Lattice Point Problems: Semigroups, Cones, and Convex Sets

By

Brittney Marsters

DISSERTATION

Submitted in partial satisfaction of the requirements for the degree of

DOCTOR OF PHILOSOPHY

in

MATHEMATICS

in the

OFFICE OF GRADUATE STUDIES

of the

UNIVERSITY OF CALIFORNIA

DAVIS

Approved:

Dr. Jesús A. De Loera, Chair

Dr. Elena Fuchs

Dr. Eugene Gorsky

Committee in Charge

2026

For My Mother: 1974 - 2007.

Contents

List of Figures

List of Tables

Notation

Convex Geometry and Width

$\mathbb{N}$	nonnegative integers $\mathbb{Z}_{\geq 0}$
$\mathrm{conv}(V)$, $\mathrm{cone}(R)$	convex hull of V; conic hull of R
tP	t-th dilation of P
$\mathrm{denom}(P)$	denominator of P: smallest D with DP a lattice polytope
$w_c(K)$, $w(K)$	lattice width of K in direction c; $w(K) = \min_{c \neq 0} w_c(K)$
$h_c(K)$	hyperplane cover of $K \cap \mathbb{Z}^d$ in direction c
$\mathrm{AR}_c(K)$	arithmetic range, $= \{c^\top x : x \in K \cap \mathbb{Z}^d\}$
$\mathrm{aw}_c(K)$, $\mathrm{aw}(K)$	arithmetic width $= \lvert \mathrm{AR}_c(K) \rvert$; $\mathrm{aw}(K) = \min_{c \neq 0} \mathrm{aw}_c(K)$
$\mathcal{S}^n_+$, $\mathcal{S}^n_+(\mathbb{Z})$	cone of $n \times n$ PSD matrices; integer PSD matrices
$\mathcal{L}^n$	Lorentz cone, $= \{(x,t) \in \mathbb{R}^n : \|x\|_2 \leq t\}$

Semigroups, Factorizations, and Ehrhart Theory

$\langle a_1, \ldots, a_k \rangle$	semigroup generated by $a_1, \ldots, a_k$
$\mathrm{cone}(S)$	real cone of an affine semigroup S
S_C	conical semigroup of a cone C, $= C \cap \mathbb{Z}^N$
$\mathrm{F}(S)$	Frobenius number of S
P_S	numerical semigroup polytope, $= \mathrm{conv}(e_1/g_1, \ldots, e_k/g_k)$
$\mathsf{Z}(n)$, $\mathsf{L}(n)$	set of factorizations of n; set of lengths of n
$L(P,t)$	Ehrhart function of P, $= \lvert tP \cap \mathbb{Z}^d \rvert$

Abstract

This dissertation studies lattice points in convex sets, objects lying at the intersection of discrete geometry, integer programming, semigroup theory, and number theory. A unifying theme is Ehrhart-type quasipolynomial behavior: many of the counting and structural functions we consider are eventually described by finitely many polynomials, one per residue class modulo a fixed period. Such functions appear in algebra as Hilbert functions, in number theory as theta functions, and in geometry as Ehrhart functions counting lattice points; the results of this dissertation are therefore of interest to researchers across several fields.

The first main contribution (Chapter 2), joint with De Loera, Xu, and Zhang, addresses the integer structure of non-polyhedral convex cones. Classical Hilbert basis theory provides a finite integer generating set for any rational polyhedral cone, but fails for non-polyhedral cones such as the positive semidefinite cone and the Lorentz cone $\mathcal{L}^n$, both of which have uncountably many extreme rays. We introduce (R, G)-finite generation as an analogue of the Hilbert basis suited to these settings: a conical semigroup $\mathcal{S}_C$ is (R, G)-finitely generated if a finitely generated group G of integer invertible linear maps acts on a finite root set R to produce all of S_C via nonnegative integer combinations. We prove three main results:

(1) the semigroup of integer positive semidefinite matrices is (R, G)-finitely generated for all n, with G generated by $\mathrm{GL}(n, \mathbb{Z})$ acting by congruence and the rank-one matrices serving as roots;

(2) the integer second-order cone is (R, G)-finitely generated for $3 \leq n \leq 10$, with the construction generalizing the classical Barning–Hall tree of Pythagorean triples; and

(3) not every conical semigroup admits an (R, G)-finite generating structure, as we exhibit through an explicit irrational planar cone.

The second main contribution (Chapter 3), joint with De Loera and O'Neill, introduces *arithmetic width* as a new invariant of convex bodies. Classical lattice width measures the continuous span of

a body in an integer direction, but is blind to gaps in the integer values attained by lattice points. Arithmetic width counts instead the number of distinct integer values a linear functional takes on the lattice points of the body, making it sensitive to these gaps and invariant under scaling of the direction vector. We prove four main results:

(1) for large dilates of any convex body, the arithmetic range is an almost arithmetic progression with fixed step size and bounded endpoint irregularities, generalizing the Structure Theorem for Sets of Lengths from numerical semigroup theory;

(2) the arithmetic width of dilated rational polytopes is an eventually quasilinear function of the dilation parameter;

(3) arithmetic width is polynomial-time computable in fixed dimension via Barvinok's algorithm and the Barvinok–Woods projection theorem; and

(4) the minimizing directions for arithmetic and lattice width can be entirely disjoint, and every finite subset of $\mathbb{Z}$ arises as the arithmetic range of some rational simplex.

Acknowledgments

I owe every bit of my success to those who have loved me, believed in me, and supported me along the way. Please indulge me in this moment of earnestness and sentimentality.

- Thank you to my dissertation committee members. You have each taught me, supported me, tested me, and showed up for me. For this, I am grateful.
- I want to acknowledge the incredible financial support I received for my work from NSF grants 2348578 and 2434665, from Dr. Matthias Köppe, from the U.C. Davis Dean summer fellowship, and from the U.C. President's Pre-professoriate Fellowship. This support allowed me to attend international conferences where I built skills, networks, and had unforgettable experiences.
- I have special appreciation for my letter of recommendation writers over the years: Jesús, Chris, Matt, Federico, Axler, Mike, Luze, and Rohit. Thank you for believing in me enough to juggle deadlines, do paperwork, and other unpleasant things.
- I want to express my gratitude to the SFSU, SDSU, and UCD Math departments. These are such special communities to belong to and have shaped my identity as a scholar and as a person.
- My advisor Dr. Jesús A. De Loera deserves his own thank you. You always wanted the best for me, advocated for me (and so many others), pushed me, and was endlessly patient with me as I navigated the waters of life. I have so much respect for how your actions align with your values.
- To Bird and my dad: love you guys! Thank you for every phone call, care package, and body-doubling session. You have given me so many opportunities.
- To Chris: it is not an exaggeration to say that meeting you saved my life, or at the very least, rerouted it towards happier directions. I could not have asked for a better role model.
- To Ailis, Evuilynn, Ally, and Mariah: my success is yours as much as it is mine. Thank you for doing this journey with me.
- Lastly, to Peyton: forever and always.

CHAPTER 1

Introduction

The primary objects of this thesis are lattice points in convex sets, fundamental objects at the intersection of discrete geometry, semigroup theory, integer optimization, and number theory. Lattice points in polytopes encode the feasible solutions of integer linear programs, connecting our work to questions in optimization, complexity, and algorithms [40]. Counting them as a polytope dilates gives the Ehrhart polynomial, a fundamental invariant with deep connections to commutative algebra and combinatorics [12, 88]. From the semigroup perspective, the factorizations of semigroup elements can be studied as lattice points within certain convex sets and their distribution reflects the arithmetic of the ambient semigroup algebra. Meanwhile, the spatial distribution of lattice points in a convex body relative to its ambient lattice leads to the notion of lattice width, which underlies some of the most important algorithms in integer programming and the geometry of numbers [83, 85]. Lattice point problems are pervasive, both in mathematics broadly and as the focus of this dissertation. This dissertation develops new invariants and structural results for these objects, with particular emphasis on the geometry of convex bodies and the factorization theory of semigroups.

A recurring theme across all three projects in this dissertation is Ehrhart-type behavior: quantities that are unpredictable for small inputs eventually become quasipolynomial, meaning polynomial on each residue class modulo some period, as the input parameter grows large. This regularity, first observed by Ehrhart in lattice point counting, turns out to be far more pervasive than its origins suggest.[1] We encounter it in the structure of arithmetic ranges of convex bodies and in the behavior of polytopal norms on affine semigroup factorizations, and we feel its absence when attempting to describe the integer points of non-polyhedral cones. The remainder of this chapter is organized as follows. Sections 1.1, 1.2, and 1.3 develop the necessary background in optimization and polyhedral geometry, semigroup theory, and Ehrhart theory, respectively. Each background section concludes with a statement of our relevant results.

[1] In fact, many authors call this behavior unreasonably ubiquitous and we are inclined to agree [116].

1.1. Optimization & Polyhedral Geometry

Optimization and polyhedral geometry are closely linked through the study of linear inequalities and the convex sets they define, and both play an important role across pure and applied mathematics [117]. Many optimization problems can be formulated as maximizing or minimizing a linear objective over a feasible region described by finitely many linear constraints, whose geometric structure, a convex polyhedron, dictates both the existence of optimal solutions and the complexity of finding them. When solutions are further required to be integral, the problem becomes one of understanding lattice points inside these polyhedra, the central objects of this thesis. This section develops the necessary background in optimization and polyhedral geometry used throughout, with particular attention to the structures needed for Chapter 3 (arithmetic width and its computation) and Chapter 2 (integer points in non-polyhedral cones). See [103] for a complete introduction.

1.1.1. Linear and Integer Programming. An optimization problem has two main ingredients: a function that determines which solutions are preferred (the objective) and a set of conditions that define the allowable solutions (the constraints). There are many classes of optimization problems, often called *programs*, distinguished by the types of objectives and constraints. In this subsection, we will follow [103].

Definition 1.1.1. *A* ***linear program*** *(LP) consists of a linear objective function to be minimized or maximized over a feasible region defined by finitely many linear inequality and equality constraints. In standard form, an LP is written as*

$$\min_{x\in\mathbb{R}^n} c^\top x \quad \textit{subject to} \quad Ax = b,\ x \geq 0,$$

where $c \in \mathbb{R}^n$ is the ***cost vector****, $A \in \mathbb{R}^{m\times n}$ is the* ***constraint matrix****, and $b \in \mathbb{R}^m$.*

Any LP can be converted to standard form, so this formulation is without loss of generality. The feasible region of an LP is a convex **polyhedron**, and when bounded, a **polytope**. If an optimal solution exists, it is attained at a vertex of the feasible polyhedron. This fact is key to the success of the simplex method, a method of solving LPs which searches for an optimal solution by moving along edges of the feasible region [103].

Example 1.1.2. *Consider the LP*

$$\max\ x_1 + x_2 \quad \textit{subject to} \quad 2x_1 + x_2 \le 5,\ x_1 + 3x_2 \le 6,\ x_1, x_2 \ge 0.$$

The feasible region is a polytope in $\mathbb{R}^2$ *with vertices* $(0,0)$*,* $(\frac{5}{2},0)$*,* $(\frac{9}{5},\frac{7}{5})$*, and* $(0,2)$*. The objective is maximized at* $(\frac{9}{5},\frac{7}{5})$*, with an optimal value of* $\frac{16}{5}$*.*

Associated to every LP is a **dual program**, obtained by associating a variable to each constraint of the original (primal) problem [103, §7.4]. The dual of the standard form LP is

$$\max_{y \in \mathbb{R}^m}\ b^\top y \quad \text{subject to} \quad A^\top y \le c.$$

Weak duality states that any dual feasible solution provides a bound on the primal optimal value. Strong duality states that when both programs are feasible, their optimal values coincide.

Before turning to the integer setting, we recall the relevant complexity-theoretic vocabulary. A problem is solvable in **polynomial time** if there exists an algorithm whose running time is bounded by a polynomial in the input size; the class of all such problems is P. The class NP consists of problems whose solutions can be verified in polynomial time, even if finding them may be hard. A problem is **NP-hard** if every problem in NP reduces to it in polynomial time, and **NP-complete** if it is additionally in NP. Whether $\mathsf{P} = \mathsf{NP}$ remains the central open question of theoretical computer science. Linear programs can be solved in polynomial time via the ellipsoid method [103, Ch. 13] or interior point methods [103, §15.1], and the simplex method [103, Ch. 11] performs well in practice despite lacking a polynomial-time guarantee. Requiring solutions to be integral, however, changes the picture entirely.

When all variables are required to be integral the problem is called an **integer linear program** (ILP); when only some are, it is called a **mixed-integer program** (MIP). ILPs are in general NP-hard [103, Ch. 18], and small changes to the feasible region can make the problem significantly harder. The **LP relaxation** of an ILP is the linear program obtained by dropping the integrality constraints. Unlike LPs, an optimal solution to an ILP need not occur at a vertex of the LP relaxation. The mismatch between integer optima and LP vertices is one of the central obstacles to solving ILPs efficiently. The standard algorithm for ILPs and MIPs is branch-and-bound [103, §24.1], which recursively partitions the feasible region into subproblems and solves LP relaxations at each node to prune the search tree. Cutting plane methods [103, Ch. 23] provide an alternative approach for ILPs and MIPs by iteratively adding valid linear inequalities to the LP relaxation until an integer solution is found; in practice, branch-and-bound and cutting plane methods are often combined into branch-and-cut algorithms [96].

