta(x)$ for some slowly varying function $\vartheta(x)$. Notice that $B(x)^{\omega/\beta}\vartheta(B(x)) = f(b_{B(x)}) \sim f(x)$. By the strong law of large numbers, we have

$$\begin{aligned} |\mathscr{A} \cap [1,x]| &\overset{\text{a.s.}}{\sim} c\sum_{n \leq x} \frac{f(n)}{B(n)}\mathbf{1}_B(n) = c\sum_{k \leq B(x)} \frac{f(b_k)}{k} \\ &\sim c\int_1^{B(x)} t^{\omega/\beta-1}\vartheta(t)\,\mathrm{d}t \\ &\sim c\left(\int_{1/B(x)}^1 u^{\omega/\beta-1}\frac{\vartheta(uB(x))}{\vartheta(B(x))}\,\mathrm{d}u\right) f(x). \end{aligned}$$

By Potter bounds (cf. BGT [**2**, Theorem 1.5.6(i)]), for any $\delta > 0$ there exists $C = C_\delta > 0$ such that, for large $x \geq x_\delta$ and $C/x \leq u \leq 1$, we have $\vartheta(ux)/\vartheta(x) \leq 2u^{-\delta}$. Selecting $\delta < \omega/2\beta$, we split the integral $\int_{1/B(x)}^1 = \int_{1/B(x)}^{C/B(x)} + \int_{C/B(x)}^1$. Since by the definition of slow variation,

$$u^{\omega/\beta-1}\frac{\vartheta(uB(x))}{\vartheta(B(x))}\mathbf{1}_{(C/B(x),1]} \xrightarrow{x\to\infty} u^{\omega/\beta-1}\mathbf{1}_{(0,1]},$$

the dominated convergence theorem implies that

$$\int_{C/B(x)}^{1} u^{\omega/\beta-1}\frac{\vartheta(uB(x))}{\vartheta(B(x))}\,\mathrm{d}u \to \int_0^1 u^{\omega/\beta-1}\,\mathrm{d}u = \frac{\beta}{\omega}$$

as $x\to\infty$. On the other hand, since $\vartheta(x)=x^{o(1)}$, the term $\int_{1/B(x)}^{C/B(x)}$ vanishes, completing the proof. □

5.1.1. Expectation of $r_{\mathscr{A},h}(n)$

We aim to compute the expectation of

$$r_{\mathscr{A},h}(n) = \sum_{\substack{x_1,\dots,x_h\in\mathbb{Z}_{\geq 0}\\ x_1+\cdots+x_h=n}} \mathbf{1}_{\mathscr{A}}(x_1)\cdots\mathbf{1}_{\mathscr{A}}(x_h).$$

To facilitate this, we introduce auxiliary representation functions that lend themselves more readily to probabilistic analysis. Let $1\leq \ell\leq h$, and $c_1,\dots,c_\ell\in\mathbb{Z}_{\geq 1}$. A solution $(x_1,\dots,x_h)$ to the equation $c_1x_1+\cdots+c_\ell x_\ell=n$ is called *exact* if the x_i's are pairwise distinct. The corresponding *exact representation function* (associated with $c_1,\dots,c_\ell$) is defined as

$$\rho_{\mathscr{A},\ell}^{(c_1,\dots,c_\ell)}(n) := \sum_{\substack{x_1,\dots,x_\ell\in\mathbb{Z}_{\geq 0}\\ c_1x_1+\cdots+c_\ell x_\ell=n\\ x_i \text{ distinct}}} \mathbf{1}_{\mathscr{A}}(x_1)\cdots\mathbf{1}_{\mathscr{A}}(x_\ell).$$

For the special case where $c_1=\cdots=c_\ell=1$, we denote this function simply by $\rho_{\mathscr{A},\ell}(n)$.

By the same reasoning as in Subsection 4.1.1, we are led to the decomposition:

$$r_{\mathscr{A},h}(n) = \rho_{\mathscr{A},h}(n) + \sum_{(c_1,\dots,c_\ell)}{}' \rho_{\mathscr{A},\ell}^{(c_1,\dots,c_\ell)}(n), \tag{5.2}$$

where the summation runs over $1\leq\ell\leq h-1$ and all $(c_1,\dots,c_\ell)\in\mathbb{Z}_{\geq 1}^{\ell}$ such that $c_1+\cdots+c_\ell=h$. The following proposition provides a key estimate for bounding contributions from non-exact solutions:

Proposition 5.2. *Let $h\geq 2H_{(\mathrm{ii})}+1$, and $1\leq\ell\leq h-1$. Let $f(x)=x^{\omega}\phi(x)$ be a function of regular variation with $\omega\geq 1/h$. Let c_1, …, $c_\ell\in\mathbb{Z}_{\geq 1}$ be such that $c_1+\cdots+c_\ell\leq C$. Then, there exists $\eta=\eta(h,f)>0$ such that*

$$\sum_{\substack{x_1,\dots,x_\ell\in B\\ c_1x_1+\cdots+c_\ell x_\ell=n}} \frac{f(x_1)}{B(x_1)}\cdots\frac{f(x_\ell)}{B(x_\ell)} \ll_C n^{-\eta}\frac{f(n)^h}{n},$$

The proof of Proposition 5.2 is given in Subsection 5.1.2. The following two lemmas show that it suffices to consider exact solutions:

Lemma 5.3. *For $n \in \mathscr{S}$, we have*

$$\mathbb{E}(\rho_{\mathscr{A},h}(n)) \sim c^h\, \mathfrak{S}_{B,h}(n)\, C_{B,h,f}\, \frac{f(n)^h}{n},$$

and $\mathbb{E}(r_{\mathscr{A},h}(n)) = (1+O(n^{-\eta}))\mathbb{E}(\rho_{\mathscr{A},h}(n))$, where η is as in Proposition 5.2.

Proof. By condition (iii) and Proposition 5.2, we have

$$\begin{aligned}\mathbb{E}(\rho_{\mathscr{A},h}(n)) &= c^h \sum_{\substack{x_1,\dots,x_h\in B\\ x_1+\cdots+x_h=n\\ x_i\text{'s distinct}}} \frac{f(x_1)}{B(x_1)}\cdots\frac{f(x_h)}{B(x_h)}\\ &= c^h \sum_{\substack{x_1,\dots,x_h\in B\\ x_1+\cdots+x_h=n}} \frac{f(x_1)}{B(x_1)}\cdots\frac{f(x_h)}{B(x_h)} - O\left(c^h \sideset{}{'}\sum_{(c_1,\dots,c_\ell)} \sum_{\substack{x_1,\dots,x_\ell\in B\\ c_1x_1+\cdots+c_\ell x_\ell=n}} \frac{f(x_1)}{B(x_1)}\cdots\frac{f(x_\ell)}{B(x_\ell)}\right)\\ &= (1+o(1))c^h\, \mathfrak{S}_{B,h}(n)\, C_{B,h,f}\,\frac{f(n)^h}{n},\end{aligned}$$

proving the first part. For the second part, by (5.2) we have

$$\mathbb{E}(r_{\mathscr{A},h}(n)) = \mathbb{E}(\rho_{\mathscr{A},h}(n)) + \sideset{}{'}\sum_{(c_1,\dots,c_\ell)} \mathbb{E}(\rho_{\mathscr{A},\ell}^{(c_1,\dots,c_\ell)}(n)),$$

and for each $(c_1,\dots,c_\ell)$ we have, by Proposition 5.2,

$$\mathbb{E}(\rho_{\mathscr{A},\ell}^{(c_1,\dots,c_\ell)}(n)) \ll \sum_{\substack{x_1,\dots,x_\ell\in B\\ c_1x_1+\cdots+c_\ell x_\ell=n}} \frac{f(x_1)}{B(x_1)}\cdots\frac{f(x_\ell)}{B(x_\ell)} \ll n^{-\eta}\frac{f(n)^h}{n},$$

completing the proof. □

Lemma 5.4. *We have*

$$\mathbb{E}(r_{\mathscr{A},h-1}(n)) \ll n^{-\eta}\frac{f(n)^h}{n}.$$

Proof. As in (5.2), we have

$$\mathbb{E}(r_{\mathscr{A},h-1}(n)) = \mathbb{E}(\rho_{\mathscr{A},h-1}(n)) + \sideset{}{''}\sum_{(c_1,\dots,c_\ell)} \mathbb{E}(\rho_{\mathscr{A},\ell}^{(c_1,\dots,c_\ell)}(n)),$$

where the sum runs over $1 \le \ell \le h-2$ and the $(c_1,\dots,c_\ell) \in \mathbb{Z}_{\ge 1}^{\ell}$ such that $c_1+\cdots+c_\ell = h-1$. As in the proof of Lemma 5.3, by Proposition 5.2 it follows that $\mathbb{E}(r_{\mathscr{A},h-1}(n)) \ll n^{-\eta} f(n)^h/n$. □

5.1.2. Proof of Proposition 5.2

Since

$$\sum_{\substack{x_1,\dots,x_\ell\in B\\ c_1x_1+\cdots+c_\ell x_\ell=n}} \frac{f(x_1)}{B(x_1)}\cdots\frac{f(x_\ell)}{B(x_\ell)} \asymp \sum_{\substack{x_1,\dots,x_\ell\in B\\ c_1x_1+\cdots+c_\ell x_\ell=n}} G(x_1)\cdots G(x_\ell)$$

for every $G(x) \asymp f(x)/B(x)$, we may substitute f by some function asymptotic to f before proceeding with the calculations. Write $f(x) = x^\omega \phi(x)$ and $f(x)/B(x) = x^{\omega-\beta}\vartheta(x)$.

- If $\omega < \beta$, substitute f by $f(x) \sim B(x)\sup_{y\geq x} f(y)/B(y)$ (cf. BGT [**2**, Theorem 1.5.3]), so that $f(x)/B(x)$ is non-increasing.
- If $\omega = \beta$, substitute f by $f(x) \sim f(x)\vartheta(x)/\xi(x)$, where

$$\xi(x) := \sup_{\substack{2^J \leq y < 2^{J+1} \\ J = \lfloor \frac{\log x}{\log 2} \rfloor}} \vartheta(y).$$

  Since ϑ is of slow variation, we have $\lim_{x\to\infty}\sup_{\lambda\in[\frac{1}{2},2]} \vartheta(\lambda x)/\vartheta(x) = 1$ by uniform convergence, therefore $\vartheta(x) \sim \xi(x)$.

For f like described above, we have the following:

Lemma 5.5. $\displaystyle\sum_{x\leq n\leq 2x} \left|\frac{f(n)}{B(n)} - \frac{f(n+1)}{B(n+1)}\right| \ll \frac{f(x)}{B(x)}$

Proof. If $\omega < \beta$, then $f(x)/B(x)$ is non-increasing, so the result follows since $f(x)/B(x) \asymp f(2x)/B(2x)$. If $\omega = \beta$, then we have a sum of the form

$$\sum_{x\leq n\leq 2x} |\xi(n) - \xi(n+1)|$$

where ξ is constant in the intervals $[2^J, 2^{J+1})$, $J \in \mathbb{Z}_{\geq 0}$. This implies that for $n \in [x, 2x]$, $\xi(n) = \xi(n+1)$ for all except possibly one n. Therefore

$$\sum_{x\leq n\leq 2x} |\xi(n) - \xi(n+1)| \leq \sup_{x\leq y\leq 2x} |\xi(y) - \xi(y+1)| \ll \xi(x) = \frac{f(x)}{B(x)}. \qquad \square$$

Now, for $\alpha \in [0,1)$, $x \in \mathbb{R}_{\geq 0}$, let

$$T(\alpha; x) := \sum_{n\leq x} \frac{f(n)}{B(n)} \mathbf{1}_B(n)\, e(\alpha n), \qquad \widetilde{T}(\alpha; x) := \sum_{x/2C\leq n\leq x} \frac{f(n)}{B(n)} \mathbf{1}_B(n)\, e(\alpha n).$$

Since every solution to $c_1x_1 + \cdots + c_\ell x_\ell = n$ has some $x_i \geq n/2C$, we have

$$\sum_{\substack{x_1,\ldots,x_\ell\in B \\ c_1x_1+\cdots+c_\ell x_\ell = n}} \frac{f(x_1)}{B(x_1)} \cdots \frac{f(x_\ell)}{B(x_\ell)} \leq \sum_{\substack{I\subseteq\{1,\ldots,\ell\} \\ I\neq\varnothing}} \sum_{\substack{x_1,\ldots,x_\ell\in B \\ c_1x_1+\cdots+c_\ell x_\ell = n \\ \forall i\in I,\, x_i\geq n/2C}} \frac{f(x_1)}{B(x_1)} \cdots \frac{f(x_\ell)}{B(x_\ell)}$$

By the orthogonality of the $e(n\alpha)$ and Hölder's inequality, we have

$$\begin{aligned}\sum_{\substack{x_1,\ldots,x_\ell\in B \\ c_1x_1+\cdots+c_\ell x_\ell = n \\ \forall i\in I,\, x_i\geq n/2C}} \frac{f(x_1)}{B(x_1)} \cdots \frac{f(x_\ell)}{B(x_\ell)} &= \int_0^1 \left(\prod_{i\in I} \widetilde{T}(c_i\alpha; n)\right)\left(\prod_{\substack{j=1 \\ j\notin I}}^{\ell} T(c_j\alpha; n)\right) e(-n\alpha)\,\mathrm{d}\alpha \\ &\leq \prod_{i\in I}\left(\int_0^1 |\widetilde{T}(c_i\alpha; n)|^\ell\,\mathrm{d}\alpha\right)^{1/\ell} \prod_{\substack{j=1 \\ j\notin I}}^{\ell}\left(\int_0^1 |T(c_j\alpha; n)|^\ell\,\mathrm{d}\alpha\right)^{1/\ell}\end{aligned}$$

$$\ll_C \left(\int_0^1 |\widetilde{T}(\alpha;n)|^\ell \, \mathrm{d}\alpha \right)^{|I|/\ell} \left(\int_0^1 |T(\alpha;n)|^\ell \, \mathrm{d}\alpha \right)^{1-|I|/\ell},$$

therefore

$$\begin{aligned} &\sum_{\substack{x_1,\dots,x_\ell \in B \\ c_1x_1+\cdots+c_\ell x_\ell = n}} \frac{f(x_1)}{B(x_1)} \cdots \frac{f(x_\ell)}{B(x_\ell)} \\ &\qquad \ll_C \sum_{j=1}^{\ell} \left(\int_0^1 |\widetilde{T}(\alpha;n)|^\ell \, \mathrm{d}\alpha \right)^{j/\ell} \left(\int_0^1 |T(\alpha;n)|^\ell \, \mathrm{d}\alpha \right)^{1-j/\ell}. \end{aligned} \tag{5.3}$$