EXAMPLE 1.1.3. *Consider the ILP*

$$\max\ x_1 + x_2 \quad \textit{subject to} \quad 2x_1 + x_2 \le 5,\ x_1 + 3x_2 \le 6,\ x_1, x_2 \ge 0,\ x_1, x_2 \in \mathbb{Z}.$$

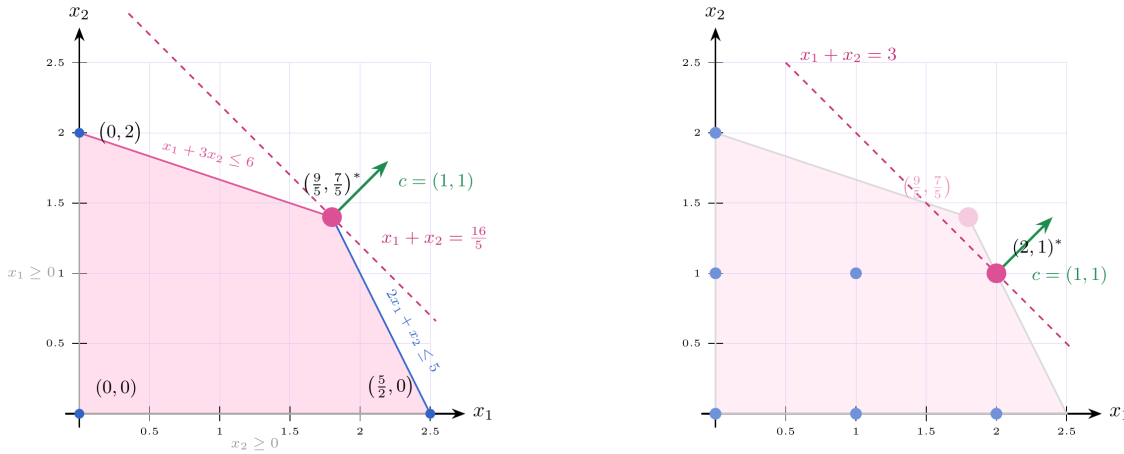
The LP relaxation has optimal solution $(\frac{9}{5}, \frac{7}{5})$ *with optimal value* $\frac{16}{5}$*, which is not integral. Meanwhile, the ILP optimum is attained at* $(2,1)$*, with optimal value* 3*. The gap between the LP and ILP optimal values illustrates that rounding an LP solution does not in general yield an optimal, or even feasible, integer solution.*

The **additive integrality gap** measures the difference between the LP relaxation optimum and the ILP optimum, and serves as a standard measure of how well LP rounding approximates integer solutions. Given a rational polytope $P \subset \mathbb{R}^d$ and a direction $c \in \mathbb{Z}^d$, it is defined as

$$I_M(P, c) = \max_{x \in P} c^\top x - \max_{x \in P \cap \mathbb{Z}^d} c^\top x.$$

In Example 1.1.3, the gap is $\frac{16}{5} - 3 = \frac{1}{5}$. In parametric integer programming, one studies how this gap behaves as the data of the ILP varies, most commonly by varying the right-hand side b in $Ax \le b$. Hoşten–Sturmfels [73] and Eisenbrand–Shmonin [52] show that the maximal additive integrality gap is finite and computable in fixed dimension, and eventually quasipolynomial as b varies along a ray. Dilating a polytope is a special case of this construction. In Chapter 3, we show that in the dilation setting the gap is not merely quasipolynomial but eventually *periodic*: for $n \gg 0$, the value $I_M(nP, c)$ depends only on the residue class of n modulo the denominator of P. Unlike LPs, ILPs do not in general admit a dual program with matching optimal value; the gap between the LP relaxation and the ILP optimum is precisely the integrality gap discussed above. The study of ILPs is closely tied to the geometry of lattice points in polyhedra, which we develop in the next subsection.

1.1.2. Polytopes, Polyhedra, and Cones. The feasible regions of linear programs introduced above are examples of polyhedra and polytopes. These objects are of mathematical interest



(a) LP relaxation with optimal vertex $\left(\frac{9}{5}, \frac{7}{5}\right)^*$.

(b) ILP with feasible lattice points and optimal vertex $(2,1)^*$.

FIGURE 1.1. Comparison of the LP relaxation and ILP from Examples 1.1.2 and 1.1.3.

independent of their significance to optimization, and we present them here from the perspective of convex and discrete geometry [117].

DEFINITION 1.1.4. *A* ***polyhedron*** $P \subseteq \mathbb{R}^n$ *is a set defined by the intersection of finitely many linear inequalities,*

$$P = \{x \in \mathbb{R}^n : Ax \leq b\},$$

where $A \in \mathbb{R}^{m \times n}$ *and* $b \in \mathbb{R}^m$*. A bounded polyhedron is called a* ***polytope****. This way of describing a polyhedron is called the* ***H-representation*** *(or halfspace representation) of* P*.*

The **dimension** of a polyhedron P, denoted $\dim(P)$, is the dimension of its affine hull. We say P is **full-dimensional** if $\dim(P) = n$. The **relative interior** of P, denoted $\mathrm{relint}(P)$, is its interior taken within its affine hull; this is the appropriate notion of interior for polyhedra that are not full-dimensional.

The simplest polytope, the **standard simplex** $\Delta_n \subset \mathbb{R}^{n+1}$, is the convex hull of the standard basis vectors,

$$\Delta_n = \mathrm{conv}(e_1, \ldots, e_{n+1}) = \left\{ x \in \mathbb{R}^{n+1} : x_i \geq 0, \sum_{i=1}^{n+1} x_i = 1 \right\}.$$

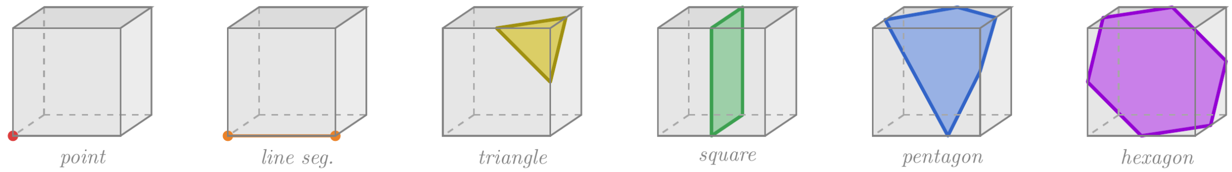


FIGURE 1.2. The six combinatorial types of cross-sections of the cube $[0,1]^3$, obtained by intersecting with hyperplanes of varying orientation.

More generally, any polytope combinatorially equivalent to Δ_n is called a **simplex**. A **unimodular simplex** is a simplex $\sigma = \mathrm{conv}(v_0, v_1, \ldots, v_n) \subset \mathbb{R}^n$ whose edge vectors $v_1 - v_0, \ldots, v_n - v_0$ form a basis for the integer lattice $\mathbb{Z}^n$, or equivalently, whose vertex matrix has determinant ± 1. Unimodular simplices are the building blocks of triangulations that interact well with the integer lattice, and appear naturally in the study of Ehrhart theory and toric geometry [**20**, **44**].

EXAMPLE 1.1.5. *Let $P \subseteq \mathbb{R}^2$ be defined by*

$$P = \{(x_1, x_2) \in \mathbb{R}^2 : x_1 \geq 0,\ x_2 \geq 0,\ x_1 + x_2 \leq 4,\ x_1 \leq 3\}.$$

This is a full-dimensional polytope in $\mathbb{R}^2$, defined by four halfspaces. Its vertices are $(0,0)$, $(3,0)$, $(3,1)$, and $(0,4)$, which are obtained by solving the systems of equations given by taking each pair of constraints to equality. The edges of P lie on the lines $x_1 = 0$, $x_2 = 0$, $x_1 + x_2 = 4$, and $x_1 = 3$, each corresponding to one of the defining halfspaces. In the language of the H-representation,

$$A^\top = \begin{pmatrix} -1 & 0 & 1 & 1 \\ 0 & -1 & 1 & 0 \end{pmatrix}, \qquad b^\top = \begin{pmatrix} 0 & 0 & 4 & 3 \end{pmatrix}.$$

Since P is full-dimensional, its relative interior coincides with its interior and consists of all points (x_1, x_2) satisfying each inequality strictly.

Polyhedra admit a second, equivalent description in terms of vertices and rays. The **convex hull** of a finite set of points $V = \{v_1, \ldots, v_k\} \subseteq \mathbb{R}^n$ is

$$\mathrm{conv}(V) = \left\{ \sum_{i=1}^{k} \lambda_i v_i : \lambda_i \geq 0,\ \sum_{i=1}^{k} \lambda_i = 1 \right\}.$$

A **ray** generated by $r \in \mathbb{R}^n$ is the set $\{\lambda r : \lambda \geq 0\}$. The **V-representation** of a polyhedron expresses it as the Minkowski sum of a polytope and a finite set of rays,

$$P = \mathrm{conv}(V) + \mathrm{cone}(R) = \left\{ \sum_i \lambda_i v_i + \sum_j \mu_j r_j : \lambda_i, \mu_j \geq 0,\ \sum_i \lambda_i = 1 \right\},$$

where $V = \{v_1, \dots, v_k\} \subset \mathbb{R}^n$ and $R = \{r_1, \dots, r_l\} \subset \mathbb{R}^n$. For bounded polyhedra, the ray set R is empty and the V-representation reduces to the convex hull of finitely many points. The equivalence of the H- and V-representations is the content of the Weyl–Minkowski theorem.

THEOREM 1.1.6 (Weyl–Minkowski [117, Thm. 1.2]). *A set $P \subseteq \mathbb{R}^n$ is a polyhedron if and only if it can be expressed as the Minkowski sum of the convex hull of finitely many points and a cone generated by finitely many rays.*

EXAMPLE 1.1.7. *The polytope P from Example 1.1.5 has V-representation $P = \mathrm{conv}(V)$ with*

$$V = \{(0,0),\ (3,0),\ (3,1),\ (0,4)\}.$$

The vertex $(3,1)$, for instance, is the intersection of the constraints $x_1 = 3$ and $x_1 + x_2 = 4$; the remaining vertices similarly come from pairs of tight constraints.

The faces of a polyhedron encode its combinatorial and geometric structure. A **supporting hyperplane** of P at a point $x_0 \in P$ is a hyperplane $H = \{x : c^\top x = b\}$ such that $c^\top x_0 = b$ and $c^\top x \leq b$ for all $x \in P$. A **face** of P is any set of the form $F = P \cap H$ for some supporting hyperplane H, together with P itself and the empty set. Faces of dimension 0, 1, $\dim(P) - 2$, and $\dim(P) - 1$ are called **vertices**, **edges**, **ridges**, and **facets**, respectively. A point $v \in P$ is a vertex if and only if it is an extreme point of P. In Example 1.1.5, the four facets of P each correspond to one of the four defining halfspaces.

Polyhedral cones can be thought of as the unbounded counterparts of polytopes. A **polyhedral cone** is a set of the form

$$C = \{x \in \mathbb{R}^n : Ax \leq 0\}$$

for some $A \in \mathbb{R}^{m \times n}$, or equivalently $C = \mathrm{cone}(R)$ for some finite set of rays $R = \{r_1, \dots, r_l\}$. A polyhedral cone is **pointed** if it contains no line, or equivalently if the origin is a vertex of C.

The **dual cone** of C is

$$C^* = \{y \in \mathbb{R}^n : \langle y, x\rangle \geq 0 \text{ for all } x \in C\},$$

where $\langle\cdot,\cdot\rangle$ denotes the standard inner product. If $C = \mathrm{cone}(R)$ for rays $R = \{r_1, \ldots, r_l\}$, then $C^* = \{y \in \mathbb{R}^n : \langle y, r_i\rangle \geq 0 \text{ for all } i\}$, so the dual cone is itself polyhedral. For any closed convex cone C, we have $C^{**} = C$. A cone is **self-dual** if $C^* = C$; common examples include the nonnegative orthant $\mathbb{R}^n_{\geq 0}$, the positive semidefinite cone $\mathcal{S}^n_+$, and the second-order cone $\mathcal{L}^n = \{(x_0, x') \in \mathbb{R} \times \mathbb{R}^{n-1} : x_0 \geq \|x'\|_2\}$.

Example 1.1.8. *Let* $C = \mathrm{cone}\{(1,0),(1,2)\} = \{\lambda_1(1,0) + \lambda_2(1,2) : \lambda_1, \lambda_2 \geq 0\}$.
For $y = (y_1, y_2)$*, the dual cone is defined by* $\langle y,(1,0)\rangle \geq 0$ *and* $\langle y,(1,2)\rangle \geq 0$*, i.e.* $y_1 \geq 0$ *and* $y_1 + 2y_2 \geq 0$*. Hence*

$$C^* = \{(y_1, y_2) : y_1 \geq 0,\ y_1 + 2y_2 \geq 0\}.$$

The boundary lines are $y_1 = 0$ *and* $y_1 + 2y_2 = 0$*, giving extreme rays* $(0,1)$ *and* $(2,-1)$*. Therefore*

$$C^* = \mathrm{cone}\{(0,1),(2,-1)\}.$$

As $C \neq C^*$*, this is an example of a cone that is not self-dual.*

1.1.3. Semidefinite and Conic Programming.

The programs discussed so far optimize a linear objective over a polyhedron. A natural generalization replaces the polyhedral feasible region with one defined by a convex cone. This is the setting of conic programming. Two cones of particular importance in optimization, and in Chapter 2 of this thesis, are the positive semidefinite cone and the second-order cone.

Definition 1.1.9. *The* ***positive semidefinite cone*** $\mathcal{S}^n_+$ *is the set of all symmetric* $n \times n$ *matrices that are positive semidefinite:*

$$\mathcal{S}^n_+ = \{A \in \mathbb{R}^{n\times n} : A = A^\top,\ x^\top A x \geq 0 \textit{ for all } x \in \mathbb{R}^n\}.$$

The PSD cone is the feasible region of semidefinite programs, which arise throughout combinatorial optimization [67, 68], control theory [16], and polynomial optimization [82]; see [13, 115] for general surveys. Unlike the nonnegative orthant, it is non-polyhedral and its integer structure is considerably more subtle. The following proposition collects its key properties.

Proposition 1.1.1. *The positive semidefinite cone $\mathcal{S}_+^n$ satisfies the following properties.*

1. *(1) $\mathcal{S}_+^n$ is a closed convex cone of dimension $\binom{n+1}{2}$.*
2. *(2) $\mathcal{S}_+^n$ is self-dual: $(\mathcal{S}_+^n)^* = \mathcal{S}_+^n$.*
3. *(3) $A \in \mathcal{S}_+^n$ if and only if all eigenvalues of A are nonnegative.*
4. *(4) $A \in \mathcal{S}_+^n$ if and only if all principal minors of A are nonnegative.*
5. *(5) The interior of $\mathcal{S}_+^n$ consists of the positive definite matrices.*
6. *(6) The extreme rays of $\mathcal{S}_+^n$ are the rank-one matrices $\{vv^\top : v \in \mathbb{R}^n \setminus \{0\}\}$.*
7. *(7) $\mathcal{S}_+^n$ is not polyhedral for $n \geq 2$, as it has uncountably many extreme rays.*
8. *(8) The group $\mathrm{GL}(n, \mathbb{Z})$ acts on the integer points $\mathcal{S}_+^n(\mathbb{Z})$ by $X \mapsto UXU^\top$.*

The second-order cone, also called the Lorentz cone, plays an analogous role in second-order cone programming and shares several structural features with $\mathcal{S}_+^n$.

Definition 1.1.10. *The **second-order cone** (SOC), also called the Lorentz cone, in $\mathbb{R}^n$ is*

$$\mathcal{L}^n = \{(x, t) \in \mathbb{R}^{n-1} \times \mathbb{R} : \|x\|_2 \leq t\}.$$

Both $\mathcal{S}_+^n$ and $\mathcal{L}^n$ are convex cones, but unlike the nonnegative orthant, neither is polyhedral: both have uncountably many extreme rays. This distinction becomes important when we ask about integer generating sets in Section 1.1.4. With these two cones defined, we can now define the optimization programs built on them.