Lemma 5.6. *Let $h \geq 2H_{(\mathrm{ii})}$ be an integer. There exists $\delta = \delta(B,h,\omega) > 0$ such that, for every $1 \leq \ell \leq h-1$,*

$$\int_0^1 |T(\alpha;n)|^\ell \, \mathrm{d}\alpha \ll n^{\max\{h\omega-1-\delta,0\}+o(1)}$$

and

$$\int_0^1 |\widetilde{T}(\alpha;n)|^\ell \, \mathrm{d}\alpha \ll n^{\max\{h\omega-1,0\}-\delta+o(1)}.$$

Proof. Let $g(\alpha;x) := \sum_{n \leq x} \mathbf{1}_B(n) e(n\alpha)$. Since $f(2x)/B(2x) \asymp f(x)/B(x)$ by condition (i), by partial summation we have

$$\begin{aligned} T(\alpha;x) &= \sum_{j \leq \frac{\log x}{\log 2}} \sum_{x/2^{j+1} < n \leq x/2^j} \frac{f(n)}{B(n)} \mathbf{1}_B(n) e(n\alpha) \\ &\ll \sum_{j \leq \frac{\log x}{\log 2}} \left(\sup_{x/2^{j+1} < y \leq x/2^j} |g(\alpha;y)| \right) \left(\frac{f(2^{-j}x)}{B(2^{-j}x)} + \sum_{x/2^{j+1} < n \leq x/2^j} \left| \frac{f(n)}{B(n)} - \frac{f(n+1)}{B(n+1)} \right| \right). \end{aligned}$$

By Lemma 5.5, we have $\sum_{x/2^{j+1} < n \leq x/2^j} \left| \frac{f(n)}{B(n)} - \frac{f(n+1)}{B(n+1)} \right| \ll f(2^{-j}x)/B(2^{-j}x)$. It follows that

$$T(\alpha;x) \ll (\log x) \max_{j \leq \frac{\log x}{\log 2}} \left(\left(\sup_{x/2^{j+1} < y \leq x/2^j} |g(\alpha;y)| \right) \frac{f(2^{-j}x)}{B(2^{-j}x)} \right).$$

So, for $\ell^* := \max\{\ell, 2H_{(\mathrm{ii})}\}$, we have

$$\begin{aligned} \int_0^1 |T(\alpha;n)|^\ell \, \mathrm{d}\alpha &\leq \left(\int_0^1 |T(\alpha;n)|^{\ell^*} \, \mathrm{d}\alpha \right)^{\ell/\ell^*} \\ &\ll (\log n)^\ell \max_{j \leq \frac{\log n}{\log 2}} \left(\left(\sup_{n/2^{j+1} < y \leq n/2^j} \int_0^1 |g(\alpha;y)|^{\ell^*} \, \mathrm{d}\alpha \right)^{\ell/\ell^*} \frac{f(2^{-j}n)^\ell}{B(2^{-j}n)^\ell} \right). \end{aligned}$$

By Parseval's identity and condition (ii), for $n/2^{j+1} < y \leq n/2^j$ we have

$$\begin{aligned} \int_0^1 |g(\alpha;y)|^{\ell^*} \, \mathrm{d}\alpha &= \int_0^1 \left| \sum_{m \leq y} \mathbf{1}_B(m) e(m\alpha) \right|^{\ell^*} \mathrm{d}\alpha \\ &\leq B(y)^{\ell^* - 2H_{(\mathrm{ii})}} \int_0^1 \left| \sum_{m \leq y} \mathbf{1}_B(m) e(m\alpha) \right|^{2H_{(\mathrm{ii})}} \mathrm{d}\alpha \end{aligned}$$

$$\leq B(y)^{\ell^*-2H_{(\mathrm{ii})}} \sum_{m\leq H_{(\mathrm{ii})}y} r_{B,H_{(\mathrm{ii})}}(m)^2$$

$$\ll \frac{B(y)^{\ell^*}}{y} y^{o(1)} \asymp \frac{B(2^{-j}n)^{\ell^*}}{2^{-j}n}(2^{-j}n)^{o(1)},$$

and thus, as $f(x) = x^{\omega+o(1)}$,

$$\int_0^1 |T(\alpha;n)|^\ell \,\mathrm{d}\alpha \ll (\log n)^\ell \max_{j\leq \frac{\log n}{\log 2}} \left(\frac{f(2^{-j}n)^{\ell+o(1)}}{(2^{-j}n)^{\ell/\ell^*}}\right) = n^{\max\{\ell\omega-\frac{\ell}{\ell^*},0\}+o(1)}. \tag{5.4}$$

By a similar argument to the one above used to bound T, we obtain

$$\begin{aligned}\int_0^1 |\widetilde{T}(\alpha;n)|^\ell \,\mathrm{d}\alpha &\leq \left(\int_0^1 |\widetilde{T}(\alpha;n)|^\ell \,\mathrm{d}\alpha\right)^{\ell/\ell^*} \\ &\ll \left(\sup_{n/2C\leq y\leq n}\int_0^1 |g(\alpha;y)|^\ell \,\mathrm{d}\alpha\right)^{\ell/\ell^*} \frac{f(n)^\ell}{B(n)^\ell} \\ &\ll \left(\frac{B(n)^{\ell^*}}{n} n^{o(1)}\right)^{\ell/\ell^*} \frac{f(n)^\ell}{B(n)^\ell} \\ &= \frac{f(n)^\ell}{n^{\ell/\ell^*}} n^{o(1)} = n^{\ell\omega-\frac{\ell}{\ell^*}+o(1)}. \end{aligned} \tag{5.5}$$

Using (5.4), (5.5), to finish the proof, it suffices to show that for every $1\leq \ell\leq h-1$, if $\ell\omega - \frac{\ell}{\ell^*}\geq 0$ then $\ell\omega-\frac{\ell}{\ell^*} < h\omega - 1$. This is trivial for $\ell\geq 2H_{(\mathrm{ii})}$ (since $\ell^*=\ell$), so suppose $\ell < 2H_{(\mathrm{ii})}$. We have $\ell\omega-\frac{\ell}{\ell^*} = \ell(\omega - \frac{1}{2H_{(\mathrm{ii})}})$, so we must have $\omega\geq \frac{1}{2H_{(\mathrm{ii})}}$; thus,

$$\begin{aligned}\ell\left(\omega-\frac{1}{2H_{(\mathrm{ii})}}\right) \leq (2H_{(\mathrm{ii})}-1)\left(\omega-\frac{1}{2H_{(\mathrm{ii})}}\right) &= 2H_{(\mathrm{ii})}\omega - \left(\omega-\frac{1}{2H_{(\mathrm{ii})}}\right)-1 \\ &< h\omega-1,\end{aligned}$$

the last line following since $h\geq 2H_{(\mathrm{ii})}+1$. □

Applying Lemma 5.6 to (5.3), we obtain

$$\begin{aligned}\sum_{\substack{x_1,\ldots,x_\ell\in B\\ c_1x_1+\cdots+c_\ell x_\ell=n}} \frac{f(x_1)}{B(x_1)}\cdots\frac{f(x_\ell)}{B(x_\ell)} &\ll_C \left(n^{\max\{h\omega-1,0\}-\delta+o(1)}\right)^{1/\ell}\left(n^{\max\{h\omega-1-\delta,0\}+o(1)}\right)^{1-1/\ell} \\ &\ll n^{\max\{h\omega-1,0\}-\delta/\ell+o(1)}.\end{aligned}$$

Since $\omega\geq 1/h$ and $f(n)^h/n = x^{h\omega-1+o(1)}$, we have

$$\sum_{\substack{x_1,\ldots,x_\ell\in B\\ c_1x_1+\cdots+c_\ell x_\ell=n}} \frac{f(x_1)}{B(x_1)}\cdots\frac{f(x_\ell)}{B(x_\ell)} \ll_C n^{-\delta/\ell+o(1)}\frac{f(n)^h}{n},$$

concluding the proof of Proposition 5.2. □

5.2. Proof of Theorem 1.17

In this section, we will prove the following:

Theorem 1.17 *Let $B \subseteq \mathbb{Z}_{\geq 0}$ be a subset and F be a regularly varying function satisfying conditions (i)–(iii) at the beginning of Chapter 5. Let $h \geq \max\{2H_{(\mathrm{ii})} + 1, H_{(\mathrm{iii})}\}$ be an integer. If $F(n)/\log n \to \infty$ as $n \to \infty$, then there exists $A \subseteq B$ such that*

$$r_{A,h}(n) \sim \mathfrak{S}_{B,h}(n)F(n) \quad \textit{for} \quad n \in \mathscr{S}.$$

If $F(n) \gg \log n$, then there exists $A \subseteq B$ such that

$$r_{A,h}(n) \asymp F(n) \quad \textit{for} \quad n \in \mathscr{S}.$$

For the remainder of this section, fix $h \geq \max\{2H_{(\mathrm{ii})} + 1, H_{(\mathrm{iii})}\}$, and assume

$$n \in \mathscr{S}, \quad n \to \infty,$$

where $\mathscr{S}$ is as in condition (iii). Consider the function $F(x) = x^{\kappa}\psi(x)$, where $\psi(x)$ is a slowly varying function, and κ is a real number satisfying $0 \leq \kappa \leq h - 1$. Define

$$f(x) := (xF(x))^{1/h} = x^{(1+\kappa)/h}\psi(x)^{1/h}.$$

Let $c > 0$ be a constant to be chosen later, and suppose that $f(x)$ satisfies

$$f(x) \gg (x \log x)^{1/h}, \quad \text{and} \quad cf(x) \leq x.$$

Using Lemma 5.3, the proof of Theorem 1.17 reduces to showing that, in the probability space defined in Section 5.1, we have

$$r_{\mathscr{A},h}(n) \overset{\text{a.s.}}{\sim} \mathbb{E}(r_{\mathscr{A},h}(n)).$$

Since an event of probability 1 is non-empty, this implies the existence of a subset $A \subseteq B$ such that $r_{A,h}(n) \sim \mathbb{E}(r_{\mathscr{A},h}(n))$.

5.2.1. Theorem 1.17: Case $\kappa > 0$

Set $c := C_{B,h,f}^{-1/h}$. We will now apply Kim–Vu's inequality to the function $\rho_{\mathscr{A},h}(n)$. Recall that, in the notation of Theorem 4.8, we have

$$\mathbb{E}_j(Y) := \max_{\substack{S \subseteq \{v_1, \ldots, v_n\} \\ \text{multiset}, |S| = j}} \mathbb{E}(\partial_S Y), \qquad \mathbb{E}'(Y) = \max_{j \geq 1} \mathbb{E}_j(Y).$$

We can estimate E and E' using Lemmas 5.3 and 5.4. Since

$$\mathbb{E}'(\rho_{\mathscr{A},h}(n)) \leq 1 + \max_{1 \leq \ell \leq h-1} \max_{k \leq n} \mathbb{E}(r_{\mathscr{A},\ell}(k)) \leq 1 + \max_{k \leq n} \mathbb{E}(r_{\mathscr{A},h-1}(k)) \ll n^{\max\{0, \kappa - \eta\} + o(1)},$$

and $\mathbb{E}(\rho_{A,h}(n)) = n^{\kappa+o(1)}$, we have

$$E = \mathbb{E}(\rho_{\mathscr{A},h}(n)), \qquad \text{and} \qquad E' \ll n^{\max\{0,\kappa-\eta\}+o(1)}.$$

Setting $\lambda = (h+1)\log n$, we find

$$\begin{aligned}\lambda^{h-\frac{1}{2}}(E'E)^{1/2} &\ll (h+1)^h(\log n)^h \left(\frac{E'}{E}\right)^{1/2} E \\ &\ll (\log n)^h \left(\frac{n^{\max\{0,\kappa-\eta\}+o(1)}}{n^{\kappa+o(1)}}\right)^{1/2} E = \frac{(\log n)^h}{n^{\min\{\kappa,\eta\}/2+o(1)}}\, E.\end{aligned}$$

This leads to the bound:

$$\Pr\left(\left|\rho_{\mathscr{A},h}(n) - \mathbb{E}(\rho_{\mathscr{A},h}(n))\right| \geq \frac{8^h\sqrt{h!}}{n^{\min\{\kappa,\eta\}/2+o(1)}}\,\mathbb{E}(\rho_{\mathscr{A},h}(n))\right) \ll n^{-2}. \tag{5.6}$$

Thus, the Borel–Cantelli lemma implies that $\rho_{\mathscr{A},h}(n) \overset{\text{a.s.}}{\sim} \mathbb{E}(\rho_{\mathscr{A},h}(n)) \sim \mathfrak{S}_{B,h}(n)F(n)$.

To handle the contribution of non-exact solutions, observe that by (5.2), it suffices to show

$$\rho_{\mathscr{A},\ell}^{(c_1,\dots,c_\ell)}(n) \overset{\text{a.s.}}{=} o(F(n)),$$

for every $1 \leq \ell \leq h-1$ and for equations $c_1x_1 + \cdots + c_\ell x_\ell = n$ with $c_1 + \cdots + c_\ell \leq h$. Applying Kim–Vu's inequality to the boolean polynomial $\rho_{\mathscr{A},\ell}^{(c_1,\dots,c_\ell)}(n)$, Lemma 5.3 gives

$$E,\, E' \ll 1 + n^{-\eta}\frac{f(n)^h}{n} = n^{\max\{0,\kappa-\eta\}+o(1)}.$$

From this, we deduce

$$\Pr\left(|\rho_{\mathscr{A},\ell}^{(c_1,\dots,c_\ell)}(n) - \mathbb{E}(\rho_{\mathscr{A},\ell}^{(c_1,\dots,c_\ell)}(n))| \geq 8^h\sqrt{h!}\,(\log n)^h\, n^{\max\{0,\kappa-\eta\}+o(1)}\right) \ll n^{-2}.$$

Thus, by the Borel–Cantelli lemma,

$$\rho_{\mathscr{A},\ell}^{(c_1,\dots,c_\ell)}(n) \overset{\text{a.s.}}{\ll} \mathbb{E}(\rho_{\mathscr{A},\ell}^{(c_1,\dots,c_\ell)}(n)) + n^{\max\{0,\kappa-\eta\}+o(1)} = o(F(n)).$$

This completes the proof. □

5.2.2. δ-small and δ-normal solutions

As in Subsection 4.1.3, to estimate $r_{\mathscr{A},h}(n)$, we divide the solutions being counted into $r_{\mathscr{A},h}(n) = r_{\mathscr{A},h}^{(\delta\text{-small})}(n) + r_{\mathscr{A},h}^{(\delta\text{-normal})}(n)$, with

$$r_{\mathscr{A},\ell}^{(\delta\text{-small})}(n) := \sum_{\substack{x_1,\dots,x_\ell \in \mathbb{Z}_{\geq 0} \\ b_1x_1+\cdots+b_\ell x_\ell = n \\ \exists j \,\mid\, x_j < n^\delta}} \mathbf{1}_{\mathscr{A}}(x_1)\cdots \mathbf{1}_{\mathscr{A}}(x_\ell),$$

$$r_{\mathscr{A},\ell}^{(\delta\text{-normal})}(n) := \sum_{\substack{x_1,\dots,x_\ell \in \mathbb{Z}_{\geq 0} \\ b_1x_1+\cdots+b_\ell x_\ell = n \\ x_1,\dots,x_\ell \geq n^\delta}} \mathbf{1}_{\mathscr{A}}(x_1)\cdots \mathbf{1}_{\mathscr{A}}(x_\ell).$$

We aim to show that δ-small solution contribute negligibly, on average.

Lemma 5.7. *Let η be as in Proposition 5.2. For every $0 < \delta < \eta$, we have*

$$\mathbb{E}(r_{\mathscr{A},h}^{(\delta\text{-small})}(n)) \ll c^h\, n^{\beta\delta - \eta + o(1)}\, \frac{f(n)^h}{n}.$$

Proof. We begin by bounding the expectation:

$$\begin{aligned}
\mathbb{E}(r_{\mathscr{A},h}^{(\delta\text{-small})}(n)) &\leq \sum_{k \leq n^\delta} \mathbb{E}(r_{\mathscr{A},h-1}(n-k)\mathbf{1}_{\mathscr{A}}(k)) \\
&\leq c \sum_{k\leq n^\delta} \frac{f(k)}{B(k)}\, \mathbf{1}_B(k)\, \mathbb{E}(r_{\mathscr{A},h-1}(n-k) \mid \mathbf{1}_{\mathscr{A}}(k) = 1).
\end{aligned}$$

For $k \leq n^\delta$, we apply Lemma 5.4 to bound the conditional expectation:

$$\begin{aligned}
\mathbb{E}(r_{\mathscr{A},h-1}(n-k) \mid \mathbf{1}_{\mathscr{A}}(k) = 1) &\leq \sum_{\ell=1}^{h-1} \mathbb{E}(r_{\mathscr{A},h-\ell}(n-\ell k)) \\
&\ll c^{h-1}\, n^{-\eta}\, \frac{f(n)^h}{n}.
\end{aligned}$$

Substituting this back, we find

$$\mathbb{E}(r_{\mathscr{A},h}^{(\delta\text{-small})}(n)) \ll c^h\, n^{-\eta} \frac{f(n)^h}{n} \sum_{k\leq n^\delta} \frac{f(k)}{B(k)}\, \mathbf{1}_B(k).$$

Since $f(k)$ and $B(k)$ are regularly varying, the sum is asymptotically proportional to $f(n^\delta)$ (by the same argument used in Lemma 5.1). Therefore, we obtain

$$\mathbb{E}(r_{\mathscr{A},h}^{(\delta\text{-small})}(n)) \asymp c^h\, n^{-\eta} f(n^\delta)\, \frac{f(n)^h}{n} = c^h\, n^{\beta\delta-\eta+o(1)}\, \frac{f(n)^h}{n}. \qquad \square$$

5.2.3. Theorem 1.17: Case $\kappa = 0$

Define $c := C_{B,h,f}^{-1/h}$. In this case, we have $\frac{f(x)^h}{x} = F(x) = x^{o(1)}$. Choose $0 < \delta < \eta$, where η is as given in Proposition 5.2. We will apply Theorem 4.9 to $\rho_{\mathscr{A},h}^{(\delta\text{-normal})}(n)$. After that, by

(5.2) and Lemma 5.7, it will remain to show that $\rho^{(\delta\text{-small})}_{\mathscr{A},h}(n)$ and $r_{\mathscr{A},h-1}(n)$ are almost surely $O(1)$.

The function $\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)$ is a homogeneous, simple boolean polynomial of degree h. Using the notation of Theorem 4.9, the partial derivatives of $\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)$ are, for $1 \le j \le h-1$, bounded by

$$\mathbb{E}_j(\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)) \le \max_{n^\delta \le k \le n} \mathbb{E}(r_{\mathscr{A},h-j}(k)) \ll_c \max_{n^\delta \le k \le n} k^{-\eta} \frac{f(k)^h}{k} \ll n^{-\eta\delta + o(1)},$$

where the second step uses Lemma 5.4. Since each monomial of $\rho_{\mathscr{A},h}(n)$ appears at most $h!$ times, the function $\frac{1}{h!}\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)$ is a normal boolean polynomial. Taking $0 < \alpha < \eta\delta$, $\gamma = 2$, and $K = K(h,\alpha,\gamma)$ in Theorem 4.9, we get:

$$\Pr\left(|\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n) - \mathbb{E}(\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n))| \ge (h!\lambda\, \mathbb{E}(\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)))^{1/2}\right) \ll n^{-2},$$

where we set $\lambda := 32hK \log n$. If $F(n)/\log n \to \infty$ as $x \to \infty$, then Lemma 5.7 implies $(\lambda \mathbb{E}(\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)))^{1/2} = o(\mathbb{E}(\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n)))$. Thus, by the Borel–Cantelli lemma, we have $\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n) \overset{\text{a.s.}}{\sim} \mathbb{E}(\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n))$. For $F \gg \log$, we can choose $c > 1$ sufficiently large to ensure that $\mathbb{E}(\rho_{\mathscr{A},h}(n)) \gg c^h F(n) > 32hK \log n$, so that it follows that $\rho^{(\delta\text{-normal})}_{\mathscr{A},h}(n) \overset{\text{a.s.}}{\asymp} F(n)$.

To bound $\rho^{(\delta\text{-small})}_{\mathscr{A},h}(n)$, we apply Lemma 4.6. By Lemma 5.4, we have:

$$\mathbb{E}(r_{\mathscr{A},\ell}(n)) \ll n^{-\eta + o(1)}, \qquad 1 \le \ell \le h-1,$$

and by Lemma 5.7 we have $\mathbb{E}(\rho^{(\delta\text{-small})}_{\mathscr{A},h}(n)) \ll n^{-\eta+\beta\delta+o(1)}$. By the disjointness lemma 4.7,

$$\Pr(\widehat{r}_{\mathscr{A},\ell}(n) \ge T) \le \left(\frac{e}{T}\right)^T n^{-T\eta + o(1)} \ll n^{-2}$$

for large $T > 0$. A similar bound holds for $\widehat{\rho}^{(\delta\text{-small})}_{\mathscr{A},h}(n)$, since $-\eta + \beta\delta > 0$. Thus, by the Borel–Cantelli lemma, we have $\widehat{r}_{\mathscr{A},\ell}(n) \overset{\text{a.s.}}{\ll} 1$ for $1 \le \ell \le h-1$ and $\widehat{\rho}^{(\delta\text{-small})}_{\mathscr{A},h}(n) \overset{\text{a.s.}}{\ll} 1$. For each $2 \le \ell \le h-1$, it follows that $\max_{k \le n} \widehat{r}_{\mathscr{A},\ell}(k) \overset{\text{a.s.}}{\ll} 1$. Substituting this into Lemma 4.6, we conclude:

$$\rho^{(\delta\text{-small})}_{\mathscr{A},h}(n) \overset{\text{a.s.}}{\ll} \widehat{\rho}^{(\delta\text{-small})}_{\mathscr{A},h}(n) \overset{\text{a.s.}}{\ll} 1.$$

Finally, to bound $r_{\mathscr{A},h-1}(n)$, if $h = 2$ then $r_{\mathscr{A},h-1}(n) \le 1$ trivially. For $h \ge 3$, we apply Lemma 4.6 again to obtain $r_{\mathscr{A},h-1}(n) \overset{\text{a.s.}}{\ll} \widehat{r}_{\mathscr{A},h-1}(n) \overset{\text{a.s.}}{\ll} 1$. This completes the proof. □

5.3. Waring subbases

In this section, we prove Theorem 1.14 by showing that $\mathbb{N}^k$ satisfies conditions (i)–(iii) of the beginning of Chapter 5.

Theorem 1.14 *Let $k \ge 2$ be an integer.*

(i) *There exists* $h_k \leq k^2(\log k + \log\log k + O(1))$ *such that the following holds: Let* $h \geq h_k$, *and* $0 < \kappa < h/k - 1$. *Then, for every* $c > 0$, *there exists a subset* $A \subseteq \mathbb{P}^k$ *such that*

$$r_{A,h}(n) \sim \mathfrak{S}_{k,h}(n)\, cn^{\kappa}.$$

The same holds for $\kappa = h/k - 1$ *but with* $0 < c \leq \frac{\Gamma(1+1/k)^h}{\Gamma(h/k)}$.

(ii) *There exists* $h'_k \ll 8^k k^2$ *such that the following holds: Let* $h \geq h'_k$, *and* F *be a regularly varying function satisfying*

$$\lim_{x\to\infty} \frac{F(x)}{\log x} = \infty, \qquad F(x) \leq (1 + o(1)) \frac{\Gamma(1 + 1/k)^h}{\Gamma(h/k)} x^{h/k-1}.$$

Then, there exists a subset $A \subseteq \mathbb{N}^k$ *such that*

$$r_{A,h}(n) \sim \mathfrak{S}_{k,h}(n) F(n).$$

In both cases, $\mathfrak{S}_{k,h}(n)$ *is the singular series for Waring's problem, given by*

$$S(a,q) := \sum_{r=1}^{q} e\bigg(\frac{ar^k}{q}\bigg), \qquad \mathfrak{S}_{k,h}(n) := \sum_{q\geq 1} \sum_{\substack{a=1\\(a,q)=1}}^{q} \frac{S(a,q)^h}{q^h} e\bigg(-\frac{na}{q}\bigg). \tag{5.7}$$

Clearly $\mathbb{N}^k$ satisfies condition (i), with $\beta = 1/k$. As noted by Wooley [**43**, Equation (1.2)], $\mathbb{N}^k$ satisfies condition (ii) for $H_{(\mathrm{ii})} \leq \frac{1}{2}k^2(\log k + \log\log k + O(1))$. More precisely,

$$\int_0^1 \bigg| \sum_{1\leq n\leq x} e(\alpha n^k) \bigg|^{2\ell} \mathrm{d}\alpha \ll x^{2\ell - k + o(1)} \tag{5.8}$$

for every $\ell \geq \frac{1}{2}k^2(\log k + \log\log k + O(1))$. By Parseval's identity, we have

$$\sum_{n\leq x} r_{\mathbb{N}^k,\ell}(n)^2 \leq \int_0^1 \bigg| \sum_{n\leq x^{1/\ell}} e(\alpha n^k) \bigg|^{2h} \mathrm{d}\alpha \ll x^{2\ell/k - 1 + o(1)},$$

which is the shape of condition (ii).

5.3.1. Waring satisfies condition (iii)

The first result we need, due to Wooley, is equivalent to condition (iii) restricted to functions of the form x^{ω}; that is, an estimate for the number of solutions to $x_1^k + \cdots + x_h^k = n$ counted with weight $(x_1 \cdots x_h)^{\omega}$ for some $\omega > 0$. By Theorem 1.17, this directly implies Theorem 1.14 (i).

Lemma 5.8 (Wooley [**43**, Theorem 1.1])**.** *There exists an integer $H_W \le k^2(\log k + \log\log k + O(1))$ such that the following holds: Let $h \ge H_W$. For any $\omega \ge 1/h$,*

$$\sum_{\substack{x_1,\dots,x_h \in \mathbb{N}^k \\ x_1+\cdots+x_h = n}} (x_1 \cdots x_h)^{\omega - \frac{1}{k}} = \mathfrak{S}_{k,h}(n) \frac{1}{k^h} \frac{\Gamma(\omega)^h}{\Gamma(h\omega)} n^{\omega h - 1} + O(n^{\omega h - 1 - \tau})$$

for some $\tau = \tau(k,h) > 0$.

To prove Theorem 1.14 (ii), we need a second result, due to Vu, on an upper bound to the number of solutions $x_1^k + \cdots + x_h^k = n$ for x_j's restricted to some box.

Lemma 5.9 (Vu [**39**, Lemma 2.1])**.** *There exists an integer $H_V \ll 8^k k^2$ such that the following holds: Let $h \ge H_V$. Given $P_1, \dots, P_h \ge 1$, the number of solutions to*

$$x_1 + \cdots + x_h = n$$

with $x_j \in \mathbb{N}^k \cap [1,P_j]$ $(1 \le j \le h)$ is

$$O\left(\frac{1}{n}(P_1 \cdots P_h)^{\frac{1}{k}} + (P_1 \cdots P_h)^{\frac{1}{k} - \frac{1}{h} - \delta}\right),$$

for some $\delta = \delta(k,h) > 0$.