Definition 1.1.11. *A **semidefinite program** (SDP) is an optimization problem of the form*

$$\min_{X \in \mathcal{S}_+^n} \langle C, X \rangle \quad \textit{subject to} \quad \langle A_i, X \rangle = b_i,\ i = 1, \ldots, m,$$

where $C, A_1, \ldots, A_m \in \mathbb{R}^{n \times n}$ are symmetric matrices, $b \in \mathbb{R}^m$, and $\langle A, B \rangle = \mathrm{tr}(A^\top B)$ denotes the matrix inner product.

The feasible region of an SDP is a **spectrahedron**, the intersection of the positive semidefinite cone with an affine subspace. Spectrahedra can take on a wide range of shapes, from smooth curved bodies to polytope-like regions with flat faces, as illustrated in Figure 1.3.

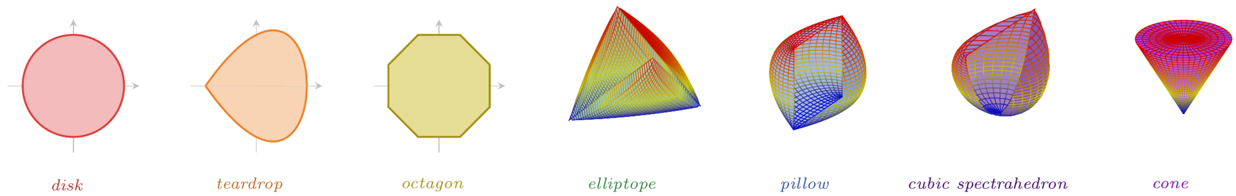


FIGURE 1.3. A selection of spectrahedra, illustrating the range of shapes that arise as feasible regions of semidefinite programs.

SDPs generalize LPs: any LP can be reformulated as an SDP by taking diagonal matrices. More generally, a **conic program** (CP) has the form

$$\min_{x \in \mathbb{R}^n} c^\top x \quad \text{subject to} \quad Ax = b, \ x \in K,$$

where $K \subseteq \mathbb{R}^n$ is a convex cone. LPs, SDPs, and second-order cone programs (SOCPs) are the cases $K = \mathbb{R}^n_{\geq 0}$, $K = \mathcal{S}^n_+$, and $K = \mathcal{L}^n$, respectively.

Linear programs are solvable in polynomial time, as first shown by Khachiyan [70]. The picture for semidefinite programs is more subtle: interior point methods compute an additive ε-approximate optimal solution to an SDP in time polynomial in the input bit-size and $\log(1/\varepsilon)$, under standard regularity assumptions such as strict feasibility and a known bounding ball on the feasible region [39]. Whether *exact* SDP feasibility can be decided in polynomial time is a long-standing open problem [97]; the obstacle is that even strictly feasible SDPs can have solutions of doubly-exponential size, as shown by a classical example of Khachiyan. Conic programs over more general cones are polynomial-time tractable only when the cone admits an efficiently computable self-concordant barrier [91]; this includes LPs, SOCPs, and SDPs but not arbitrary closed convex cones.

EXAMPLE 1.1.12. *Consider the SDP*

$$\min \ x_{11} + x_{22} \quad \textit{subject to} \quad x_{12} = 1, \ X = \begin{pmatrix} x_{11} & x_{12} \\ x_{12} & x_{22} \end{pmatrix} \succeq 0.$$

The constraint $X \succeq 0$ requires $x_{11}, x_{22} \geq 0$ and $x_{11}x_{22} \geq x_{12}^2 = 1$. By the arithmetic-geometric mean inequality, $x_{11} + x_{22} \geq 2\sqrt{x_{11}x_{22}} \geq 2$, with equality at $x_{11} = x_{22} = 1$. The optimal solution is $X = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ with optimal value 2.

The program classes introduced above differ substantially in their structure, complexity, and the geometric properties of their feasible regions. Table 1.1 collects these distinctions for convenience.

	LP	**ILP**	**MIP**	**SDP**	**SOCP**
Feasible region	polyhedron	polyhedron	polyhedron	spectrahedron	convex cone slice
Convex feasible region	yes	no	no	yes	yes
Objective	linear	linear	linear	linear[1]	linear
Optimal location	vertex	integer point	mixed point	boundary	boundary
Strong duality	yes	no	no	yes (generically)	yes (generically)
Key algorithm(s)	simplex, IPM	branch-and-bound, cutting planes	branch-and-bound, cutting planes	IPM	IPM
Complexity	poly	NP-hard	NP-hard	weakly poly[2]	weakly poly[2]

Table 1.1. Comparison of optimization program classes where IPM stands for interior point method.

1.1.4. Hilbert Bases. When working over the integers, the generating set of a polyhedral cone requires care. Given a rational polyhedral cone $C = \text{cone}(R)$, the real generators in R need not suffice to represent all integer points of C as nonnegative integer combinations: real conic combinations allow scaling by any nonnegative real, whereas integer combinations require integer coefficients, so lattice points can fall strictly between the generators.

Definition 1.1.13. *Let $C \subseteq \mathbb{R}^n$ be a rational polyhedral cone. A* ***Hilbert basis*** *of C is a finite set $H \subseteq C \cap \mathbb{Z}^n$ such that every integer point in C can be written as a nonnegative integer combination of elements of H:*

$$C \cap \mathbb{Z}^n = \left\{ \sum_{h \in H} \lambda_h h : \lambda_h \in \mathbb{Z}_{\geq 0} \right\}.$$

The name echoes Hilbert's basis theorem in commutative algebra: just as every ideal in a polynomial ring is finitely generated, every rational polyhedral cone has a finite integer generating set. By

[1]Linear in the matrix variable X, i.e., the objective $\langle C, X \rangle = \text{tr}(C^\top X)$ is linear in the entries of X.
[2]Polynomial in the input size and $\log(1/\varepsilon)$ for additive ε-approximate solutions, under standard regularity assumptions; exact polynomial-time solvability of SDP feasibility is an open problem [97].

Gordan's lemma, every rational polyhedral cone admits a Hilbert basis. For pointed cones, the minimal such basis is unique: it consists precisely of those integer points in C that cannot be written as the sum of two other nonzero integer points in C [103, §16.4]. Hilbert bases are the integer analogue of generating sets for polyhedral cones and are fundamental to integer programming and the theory of affine semigroups [20].

EXAMPLE 1.1.14. *Consider the cone $C = \operatorname{cone}(\{(2,1),(1,2)\})$. The point $(1,1) \in C \cap \mathbb{Z}^2$ cannot be written as a nonnegative integer combination of $(2,1)$ and $(1,2)$, so these generators do not form a Hilbert basis. The minimal Hilbert basis of C is $H = \{(2,1),(1,1),(1,2)\}$.*

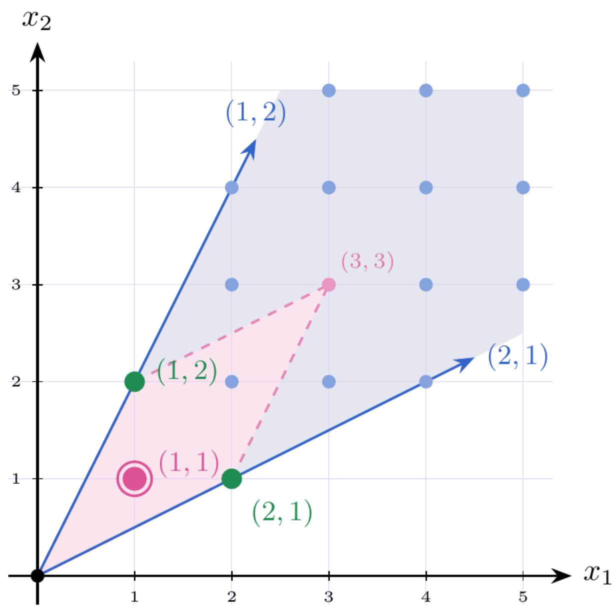


FIGURE 1.4. The cone $C = \operatorname{cone}(\{(2,1),(1,2)\})$ with integer points marked. The generators $(2,1)$ and $(1,2)$ are shown in green, and the fundamental parallelepiped is shaded in pink. The point $(1,1)$ lies inside the parallelepiped but cannot be written as a nonnegative integer combination of the two generators, and so must be added to form the Hilbert basis $H = \{(2,1),(1,1),(1,2)\}$.

Hilbert bases also play a central role in integer programming through the notion of total dual integrality. A system $Ax \leq b$ is **totally dual integral** (TDI) if for every integer objective vector c for which $\max\{c^\top x : Ax \leq b\}$ is finite, the dual minimum is attained by an integer vector. A classical result of Giles and Pulleyblank states that $Ax \leq b$ is TDI if and only if for every face of the polyhedron $\{x : Ax \leq b\}$, the rows of A active at that face form a Hilbert basis for their conic span [65]. This connection between Hilbert bases and TDI extends naturally to the conic setting and is one of the motivations for Chapter 2.

The existence and computability of Hilbert bases for polyhedral cones stands in sharp contrast to the non-polyhedral case: neither $\mathcal{S}_+^n$ nor $\mathcal{L}^n$ admits a finite Hilbert basis, a gap that Chapter 2 addresses by introducing a generalization using group actions. The interplay between Hilbert bases and the integer structure of polyhedral cones reappears throughout this thesis. We next turn to a different measure of how a convex body interacts with the integer lattice: its lattice width.

1.1.5. Our Contributions: (R, G)-Finite Generation. The Hilbert basis gives a complete finite description of the integer points of any rational polyhedral cone. A natural question is whether any analogous finite description exists for the integer points of non-polyhedral convex cones. The positive semidefinite cone $\mathcal{S}_+^n$ and the second-order cone $\mathcal{L}^n$ are both non-polyhedral and have infinitely many extreme rays, so no finite Hilbert basis in the classical sense exists. Nevertheless, both cones are fundamental objects in optimization, and understanding their integer structure is a natural and important question.

In joint work with De Loera, Xu, and Zhang [43], we introduce (R, G)-**finite generation** as an analogue of the Hilbert basis for non-polyhedral convex cones. Given a convex cone $C \subseteq \mathbb{R}^N$, we say the conical semigroup $S_C = C \cap \mathbb{Z}^N$ is (R, G)-**finitely generated** if there exists a finite set of roots $R \subseteq S_C$ and a finitely generated group G of integer invertible linear maps such that

$$S_C = \left\{ \sum_i \lambda_i g_i(r_i) : \lambda_i \in \mathbb{Z}_{\geq 0},\ r_i \in R,\ g_i \in G \right\}.$$

The classical Hilbert basis is recovered when $G = \{I\}$. The key step in each of our main results is identifying which integer points of the cone are minimal in height (that is, cannot be written as a sum of two other nonzero integer points in the cone) and must therefore appear as roots.

Theorem 1.1.15 (De Loera, Marsters, Xu, Zhang [43]). *The semigroup $\mathcal{S}_+^n(\mathbb{Z})$ of integer positive semidefinite matrices is (R, G)-finitely generated for all n.*

Theorem 1.1.16 (De Loera, Marsters, Xu, Zhang [43]). *For $3 \leq n \leq 10$, the semigroup $\mathcal{L}^n \cap \mathbb{Z}^n$ of integer second-order cone vectors is (R, G)-finitely generated.*

For the PSD cone, the group G is $\mathrm{GL}(n, \mathbb{Z})$ acting by congruence $X \mapsto UXU^\top$, and the roots are the rank-one PSD matrices $vv^\top$ for integer vectors v.

1.1.6. Lattice Width. One of the most important ways to measure how a convex body $K \subseteq \mathbb{R}^d$ interacts with the integer lattice is its **lattice width**. For a nonzero integer vector $c \in \mathbb{Z}^d$, the lattice width of K in direction c is

$$w_c(K) = \max_{x,y \in K} c^\top (x - y).$$

Geometrically, $w_c(K)$ measures the Euclidean distance between two parallel supporting hyperplanes with normal c, scaled by $\|c\|$. Equivalently, when we consider primitive integer direction vectors, it counts the number of integer hyperplanes $\{x : c^\top x = k\}$, $k \in \mathbb{Z}$, that K intersects in direction c, minus one. The **lattice width** of K is the minimum over all nonzero integer directions:

$$w(K) = \min_{c \in \mathbb{Z}^d \setminus \{0\}} w_c(K).$$

Example 1.1.17. *Let $P = \operatorname{conv}((0,0),(4,1),(4,2)) \subset \mathbb{R}^2$. In direction $c = (1,0)$, the functional $c^\top x = x_1$ ranges from 0 to 4 on P, giving $w_{(1,0)}(P) = 4$. In direction $c = (0,1)$, the functional x_2 ranges from 0 to 2, giving $w_{(0,1)}(P) = 2$. One can verify that $w(P) = 2$, attained at $(0,1)$ and $(1,-2)$ among others.*

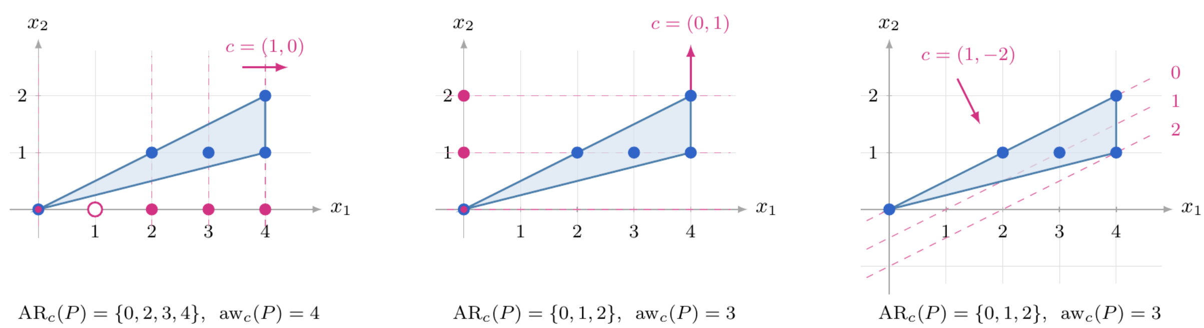


Figure 1.5. The polytope P from Example 1.1.17 under three functionals.

Lattice width is a well-studied invariant with connections across discrete geometry, integer programming, and cryptography [**87**, **103**]. We collect its key properties here.

Proposition 1.1.2. *Let $K \subseteq \mathbb{R}^d$ be a convex body and $c \in \mathbb{Z}^d \setminus \{0\}$. The lattice width satisfies the following properties.*

(1) The lattice width scales linearly under dilation: $w_c(nK) = n \cdot w_c(K)$ for all $n > 0$, and $w(nK) = n \cdot w(K)$ for all $n \in \mathbb{Z}_{>0}$.

(2) The lattice width is preserved under unimodular transformations: $w(UK) = w(K)$ for any $U \in \mathrm{GL}(d, \mathbb{Z})$.

(3) Scaling the direction vector scales the width proportionally: $w_{\lambda c}(K) = |\lambda| \cdot w_c(K)$ for any nonzero $\lambda \in \mathbb{Z}$, so parallel directions give proportional lattice widths.