Let ϕ be a slowly varying function. By uniform convergence (cf. BGT [**2**, Theorem 1.2.1]), given $0 < \mu < 1$, for every $\varepsilon > 0$ there exists $x_{\mu,\varepsilon} \in \mathbb{R}$ such that, for every $x \ge x_{\mu,\varepsilon}$,

$$\left| \frac{\phi(\lambda x)}{\phi(x)} - 1 \right| < \varepsilon, \qquad \forall \lambda \in [\mu,1].$$

Taking $\mu = 1/j$, $j \in \mathbb{Z}_{\ge 1}$, for large x we define $\epsilon(x) := j$ for $x \in [x_{\frac{1}{j},\frac{1}{j}}, x_{\frac{1}{j+1},\frac{1}{j+1}})$. This defines a non-decreasing function $\epsilon(x) \to \infty$ such that

$$\frac{\phi(y)}{\phi(x)} \to 1 \text{ uniformly for } y \in \left[\frac{x}{\epsilon(x)}, x\right). \tag{5.9}$$

Lemma 5.10. *Let $h \ge \max\{H_V, H_W\}$. We have:*

$$\sum_{\substack{x_1,\dots,x_h \in \mathbb{N}^k \\ x_1+\cdots+x_h = n}} \frac{f(x_1)}{x_1^{1/k}} \cdots \frac{f(x_h)}{x_h^{1/k}} \sim \frac{1}{k^h} \frac{\Gamma(\omega)^h}{\Gamma(h\omega)} \mathfrak{S}_{k,h}(n) \frac{f(n)^h}{n}.$$

Proof. Let $\epsilon(x)$ be as in (5.9). Start by separating the sum into

$$S_1 := \sum_{\substack{x_1,\dots,x_h \in \mathbb{N}^k \\ x_1+\cdots+x_h = n \\ \exists j \,|\, x_j < n/\epsilon(n)}} \frac{f(x_1)}{x_1^{1/k}} \cdots \frac{f(x_h)}{x_h^{1/k}}, \qquad S_2 := \sum_{\substack{x_1,\dots,x_h \in \mathbb{N}^k \\ x_1+\cdots+x_h = n \\ \forall j, x_j \ge n/\epsilon(n)}} \frac{f(x_1)}{x_1^{1/k}} \cdots \frac{f(x_h)}{x_h^{1/k}}.$$

We start with S_1. Let $\mathcal{P}$ be the set of all h-tuples $\mathbf{p} = (P_1, \dots, P_h)$ with $P_1 \in \{1,2,4\dots,2^L\}$, and $P_j \in \{1,2,4,\dots,2^J\}$ $(2 \le j \le h)$, where L (resp. J) is the smallest integer for which $2^L \ge n/\varepsilon(n)$ (resp. $2^J \ge n$), and write

$$\sigma_{\mathbf{p}} := \sum_{\substack{x_1,\dots,x_h \in \mathbb{N}^k \\ x_1+\cdots+x_h=n \\ \frac{P_j}{2}-\frac{1}{2} \le x_j < P_j,\ \forall j}} \frac{f(x_1)}{x_1^{1/k}} \cdots \frac{f(x_h)}{x_h^{1/k}}$$

(where "$f(0)/0 = 1$"). We have $S_1 \le \sum_{\mathbf{p}\in\mathcal{P}} \sigma_{\mathbf{p}}$. Since the number of terms in $\sigma_{\mathbf{p}}$ is, by Lemma 5.9, $O(\frac{1}{n}(P_1\cdots P_h)^{\frac{1}{k}} + (P_1\cdots P_h)^{\frac{1}{k}-\frac{1}{h}-\delta})$, we have:

$$\begin{aligned}
S_1 &\le \sum_{\mathbf{p}\in\mathcal{P}} \sigma_{\mathbf{p}} \\
&\ll \sum_{\mathbf{p}\in\mathcal{P}} \left(\frac{1}{n}(P_1\cdots P_h)^{\frac{1}{k}} + (P_1\cdots P_h)^{\frac{1}{k}-\frac{1}{h}-\delta}\right) \frac{f(P_1)}{P_1^{\frac{1}{k}}} \cdots \frac{f(P_h)}{P_h^{\frac{1}{k}}} \\
&= \frac{1}{n}\sum_{\mathbf{p}\in\mathcal{P}} f(P_1)\cdots f(P_h) + \sum_{\mathbf{p}\in\mathcal{P}} \frac{f(P_1)}{P_1^{\frac{1}{h}+\delta}} \cdots \frac{f(P_h)}{P_h^{\frac{1}{h}+\delta}} \\
&\ll \frac{1}{n}\left(\sum_{j=0}^{L} f(2^j)\right)\left(\sum_{j=0}^{J} f(2^j)\right)^{h-1} + \left(\sum_{j=0}^{L} \frac{f(2^j)}{(2^j)^{\frac{1}{h}+\delta}}\right)\left(\sum_{j=0}^{J} \frac{f(2^j)}{(2^j)^{\frac{1}{h}+\delta}}\right)^{h-1}.
\end{aligned} \tag{5.10}$$

Since $f(x) = x^\omega \phi(x)$, we have $\sum_{j=0}^{J} f(2^j) \ll_\varepsilon f(n)\sum_{j=0}^{J} 2^{-j(\omega-\varepsilon)} \ll f(n)$, hence

$$\frac{1}{n}\left(\sum_{j=0}^{L} f(2^j)\right)\left(\sum_{j=0}^{J} f(2^j)\right)^{h-1} \ll \frac{f(n/\epsilon(n))f(n)^{h-1}}{n} = o\left(\frac{f(n)^h}{n}\right).$$

For the other term, if $\omega > 1/h$ then

$$\sum_{j=0}^{J} \frac{f(2^j)}{(2^j)^{\frac{1}{h}+\delta}} \ll_\varepsilon \frac{f(n)}{n^{\frac{1}{h}+\delta}} \sum_{j=0}^{J} (2^{-j})^{\omega-(\frac{1}{h}+\delta)-\varepsilon} \ll \frac{f(n)}{n^{1/h}},$$

and if $\omega = 1/h$ then $\sum_{j=0}^{J} \frac{f(2^j)}{(2^j)^{\frac{1}{h}+\delta}} \ll_\varepsilon \sum_{j=0}^{J} 2^{-j(\delta-\varepsilon)} \ll 1 = o(f(n)^h/n)$. Therefore, it follows from (5.10) that $S_1 = o(f(n)^h/n)$.

For S_2, since $f(x) = x^\omega\phi(x)$, by the definition of $\epsilon(x)$ we have

$$\begin{aligned}
S_2 &\sim \phi(n)^h \sum_{\substack{x_1,\dots,x_h\in\mathbb{N}^k \\ x_1+\cdots+x_h=n \\ x_j \ge n/\epsilon(n),\forall j}} (x_1\cdots x_h)^{\omega-\frac{1}{k}} \frac{\phi(x_1)}{\phi(n)} \cdots \frac{\phi(x_h)}{\phi(n)} \\
&\sim \phi(n)^h \sum_{\substack{x_1,\dots,x_h\in\mathbb{N}^k \\ x_1+\cdots+x_h=n \\ x_j \ge n/\epsilon(n),\forall j}} (x_1\cdots x_h)^{\omega-\frac{1}{k}}
\end{aligned} \tag{5.11}$$

Using the same methods used to calculate S_1, one can show that

$$S_3 := \phi(n)^h \sum_{\substack{x_1,\dots,x_h\in\mathbb{N}^k \\ x_1+\cdots+x_h=n \\ \exists j \,|\, x_j<n/\epsilon(n)}} (x_1\cdots x_h)^{\omega-\frac{1}{k}} = o\left(\frac{f(n)^h}{n}\right).$$

Thus, from Lemma 5.8, (5.11) implies that

$$S_2 \sim \frac{1}{k^h}\frac{\Gamma(\omega)^h}{\Gamma(h\omega)}\mathfrak{S}_{k,h}(n)\frac{f(n)^h}{n},$$

concluding the proof. □

Lemma 5.10 implies that $\mathbb{N}^k$ satisfies condition (iii) for every admissible regularly varying F with $H_{(\mathrm{iii})} \le \max\{H_V, H_W\} \ll 8^k k^2$. Therefore, since $\max\{2H_{(\mathrm{ii})}+1, H_{(\mathrm{iii})}\} \ll 8^k k^2$, Theorem 1.14 (ii) follows from Theorem 1.17.

5.4. Proof of Theorem 1.15

For the next two sections, we will deal with $\mathbb{P}^k$. In this section we will prove the following:

Theorem 1.15 *Let $k \ge 1$ be an integer, and*

$$h \ge h_k^* := \begin{cases} 2^k+1 & \text{if } 1\le k\le 11, \\ \lceil 2k^2(2\log k+\log\log k+2.5)\rceil & \text{if } k\ge 12. \end{cases} \tag{5.12}$$

For every $\omega \ge 1/h$, we have

$$\sum_{\substack{x_1,\dots,x_h\in\mathbb{P}^k \\ x_1+\cdots+x_h=N}} (x_1\cdots x_h)^{\omega-\frac{1}{k}}(\log x_1\cdots\log x_h) = \mathfrak{S}^*_{k,h}(N)\,\frac{\Gamma(\omega)^h}{\Gamma(h\omega)}\,N^{h\omega-1} + O_R\left(\frac{N^{h\omega-1}}{(\log N)^R}\right)$$

for every $R>1$. Here, $\mathfrak{S}^*_{k,h}(N)$ is the singular series associated to Waring–Goldbach's problem, defined as

$$S(a,q) := \sum_{r=1}^{q} e\left(\frac{ar^k}{q}\right), \qquad \mathfrak{S}^*_{k,h}(N) := \sum_{q\ge1}\sum_{\substack{a=1 \\ (a,q)=1}}^{q} \frac{S(q,a)^h}{\varphi(q)^h}e\left(-\frac{Na}{q}\right). \tag{5.13}$$

Fix $h \ge h_k^*$ an integer, let $\omega \ge 1/h$ be a real number, and N be a large integer. Define

$$T(\alpha;x) = \sum_{n\le x} n^{\omega}\frac{\mathbf{1}_{\mathbb{P}^k}(n)}{n^{1/k}/\log n}\,e(\alpha n), \qquad \widetilde{T}(\alpha;x) = \sum_{x/h\le n\le x} n^{\omega}\frac{\mathbf{1}_{\mathbb{P}^k}(n)}{n^{1/k}/\log n}\,e(\alpha n), \tag{5.14}$$

so that, by the orthogonality of the $e(N\alpha)$,

$$\sum_{\substack{x_1,\dots,x_h\in\mathbb{P}^k \\ x_1+\cdots+x_h=N}} (x_1\cdots x_h)^{\omega-\frac{1}{k}}(\log x_1\cdots\log x_h) = \int_0^1 T(\alpha;N)^h\,e(-N\alpha)\,\mathrm{d}\alpha.$$

If $x_1 + \cdots + x_h = N$, then $x_i \geq N/h$ for at least one x_i. Hence,

$$\int_0^1 (T(\alpha; N) - \widetilde{T}(\alpha; N))^h \, e(-N\alpha) \, \mathrm{d}\alpha = 0.$$

Therefore,

$$\begin{aligned}
&\sum_{\substack{x_1,\ldots,x_h \in \mathbb{P}^k \\ x_1+\cdots+x_h=N}} (x_1 \cdots x_h)^{\omega - \frac{1}{k}} (\log x_1 \cdots \log x_h) \\
&\qquad = \int_0^1 \Big(T(\alpha; N)^h - (T(\alpha; N) - \widetilde{T}(\alpha; N))^h \Big) \, e(-N\alpha) \, \mathrm{d}\alpha \\
&\qquad = \sum_{j=1}^{h} (-1)^{j+1} \binom{h}{j} \int_0^1 \widetilde{T}(\alpha; N)^j \, T(\alpha; N)^{h-j} \, e(-N\alpha) \, \mathrm{d}\alpha. \qquad (5.15)
\end{aligned}$$

By (5.15), Theorem 1.15 will follow from a combination of Propositions 5.11 and 5.19 below.

5.4.1. Major arcs

Let N be a large integer. As is standard in the circle method, we divide [0,1] into major arcs $\mathfrak{M}$ and minor arcs $\mathfrak{m}$, where the major arcs $\mathfrak{M} = \mathfrak{M}_N$ are defined as

$$\mathfrak{M} := \bigsqcup_{q \leq Q} \bigsqcup_{\substack{a=1 \\ (a,q)=1}}^{q} \mathfrak{M}(q,a), \quad \mathfrak{M}(q,a) := \left\{ \alpha \in [0,1] \;\middle|\; \left| \alpha - \frac{a}{q} \right| \leq \frac{Q}{N} \right\}$$

for a parameter $Q = Q(N) := (\log N)^C$, where $C > 1$ is a large fixed constant. The minor arcs are defined as the complement, $\mathfrak{m} = \mathfrak{m}_N := [0,1] \setminus \mathfrak{M}$. Splitting the integral in (5.15) as $\int_0^1 = \int_{\mathfrak{M}} + \int_{\mathfrak{m}}$, we anticipate that the contribution from the minor arcs is negligible (see subsection 5.4.2). The goal of this subsection is to prove the following:

Proposition 5.11 (Major arcs)**.** *We have*

$$\begin{aligned}
&\sum_{j=1}^{h} (-1)^{j+1} \binom{h}{j} \int_{\mathfrak{M}} \widetilde{T}(\alpha; N)^j \, T(\alpha;\, N)^{h-j} \, e(-N\alpha) \, \mathrm{d}\alpha \\
&\qquad\qquad = \mathfrak{S}^*_{k,h}(N) \, \frac{\Gamma(\omega)^h}{\Gamma(h\omega)} \, N^{h\omega - 1} + O_R\bigg(\frac{N^{h\omega-1}}{(\log N)^R} \bigg),
\end{aligned}$$

where $\mathfrak{S}^*_{k,h}(N)$ is as in (5.13)*, and $R(C) \to \infty$ as $C \to \infty$.*

5.4.1.1. Lemmas. Given $q \geq 1$, $1 \leq a \leq q$, define

$$\pi(x; q,a) := \sum_{\substack{n \leq x \\ n \equiv a(q)}} \mathbf{1}_{\mathbb{P}}(n).$$

We start with the classical estimate for primes in arithmetic progressions due to Siegel and Walfisz (cf. Montgomery–Vaughan [**25**, Corollary 11.21]).

Lemma 5.12 (Siegel–Walfisz)**.** *Uniformly for $q \le Q$, $1 \le a \le q$ with $(a,q) = 1$, we have*

$$\pi(x;q,a) = \left(1 + O_{C,R}\left(\frac{1}{(\log x)^R}\right)\right)\frac{\mathrm{li}(x)}{\varphi(q)}$$

for every $R > 1$, where $\mathrm{li}(x) = \int_{2^-}^{x} (\log t)^{-1}\,\mathrm{d}t$.

Corollary 5.13. *Uniformly for $q \le Q$, $1 \le a \le q$ with $(a,q) = 1$, we have*

$$\sum_{\substack{n \le x \\ n \equiv a(q)}} n^{\omega}\frac{\mathbf{1}_{\mathbb{P}^k}(n)}{n^{1/k}/\log n} = \left(1 + O_{C,R}\left(\frac{1}{(\log x)^R}\right)\right)\frac{P_k(q,a)}{\varphi(q)}\frac{x^{\omega}}{\omega},$$

for every $R > 1$, where $P_k(q,a) := |\{1 \le r \le q \mid r^k \equiv a \pmod{q}\}|$.

Proof. Write $P = P_k(q,a)$, and let $1 \le r_1, \ldots, r_P \le q$ be such that $r_i^k \equiv a \pmod{q}$. Since $\{n \le x \mid n \in \mathbb{P}^k, n \equiv a \pmod{q}\} = \sum_{i=1}^{P} \pi(x^{1/k};q,r_i)$, we have

$$\begin{aligned}\sum_{\substack{n \le x \\ n \equiv a(q)}} n^{\omega}\frac{\mathbf{1}_{\mathbb{P}^k}(n)}{n^{1/k}/\log n} &= \sum_{i=1}^{P}\int_{2^-}^{x}\frac{t^{\omega}}{t^{1/k}/\log t}\,\mathrm{d}\pi(t^{1/k};q,r_i) \\ &= \frac{P}{\varphi(q)}\frac{x^{\omega}}{\omega} + \sum_{i=1}^{P}\int_{2^-}^{x}\frac{t^{\omega}}{t^{1/k}/\log t}\,\mathrm{d}\left(\pi(t^{1/k};q,r_i) - \frac{\mathrm{li}(t^{1/k})}{\varphi(q)}\right).\end{aligned}$$

By partial summation, Lemma 5.12 implies that

$$\begin{aligned}&\int_{2^-}^{x}\frac{t^{\omega}}{t^{1/k}/\log t}\,\mathrm{d}\left(\pi(t^{1/k};q,r_i) - \frac{\mathrm{li}(t^{1/k})}{\varphi(q)}\right) \\ &\qquad = \left(\pi(x^{1/k};q,r_i) - \frac{\mathrm{li}(x^{1/k})}{\varphi(q)}\right)\frac{x^{\omega}}{x^{1/k}/\log x} \\ &\qquad\quad - \int_{2^-}^{x}\left(\pi(t^{1/k};q,r_i) - \frac{\mathrm{li}(t^{1/k})}{\varphi(q)}\right)t^{\omega-\frac{1}{k}-1}(1 + (\omega - \tfrac{1}{k})\log t)\,\mathrm{d}t \\ &\qquad \ll_{C,R} \frac{x^{\omega}}{(\log x)^R},\end{aligned}$$

which, since $P \le k$, concludes the proof. □

Next, we prove a lemma ensures that the singular series $\mathfrak{S}^*_{k,h}(N)$ converges absolutely and is bounded away from 0 and ∞ for $N \equiv h \pmod{K(k)}$, where $K(k)$ is as in (5.22).

Lemma 5.14 (Singular series)**.** *For $N \equiv h \pmod{K(k)}$, we have $\mathfrak{S}^*_{k,h}(N) \asymp 1$. Moreover, let*

$$\mathfrak{S}^*_{k,h}(N,Q) := \sum_{q \le Q}\sum_{\substack{a=1 \\ (a,q)=1}}^{q}\frac{S(q,a)^h}{\varphi(q)^h}e\left(-\frac{Na}{q}\right),$$

where $S(q,a)$ *be as in* (5.7). *Then, for every* $\varepsilon > 0$,

$$\mathfrak{S}^*_{k,h}(N,Q) = \left(1 + O_\varepsilon\left(\frac{1}{Q^{1/k-\varepsilon}}\right)\right)\mathfrak{S}^*_{k,h}(N) \quad as \quad Q \to \infty.$$

Proof. By Lemmas 8.10 and 8.12 in Hua [**19**], we have $\mathfrak{S}^*_{k,\ell}(N) \gg 1$ for $N \equiv h \pmod{K(k)}$ whenever $\ell \geq 3$ for $k = 1$, $\ell \geq 5$ for $k = 2$, and $\ell \geq 3k$ for $k \geq 3$. In all cases, this holds true for $h \geq h^*_k$.

For the second part, let $q \geq 1$, $1 \leq a \leq q$ with $(a,q) = 1$. By [**19**, Theorem 1], we have $S(q,a) \ll_\varepsilon q^{1-1/k+\varepsilon}$ uniformly in q. Thus, since $\varphi(q) \gg_\varepsilon q^{1-\varepsilon}$ and $h \geq h^*_k \geq 2k+1$, we have

$$\begin{aligned} |\mathfrak{S}^*_{k,h}(N) - \mathfrak{S}^*_{k,h}(N,Q)| &\leq \sum_{q>Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left|\frac{S(q,a)^h}{\varphi(q)^h}\right| \\ &\ll_\varepsilon \sum_{q>Q} (q^{-1/k+\varepsilon})^h\, q \\ &\ll_\varepsilon \sum_{q>Q} q^{-1-1/k+\varepsilon} \asymp Q^{-1/k+\varepsilon}. \end{aligned}$$

□

5.4.1.2. Integral over major arcs. In order to calculate the integral in Proposition 5.11, we will approximate T and $\widetilde{T}$ in terms of, respectively,

$$u(\vartheta;x) := \sum_{n\leq x} n^{\omega-1} e(n\vartheta), \qquad \widetilde{u}(\vartheta;x) := \sum_{n\leq x} n^{\omega-1} e(n\vartheta). \tag{5.16}$$

Lemma 5.15. *Let* $q \leq Q$, *and* $1 \leq a \leq q$ *with* $(a,q) = 1$. *For* $\alpha \in \mathfrak{M}(q,a)$, *write* $\vartheta := \alpha - \frac{a}{q}$. *Then, for every* $R > 1$, *we have*

$$\begin{aligned} T(\alpha;N) &= \frac{S(q,a)}{\varphi(q)} u(\vartheta;N) + O_R\left(\frac{N^\omega}{(\log N)^R}\right), \\ \widetilde{T}(\alpha;N) &= \frac{S(q,a)}{\varphi(q)} \widetilde{u}(\vartheta;N) + O_R\left(\frac{N^\omega}{(\log N)^R}\right) \end{aligned}$$

uniformly in $q \leq Q$.

Proof. We prove the lemma for T; the argument for $\widetilde{T}$ is analogous. By Lemma 5.13, we have

$$\begin{aligned} T\left(\frac{a}{q};x\right) &= \sum_{n\leq x} n^\omega \frac{\mathbf{1}_{\mathbb{P}^k}(n)}{n^{1/k}/\log n} e\left(\frac{na}{q}\right) \\ &= \sum_{\substack{r=1 \\ (r,q)=1}}^{q} \left(\sum_{\substack{n\leq x \\ n\equiv r(q)}} n^\omega \frac{\mathbf{1}_{\mathbb{P}^k}(n)}{n^{1/k}/\log n}\right) e\left(\frac{ra}{q}\right) + O(Q) \\ &= \left(\sum_{\substack{r=1 \\ (r.q)=1}}^{q} P_k(q,r)\, e\left(\frac{ra}{q}\right)\right) \frac{1}{\varphi(q)} \frac{x^\omega}{\omega} + O_R\left(\frac{x^\omega}{(\log x)^R}\right) \end{aligned}$$

$$= \frac{S(q,a)}{\varphi(q)}\frac{x^\omega}{\omega} + O_R\biggl(\frac{x^\omega}{(\log x)^R}\biggr). \tag{5.17}$$

(Note that $\widetilde{T}(\frac{a}{q};x) = T(\frac{a}{q};x) - T(\frac{a}{q};\frac{x}{h}-1)$.) We have

$$T(\alpha;N) - \frac{S(q,a)}{\varphi(q)}u(\vartheta;N) = \sum_{n\le N}\underbrace{\biggl(n^\omega\frac{\mathbf{1}_{\mathbb{P}}(n)}{n^{1/k}/\log n}e\Bigl(\frac{na}{q}\Bigr) - \frac{S(q,a)}{\varphi(q)}n^{\omega-1}\biggr)}_{=:\,D(n)}e(n\vartheta)$$

By (5.17), and the fact that $\sum_{n\le t} n^{\omega-1} = \frac{t^\omega}{\omega} + O(1)$, we have $\sum_{n\le t} D(n) = O_R(t/(\log t)^R)$. By using partial summation we conclude, since $|\vartheta| \le Q/N = (\log N)^C/N$, that

$$\begin{aligned} T(\alpha;N) - \frac{S(q,a)}{\varphi(q)}u(\vartheta;N) &= \biggl(\sum_{n\le N} D(n)\biggr)e(N\vartheta) - 2\pi i\vartheta\int_1^N\biggl(\sum_{n\le t} D(n)\biggr)e(t\vartheta)\,\mathrm{d}t \\ &\ll \biggl|\sum_{n\le N} D(n)\biggr| + N|\vartheta|\max_{t\le N}\biggl(\sum_{n\le t} D(n)\biggr) \\ &= O_R\biggl(\frac{N^\omega}{(\log N)^R}\biggr). \end{aligned}$$

□

Lemma 5.16. *For $-\frac{1}{2} \le \vartheta \le \frac{1}{2}$, $\vartheta \ne 0$, we have*

$$|u(\vartheta;N)| \ll \min\{N^\omega, |\vartheta|^{-\omega}\}, \qquad |\widetilde{u}(\vartheta;N)| \ll N^{\omega-1}|\vartheta|^{-1},$$

Proof. We have $|u(\vartheta;N)| \le u(0;N) = \frac{1}{\omega}N^\omega + O(1)$. On the other hand, let $M := \lfloor|\vartheta|^{-1}\rfloor$, so that

$$|u(\vartheta;N)| \le \sum_{n\le M} n^{\omega-1} + \biggl|\sum_{n=M+1}^{N} n^{\omega-1}e(n\vartheta)\biggr| \ll M^\omega + \biggl|\sum_{n=M+1}^{N} n^{\omega-1}e(n\vartheta)\biggr|. \tag{5.18}$$

Let $E(x) := \sum_{n\le x} e(n\vartheta)$. Since $|1-e(\vartheta)| = |e(-\vartheta/2) - e(\vartheta/2)| = 2|\sin\pi\vartheta| \ge 2|\vartheta|$ for ϑ in the range considered, we have

$$|E(x)| = \biggl|\sum_{n\le x} e(n\vartheta)\biggr| = \biggl|\frac{1-e((\lfloor x\rfloor+1)\vartheta)}{1-e(\vartheta)}\biggr| \le \frac{1}{|\vartheta|^{-1}}.$$

By using that $E(x) \ll |\vartheta|^{-1}$, we obtain from partial summation that

$$\begin{aligned} \sum_{n=M+1}^{N} n^{\omega-1}e(n\vartheta) &= N^{\omega-1}E(N) - M^{\omega-1}E(M) - (\omega-1)\int_M^N E(t)t^{\omega-2}\,\mathrm{d}t \\ &\ll (N^{\omega-1} + M^{\omega-1})\,|\vartheta|^{-1} \ll M^\omega \asymp |\vartheta|^{-\omega}, \end{aligned}$$

so the result follows from (5.18).

Similarly, for $\widetilde{u}$, we have

$$\widetilde{u}(\vartheta;N) = \sum_{N/h\le n\le N} n^{\omega-1}e(n\vartheta)$$

$$= N^{\omega-1}E(N) - \left(\frac{N}{h}\right)^{\omega-1} E(N/h) - (\omega-1)\int_{N/h}^{N} E(t)t^{\omega-2}\,\mathrm{d}t$$
$$\ll N^{\omega-1}|\vartheta|^{-1}. \qquad \square$$

Lemma 5.17. *For $1 \le j \le h$, we have, for every $\varepsilon > 0$,*

$$\int_{\mathfrak{M}} \widetilde{T}(\alpha;N)^j\, T(\alpha;N)^{h-j}\, e(-N\alpha)\,\mathrm{d}\alpha$$
$$= \left(1 + O_\varepsilon\left(\frac{1}{(\log N)^{C/k-\varepsilon}}\right)\right)\mathfrak{S}^*_{k,h}(N)\int_0^1 \widetilde{u}(\vartheta;N)^j\, u(\vartheta;N)^{h-j}\, e(-N\vartheta)\,\mathrm{d}\vartheta$$
$$+ O\left(\frac{N^{h\omega-1}}{(\log N)^{C(h-1)\omega}}\right).$$

Proof. Since $|u(\vartheta;N)| \le u(0;N) = \frac{1}{\omega}N^\omega + O(1)$, Lemma 5.15 implies that

$$T(\alpha;N)^h = \frac{S(q,a)^h}{\varphi(q)^h}u(\vartheta;N)^h + O_R\left(\frac{N^{h\omega}}{(\log N)^R}\right),$$

and similarly for $\widetilde{T}$, $\widetilde{u}$. Using that $\int_{\mathfrak{M}(q,a)}\mathrm{d}\alpha = 2Q/N$, this leads to the estimate

$$\int_{\mathfrak{M}} \widetilde{T}(\alpha;N)^j\, T(\alpha;N)^{h-j}\, e(-N\alpha)\,\mathrm{d}\alpha$$
$$= \sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} \widetilde{T}(\alpha;N)^j\, T(\alpha;N)^{h-j}\, e(-N\alpha)\,\mathrm{d}\alpha$$
$$= \sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q} \frac{S(q,a)^h}{\varphi(q)^h}\int_{\mathfrak{M}(q,a)} \widetilde{u}\left(\alpha-\frac{a}{q};N\right)^j u\left(\alpha-\frac{a}{q};N\right)^{h-j} e(-N\alpha)\,\mathrm{d}\alpha$$
$$+ O_R\left(\frac{QN^{\omega h-1}}{(\log N)^R}\right)$$
$$= \underbrace{\sum_{q\le Q}\sum_{\substack{a=1\\(a,q)=1}}^{q} \frac{S(q,a)^h}{\varphi(q)^h} e\left(-\frac{Na}{q}\right)}_{=\mathfrak{S}_h(N,Q)} \int_{-Q/N}^{Q/N} \widetilde{u}(\vartheta;N)^j u(\vartheta;N)^{h-j}\, e(-N\vartheta)\,\mathrm{d}\vartheta$$
$$+ O_R\left(\frac{N^{\omega h-1}}{(\log N)^R}\right)$$
$$= \left(1 + O_\varepsilon\left(\frac{1}{(\log N)^{C/k-\varepsilon}}\right)\right)\mathfrak{S}^*_{k,h}(N)\int_{-Q/N}^{Q/N} \widetilde{u}(\vartheta;N)^j u(\vartheta;N)^{h-j}\, e(-N\vartheta)\,\mathrm{d}\vartheta$$
$$+ O_R\left(\frac{N^{\omega h-1}}{(\log N)^R}\right),$$

where the last line follows from Lemma 5.14. By Lemma 5.16, we have

$$\left|\int_{[-\frac12,-\frac{Q}{N}]\cup[\frac{Q}{N},\frac12]} \widetilde{u}(\vartheta;N)^j u(\vartheta;N)^{h-j} e(-N\vartheta)\,\mathrm{d}\vartheta\right| \le \int_{[-\frac12,-\frac{Q}{N}]\cup[\frac{Q}{N},\frac12]} |\widetilde{u}(\vartheta;N)|^j\, |u(\vartheta;N)|^{h-j}\,\mathrm{d}\vartheta$$

$$\ll \frac{N^{j\omega}}{Q^j}\int_{Q/N}^{1/2}\vartheta^{-(h-j)\omega}\,\mathrm{d}\vartheta$$
$$\ll \frac{N^{h\omega-1}}{Q^{h\omega-1+j(1-\omega)}} \ll \frac{N^{h\omega-1}}{Q^{(h-1)\omega}}.$$