(4) The lattice width is nonnegative and real-valued, with $w_c(K) = 0$ if and only if K is contained in a single hyperplane with normal c.

(5) In fixed dimension d, the lattice width of a rational polytope is computable in polynomial time [29, 83].

Lattice width plays a central role across several areas of mathematics. In integer programming, it is the key ingredient in Lenstra's celebrated algorithm, which solves ILPs in polynomial time when the dimension is fixed by branching on the direction of minimum lattice width [83]. It also underlies the **flatness theorem**, which states that for each dimension d there exists a **flatness constant** $\omega(d)$ such that any convex body with no interior lattice points has lattice width at most $\omega(d)$ [76]. The flatness theorem is fundamental to the geometry of numbers and has been strengthened and applied in the study of lattice-free convex bodies [31, 86]. The exact value of $\omega(d)$ is unknown even in dimension 3, but is conjectured to grow roughly linearly in d [31]. In the geometry of numbers, lattice width appears in sphere-packing and covering problems and Borsuk-type partitioning results [35]. In cryptography, algorithms for computing the shortest lattice vector, which is closely related to lattice width, are foundational to lattice-based cryptographic schemes [14, 87, 114]. In computer graphics, lattice width is used to characterize straightness in digital spaces [56].

However, lattice width has a fundamental limitation: it measures the continuous span of K in a given direction, but says nothing about which integer values within that span are actually attained by lattice points of K. A convex body can have large lattice width in a direction while its lattice points slip through the integer hyperplanes, leaving gaps in the attained values. Returning to Example 1.1.17, the lattice points of P project onto $\{0, 2, 3, 4\}$ in direction $c = (1, 0)$, we notice that the value 1 is missing, yet the lattice width $w_{(1,0)}(P) = 4$ is blind to this gap. Moreover, as property (3) of Proposition 1.1.2 shows, parallel integer directions give proportional lattice widths, so the lattice width depends on the magnitude of c as well as its direction.

This limitation motivates the notion of arithmetic width, which we introduce in Section 1.3.3 after developing the necessary Ehrhart-theoretic background.

Lattice Width	**Arithmetic Width**
Real-valued	Integer-valued
Insensitive to gaps	Sensitive to gaps
Parallel vectors give proportional lattice widths	Parallel vectors give equal arithmetic width
Obtained by short lattice directions	Magnitude of direction is irrelevant
$\mathrm{aw}_c(K) \le w_c(K) + 1$	$\mathrm{aw}_c(K) = \lvert \mathrm{AR}_c(K) \rvert$
$w(\lambda K) = \lambda\, w(K)$ for $\lambda > 0$	$\mathrm{aw}(nP)$ eventually quasilinear in n

TABLE 1.2. A comparison of lattice width and arithmetic width.

1.2. Semigroups & More Semigroups

A **semigroup** $(S, +)$ consists of a nonempty set S and a binary associative operation $+ : S \times S \to S$. Semigroups arise naturally across mathematics, including in commutative algebra, algebraic geometry, number theory, algebraic statistics, optimization, and discrete geometry [40, 88]. In this thesis, we work with four types of semigroups: affine, numerical, polytopal, and conical. In this section, we will introduce each in turn and develop the factorization-theoretic background that connects them.

NOTATION 1. *Throughout, we adopt the convention* $\mathbb{N} = \mathbb{Z}_{\geq 0}$.

1.2.1. Affine Semigroups.

Affine semigroups are the discrete analogues of polyhedral cones: they encode the feasibility sets of integer linear programs, and questions about optimization, solution counting, and factorization all correspond to geometric and algebraic properties of these objects [20].

DEFINITION 1.2.1. *An **affine semigroup** is a finitely generated subsemigroup $S \subseteq \mathbb{Z}^d$ under addition. Equivalently, $S = \mathbb{N}a_1 + \cdots + \mathbb{N}a_k$ for some vectors $a_1, \ldots, a_k \in \mathbb{Z}^d$, called **generators** of S. We write $S = \langle a_1, \ldots, a_k \rangle$ and represent S by the matrix $A = \begin{pmatrix} a_1 & \cdots & a_k \end{pmatrix} \in \mathbb{Z}^{d \times k}$ whose columns are the generators.*

Associated to an affine semigroup $S = \langle a_1, \ldots, a_k \rangle$ is its **cone**

$$\mathrm{cone}(S) = \{\lambda_1 a_1 + \cdots + \lambda_k a_k : \lambda_i \in \mathbb{R}_{\geq 0}\} \subseteq \mathbb{R}^d,$$

the set of all nonnegative real combinations of the generators. The integer points of $\mathrm{cone}(S)$ always contain S, but the two need not be equal. When they are, S is called **normal**.

DEFINITION 1.2.2. *An affine semigroup $S \subseteq \mathbb{Z}^d$ is **normal** if $S = \mathrm{cone}(S) \cap \mathbb{Z}^d$.*

EXAMPLE 1.2.3. *Consider the affine semigroup $S = \langle (2,0),\ (1,1),\ (0,2) \rangle \subseteq \mathbb{Z}^2$. The cone $\mathrm{cone}(S) = \mathbb{R}^2_{\geq 0}$ is the first quadrant, since the generators span it over the nonnegative reals. However, the lattice point $(1,0)$ lies in $\mathrm{cone}(S) \cap \mathbb{Z}^2$ but not in S: no nonnegative integer combination of $(2,0)$, $(1,1)$, $(0,2)$ yields $(1,0)$. Therefore S is not normal.*

A special class of normal affine semigroups comes from lattice polytopes.

DEFINITION 1.2.4. *The **polytopal semigroup** of a lattice polytope $P \subset \mathbb{R}^d$ is*

$$S_P := \{(k, x) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}^d : x \in kP\},$$

the set of integer points in the cone over $P \times \{1\}$.

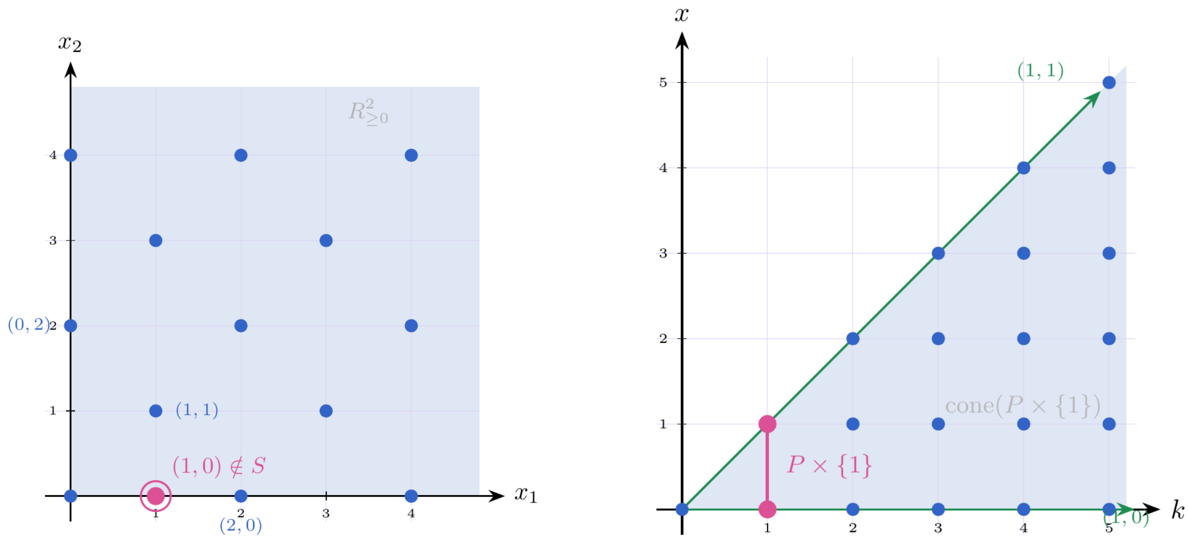
EXAMPLE 1.2.5. *Let $P = [0,1] \subset \mathbb{R}$ be the unit interval. The polytopal semigroup S_P consists of pairs (k, x) with $0 \leq x \leq k$, which is the set of lattice points in the cone over $[0,1] \times \{1\}$. This is a normal affine semigroup.*

1.2.1.1. *Semigroup Algebras.* To every semigroup S one can associate a **semigroup algebra**, a commutative ring that encodes the combinatorial and arithmetic structure of S in algebraic terms.

DEFINITION 1.2.6. *Let $S \subseteq \mathbb{Z}^d$ be an affine semigroup and $\Bbbk$ a field. The **semigroup algebra** $\Bbbk[S]$ is the $\Bbbk$-vector space with basis $\{t^s : s \in S\}$, with $\Bbbk$-algebra structure given by*

$$\left(\sum_{s \in S} a_s t^s\right) \cdot \left(\sum_{s \in S} b_s t^s\right) = \sum_{s \in S} \left(\sum_{u+v=s} a_u b_v\right) t^s,$$

where all but finitely many coefficients $a_s, b_s \in \Bbbk$ are zero. Equivalently, $\Bbbk[S]$ is the subalgebra of the Laurent polynomial ring $\Bbbk[t_1^{\pm 1}, \ldots, t_d^{\pm 1}]$ generated by the monomials $\{t^s : s \in S\}$, where



(a) The non-normal semigroup $S = \langle (2,0),(1,1),(0,2)\rangle$. The point $(1,0)$ lies in $\mathrm{cone}(S) \cap \mathbb{Z}^2$ but not in S.

(b) The normal polytopal semigroup S_P of the unit interval $P = [0,1]$, consisting of all (k,x) with $0 \leq x \leq k$.

FIGURE 1.6. A non-normal affine semigroup (left) and a normal polytopal semigroup (right), illustrating the distinction from Examples 1.2.3 and 1.2.5.

*$t^s = t_1^{s_1} \cdots t_d^{s_d}$ for $s = (s_1, \ldots, s_d)$. More generally, any affine semigroup algebra $\Bbbk[S]$ is a quotient of a polynomial ring by a toric ideal. More specifically, if $S = \langle a_1, \ldots, a_k\rangle \subseteq \mathbb{Z}^d$, then $\Bbbk[S]$ is the image of the ring map $\phi : \Bbbk[x_1, \ldots, x_k] \to \Bbbk[t_1^{\pm 1}, \ldots, t_d^{\pm 1}]$ sending $x_i \mapsto t^{a_i}$, so $\Bbbk[S] \cong \Bbbk[x_1, \ldots, x_k]/I_S$ where $I_S = \ker \phi$ is the **toric ideal** of S.*

When $S = \mathbb{N}^d$, the semigroup algebra $\Bbbk[S]$ is just the polynomial ring $\Bbbk[x_1, \ldots, x_d]$.

EXAMPLE 1.2.7. *For $S = \langle 6, 9, 20\rangle \subseteq \mathbb{N}$, the semigroup algebra is $\Bbbk[S] = \Bbbk[t^6, t^9, t^{20}] \subseteq \Bbbk[t]$, the subring of the polynomial ring generated by the monomials t^6, t^9, and t^{20}. It is the image of the map $\phi : \Bbbk[x_1, x_2, x_3] \to \Bbbk[t]$ sending $x_1 \mapsto t^6$, $x_2 \mapsto t^9$, $x_3 \mapsto t^{20}$, giving an isomorphism*

$$\Bbbk[S] \cong \frac{\Bbbk[x_1, x_2, x_3]}{\langle x_1^3 - x_2^2,\ x_1^{10} - x_3^3\rangle},$$

where the two generators of I_S correspond to the relations $3 \cdot 6 = 2 \cdot 9$ and $10 \cdot 6 = 3 \cdot 20$ in S. The element $t^{120} \in \Bbbk[S]$ admits multiple expressions as products of monomials in t^6, t^9, t^{20}, corresponding exactly to the factorizations of $120 \in S$. For instance, $t^{120} = (t^6)^{20} = (t^6)^{10}(t^{20})^3$.

The Hilbert function of $\Bbbk[S]$, which records the dimension of each graded piece, is a primary algebraic invariant of the semigroup. For a polytopal semigroup S_P, the Hilbert function coincides with the Ehrhart function $L(P,t)$, making the semigroup algebra the algebraic home of Ehrhart theory [94, 107]. Algebraic properties of $\Bbbk[S]$ also reflect geometric properties of S: normality of S is equivalent to $\Bbbk[S]$ being integrally closed [88], and the generators of the toric ideal $I_S = \ker(\Bbbk[x_1,\dots,x_k] \to \Bbbk[S])$ are precisely the trades in S, which we turn to next.

Example 1.2.8. *Continuing the previous example, we record two generating functions naturally associated to $\Bbbk[S]$. First, grading $\Bbbk[S]$ by value in S, that is, setting $\deg(t^n) = n$ for $n \in S$, each graded piece $\Bbbk[S]_n$ is one-dimensional for $n \in S$ and zero otherwise. The Hilbert series of $\Bbbk[S]$ is therefore*

$$\mathrm{Hilb}(\Bbbk[S],t) = \sum_{n\in S} t^n = \frac{1-t^{18}-t^{60}+t^{78}}{(1-t^6)(1-t^9)(1-t^{20})}.$$

encoding which elements belong to S.

However, there are additional gradings worth considering. For example, the Hilbert series of the ambient polynomial ring $\Bbbk[x_1,x_2,x_3]$ with the weighted grading $\deg(x_i) = a_i$:

$$F_S(t) = \frac{1}{(1-t^6)(1-t^9)(1-t^{20})} = \sum_{n\geq 0} \left|\{(a,b,c)\in\mathbb{Z}^3_{\geq 0} : 6a+9b+20c = n\}\right| t^n$$

counts how many ways each element of S can be written as a nonnegative integer combination of the generators. For instance, $[t^{18}]\,F_S(t) = 2$, corresponding to the two representations $3\cdot 6 = 18$ and $2\cdot 9 = 18$, and $[t^{120}]\,F_S(t) = 12$.

Finally, the ***length generating function*** *at degree 120 tracks the total number of generators used in each representation. Specializing $x_i \mapsto z$ in the multivariate series $F_S(x_1,x_2,x_3) = 1/((1-x_1)(1-x_2)(1-x_3))$ and extracting the coefficient of t^{120} under $x_i \mapsto t^{a_i}$ gives*

$$z^6 + z^{10} + z^{11} + z^{12} + \cdots + z^{20},$$

whose exponents are exactly the values $a+b+c$ attained by integer solutions to $6a+9b+20c = 120$. The choice of grading determines what information the Hilbert series captures. Grading by value recovers the membership structure of S; grading by generator tracks factorization counts; grading by length tracks factorization complexity. Each grading makes a different aspect of the algebra visible, and so it is worth exploring a few less standard gradings.

1.2.1.2. *Relations in Affine Semigroups.* Trades, circuits, and Graver bases are the combinatorial backbone connecting the geometry of affine semigroups to their algebraic and arithmetic properties. Trades govern how factorizations of a fixed element relate to one another, and the structure of $\ker_{\mathbb{Z}}(A)$ determines the complexity of non-unique factorization. A **trade** in an affine semigroup $A = \mathbb{N}a_1 + \cdots + \mathbb{N}a_k$ is a vector $\mathbf{t} = \mathbf{t}^+ - \mathbf{t}^- \in \ker_{\mathbb{Z}}(A)$, where $\mathbf{t}^+, \mathbf{t}^- \in \mathbb{Z}^k_{\geq 0}$ have disjoint support. A trade encodes the substitution of generators indexed by $\mathbf{t}^-$ for those indexed by $\mathbf{t}^+$ without changing the element of A: if $\mathbf{z} \in \mathsf{Z}(b)$ and $\mathbf{z} \geq \mathbf{t}^-$ component-wise, then $\mathbf{z} - \mathbf{t}^- + \mathbf{t}^+$ is another factorization of b. The kernel $\ker_{\mathbb{Z}}(A)$ is thus the natural home for all possible trades, and understanding its structure is equivalent to understanding how factorizations of elements of A relate to one another.

Not all trades are equally important. We say a trade $\mathbf{t}$ is a **circuit** if its support $\text{supp}(\mathbf{t}) = \{i : t_i \neq 0\}$ is minimal among all nonzero elements of $\ker_{\mathbb{Z}}(A)$, meaning no proper subset of the generators involved admits a nontrivial relation. Circuits are the atomic moves: every trade decomposes as a sign-consistent sum of circuits, and the circuits generate the kernel $\ker_{\mathbb{Z}}(A)$ as a vector space over $\mathbb{Q}$ [109]. Algebraically, I_A is the kernel of the ring map $\Bbbk[x_1, \ldots, x_k] \to \Bbbk[t_1^{\pm 1}, \ldots, t_d^{\pm 1}]$ sending $x_i \mapsto t^{a_i}$; each trade $\mathbf{t} = \mathbf{t}^+ - \mathbf{t}^-$ corresponds to the binomial $x^{\mathbf{t}^+} - x^{\mathbf{t}^-} \in I_A$.

EXAMPLE 1.2.9. *Returning to $S = \langle 6, 9, 20 \rangle$ and its semigroup algebra $\Bbbk[S] \cong \Bbbk[x_1, x_2, x_3]/I_S$, the numerator $1 - t^{18} - t^{60} + t^{78}$ of $\text{Hilb}(\Bbbk[S], t)$ is not arbitrary: it encodes the relations in I_S via the circuits of S. The two generators of I_S correspond to the trades $3 \cdot 6 = 2 \cdot 9$ and $10 \cdot 6 = 3 \cdot 20$, which are the* ***minimal trades*** *in S: each is a relation between generators that cannot be decomposed into smaller relations. These trades are first encountered at the elements 18 and 60 of S. At $n = 18$, the only two ways to write 18 as a nonnegative integer combination of 6, 9, and 20 are $3 \cdot 6$ and $2 \cdot 9$, which share no generators. At $n = 60$, the representation $3 \cdot 20$ shares no generators with any of the representations using only 6s and 9s. These are the elements at which the non-uniqueness of representation is irreducible, and they are called the* ***Betti elements*** *of S. By inclusion-exclusion over these two elements, the numerator factors as*

$$(1 - t^{18})(1 - t^{60}) = 1 - t^{18} - t^{60} + t^{78},$$

where the $-t^{18}$ and $-t^{60}$ terms subtract the overcounting at each Betti element, and the $+t^{78} = t^{18+60}$ term corrects for having subtracted their overlap twice. More precisely, this numerator arises *from the free resolution of* $\Bbbk[S]$ *as a* $\Bbbk[x_1, x_2, x_3]$*-module:*

$$0 \to \Bbbk[x_1, x_2, x_3](-78) \to \Bbbk[x_1, x_2, x_3](-18) \oplus \Bbbk[x_1, x_2, x_3](-60) \to \Bbbk[x_1, x_2, x_3] \to \Bbbk[S] \to 0,$$

where $\Bbbk[x_1, x_2, x_3](-k)$ *denotes the free module with generator in degree* k*. Reading off the alternating sum of Hilbert series recovers*

$$\mathrm{Hilb}(\Bbbk[S], t) = \frac{(1-t^{18})(1-t^{60})}{(1-t^6)(1-t^9)(1-t^{20})}.$$

While circuits are defined by minimality of support, the relevant notion for integer programming is stronger. The **Graver basis** $\mathrm{Gr}(A)$ of A is the set of all *primitive* elements of $\ker_{\mathbb{Z}}(A)$: those that admit no decomposition $\mathbf{t} = \mathbf{u}+\mathbf{v}$ where $\mathbf{u}$ and $\mathbf{v}$ are nonzero, lie in $\ker_{\mathbb{Z}}(A)$, and are sign-consistent with $\mathbf{t}$ (i.e., $u_i v_i \geq 0$ for all i). Every circuit is in the Graver basis, but the Graver basis can be strictly larger: it captures trades that are primitive but whose support is not minimal. The Graver basis is finite and satisfies the containment

$$\text{circuits} \subseteq \mathrm{Gr}(A) \subseteq \ker_{\mathbb{Z}}(A),$$

with equality on the left when A is totally unimodular [**60**, **103**]. The Graver basis plays a central role in integer programming: it provides a universal test set for optimality, in the sense that for any linear objective and any feasible point, a Graver basis element always exists that improves the objective if improvement is possible [**40**].

The three bases also sit in a broader hierarchy. A **Markov basis** for A is a set $\mathcal{M} \subseteq \ker_{\mathbb{Z}}(A)$ such that for every $b \in A$, any two factorizations of b can be connected by a sequence of trades from $\mathcal{M}$. The Graver basis is always a Markov basis, but minimal Markov bases can be smaller. When $A \in \mathbb{N}^{1\times k}$, that is, when S is a numerical semigroup, the Markov basis, Graver basis, and circuits all coincide with the minimal generating set of I_A [**60**].

Example 1.2.10. *Let* $A = \mathbb{N}(2,0) + \mathbb{N}(1,1) + \mathbb{N}(0,2) \subseteq \mathbb{Z}^2$*. The kernel* $\ker_{\mathbb{Z}}(A)$ *is spanned by* $(1,-2,1)$*, corresponding to the single circuit* $(2,0)+(0,2) = 2\cdot(1,1)$*. The Graver basis is* $\{(1,-2,1)\}$*, the toric ideal is* $I_A = \langle x_1x_3 - x_2^2\rangle$*, and any Markov basis must contain this single element. Since there is only one circuit, the three bases coincide. The factorizations of* $(4,4)$ *computed* *earlier,* $(0,4,0)$*,* $(1,2,1)$*, and* $(2,0,2)$*, are all related by repeated application of this trade, and the factorization graph on* $\mathsf{Z}(4,4)$ *is a path of length* 2*.*

EXAMPLE 1.2.11. *Let* $A = \mathbb{N}(1,0)+\mathbb{N}(0,1)+\mathbb{N}(2,1)+\mathbb{N}(1,2) \subseteq \mathbb{Z}^2$*. Here* $\ker_{\mathbb{Z}}(A)$ *has rank* 2*, with two circuits:*

$$C_1 : 2\cdot(1,0)+(0,1) = (2,1), \quad \mathbf{t}_1 = (2,1,-1,0),$$

$$C_2 : (1,0)+2\cdot(0,1) = (1,2), \quad \mathbf{t}_2 = (1,2,0,-1).$$

The toric ideal $I_A = \langle x_1^2x_2 - x_3,\ x_1x_2^2 - x_4\rangle$ *is generated by these two circuits. The Graver basis, however, is strictly larger: in addition to* C_1 *and* C_2*, it contains*

$$G_3 = (3,3,-1,-1), \quad \textit{meaning} \quad 3\cdot(1,0)+3\cdot(0,1) = (2,1)+(1,2).$$

The element G_3 *is primitive: the decomposition* $G_3 = \mathbf{t}_1 + \mathbf{t}_2$ *has both summands sign-consistent with* G_3*, so no proper sign-consistent subtrade exists. Thus* $G_3 \in \mathrm{Gr}(A)$ *even though its support* $\{1,2,3,4\}$ *is not minimal. This illustrates the general phenomenon: minimality of support and primitivity are distinct conditions, and the Graver basis, not the set of circuits, captures the right notion for integer programming applications.*

1.2.2. Numerical Semigroups. Numerical semigroups are the one-dimensional case of affine semigroups and have a particularly rich theory [2]. They appear in algebraic geometry as value semigroups of singular curves, in commutative algebra via semigroup rings [18, 72], and in additive number theory through the Frobenius problem [2]. In this setting, one studies non-unique factorizations and their associated invariants [26, 62]. They will appear in our results on factorization theory and sets of lengths. We begin by familiarizing the reader with the basics of the field.

DEFINITION 1.2.12. *A* ***numerical semigroup*** *is a subsemigroup* $S \subseteq \mathbb{N}$ *such that* $0 \in S$ *and* $\mathbb{N} \setminus S$ *is finite. Equivalently,* $S = \langle g_1, \dots, g_k\rangle = \mathbb{N}g_1 + \cdots + \mathbb{N}g_k$ *for positive integers* $g_1, \dots, g_k$ *with* $\gcd(g_1, \dots, g_k) = 1$*.*

Note, we will adopt the convention that $g_1 < \ldots < g_k$. The finite set $\mathbb{N} \setminus S$ is called the set of **gaps** of S, and its largest element is the **Frobenius number** $\mathrm{F}(S)$. The number of gaps is the **genus** of S, denoted $\mathrm{g}(S)$.

Example 1.2.13. *Let $S = \langle 6, 9, 20\rangle$, sometimes called the* ***Chicken McNugget monoid*** *after the original Chicken McNugget pack sizes [26]. Since* $\gcd(6, 9, 20) = 1$, *this is a numerical semigroup. Its elements begin*

$$S = \{0, 6, 9, 12, 15, 18, 20, 21, 24, 26, 27, 29, 30, 32, 33, 35, 36, 38, 39, 40, 41, 42, 44, \ldots\},$$

and its gaps are

$$\mathbb{N} \setminus S = \{1, 2, 3, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 22, 23, 25, 28, 31, 34, 37, 43\}.$$

The Frobenius number is $\mathrm{F}(S) = 43$ *and the genus is* $\mathrm{g}(S) = 22$.

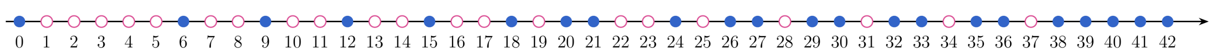


Figure 1.7. Elements and gaps of $S = \langle 6, 9, 20\rangle$ up to 42 from Example 1.2.13.

1.2.3. Conical Semigroups. Conical semigroups generalize polytopal semigroups by replacing the cone over a polytope with the cone over a general convex body. They appear naturally in conic integer programming, algebraic geometry, and number theory [43, 75], and understanding their integer structure is a central problem connecting all three of these areas. A particularly important source of conical semigroups in algebraic geometry is the theory of **Newton–Okounkov bodies**: given a graded linear series on an algebraic variety, the associated semigroup of lattice points is a conical semigroup whose convex-geometric properties encode intersection-theoretic data of the original variety. The semigroup of lattice points associated to a Newton–Okounkov body is itself a conical semigroup in the sense above, with the convex body K encoding asymptotic data such as the growth rate of the Hilbert function [75]. Understanding the integer structure of such semigroups, when they admit finite generating sets and of what form, is precisely the question taken up in Chapter 2.

Definition 1.2.14. *Given a convex cone $C \subseteq \mathbb{R}^N$, the set of integer points $S_C := C \cap \mathbb{Z}^N$ forms a semigroup under addition, called the* ***conical semigroup*** *of C. More generally, for any compact convex body $K \subseteq \mathbb{R}^n$, the integer points of* $\mathrm{cone}(K \times \{1\}) \subseteq \mathbb{R}^{n+1}$ *form a conical semigroup.*

When C is a rational polyhedral cone, the conical semigroup $S_C = C \cap \mathbb{Z}^N$ is a normal affine semigroup whose integer structure is fully captured by a finite Hilbert basis, the unique minimal set of integer points whose nonnegative integer combinations produce all of S_C. The conical and affine settings thus overlap precisely in the normal case, as illustrated in Figure 1.8. Once we move beyond polyhedra to cones such as the positive semidefinite (PSD) cone $\mathcal{S}_+^n$ or the second-order cone $\mathcal{L}^n$, this finite generation fails: both have uncountably many extreme rays, so no finite set of integer points can generate all of S_C under nonnegative integer combinations in the classical sense.

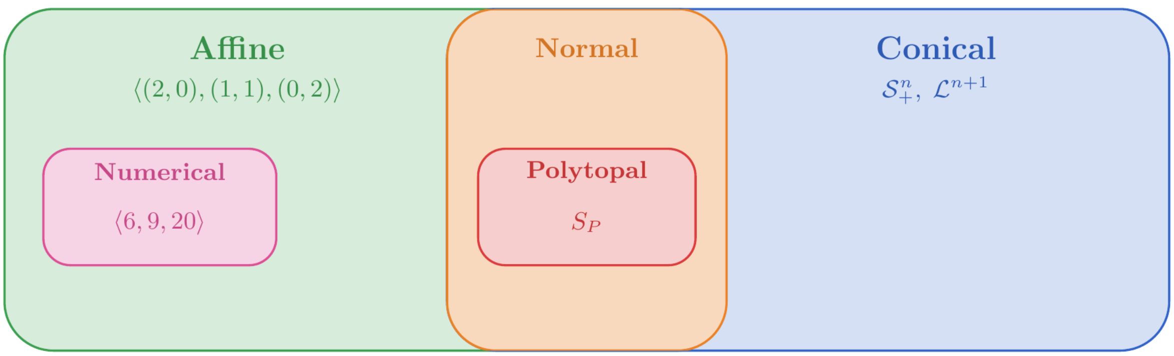


FIGURE 1.8. A Venn Diagram of five types of semigroups.

EXAMPLE 1.2.15. *The integer PSD matrices $\mathcal{S}_+^n(\mathbb{Z}) = \mathcal{S}_+^n \cap \mathbb{Z}^{n\times n}$ form a conical semigroup under matrix addition, since the sum of two PSD matrices is PSD. Similarly, the integer points $\mathcal{L}^n \cap \mathbb{Z}^n$ of the second-order cone form a conical semigroup. Both are fundamental to modern conic optimization, and both are non-polyhedral, so they admit no finite Hilbert basis. These are the central objects of Chapter 2, where we establish a generalized notion of finite generation for their integer points; see Section 1.1.5 for a summary.*

1.2.4. Factorization Theory. Once a generating set for a semigroup is fixed, one can study how elements decompose into generators. In the integers, the Fundamental Theorem of Arithmetic guarantees that every positive integer factors uniquely into primes. In a semigroup, inverses and cancellation are generally absent, and unique factorization fails. This non-uniqueness is not a defect but a source of rich combinatorial structure, and measuring it is the subject of **factorization theory** [62, 63, 95].