Since $\mathfrak{S}^*_{k,h}(N) \asymp 1$, this finishes the proof. □

5.4.1.3. The singular integral. Lemma 5.17 reduces Proposition 5.11 to the calculation of the integral in u, $\tilde{u}$ that appears in its statement, which is done in the following lemma:

Lemma 5.18. *We have*

$$\sum_{j=1}^{h}(-1)^{j+1}\binom{h}{j}\int_0^1 \tilde{u}(\vartheta;N)^j\,u(\vartheta;N)^{h-j}\,e(-N\vartheta)\,\mathrm{d}\vartheta = (1+O(N^{-\omega}))\frac{\Gamma(\omega)^h}{\Gamma(h\omega)}N^{h\omega-1}$$

Proof. By the same argument used to obtain (5.15), we deduce from (5.16) that

$$\sum_{j=1}^{h}(-1)^{j+1}\binom{h}{j}\int_0^1 \tilde{u}(\vartheta;N)^j\,u(\vartheta;N)^{h-j}\,e(-N\vartheta)\,\mathrm{d}\vartheta = \int_0^1 u(\vartheta;N)^h\,e(-N\vartheta)\,\mathrm{d}\vartheta$$
$$= \sum_{\substack{x_1,\ldots,x_h\in\mathbb{Z}_{\geq 1}\\ x_1+\cdots+x_h=N}}(x_1\cdots x_h)^{\omega-1},$$

For $\ell \geq 2$ and $n \in \mathbb{Z}_{\geq 1}$, we claim that

$$S_\ell(n) := \sum_{\substack{x_1,\ldots,x_\ell\in\mathbb{Z}_{\geq 1}\\ x_1+\cdots+x_\ell=n}}(x_1\cdots x_\ell)^{\omega-1} = \frac{\Gamma(\omega)^\ell}{\Gamma(\ell\omega)}n^{\ell\omega-1} + O(n^{(\ell-1)\omega-1}), \tag{5.19}$$

which will finish the proof. The case $\ell = 2$ is a consequence of Lemma 2.9 of Vaughan [**38**], which says that

$$\sum_{m=1}^{n-1} m^{a-1}(n-m)^{b-1} = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}n^{a+b-1} + O_{a,b}(n^{a-1}) \tag{5.20}$$

for any real numbers $a \geq b > 0$. Assuming by induction that (5.19) holds for some $\ell \geq 2$, we obtain from (5.20) that

$$\begin{aligned}
S_{\ell+1}(n) &= \sum_{\substack{x_1,\ldots,x_\ell\in\mathbb{Z}_{\geq 1}\\ x_1+\cdots+x_\ell\leq n}}(x_1\cdots x_\ell)^{\omega-1}\Big(n-(x_1+\cdots+x_\ell)\Big)^{\omega-1}\\
&= \sum_{m=1}^{n-1} S_\ell(m)\,(n-m)^{\omega-1}\\
&= \frac{\Gamma(\omega)^\ell}{\Gamma(\ell\omega)}\sum_{m=1}^{n-1} m^{\ell\omega-1}(n-m)^{\omega-1} + O\left(\sum_{m=1}^{n-1} m^{(\ell-1)\omega-1}(n-m)^{\omega-1}\right)\\
&= \frac{\Gamma(\omega)^{\ell+1}}{\Gamma((\ell+1)\omega)}n^{(\ell+1)\omega-1} + O(n^{\ell\omega-1}),
\end{aligned}$$

concluding the proof. ☐

Proof of Proposition 5.11. Since both $C/2^{k-1}-\varepsilon\to\infty$ and $C(h-1)\omega\to\infty$ as $C\to\infty$, by Lemmas 5.17 and 5.18, we have

$$\begin{aligned}
&\sum_{j=1}^{h}(-1)^{j+1}\binom{h}{j}\int_{\mathfrak{M}}\widetilde{T}(\alpha;N)^j\,T(\alpha;N)^{h-j}\,e(-N\alpha)\,\mathrm{d}\alpha\\
&=\left(1+O_R\left(\frac{1}{(\log N)^R}\right)\right)\mathfrak{S}^*_{k,h}(N)\sum_{j=1}^{h}(-1)^{j+1}\binom{h}{j}\int_0^1\widetilde{u}(\vartheta;N)^j\,u(\vartheta;N)^{h-j}\,e(-N\vartheta)\,\mathrm{d}\vartheta\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad+O\left(\frac{N^{h\omega-1}}{(\log N)^R}\right)\\
&=\left(1+O\left(\frac{1}{(\log N)^R}\right)\right)(1+O(N^{-\omega}))\mathfrak{S}^*_{k,h}(N)\frac{\Gamma(\omega)^h}{\Gamma(h\omega)}N^{h\omega-1}+O\left(\frac{N^{h\omega-1}}{(\log N)^R}\right),
\end{aligned}$$

where $R=R(C)\to\infty$ as $C\to\infty$. Since $\mathfrak{S}^*_{k,h}(N)\ll 1$ by Lemma 5.14, rearranging the error terms concludes the proof. ☐

5.4.2. Minor arcs

We now turn our attention to the minor arcs $\mathfrak{m}$, as defined in the beginning of the last subsection. Together with (5.15) and Proposition 5.11, the next result directly implies Theorem 1.15.

Proposition 5.19 (Minor arcs)**.** *We have*

$$\sum_{j=1}^{h}\left|\int_{\mathfrak{m}}\widetilde{T}(\alpha;N)^j\,T(\alpha;N)^{h-j}\,e(-N\alpha)\,\mathrm{d}\alpha\right|\ll_R\frac{N^{h\omega-1}}{(\log N)^R},$$

where $R=R(C)\to\infty$ as $C\to\infty$.

5.4.2.1. Lemmas. Define the function

$$g(\alpha;x):=\sum_{n\le x}\mathbf{1}_{\mathbb{P}^k}(n)e(n\alpha).$$

The first lemma we need is equivalent to showing that $\mathbb{P}^k$ satisfies condition (ii) of Theorem 1.17 with $H_{(\mathrm{ii})}\le\frac{1}{2}h_k^*-1$.

Lemma 5.20 (Mean-value estimate)**.** *There exists $\xi\in\mathbb{R}$ such that, for every*

$$\ell\ge h_0:=\begin{cases}2^{k-1} & \text{if } 1\le k\le 11,\\ \lceil k^2(2\log k+\log\log k+2.5)\rceil-2 & \text{if } k\ge 12,\end{cases}$$

we have

$$\sum_{n\le x}r_{\mathbb{P}^k,\ell}(n)^2\ll x^{2\ell/k-1}(\log x)^{\xi}.$$

Proof. By Parseval's identity, we have

$$\sum_{n\le x} r_{\mathbb{P}^k,\ell}(n)^2 \le \int_0^1 |g(\alpha;x)|^{2\ell}\,\mathrm{d}\alpha \le \sum_{n\le \ell x} r_{\mathbb{P}^k,\ell}(n)^2,$$

where the middle term, by the orthogonality of the $e(\alpha n)$, counts the number of solutions to the equation

$$n_1 + \cdots + n_\ell = m_1 + \cdots + m_\ell \tag{5.21}$$

with $n_i,m_j \le x$ and $n_i,m_j \in \mathbb{P}^k$.

For $1 \le k \le 11$, by Hua's inequality (cf. Hua [**19**, Theorem 4]), there exists $c(k) \in \mathbb{R}$ such that

$$\int_0^1 \left| \sum_{1\le n\le x} e(\alpha n^k) \right|^{2\ell} \mathrm{d}\alpha \ll x^{2\ell-k}(\log x)^{c(k)}.$$

for every $\ell \ge 2^{k-1}$. In other words, the number of solutions to (5.21) with $n_i,m_j \le x$, $n_i,m_j \in \mathbb{N}^k$ is $O(x^{2^k/k-1}(\log x)^{c(k)})$, which is an upper bound to the number of solutions with $n_i,m_j \in \mathbb{P}^k$. Therefore, since $|g(\alpha;x)| \le g(0;x) \asymp x^{1/k}/\log x$, for $\ell \ge 2^{k-1}$ we have

$$\begin{aligned}\int_0^1 |g(\alpha;x)|^{2\ell}\,\mathrm{d}\alpha &\le |g(0;x)|^{2\ell-2^k} \int_0^1 |g(\alpha;x)|^{2^k}\,\mathrm{d}\alpha \\ &\ll \left(\frac{x^{1/k}}{\log x}\right)^{2\ell-2^k} x^{2^k/k-1}(\log x)^{c(k)} \\ &\ll x^{2\ell/k-1}(\log x)^{c(k)}.\end{aligned}$$

For $k \ge 12$, by [**19**, Lemma 7.13] we have

$$\int_0^1 \left| \sum_{1\le n\le x} e(\alpha n^k) \right|^{2\ell} \mathrm{d}\alpha \ll x^{2\ell-k}$$

for every $\ell > k^2(2\log k + \log\log k + 2.5) - 2$, so the lemma follows by the same argument as above. ☐

Next, we bound the value of $g(\alpha;x)$ for $\alpha \in \mathfrak{m}$. To this end, we employ a lemma due to Harman, in the form stated by Kumchev–Tolev [**22**, Lemma 3.3].

Lemma 5.21 (Harman [**18**])**.** *Let $\alpha \in [0,1]$ be such that $|\alpha - \frac{a}{q}| \le q^{-2}$, where a, q are integers with $1 \le q \le x$ and $(a,q) = 1$. Then, there exists a constant $G = G(k) > 0$ such that*

$$g(\alpha;x) \ll \left(q^{-1} + x^{-1/2k} + q^{1/2}x^{-1}\right)^{4^{1-k}} x^{1/k}(\log x)^G$$

Corollary 5.22. $\sup_{\alpha\in\mathfrak{m}} |g(\alpha;N)| \ll \dfrac{N^{1/k}}{(\log N)^{4^{1-k}C-G}}.$

Proof. By Dirichlet's theorem (cf. Nathanson [**27**, Theorem 4.1]), for any $\alpha \in [0,1]$ there exists $1 \le q \le N/Q$ and $0 \le a \le q$ such that

$$\left|\alpha - \frac{a}{q}\right| \le \frac{Q}{qN} \le \min\left(\frac{Q}{N},\frac{1}{q^2}\right).$$

Since $\alpha \in \mathfrak{m}$, we must have $q > Q$ (otherwise, $\alpha \in \mathfrak{M}_N(q,a)$ by definition), so $Q < q \le N/Q$. Hence, by Lemma 5.21,

$$\begin{aligned} g(\alpha; N) &\ll \left(Q^{-1} + N^{-1/2k} + \left(\frac{N}{Q}\right)^{1/2} N^{-1}\right)^{4^{1-k}} N^{1/k}(\log N)^G \\ &\ll \frac{N^{1/k}}{Q(\log N)^{-G}} = \frac{N^{1/k}}{(\log N)^{4^{1-k}C-G}}. \end{aligned}$$ □

5.4.2.2. Integral over minor arcs. In order to prove Proposition 5.19, we first need two auxiliary lemmas concerning the integral of $\widetilde{T}$.

Lemma 5.23. *Let h_0, ξ be as in Lemma 5.20. For $\ell \ge 2h_0$, we have*

$$\int_0^1 |\widetilde{T}(\alpha; x)|^\ell \,\mathrm{d}\alpha \ll x^{\ell\omega-1}(\log x)^{\xi+2h_0}.$$

Proof. The integral $\int_0^1 |\widetilde{T}(\alpha; x)|^{2\ell} \,\mathrm{d}\alpha$ counts the number of solutions to the Diophantine equation (5.21) with weights

$$(n_1 \dots n_\ell m_1 \cdots m_\ell)^{\omega-\frac{1}{k}}(\log n_1)\cdots(\log n_\ell)(\log m_1)\cdots(\log m_\ell) \ll \left(\frac{x^\omega}{x^{1/k}/\log x}\right)^{2\ell},$$

for $x/h \le n_i,m_j \le x$. Thus, by considering this underlying equation, Lemma 5.20 yields the upper bound

$$\int_0^1 |\widetilde{T}(\alpha; x)|^{2\ell} \,\mathrm{d}\alpha \ll \frac{x^{2\ell\omega}}{(x^{1/k}/\log x)^{2\ell}} \int_0^1 |g(\alpha; x)|^{2\ell} \,\mathrm{d}\alpha \ll x^{2\ell\omega-1}(\log x)^{\xi+2\ell}.$$

Using the trivial estimate

$$|\widetilde{T}(\alpha; x)| \le \widetilde{T}(0; x) \ll x^{\omega-\frac{1}{k}}(\log x) \sum_{x/2\le n\le x} \mathbf{1}_{\mathbb{P}^k}(n) \ll x^\omega,$$

for $\ell \ge 2h_0$ we get

$$\int_0^1 |\widetilde{T}(\alpha; x)|^\ell \,\mathrm{d}\alpha \ll x^{(\ell-2h_0)\omega} \int_0^1 |\widetilde{T}(\alpha; x)|^{2h_0} \,\mathrm{d}\alpha \ll x^{\ell\omega-1}(\log x)^{\xi+2h_0}.$$ □

Lemma 5.24. *We have*

$$\int_{\mathfrak{m}} |\widetilde{T}(\alpha; N)|^h \,\mathrm{d}\alpha \ll \frac{N^\omega}{(\log N)^{r(C)}},$$

where $r(C) \to \infty$ as $C \to \infty$.

Proof. By Corollary 5.22, for $\alpha \in \mathfrak{m}$, partial summation yields

$$\begin{aligned}
&\widetilde{T}(\alpha;N)\\
&\quad= \frac{N^\omega}{N^{1/k}/\log N} g(\alpha;N) - \frac{(N/h)^\omega}{(N/h)^{1/k}/(\log N/h)} g(\alpha;N/h) - \int_{N/h}^{N} g(\alpha;t)\,\mathrm{d}\!\left(\frac{t^\omega}{t^{1/k}/\log t}\right)\\
&\quad\ll N^{\omega-\frac{1}{k}}(\log N)\,\frac{N^{1/k}}{(\log N)^{4^{1-k}C-G}} = \frac{N^\omega}{(\log N)^{4^{1-k}C-G-1}}.
\end{aligned}$$

Since $h \geq h_k^* \geq 2h_0+1$, where h_0 is as in Lemma 5.20, it follows from Lemma 5.23 that

$$\begin{aligned}
\int_{\mathfrak{m}} |\widetilde{T}(\alpha;N)|^h \,\mathrm{d}\alpha &\leq \left(\sup_{\alpha\in\mathfrak{m}} |\widetilde{T}(\alpha;N)|^{h-2h_0}\right) \int_0^1 |\widetilde{T}(\alpha;N)|^{2h_0}\,\mathrm{d}\alpha\\
&\ll \left(\frac{N^\omega}{(\log N)^{4^{1-k}C-G-1}}\right)^{h-2h_0} N^{2h_0\omega-1}(\log N)^{\xi+2h_0}\\
&= \frac{N^{h\omega-1}}{(\log N)^{r(C)}},
\end{aligned}$$

where $r(C) = (h-h_0)(4^{1-k}C-G-1)-\xi-2h_0$. □

Proof of Proposition 5.19. The series $T(\alpha;N)$ can be written as

$$T(\alpha;N) = \sum_{j\leq \frac{\log N}{\log h}} \widetilde{T}'(\alpha;h^{-j}N).$$

where $\widetilde{T}'(\alpha;x) := \sum_{x/h<n\leq x} n^\omega \frac{\mathbf{1}_{\mathbb{P}^k}(n)}{n^{1/k}/\log n}\, e(\alpha n)$. Clearly, both Lemmas 5.23 and 5.24 apply to $\widetilde{T}'$ as well. Therefore, by Hölder's inequality[1] and Lemma 5.23, it follows that

$$\begin{aligned}
\int_0^1 |T(\alpha;N)|^h\,\mathrm{d}\alpha &\leq (\log N)^{h-1}\int_0^1 \left(\sum_{j\leq\frac{\log N}{\log h}} |\widetilde{T}'(\alpha;h^{-j}N)|^h\right)\mathrm{d}\alpha\\
&\ll (\log N)^h \max_{j\leq\frac{\log N}{\log h}} \int_{\mathfrak{m}} |\widetilde{T}'(\alpha;h^{-j}N)|^h\,\mathrm{d}\alpha\\
&\ll (\log N)^{h+\xi+2h_0}\, N^{h\omega-1}.
\end{aligned}$$

By Lemma 5.24, another application of Hölder's inequality yields

$$\begin{aligned}
&\sum_{j=1}^{h}\left|\int_{\mathfrak{m}} \widetilde{T}(\alpha;N)^j\, T(\alpha;N)^{h-j}\, e(-N\alpha)\,\mathrm{d}\alpha\right|\\
&\qquad\leq \sum_{j=1}^{h}\left(\int_{\mathfrak{m}} |\widetilde{T}(\alpha;N)|^h\,\mathrm{d}\alpha\right)^{j/h}\left(\int_0^1 |T(\alpha;N)|^h\,\mathrm{d}\alpha\right)^{1-j/h}\\
&\qquad\leq \sum_{j=1}^{h}\left(\frac{N^{h\omega-1}}{(\log N)^{r(C)}}\right)^{j/h}\left((\log N)^{h+\xi+2h_0}N^{h\omega-1}\right)^{1-j/h}
\end{aligned}$$

[1]With "$p = h$", "$q = h/(h-1)$".

$$\ll \frac{N^{h\omega-1}}{(\log N)^{r(C)/h-(h+\xi+2h_0)(h-1)/h}}.$$

Writing $R = R(C) := r(C)/h - (h+\xi+2h_0)(h-1)/h$, we see that choosing C large, R can be taken to be as large as desired, concluding the proof. ☐

5.5. Waring–Goldbach subbases

We are now in shape to prove Theorem 1.16. Given a prime p, let $\theta = \theta(k,p)$ be the unique integer such that $p^\theta \mid k$ but $p^{\theta+1} \nmid k$. Define

$$\gamma = \gamma(k,p) := \begin{cases} \theta+2 & \text{if } p=2, 2 \mid k, \\ \theta+1 & \text{otherwise,} \end{cases} \qquad K(k) := \prod_{(p-1)\mid k} p^\gamma. \tag{5.22}$$

Theorem 1.16 *Let $k \geq 1$ be an integer, $h \geq h_k^*$ where h_k^* is as in* (5.12)*, and suppose that $n \equiv h \pmod{K(k)}$, where $K(k)$ is as in* (5.22)*.*

(i) *For every $0 < \kappa < h/k - 1$ and $c > 0$, there exists a subset $A \subseteq \mathbb{P}^k$ such that*

$$r_{A,h}(n) \sim \mathfrak{S}^*_{k,h}(n)\, cn^\kappa,$$

where $\mathfrak{S}^*_{k,h}(n)$ is the singular series for Waring–Goldbach's problem (5.13)*.*

(ii) *Let $0 \leq \kappa \leq h/k-1$, ψ be a measurable positive real function satisfying $\psi(x) \asymp_\lambda \psi(x^\lambda)$ for every $\lambda > 0$, and write $F(x) = x^\kappa\psi(x)$. If $\log x \ll F(x) \ll x^{h/k-1}/(\log x)^h$, then there exists a subset $A \subseteq \mathbb{P}^k$ such that*

$$r_{A,h}(n) \asymp F(n).$$

By the prime number theorem, $|\mathbb{P}^k \cap [1,x]| \sim kx^{1/k}/(\log x)$, which is a regularly varying function, so $\mathbb{P}^k$ satisfies condition (i) of Theorem 1.17. By Lemma 5.20, $\mathbb{P}^k$ also satisfies condition (ii), with $H_{\text{(ii)}} \leq \frac{1}{2}h_k^* - 1$.

For condition (iii), we claim that $H_{\text{(iii)}} \leq h_k^*$ for the functions considered in Theorem 1.16. Let $h \geq h_k^*$, and $F(x) = x^\kappa\psi(x)$ be a regularly varying function with

$$F(x) \leq (1+o(1))\frac{\Gamma(1/k)^h}{\Gamma(h/k)}\frac{x^{h/k-1}}{(\log x)^h}.$$

Note that the upper bound for F comes from the total number of representations of n as a sum of h k-th powers of primes (cf. Hua [**19**, Theorem 11]). Define $f(x) := (xF(x))^{1/h}$, so that $f(x) \ll (1+o(1))\pi(x^{1/k}) \asymp x^{1/k}/(\log x)$. For the $\eta = \eta(f,k,h)$ of Proposition 5.2, we have

$$\sum_{\substack{x_1,\ldots,x_h \in \mathbb{P}^k \\ x_1+\cdots+x_h=n \\ \exists i \,\mid\, x_i<n^{\eta/2}}} \frac{f(x_1)}{\pi(x_1^{1/k})}\cdots\frac{f(x_h)}{\pi(x_h^{1/k})} \leq \sum_{m\leq n^{\eta/2}} \frac{f(m)}{\pi(m^{1/k})} \sum_{\substack{x_1,\ldots,x_{h-1}\in\mathbb{P}^k \\ x_1+\cdots+x_{h-1}=n-m}} \frac{f(x_1)}{\pi(x_1^{1/k})}\cdots\frac{f(x_{h-1})}{\pi(x_{h-1}^{1/k})}$$

$$\ll n^{\eta/2}\, n^{-\eta}\frac{f(n)^h}{n} = n^{-\eta/2}F(n),$$

therefore

$$\sum_{\substack{x_1,\dots,x_h\in\mathbb{P}^k\\ x_1+\cdots+x_h=n}} \frac{f(x_1)}{\pi(x_1^{1/k})}\cdots\frac{f(x_h)}{\pi(x_h^{1/k})} = \sum_{\substack{x_1,\dots,x_h\in\mathbb{P}^k\\ x_1+\cdots+x_h=n\\ \forall i,\, x_i\geq n^{\eta/2}}} \frac{f(x_1)}{\pi(x_1^{1/k})}\cdots\frac{f(x_h)}{\pi(x_h^{1/k})} + O(n^{-\eta/2}F(n))$$

$$= (1+o(1))\frac{1}{k^h}\sum_{\substack{x_1,\dots,x_h\in\mathbb{P}^k\\ x_1+\cdots+x_h=n\\ \forall i,\, x_i\geq n^{\eta/2}}} \frac{f(x_1)}{x_1^{1/k}}\cdots\frac{f(x_h)}{x_h^{1/k}}(\log x_1\cdots\log x_h) + O(n^{-\eta/2}F(n)) \tag{5.23}$$

Choosing $F(x) := cx^\kappa$ with $0<\kappa<h/k-1$ and $c>0$, we get $f(x) = c^{1/h}x^\omega$ with $\omega = (1+\kappa)/h$, so $1/h<\omega<1/k$. Therefore, Theorem 1.15 together with (5.23) implies that for such F, $\mathbb{P}^k$ satisfies condition (iii).

Choose $F(x) := x^\kappa\psi(x)$ for some $0\leq\kappa\leq h/k-1$ and some measurable positive real function ψ satisfying $\psi(x)\asymp_\lambda \psi(x^\lambda)$ for every $\lambda>0$. Suppose that $\log n \ll F(n) \ll x^{h/k-1}/(\log n)^h$. We have $f(x) = x^{(1+\kappa)/h}\psi(x)^{1/h}$, where $1/h\leq(1+\kappa)/h\leq 1/k$. By uniform convergence,[2] it follows that $\psi(x_i)\asymp\psi(n)$ for $n^{\eta/2}\leq x_i\leq n$, so Theorem 1.15 implies that the sum in (5.23) is $\asymp n^\kappa\psi(n)$ for $n\equiv h \pmod{K(k)}$. Using the fact that $\psi\asymp\phi$ for some ϕ of regular variation (see Remark 5.25), we can apply Theorem 1.17 to $x^\kappa\phi(x)$ instead, so that this fits into condition (iii) (with "$\mathfrak{S}_{B,h}(n)$" different from $\mathfrak{S}^*_{k,h}(n)$, but still $\asymp 1$).

Since $\max\{2H_{(\mathrm{ii})}+1, H_{(\mathrm{iii})}\}\leq h^*_k$, the conclusion of Theorem 1.16 follows.

Remark 5.25. In order to apply Theorem 1.17 to $F(x) = x^\kappa\psi(x)$ with $\psi(x)\asymp_\lambda\psi(x^\lambda)$, we need the fact that $\psi(x)\asymp\phi(x)$ for some $\phi(x)$ of slow variation. We are assuming that $\psi(e^x)\asymp_\lambda\psi(e^{\lambda x})$, that is, that $\psi(e^x)$ is of O-regular variation. By the representation theorem for O-regular varying functions [**2**, Theorem 2.2.7], there exist measurable bounded functions α, $\xi:\mathbb{R}_{>0}\to\mathbb{R}$ such that

$$\psi(e^x) = \exp\left(\alpha(x) + \int_1^x \frac{\xi(t)}{t}\,\mathrm{d}t\right).$$

Writing $y=e^x$, we have

$$\psi(y)\asymp\exp\left(\int_1^{\log y}\frac{\xi(t)}{t}\,\mathrm{d}t\right) = \exp\left(\int_1^y \frac{\xi(\log u)}{u\log u}\,\mathrm{d}u\right)$$

Writing $\epsilon(u) := \xi(\log u)/\log u$, since ξ is bounded, $\epsilon(u)\to 0$ as $u\to\infty$. Therefore $\psi(x)\asymp\phi(x) := \exp(\int_1^x \epsilon(t)/t\,\mathrm{d}t)$, which is a slowly varying function (cf. [**2**, Theorem 1.3.1]).

[2] [**2**, Theorem 2.0.8] applied to $g(x) := \psi(e^x)$, so that $g(\lambda x)\asymp_\lambda g(x)$.

Appendix A

$(hA)^{(t)}$ is always structured if $|A| = 3$

Let $A = \{0 = a_0 < a_1 < \cdots < a_\ell < a_{\ell+1} = m\} \subseteq \mathbb{Z}$ be a finite set of integers with $\gcd(A) = 1$, and let $t \geq 1$ be a fixed integer. For $h \geq 1$, write

$$R_{A,h}(n) = \{(k_0, \ldots, k_{\ell+1}) \in \mathbb{Z}_{\geq 0}^{\ell+2} \mid k_0 a_0 + \cdots + k_{\ell+1} a_{\ell+1} = n, \sum_{i=0}^{\ell+1} k_i = h\}$$

for the number of ways to write n as a sum of h elements of A, and $(hA)^{(t)} = \{n \in \mathbb{Z}_{\geq 0} \mid R_{A,h}(n) \geq t\}$. Recall that $(hA)^{(t)}$ is said to be structured if

$$(hA)^{(t)} = [hm] \setminus \Big(\mathcal{E}_t(A) \cup (hm - \mathcal{E}_t(m - A))\Big),$$

where $\mathcal{E}_t(A) = \{n \in \mathbb{Z}_{\geq 0} \mid R_A(n) < t\}$ is the t-exceptional set of A, with $R_A(n) = \lim_{h\to\infty} R_{A,h}(n)$.

In comparison, Nathanson's original definition of structure in [**26, 30**] is as follows: there exist c, $d \in \mathbb{Z}_{\geq 0}$ and subsets $C \subseteq [0,c-2]$, $D \subseteq [0,d-2]$, all depending on A and t, such that

$$(hA)^{(t)} = C \cup [c, hm - d] \cup (hm - D). \tag{A.1}$$

If one requires that $c \leq hm - d$ in order for the interval to be non-empty, then (A.1) becomes equivalent to having $(hA)^{(t)} = [hm] \setminus \Big(\mathcal{E}_t(A) \cup (hm - \mathcal{E}_t(m - A))\Big)$ *and* $h > (\mathrm{Fr}_t(A) + \mathrm{Fr}_t(m - A) + 1)/m$, where $\mathrm{Fr}_t(A) = \max_{n \in \mathcal{E}_t(A)} n$.[1] For instance, Yang–Zhou's [**45**] "$h \geq \sum_{i=2}^{\ell+1}(ta_i - 1) - 1$" is sharp in the sense that, for every $m \geq 4$ and $t \geq 1$, the set $A = \{0,m-1,m\}$ is such that $(hA)^{(t)}$ satisfies (A.1) with a non-empty interval only for $h \geq tm - 2$. At the same time, in this appendix we will show that if $|A| = 3$, then $(hA)^{(t)}$ is structured for every h, $t \geq 1$, and $\mathrm{Fr}_t(A) = tam - a - m$. The case $t = 1$ is Theorem 4 of Granville–Shakan [**13**].

Let $m \geq 2$ be an integer, and $A = \{0 < a < m\}$ with $\gcd(a,m) = 1$. The first lemma is Theorem 4.4.1 of Ramírez-Alfonsín [**33**], written as in Austin [**1**].

[1] If $\{n+1, \ldots, n+m\} \subseteq \mathcal{P}_t(A)$, then since $m + \mathcal{P}_t(A) \subseteq \mathcal{P}_t(A)$, we have $\{n+1, n+2, \ldots\} \subseteq \mathcal{P}_t(A)$. So if $\{n+1, \ldots, n+m\} \subseteq [hm] \setminus \big(\mathcal{E}_t(A) \cup (hm - \mathcal{E}_t(m - A))\big)$, then we must have $n \geq \mathrm{Fr}_t(A)$ and $n + m \leq hm - \mathrm{Fr}_t(m - A) - 1$.