DEFINITION 1.2.16. *Let $S = \langle g_1, \dots, g_k \rangle$ be a numerical or affine semigroup. A* ***factorization*** *of $n \in S$ is a vector $\mathbf{a} = (a_1, \dots, a_k) \in \mathbb{Z}_{\geq 0}^k$ such that $a_1 g_1 + \cdots + a_k g_k = n$. The* ***set of factorizations*** *of n is*

$$\mathsf{Z}(n) = \{\mathbf{a} \in \mathbb{Z}_{\geq 0}^k : a_1 g_1 + \cdots + a_k g_k = n\}.$$

The ***length*** *of a factorization $\mathbf{a}$ is its ℓ_1-norm $|\mathbf{a}| = a_1 + \cdots + a_k$, and the* ***set of lengths*** *of n is*

$$\mathsf{L}(n) = \{|\mathbf{a}| : \mathbf{a} \in \mathsf{Z}(n)\}.$$

EXAMPLE 1.2.17. *In $S = \langle 6, 9, 20 \rangle$, consider $n = 120$. A factorization of 120 is a vector $(a, b, c) \in \mathbb{Z}_{\geq 0}^3$ satisfying $6a + 9b + 20c = 120$; its length is $a + b + c$. The complete set of factorizations is*

$$\begin{aligned}\mathsf{Z}(120) = \{\ & (20,0,0),\ (17,2,0),\ (14,4,0),\ (11,6,0),\ (8,8,0),\ (5,10,0), \\ & (2,12,0),\ (10,0,3),\ (7,2,3),\ (4,4,3),\ (1,6,3),\ (0,0,6)\ \},\end{aligned}$$

so $|\mathsf{Z}(120)| = 12$. The corresponding lengths are

$$\mathsf{L}(120) = \{6, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\}.$$

Geometrically, $\mathsf{Z}(120)$ is the set of lattice points in $120P_S$, where P_S is the numerical semigroup polytope. The dilation $120P_S$ is the triangle in $\mathbb{R}^3$ cut out by

$$6a + 9b + 20c = 120, \qquad a, b, c \geq 0,$$

with vertices $(20, 0, 0)$, $(0, \frac{40}{3}, 0)$, and $(0, 0, 6)$. Two vertices are integer points, appearing in $\mathsf{Z}(120)$ with lengths 20 and 6; the third, $(0, \frac{40}{3}, 0)$, is non-integer and contributes no factorization. Moving between factorizations is accomplished via ***trades****: replacements of one set of generators for another of equal total value. The semigroup S has two circuit trades, $3 \cdot 6 = 2 \cdot 9$ and $10 \cdot 6 = 3 \cdot 20$, together with one additional Graver basis trade $6 + 6 \cdot 9 = 3 \cdot 20$ obtained as a sign-consistent combination of the two circuits; every trade in S decomposes into these three. Geometrically, each trade type corresponds to a family of parallel edges in $120P_S$: the trade $3 \cdot 6 = 2 \cdot 9$ moves along the two horizontal rows, $10 \cdot 6 = 3 \cdot 20$ connects the rows vertically, and $6 + 6 \cdot 9 = 3 \cdot 20$ crosses diagonally. Together they explain the gap $\{7, 8, 9\} \not\subset \mathsf{L}(120)$: no trade changes length by 1, 2, or 3, so those lengths are unreachable from either extreme. See Figure 1.9.*

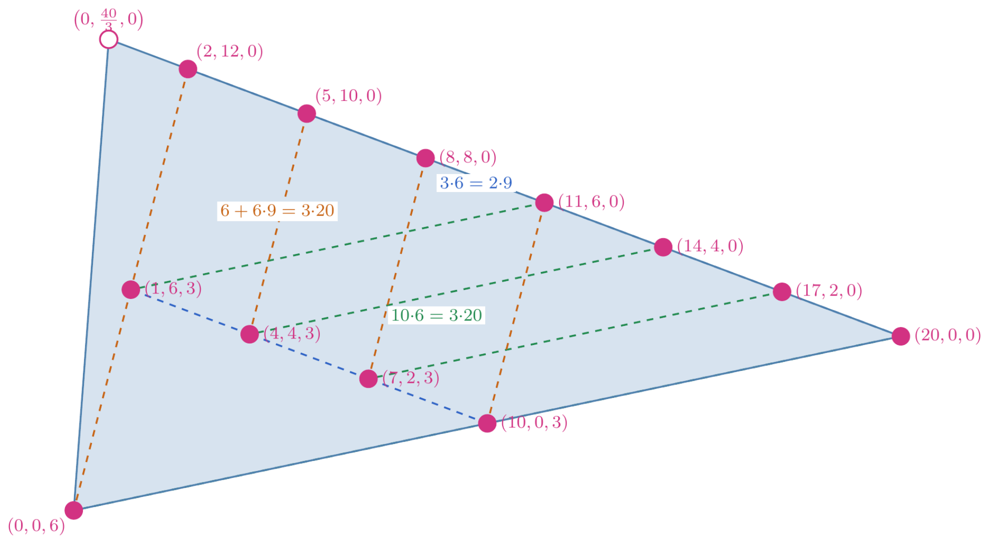


FIGURE 1.9. The factorization polytope $120P_S$ for $S = \langle 6, 9, 20\rangle$, projected to $\mathbb{R}^2$ from its ambient plane in $\mathbb{R}^3$. Dashed edges indicate the three Graver basis trades.

Several invariants measure the complexity of $\mathsf{L}(n)$ and $\mathsf{Z}(n)$ [62,63]. Elasticity captures how "spread out" the length set is: an element with elasticity close to 1 has factorizations of nearly equal length, while large elasticity signals that very short and very long factorizations coexist. The delta set records the gaps between consecutive lengths, measuring how far $\mathsf{L}(n)$ is from being an arithmetic progression. The catenary degree measures how hard it is to navigate between factorizations via trades: a small catenary degree means any two factorizations can be connected by a short chain of small trades, while a large catenary degree signals the presence of factorizations that are difficult to reach from one another. Betti elements are those for which $\mathsf{Z}(n)$ splits into components with no shared generators at all, making them the primary obstruction to a small catenary degree [27,59]. For the semigroup as a whole, these invariants are taken over all elements, giving a global picture of how non-unique factorization behaves in S.

DEFINITION 1.2.18. *Let $n \in S$ with $\mathsf{L}(n) = \{\ell_1 < \ell_2 < \cdots < \ell_r\}$ and $\mathbf{z}_1, \mathbf{z}_2 \in \mathsf{Z}(n)$.*

- *The **elasticity** of an element $n \in S$ is $\rho(n) = \frac{\ell_r}{\ell_1}$. The **elasticity** of the semigroup S is $\rho(S) = \sup_{n \in S} \rho(n)$.*
- *The **delta set** of an element $n \in S$ is $\Delta(n) = \{\ell_{i+1} - \ell_i : 1 \leq i \leq r-1\}$. The **delta set** of the semigroup S is $\Delta(S) = \bigcup_{n \in S} \Delta(n)$.*

- *The **distance** between two factorizations* $\mathbf{z}_1$ *and* $\mathbf{z}_2$ *is* $\mathsf{d}(\mathbf{z}_1, \mathbf{z}_2) = \max\big(|\mathbf{z}_1| - |\gcd(\mathbf{z}_1, \mathbf{z}_2)|,\ |\mathbf{z}_2| - |\gcd(\mathbf{z}_1, \mathbf{z}_2)|\big)$*, where* $\gcd$ *is taken component-wise as the entry-wise minimum.*
- *The **catenary degree** of an element* $n \in S$ *is the smallest* N *such that any two factorizations of* n *can be connected by a sequence* $\mathbf{z}_1 = \mathbf{w}_0, \dots, \mathbf{w}_k = \mathbf{z}_2$ *in* $\mathsf{Z}(n)$ *with* $\mathsf{d}(\mathbf{w}_i, \mathbf{w}_{i+1}) \le N$ *for all* i*. It is denoted* $\mathsf{c}(n)$*. The **catenary degree** of* S *is* $\mathsf{c}(S) = \sup_{n \in S} \mathsf{c}(n)$*.*
- *An element* $n \in S$ *is a **Betti element** if the graph on* $\mathsf{Z}(n)$ *with edges* $\mathbf{z}_1 \sim \mathbf{z}_2$ *whenever* $\gcd(\mathbf{z}_1, \mathbf{z}_2) \ne \mathbf{0}$ *is disconnected.*

Example 1.2.19. *Continuing Example 1.2.17, we have* $\mathsf{L}(120) = \{6, 10, 11, \dots, 20\}$*, so* $\rho(120) = 20/6 = 10/3$ *and* $\Delta(120) = \{1, 4\}$*: one large gap of* 4 *from* 6 *to* 10*, then steps of* 1 *the rest of the way. For the semigroup,* $\rho(S) = 10/3$ *and* $\Delta(S) = \{1, 2, 3, 4\}$*.*

The structure of $\Delta(120)$ *is explained by the Graver basis trades. Each trade changes length by a fixed amount: the trade* $3{\cdot}6 = 2{\cdot}9$ *changes length by* ± 1*, the trade* $6 + 6{\cdot}9 = 3{\cdot}20$ *by* ± 4*, and the trade* $10{\cdot}6 = 3{\cdot}20$ *by* ± 7*. The gaps in* $\mathsf{L}(120)$ *are precisely those lengths unreachable by any combination of these jumps from an element of* $\mathsf{Z}(120)$*. In particular,* $(1, 6, 3)$ *of length* 10 *has only one downward trade available: the trade* $6 + 6{\cdot}9 = 3{\cdot}20$ *sends it to* $(0, 0, 6)$ *of length* 6*, a jump of* 4*, skipping lengths* 7*,* 8*, and* 9*. More generally,* $\min \Delta(S)$ *divides every length change of a Graver basis trade of* S*; here those length changes are* 1*,* 4*, and* 7*, with* $\gcd(1, 4, 7) = 1$*, consistent with* $\min \Delta(S) = 1$*.*

Turning to the catenary degree, the Betti elements of S *are* 18 *and* 60*. For* $n = 18$*,*

$$\mathsf{Z}(18) = \{(3, 0, 0),\ (0, 2, 0)\},$$

and $\gcd\big((3, 0, 0), (0, 2, 0)\big) = \mathbf{0}$*, so the two factorizations share no generator. This is the circuit trade* $3{\cdot}6 = 2{\cdot}9$ *in its starkest form: the two sides use entirely disjoint sets of generators. For* $n = 60$*, we have*

$$\mathsf{Z}(60) = \{(0, 0, 3)\} \sqcup \{(1, 6, 0),\ (4, 4, 0),\ (7, 2, 0),\ (10, 0, 0)\},$$

where $(0, 0, 3)$ *shares no generator with any factorization in the second component. The catenary degree is realized at this element:* $\mathsf{d}\big((0, 0, 3), (1, 6, 0)\big) = \max(3, 7) = 7$*, so* $\mathsf{c}(60) = \mathsf{c}(S) = 7$*.*

Example 1.2.20. *The **factorization graph** of $n \in S$ is the graph $\nabla(n)$ whose vertices are the elements of $\mathsf{Z}(n)$ and whose edges connect $\mathbf{z}_1, \mathbf{z}_2 \in \mathsf{Z}(n)$ whenever $\gcd(\mathbf{z}_1, \mathbf{z}_2) \neq \mathbf{0}$, that is, whenever the two factorizations share at least one generator. The factorization graphs of the Betti elements of $S = \langle 6, 9, 20 \rangle$ are shown in Figure 1.10. At $n = 18$, the only two factorizations are $(3, 0, 0)$ and $(0, 2, 0)$, corresponding to $3 \cdot 6$ and $2 \cdot 9$. Since $\gcd\big((3, 0, 0), (0, 2, 0)\big) = \mathbf{0}$, they share no generator, and $\nabla(18)$ is disconnected. At $n = 60$, the factorization $(0, 0, 3)$ shares no generator with any of the four factorizations using only 6s and 9s, so $\nabla(60)$ again splits into two components. These are precisely the elements at which the circuit trades $3 \cdot 6 = 2 \cdot 9$ and $10 \cdot 6 = 3 \cdot 20$ first create an irreducible conflict between representations, and no trade can bridge the two components without passing through a factorization outside $\mathsf{Z}(n)$.*

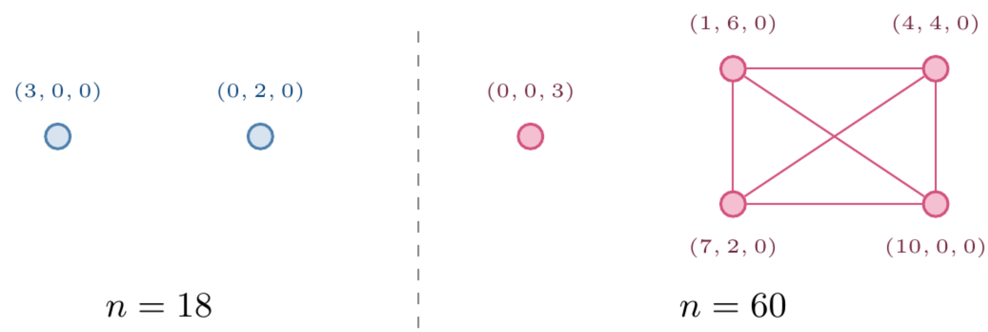


Figure 1.10. Factorization graphs of the Betti elements 18 and 60 of $S = \langle 6, 9, 20 \rangle$.

A key structural property of length sets in numerical semigroups is that they are eventually almost arithmetic progressions. Intuitively, for large enough $n \in S$, the set $\mathsf{L}(n)$ looks like an arithmetic progression everywhere except near its minimum and maximum, where finitely many lengths may be missing. This regularization of non-unique factorization as n grows is one of the deepest structural results in the theory.

Definition 1.2.21. *A finite set $L = \{a, a+d, a+2d, \ldots, a+(r-1)d\} \cup E$ of integers is an **almost arithmetic progression** (AAP) with step d, minimum a, and bound M if $E \subseteq [a, a+Md] \cup [a+(r-1-M)d, a+(r-1)d]$, that is, all exceptions lie within M steps of the endpoints.*

Equivalently, following the convention of [42], we say L is an AAP with step size λ, left bound t, and right bound t' if

$$L = \{m, m+\lambda, \dots, M-\lambda, M\} \setminus (A \cup A')$$

for some $A \subseteq [m, m+t] \cap (\lambda\mathbb{Z} + m)$ and $A' \subseteq [M-t', M] \cap (\lambda\mathbb{Z} + m)$, where $m = \min(L)$ and $M = \max(L)$. Said another way, L contains every element of the AP $\{m, m+\lambda, \dots, M\}$ in the interior window $[m+t, M-t']$, and is unconstrained outside it. The elements $\text{gaps}_l(L) = A$ and $\text{gaps}_r(L) = A'$ are called the **left** and **right gaps** of L.