Lemma A.1. *Write* $\{x\} := x - \lfloor x \rfloor$*. For any* $n \in \mathbb{Z}_{\geq 0}$*, we have*

$$R_A(n) = \frac{n}{am} - \left\{\frac{na^{-1}}{m}\right\} - \left\{\frac{nm^{-1}}{a}\right\} + 1,$$

where a^{-1} (resp. m^{-1}) *is an inverse of* $a \pmod{m}$ (resp. $m \pmod{a}$).

Proof. Let u_0 be the unique $0 \leq u_0 < m$ such that $n \equiv au_0 \pmod{m}$. Then, as $\gcd(a,m) = 1$, there is $v_0 \in \mathbb{Z}_{>-a}$ for which $n = au_0 + mv_0$. If $v_0 \geq 0$, then the set of solutions to $n = au + mv$ ($u,v \in \mathbb{Z}_{\geq 0}$) is described by

$$u = u_0 + im,\ v = v_0 - ia \qquad \text{for } 0 \leq i \leq \lfloor v_0/a \rfloor, \tag{A.2}$$

while if $v_0 < 0$, there are no solutions $u,v \in \mathbb{Z}_{\geq 0}$. Therefore, if $R_A(n) = t$ for some $t \geq 0$, we have $\lfloor v_0/a \rfloor = t - 1$, and thus

$$v_0 = (t-1)a + \left\{\frac{v_0}{a}\right\} a. \tag{A.3}$$

This implies that

$$n = au_0 + am(t-1) + \{v_0/a\}am, \tag{A.4}$$

so

$$\begin{aligned} R_A(n) = t &= \frac{n}{am} - \frac{u_0}{m} - \left\{\frac{v_0}{a}\right\} + 1 \\ &= \frac{n}{am} - \left\{\frac{na^{-1}}{m}\right\} - \left\{\frac{nm^{-1}}{a}\right\} + 1. \end{aligned}$$

□

Corollary A.2. *We have:*

(i) $\mathcal{P}_t(A) = (t-1)am + \mathcal{P}(A)$;

(ii) $\mathcal{E}_t(A) = [(t-1)am - 1] \cup \big((t-1)am + \mathcal{E}(A)\big)$.

Proof. By Lemma A.1, note that for $N \geq 1$ and $0 \leq k < am$, we have $R_A(k) \leq 1$ and

$$\begin{aligned} R_A(Nam + k) &= N + \frac{k}{am} - \left\{\frac{ka^{-1}}{m}\right\} - \left\{\frac{km^{-1}}{a}\right\} + 1 \\ &= N + R_A(k). \end{aligned}$$

so $\min_{n \in \mathcal{P}_t(A)} n = (t-1)am$, corresponding to $N = t-1$ and $k = 0$. For $n \geq (t-1)am$, it follows that $R_A(n - (t-1)am) \geq 1$ (i.e., $n - (t-1)am \in \mathcal{P}(A)$) if and only if $R_A(n) \geq t$ (i.e., $n \in \mathcal{P}_t(A)$), concluding part (i). For part (ii),

$$\begin{aligned} \mathcal{E}_t(A) = \mathbb{Z}_{\geq 0} \setminus \mathcal{P}_t(A) &= \mathbb{Z}_{\geq 0} \setminus \big((t-1)am + \mathcal{P}(A)\big) \\ &= [(t-1)am - 1] \cup \big((t-1)am + \mathcal{E}(A)\big). \end{aligned}$$

□

Corollary A.3. *We have:*

(i) $\mathrm{Fr}_t(A) = tam - a - m$;

(ii) $\#\mathcal{E}_t(A) = (t-1)am + \frac{1}{2}(a-1)(m-1)$.

Proof. By Corollary A.2, it suffices to show the result for $t = 1$; that is, $\mathrm{Fr}(A) = am - a - m$ and $\#\mathcal{E}(A) = \frac{1}{2}(a-1)(m-1)$. These are Theorems 2.1.1 and 5.1.1 in Ramírez-Alfonsín [**33**], respectively, to which we provide a short proof.

First, using Lemma A.1 one checks that $R_A(am - a - m) = 0$, while $R_A(n) > 0$ whenever $n > am - a - m$, thus proving (i). For (ii), we claim that $R_A(n) + R_A(am - n) = 1$ for every $0 \le n \le am$ such that $a \nmid n$, $m \nmid n$. Indeed,

$$\begin{aligned} R_A(am-n) &= \frac{am-n}{am} - \left\{\frac{(am-n)a^{-1}}{m}\right\} - \left\{\frac{(am-n)m^{-1}}{a}\right\} + 1 \\ &= 1 - \frac{n}{am} - \left\{-\frac{na^{-1}}{m}\right\} - \left\{-\frac{nm^{-1}}{a}\right\} + 1 \\ &= 1 - \frac{n}{am} + \left\{\frac{na^{-1}}{m}\right\} + \left\{\frac{nm^{-1}}{a}\right\} - 1 = 1 - R_A(n). \end{aligned}$$

So, for n such that $a \nmid n$, $m \nmid n$, we have $n \in [am] \setminus \mathcal{E}(A)$ if and only if $am - n \in \mathcal{E}(A)$ This, together with the fact that multiples of a or m are representable, yields

$$\begin{aligned} \#\mathcal{E}(A) &= \#[am] - \#(am - \mathcal{E}(A)) - \#\{n \in [am]\ ;\ a \mid n \text{ or } m \mid n\} \\ &= (am+1) - \#\mathcal{E}(A) - (a+m) = (a-1)(m-1) - \#\mathcal{E}(A), \end{aligned}$$

therefore $\#\mathcal{E}(A) = \frac{1}{2}(a-1)(m-1)$. □

Theorem A.4. *For every h, $t \ge 1$,*

$$(hA)^{(t)} = [hm] \setminus \Big(\mathcal{E}_t(A) \cup (hm - \mathcal{E}_t(m-A))\Big);$$

i.e., $(hA)^{(t)}$ is always structured.

Proof. Let $h \ge 1$, and take $n \in [hm]$ with $n \notin \mathcal{E}_t(A) \cup (hm - \mathcal{E}_t(m-A))$ – i.e., $R_A(n)$, $R_{m-A}(hm-n) \ge t$. We want to show that this implies that $n \in (hA)^{(t)}$. As in (A.2), since i can go up to at least $t-1$, we have at least t representations $n = au + mv$ with u, v satisfying, by (A.3),

$$\begin{aligned} u + v &= u_0 + v_0 + i(m-a) \\ &\le u_0 + v_0 + (t-1)m - (t-1)a \\ &= u_0 + (t-1)m + \left\{\frac{v_0}{a}\right\} a. \end{aligned}$$

Now we apply the same argument to $m - A$. Let u_0' be the unique $0 \le u_0' < m$ such that $hm - n \equiv (m-a)u_0' \pmod{m}$, and v_0' such that $hm - n = (m-a)u_0' + mv_0'$. But

$0 \equiv hm = n + (hm - n) \equiv au_0 + (m-a)u_0' \equiv a(u_0 - u_0') \pmod{m}$, implying that $u_0 = u_0'$. Thus, applying (A.4) to n (with respect to A) and to $hm - n$ (with respect to $m - A$), we get

$$\begin{aligned}
hm = n + (hm - n) &= \left(au_0 + (t-1)am + \left\{\frac{v_0}{a}\right\}am\right) \\
&\qquad + \left((m-a)u_0' + (t-1)(m-a)m + \left\{\frac{v_0'}{m-a}\right\}(m-a)m\right) \\
&= a(u_0 - u_0') + m\left(u_0' + (t-1)m + \left\{\frac{v_0}{a}\right\}a + \left\{\frac{v_0'}{m-a}\right\}(m-a)\right) \\
&\geq m\left(u_0 + (t-1)m + \left\{\frac{v_0}{a}\right\}a\right),
\end{aligned}$$

and so $u + v \leq h$, implying that $R_{A,h}(n) \geq t$. □

References

[1] D. Austin. The Frobenius problem: How I bought Chicken McNuggets with exact change. AMS Feature Column. Retrieved June 23, 2022, from `http://www.ams.org/publicoutreach/feature-column/fc-2013-08`, 2013.

[2] N. H. Bingham, C. M. Goldie, and J. L. Teugels. *Regular Variation*. Cambridge Univ. Press, 1989.

[3] R. B. Boppana and J. H. Spencer. A useful elementary correlation inequality. *J. Comb. Theory A*, 50:305–307, 1989.

[4] A. Brøndsted. *An introduction to convex polytopes*, volume 90 of *Graduate Texts in Mathematics*. Springer, 1989.

[5] J. Brüdern and T. D. Wooley. On Waring's problem for larger powers. *J. Reine Angew. Math.*, 805:115–142, 2023.

[6] Y.-G. Chen, F.-J. Chen, and J.-D. Wu. On the structure of the sumsets. *Discrete Math.*, 331(6):408–412, 2011.

[7] M. J. Curran and L. Goldmakher. Khovanskii's theorem and effective results on sumset structure. *Discrete Analysis*, 27:25 pp., 2021.

[8] P. Erdős. Problems and results in additive number theory. In *Colloque sur la Theorie des Nombres (CBRM)*, pages 127–137, Bruxelles, 1956.

[9] P. Erdős. Problems and results on additive properties of general sequences, II. *Acta Math. Hung.*, 48:127–137, 1986.

[10] P. Erdős and P. Tetali. Representations of integers as the sum of k terms. *Random Struct. Algor.*, 1:245–261, 1990.

[11] J.-H. Fang. On Cilleruelo–Nathanson's method in Sidon sets. *J. Number Theory*, 260:223–231, 2024.

[12] A. Granville. Refinements of Goldbach's conjecture, and the generalized Riemann hypothesis. *Funct. Approx. Comment. Math.*, 37:159–173, 2007.

[13] A. Granville and G. Shakan. The Frobenius postage stamp problem, and beyond. *Acta Math. Hungarica*, 161(2):700–718, 2020.

[14] A. Granville, G. Shakan, and A. Walker. Effective results on the size and structure of sumsets. *Combinatorica*, 43:1139–1178, 2023.

[15] A. Granville, J. Smith, and A. Walker. Improved stability for the size and structure of sumsets. `arXiv:1311.5939`, 2024.

[16] A. Granville and A. Walker. A tight structure theorem for sumsets. *Proc. Am. Math. Soc.*, 149(10):4073–4082, 2021.

[17] H. Halberstam and K. F. Roth. *Sequences*. Springer, revised edition, 1983.

[18] G. Harman. Trigonometric sums over primes, I. *Mathematika*, 28:249–254, 1981.

[19] L. K. Hua. *Additive theory of prime numbers*. American Mathematical Society, 1965.

[20] A. Khovanskii. The Newton polytope, the Hilbert polynomial and sums of finite sets. *Funktsional. Anal. i Prilozhen*, 26(4):57–63, 96, 1992.

[21] J. H. Kim and V. H. Vu. Concentration of multivariate polynomials and its applications. *Combinatorica*, 20(3):417–434, 2000.

[22] A. V. Kumchev and D. I. Tolev. An invitation to additive prime number theory. *Serdica Math J.*, 31:1–74, 2005.

[23] B. Landreau. Étude probabiliste des sommes des puissances s-ièmes. *Compos. Math.*, 99:1–31, 1995.

[24] V. F. Lev. The structure of higher sumsets. *Proc. Am. Math. Soc.*, 150(12):5165–5177, 2022.

[25] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory I: Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[26] M. B. Nathanson. Sums of finite sets of integers. *Amer. Math. Monthly*, 79(9):1010–1012, 1972.

[27] M. B. Nathanson. *Additive Number Theory: The Classical Bases*, volume 164 of *Graduate Texts in Mathematics*. Springer, 2nd edition, 1996.

[28] M. B. Nathanson. Every function is the representation function of an additive basis for the integers. *Port. Math.*, 62:55–72, 2005.

[29] M. B. Nathanson. Cassels bases. In D. Chudnovsky and G. Chudnovsky, editors, *Additive number theory: Festschrift in honor of the sixtieth birthday of Melvyn B. Nathanson*, pages 259–285. Springer, New York, 2010.

[30] M. B. Nathanson. Sums of finite sets of integers II. *Amer. Math. Monthly*, 128(10):888–896, 2021.

[31] M. B. Nathanson and I. Z. Ruzsa. Polynomial growth of sumsets in abelian semigroups. *J. Théor. Nombr. Bordx.*, 14(2):553–560, 2002.

[32] J. Pliego. On Vu's theorem in Waring's problem for thinner sequences. `arXiv:2410.11832`, 2024.

[33] J. L. Ramírez-Alfonsín. *The Diophantine Frobenius problem*. Oxford University Press, 2006.

[34] J. J. Sylvester. On subinvariants; i.e. semi-invariants to binary quantics of an unlimited order. *American Journal of Mathematics*, 5(1):79–136, 1882.

[35] C. Táfula. An extension of the Erdős–Tetali theorem. *Random Struct. Algor.*, 55(1):173–214, 2019.

[36] C. Táfula. Representation functions with prescribed rates of growth. `arXiv:2405.01530`, 2024.

[37] T. Tao and V. H. Vu. *Additive combinatorics*, volume 105 of *Cambridge Stud. Adv. Math.* Cambridge Univ. Press, 2006.

[38] R. C. Vaughan. *The Hardy–Littlewood method*. Cambridge Univ. Press, 2nd edition, 1997.

[39] V. H. Vu. On a refinement of Waring's problem. *Duke Math. J.*, 105:107–134, 2000.

[40] V. H. Vu. On the concentration of multivariate polynomials with small expectation. *Random Struct. Algor.*, 16:344–363, 2000.

[41] E. Wirsing. Thin subbases. *Analysis*, 6:285–308, 1986.

[42] T. D. Wooley. On Vu's thin basis theorem in Waring's problem. *Duke Math. J.*, 120:1–34, 2003.

[43] T. D. Wooley. A light-weight version of Waring's problem. *J. Austral. Math. Soc.*, 76:303–316, 2004.

[44] J.-A. Yan. A simple proof of two generalized Borel–Cantelli lemmas. In M. Émery and Y. Marc, editors, *In memoriam Paul-André Meyer - Séminaire de Probabilités XXXIX*, volume 1874 of *Lecture Notes in Mathematics*, pages 77–79. Springer Berlin, Heidelberg, 2006.

[45] Q.-H. Yang and J.-Y. Zhou. On the structure of the h-fold sumsets. *Comptes Rendus Acad. Sci. Paris*, 359(4):493–500, 2021.