Example 1.2.22. *In $S = \langle 6, 9, 20\rangle$, the length set $\mathsf{L}(60) = \{3, 7, 8, 9, 10\}$ is an AAP with step $\lambda = 1$, left bound $t = 3$, and right bound $t' = 0$. The full AP with step 1 from $m = 3$ to $M = 10$ is $\{3, 4, 5, 6, 7, 8, 9, 10\}$; the left gaps are $\{4, 5, 6\}$, each within $t = 3$ steps of the minimum, and there are no right gaps. Similarly, $\mathsf{L}(120) = \{6, 10, 11, \dots, 20\}$ is an AAP with $\lambda = 1$, $t = 4$, $t' = 0$: the left gaps $\{7, 8, 9\}$ lie within 4 steps of the minimum 6, and the interior $\{10, 11, \dots, 20\}$ is a complete AP.*

The connection between length sets and arithmetic ranges is exact. Applying the linear functional $c = (1, \dots, 1)$ to a factorization $(x_1, \dots, x_k) \in nP_S \cap \mathbb{Z}^k$ yields its length $x_1 + \cdots + x_k$, so

$$\mathsf{L}(n) = \text{AR}_c(nP_S).$$

The length set of $n \in S$ is precisely the arithmetic range of the dilated numerical semigroup polytope in the all-ones direction. This geometric rephrasing is what allows the arithmetic width machinery of Chapter 3 to bear on factorization theory.

The following theorem, a cornerstone of factorization theory, asserts that length sets are eventually AAPs.

Theorem 1.2.23 (Structure Theorem for Sets of Lengths [61,90]). *Let S be a numerical semigroup. There exist constants λ, t, t' depending only on S such that for all $n \in S$ with $n \gg 0$, the set $\mathsf{L}(n)$ is an AAP with step λ, left bound t, and right bound t'.*

In particular, $\lambda = \min \Delta(S)$ and the bounds t, t' are uniform across all sufficiently large elements. For $S = \langle 6, 9, 20\rangle$, where $\min \Delta(S) = 1$, this says that for $n \gg 0$ the length set $\mathsf{L}(n)$ is eventually gapless in its interior, with all deviations from the AP $\{m, m+1, \dots, M\}$ confined to windows of fixed width at the extremes. The isolated outlier at the minimum (such as 6 in $\mathsf{L}(120)$, separated from $\{10, \ldots, 20\}$ by a gap of 4) is a geometric artifact: it corresponds to the factorization at the non-integer vertex $(0, \frac{40}{3}, 0)$ of P_S, which contributes no lattice point but distorts the AP structure near the minimum of the length set.

This theorem is a special case of the arithmetic width results in Chapter 3. Applying Theorem 1.3.14 to the numerical semigroup polytope P_S with functional $c = (1, \ldots, 1)$ recovers Theorem 1.2.23 directly, since $\mathrm{AR}_c(nP_S) = \mathsf{L}(n)$ and the constants t, t', λ in the arithmetic width theorem depend only on $K = P_S$, hence only on S. In this sense, the structure theorem for sets of lengths is not merely analogous to the arithmetic range theorem; it is a corollary of it.

1.3. Ehrhart Theory and Quasipolynomials

Ehrhart theory studies the enumeration of lattice points in dilations of convex polytopes. Initiated by Eugène Ehrhart in the 1960s, the theory establishes that for a rational polytope $P \subset \mathbb{R}^d$, the function $n \mapsto |nP \cap \mathbb{Z}^d|$ is a quasipolynomial in the dilation parameter n [**12**]. Since its introduction, Ehrhart theory has become central to discrete geometry, combinatorics, and commutative algebra. Its language and results are indispensable for the arithmetic width and polytopal norms projects in this thesis, and the quasipolynomial theme recurs throughout. In this section, we introduce the field.

1.3.1. The Ehrhart Function.

Definition 1.3.1. *Let $P \subseteq \mathbb{R}^d$ be a polytope and $t \in \mathbb{Z}_{>0}$. The t-th **dilation** of P is*

$$tP = \{tx : x \in P\}.$$

*The **Ehrhart function** of P is*

$$L(P, t) = |tP \cap \mathbb{Z}^d|,$$

the number of lattice points in the t-th dilate of P.

Example 1.3.2. *Let $P = [0,1]^2 \subseteq \mathbb{R}^2$. The dilation $tP = [0,t]^2$ contains $(t+1)^2$ lattice points, so $L(P,t) = t^2 + 2t + 1$. This is a polynomial of degree $2 = \dim(P)$ with leading coefficient $1 = \mathrm{vol}(P)$.*

For a lattice polytope, $L(P, t)$ is always a polynomial; for a rational polytope, it is a quasipolynomial. These results are referred to as **Ehrhart's Theorem** [**12**].

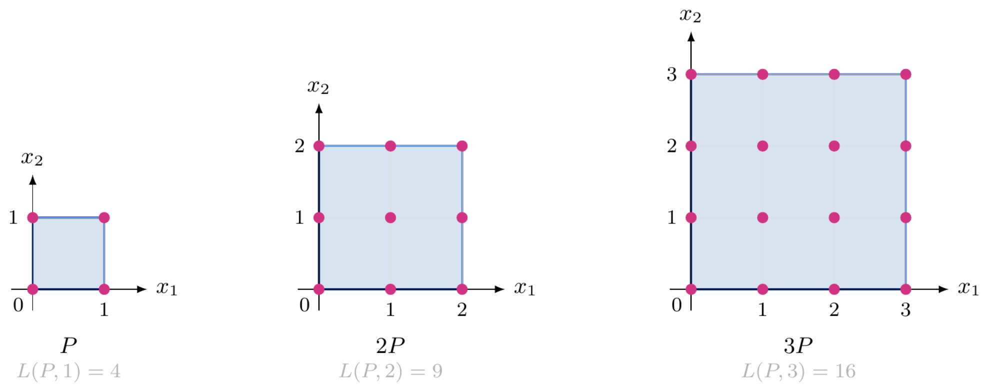


FIGURE 1.11. Dilations P, $2P$, $3P$ of the unit square $[0,1]^2$ with lattice points marked. The counts 4, 9, 16 agree with $L(P,t)=(t+1)^2$ at $t=1,2,3$.

DEFINITION 1.3.3. *A function $f : \mathbb{Z}_{\geq 0} \to \mathbb{Q}$ is a* ***quasipolynomial*** *of* ***period*** *m and* ***degree*** *d if there exist polynomials $p_0, \ldots, p_{m-1} \in \mathbb{Q}[n]$ of degree at most d such that $f(n) = p_r(n)$ where $r \equiv n \pmod{m}$. A polynomial is a quasipolynomial of period 1. We say f is* ***eventually quasipolynomial*** *if it agrees with a quasipolynomial for all sufficiently large n.*

THEOREM 1.3.4 (Ehrhart [12]). *Let $P \subseteq \mathbb{R}^d$ be a polytope.*

(a) If P is a lattice polytope, then $L(P,t)$ is a polynomial in t of degree $\dim(P)$, *with leading coefficient* $\mathrm{vol}(P)$ *and constant term 1.*

(b) If P is a rational polytope, then $L(P,t)$ is a quasipolynomial in t of degree $\dim(P)$ *whose period divides the* ***denominator*** *of P, the smallest positive integer D such that DP has integer vertices.*

EXAMPLE 1.3.5. *Let $P = [0,1/2]^2$, with denominator 2. Considering the dilation $tP = [0,t/2]^2$ yields*

$$L(P,t) = \begin{cases} \left(\dfrac{t}{2}+1\right)^2 & t \text{ even}, \\ \left(\dfrac{t+1}{2}\right)^2 & t \text{ odd}, \end{cases}$$

a quasipolynomial of period 2 and degree 2. The formula holds because the lattice points of tP are exactly the integer points (x_1,x_2) with $0 \leq x_i \leq t/2$, and the number of integers in $[0,t/2]$ is $\lfloor t/2 \rfloor + 1$, which alternates between $t/2+1$ and $(t+1)/2$ depending on the parity of t. Unlike the unit square, where every dilation adds a new row and column of lattice points, here the half-integer *boundary of odd dilations falls strictly between integers, contributing nothing new: the counts for $t = 2$ and $t = 3$ are both 4, as seen in Figure 1.12. The leading coefficient $1/4 = \mathrm{vol}(P)$ is consistent across both cases, as guaranteed by Ehrhart's theorem for rational polytopes.*

EXAMPLE 1.3.6. *The factorizations of an element $n \in S$ are precisely the lattice points of the dilated polytope nP_S, so the Ehrhart function $L(P_S, n) = |nP_S \cap \mathbb{Z}^3| = |\mathsf{Z}(n)|$ counts factorizations. Ehrhart theory thus guarantees that the number of factorizations of n is eventually quasipolynomial in n. Let $S = \langle 6, 9, 20\rangle$ with numerical semigroup polytope*

$$P_S = \mathrm{conv}\left\{\tfrac{1}{6}e_1,\ \tfrac{1}{9}e_2,\ \tfrac{1}{20}e_3\right\} \subset \mathbb{R}^3.$$

Since P_S is a rational simplex with denominator $D = \mathrm{lcm}(6, 9, 20) = 180$, Theorem 1.3.4 guarantees that $L(P_S, n)$ is a quasipolynomial of degree 2 and period dividing 180. The leading coefficient is $\mathrm{Vol}_2(P_S) = \frac{1}{2160}$ across all residue classes, consistent with $2! \cdot \frac{1}{2160} = \frac{1}{1080}$.

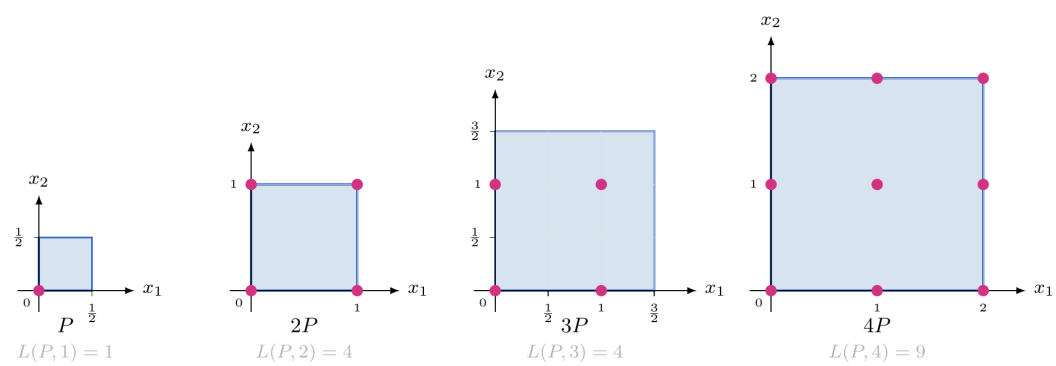


FIGURE 1.12. Dilations P, $2P$, $3P$, $4P$ of $[0, \frac{1}{2}]^2$ with lattice points marked. The counts $1, 4, 4, 9$ reflect the period-2 behavior: odd dilations introduce no new lattice points relative to the preceding even dilation.

The Ehrhart function can be encoded as a generating function. The **Ehrhart series** of P is

$$\mathrm{Ehr}(P, z) = \sum_{t=0}^{\infty} L(P, t)\, z^t.$$

For a lattice polytope of dimension d, this series is rational:

$$\mathrm{Ehr}(P, z) = \frac{h^*(z)}{(1 - z)^{d+1}},$$

where $h^*(z) = h_0^* + h_1^* z + \cdots + h_d^* z^d$ is the **h^*-polynomial** of P, which has nonnegative integer coefficients [107].

Example 1.3.7. *For $P = [0,1]^2$, we have $L(P,t) = (t+1)^2$, and*

$$\mathrm{Ehr}(P,z) = \frac{1+z}{(1-z)^3}, \qquad h^*(z) = 1+z.$$

To see where this comes from, consider the cone $C = \mathrm{cone}(P \times \{1\}) \subseteq \mathbb{R}^3$, whose lattice points are the triples $(a,b,t) \in \mathbb{Z}^3_{\geq 0}$ with $0 \leq a \leq t$ and $0 \leq b \leq t$. These are generated as a semigroup by the four vertices of P lifted to height 1:

$$v_1 = (0,0,1), \quad v_2 = (1,0,1), \quad v_3 = (0,1,1), \quad v_4 = (1,1,1).$$

Assigning each generator a monomial weight tracking its coordinates,

$$v_1 \mapsto z, \quad v_2 \mapsto x_1 z, \quad v_3 \mapsto x_2 z, \quad v_4 \mapsto x_1 x_2 z,$$

the multivariate generating function for $C \cap \mathbb{Z}^3$ is

$$F(x_1,x_2,z) = \frac{1 - x_1x_2z^2}{(1-z)(1-x_1z)(1-x_2z)(1-x_1x_2z)}. \tag{1.1}$$

The denominator has one factor for each generator; the numerator accounts for the single relation $v_2 \cdot v_3 = v_1 \cdot v_4$ (i.e., $(1,0,1)+(0,1,1) = (0,0,1)+(1,1,1)$), whose monomial weight is $(x_1z)(x_2z) = x_1x_2z^2$.

Expanding (1.1) as a power series in z, the coefficient of z^t is

$$[z^t]\, F(x_1,x_2,z) = \sum_{a=0}^{t}\sum_{b=0}^{t} x_1^a x_2^b = \left(\sum_{a=0}^{t} x_1^a\right)\left(\sum_{b=0}^{t} x_2^b\right),$$

since each lattice point (a,b,t) in tP contributes the monomial $x_1^a x_2^b z^t$. For example, the z^1 coefficient is $1 + x_1 + x_2 + x_1x_2$, one term for each of the four lattice points $(0,0)$, $(1,0)$, $(0,1)$, $(1,1)$ of P. Substituting $x_1 = x_2 = 1$ collapses each monomial $x_1^a x_2^b$ to 1, so the coefficient of z^t becomes the count $|\{(a,b) : 0 \leq a,b \leq t\}| = (t+1)^2$, and

$$F(1,1,z) = \frac{1-z^2}{(1-z)^4} = \frac{(1-z)(1+z)}{(1-z)^4} = \frac{1+z}{(1-z)^3} = \mathrm{Ehr}(P,z).$$

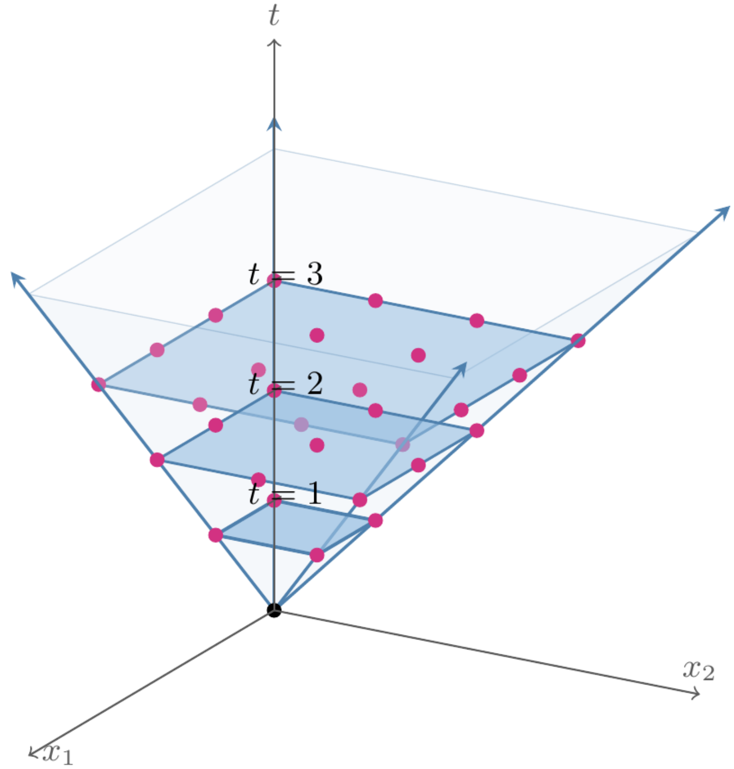


FIGURE 1.13. The cone $C = \text{cone}(P \times \{1\}) \subseteq \mathbb{R}^3$ over the unit square $P = [0, 1]^2$, with the discrete slices at $t = 1, 2, 3$.

Computing $L(P, t)$ directly is expensive as dimension grows: the number of lattice points in tP can be exponentially large in the bit-length of the input, even for fixed d. The difficulty is not merely counting but *representing* the answer efficiently. In variable dimension, determining whether a polytope contains even a single lattice point is already NP-complete [**114**], and lattice width is NP-hard to compute. Fixing the dimension changes the picture entirely: with d fixed, the number of "directions" to check is bounded, and Lenstra's algorithm shows that integer feasibility is polynomial *in fixed dimension* [**83**]. Barvinok's algorithm goes further, giving a polynomial-time algorithm for the lattice point count.

THEOREM 1.3.8 (Barvinok [**8**]). *For fixed dimension d, the number of lattice points in a rational polytope $P \subseteq \mathbb{R}^d$ can be computed in polynomial time in the input size of P.*

The key idea is to encode lattice points as exponent vectors of monomials. Given a rational polytope $P \subseteq \mathbb{R}^d$, define its **generating function**

$$g_P(\mathbf{x}) = \sum_{\alpha \in P \cap \mathbb{Z}^d} \mathbf{x}^\alpha = \sum_{\alpha \in P \cap \mathbb{Z}^d} x_1^{\alpha_1} \cdots x_d^{\alpha_d}.$$

Naively, this sum has one term per lattice point — potentially exponentially many. Barvinok's algorithm decomposes the indicator function of P into a signed sum of indicator functions of **unimodular cones** (cones whose generating rays form a basis for $\mathbb{Z}^d$), each of which admits a compact rational generating function. The result is a representation

$$g_P(\mathbf{x}) = \sum_{i \in I} \epsilon_i \frac{\mathbf{x}^{u_i}}{\prod_{j=1}^d (1 - \mathbf{x}^{v_{ij}})},$$

where I is a *polynomial-size* index set, $\epsilon_i \in \{+1, -1\}$, and $u_i, v_{ij} \in \mathbb{Z}^d$. Setting $x_1 = \cdots = x_d = 1$ recovers $|P \cap \mathbb{Z}^d|$; more generally, any monomial substitution can be performed in polynomial time, which is what allows the computation of arithmetic ranges and Ehrhart series efficiently.

Example 1.3.9. *Let $P = [0,1]^2$. The tangent cone at each vertex of P is already unimodular, so Barvinok's decomposition requires no further subdivision. At each vertex v, the tangent cone has generating function $\mathbf{x}^v / \prod_j (1 - \mathbf{x}^{r_j})$ where r_j are the edge directions at v, normalized to point inward. Computing each:*

$$\begin{aligned}
\textit{at } (0,0) &: \frac{1}{(1-x_1)(1-x_2)}, \\
\textit{at } (1,0) &: \frac{x_1}{(1-x_1^{-1})(1-x_2)} = \frac{-x_1^2}{(1-x_1)(1-x_2)}, \\
\textit{at } (0,1) &: \frac{x_2}{(1-x_1)(1-x_2^{-1})} = \frac{-x_2^2}{(1-x_1)(1-x_2)}, \\
\textit{at } (1,1) &: \frac{x_1 x_2}{(1-x_1^{-1})(1-x_2^{-1})} = \frac{x_1^2 x_2^2}{(1-x_1)(1-x_2)}.
\end{aligned}$$

Summing these four terms (all with sign $+1$, since all cones are unimodular):

$$g_P(x_1, x_2) = \frac{1 - x_1^2 - x_2^2 + x_1^2 x_2^2}{(1-x_1)(1-x_2)} = \frac{(1-x_1^2)(1-x_2^2)}{(1-x_1)(1-x_2)} = (1+x_1)(1+x_2).$$

Expanding: $g_P = 1 + x_1 + x_2 + x_1 x_2$, one monomial per lattice point of P: $(0,0)$, $(1,0)$, $(0,1)$, $(1,1)$. Setting $x_1 = x_2 = 1$ gives $4 = |P \cap \mathbb{Z}^2|$. The crucial point is that this rational expression *has four terms regardless of the dilation: to count $|tP \cap \mathbb{Z}^2|$ for any t, one works with the cone over P and reads off coefficients from the same compact representation, recovering $L(P,t) = (t+1)^2$ without enumerating the $(t+1)^2$ lattice points individually.*

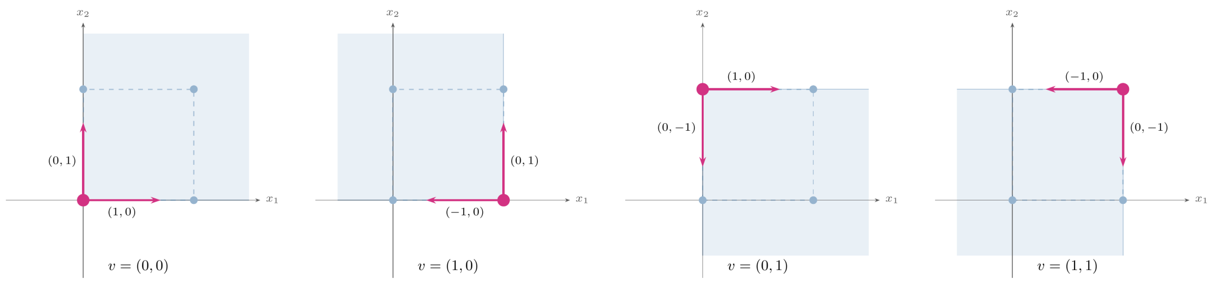


FIGURE 1.14. The four tangent cones of $P = [0,1]^2$ at each vertex, with inward edge directions marked. Each cone contributes one term to the generating function $g_P(x_1, x_2)$ in Barvinok's decomposition.

Barvinok's algorithm is used directly in our proof that arithmetic width is polynomial-time computable in fixed dimension. Given $g_P(\mathbf{x})$ in compact rational form, applying the linear functional $\ell_c(\mathbf{x}) = c^\top \mathbf{x}$ as a monomial substitution $x_i \mapsto z^{c_i}$ yields a univariate generating function whose monomials are exactly $\{z^{\ell_c(\alpha)} : \alpha \in P \cap \mathbb{Z}^d\} = \{z^j : j \in \mathrm{AR}_c(P)\}$. The arithmetic width $\mathrm{aw}_c(P) = |\,\mathrm{AR}_c(P)|$ is then the number of distinct monomials in this univariate function, computable in polynomial time via the Barvinok–Woods projection theorem [9]. See Section 1.3.3 for details.

1.3.2. Quasipolynomials in Combinatorics and Algebra. Quasipolynomials appear far beyond Ehrhart theory. They arise whenever a counting problem has periodic arithmetic structure, and they are stable under a wide range of constructions. Some common sources include:

- lattice-point enumeration in dilated rational polytopes (Ehrhart theory) [10, 12, 30],
- restricted partition functions [4, 77, 101],
- vector partition functions [45, 108, 112],
- Hilbert functions of finitely generated graded semigroup rings [21, 22, 37, 107], and
- factorization invariants in affine and numerical semigroups [25, 58, 94].

The following theorem collects equivalent characterizations of eventual quasipolynomiality that are each useful in different contexts. We will appeal to several of them throughout this thesis.

These characterizations and their equivalence are standard, but seldom are they presented together; see [**12**, **107**, **116**].

Theorem 1.3.10. *Let $f : \mathbb{N} \to \mathbb{Q}$. If any of the following hold, then f is eventually quasipolynomial. In each case the period is indicated.*

(1) (Periodic polynomials) *There exist $m \geq 1$ and polynomials $p_0, \ldots, p_{m-1} \in \mathbb{Q}[t]$ such that $f(n) = p_r(n)$ for all sufficiently large $n \equiv r \pmod{m}$. The period divides m.*

(2) (Rational generating function) *There exist $P(t) \in \mathbb{Q}[t]$ and $m_j, e_j \in \mathbb{Z}_{>0}$ such that*

$$\sum_{n\geq 0} f(n)t^n = \frac{P(t)}{\prod_{j=1}^{N}(1-t^{m_j})^{e_j}}.$$

The degree of f is at most $\sum_{j=1}^{N} e_j - 1$ and the period divides $\operatorname{lcm}(m_1, \ldots, m_N)$.

(3) (Finite differences) *There exist $d \geq 0$ and $m \geq 1$ such that for each $r \in \{0, \ldots, m-1\}$, $\Delta^{d+1} f(mn + r) = 0$ for all sufficiently large n, where $\Delta f(n) = f(n+1) - f(n)$ and $\Delta^k = \Delta \circ \Delta^{k-1}$. The degree is at most d and the period divides m.*

(4) (Ehrhart function) *There exists a rational polytope $P \subseteq \mathbb{R}^d$ such that $f(n) = |nP \cap \mathbb{Z}^d|$ for all sufficiently large n. The degree equals $\dim P$ and the period divides the denominator of P.*

(5) (Vector partition function) *There exist a fixed integer matrix $A \in \mathbb{Z}^{d\times k}$ and a linear function $b(n)$ such that $f(n) = \#\{x \in \mathbb{Z}^k_{\geq 0} : Ax = b(n)\}$ for all sufficiently large n. The period divides the lcm of the maximal minors of A.*

(6) (Hilbert function) *There exist a finitely generated graded commutative algebra R and a finitely generated graded R-module M such that $f(n) = \dim_{\Bbbk} M_n$ for all sufficiently large n. The period divides the lcm of the degrees of the generators of R.*

(7) (Presburger arithmetic) *There exists a formula $\Phi(x, n)$ in the first-order theory of $(\mathbb{Z}, +, \leq)$ such that $f(n) = \#\{x \in \mathbb{Z}^k : \Phi(x, n)\}$ for all sufficiently large n. The period is determined by the modular constraints appearing in Φ.*

(8) (Closure) *f is obtained from eventually quasipolynomial functions $g_1, \ldots, g_r$ of periods $m_1, \ldots, m_r$ by finitely many applications of addition, subtraction, scalar multiplication, multiplication, shifts $n \mapsto f(n + c)$, restriction to arithmetic progressions $n \mapsto f(an + b)$, finite convolution, or finite summation $\sum_{k=0}^{n} f(k)$. The period divides $\operatorname{lcm}(m_1, \ldots, m_r)$.*

Moreover, conditions (1), (2), *and* (3) *are not merely sufficient but also necessary: f is eventually quasipolynomial if and only if any one of* (1), (2), *or* (3) *holds.*

The following example illustrates characterizations (1), (2), and (4) concretely, showing how the same quasipolynomial can be expressed in several equivalent forms and how the period and degree can be read off from each.

Example 1.3.11. *Let*

$$f(n) = \#\{(x, y) \in \mathbb{Z}^2_{\geq 0} :\ 2x + 3y = n\}.$$

By characterization (4), f is a vector partition function with $A = \begin{pmatrix} 2 & 3 \end{pmatrix}$ and $b(n) = n$, so it is immediately quasipolynomial. We now find the period and degree explicitly via characterizations (1) and (2). Solving for x gives $x = \frac{n-3y}{2}$, which is a nonnegative integer if and only if

(1) $n - 3y \geq 0$, so $y \leq \lfloor n/3 \rfloor$,

(2) $n - 3y$ is even, i.e. $n \equiv y \pmod 2$.

Thus

$$f(n) = \#\{\, 0 \leq y \leq \lfloor n/3 \rfloor :\ y \equiv n \pmod 2 \,\}.$$

Letting $M = \lfloor n/3 \rfloor$, among $0, 1, \ldots, M$ the integers congruent to n modulo 2 are those with the same parity as n, giving

$$f(n) = \begin{cases} \left\lfloor \dfrac{M}{2} \right\rfloor + 1 & \text{if } n \text{ is even,} \\ \left\lfloor \dfrac{M+1}{2} \right\rfloor & \text{if } n \text{ is odd.} \end{cases}$$

Since $M = \lfloor n/3 \rfloor$, the value of $f(n)$ depends only on $n \bmod 6$. Writing $n = 6k + r$ with $0 \leq r < 6$, one obtains

$$f(n) = \begin{cases} k+1 & r = 0, \\ k & r = 1, \\ k+1 & r = 2, \\ k+1 & r = 3, \\ k+1 & r = 4, \\ k+1 & r = 5. \end{cases}$$

Thus f is a quasipolynomial of period 6 and degree 1, confirming characterization (1) with $m = 6$. For characterization (2), the generating function is

$$\sum_{n=0}^{\infty} f(n)\, t^n = \frac{1}{(1-t^2)(1-t^3)},$$

a rational function with denominator $(1-t^2)(1-t^3)$, from which the degree $\sum e_j - 1 = 2 - 1 = 1$ and period dividing $\operatorname{lcm}(2,3) = 6$ can be read off immediately.

Example 1.3.12. *Figure 1.15 collects twelve scatter plots illustrating the range of behaviors that quasipolynomials and eventually quasipolynomials can exhibit. Each panel plots a function of one integer variable n, with points colored by residue class modulo the relevant period so that the polynomial pieces of the quasipolynomial are visually separated. Table 1.3 records the formula, type, degree, period, and threshold of each panel.*

Many classical factorization invariants (length functions, elasticity, delta sets, and their growth functions) are built from the basic counting functions via finite sums, maxima, minima, and similar operations. Since quasipolynomial functions are stable under all of these (characterization (8) of Theorem 1.3.10), the resulting invariants inherit eventual quasipolynomial behavior. In this way, quasipolynomiality in factorization theory ultimately reflects the polyhedral structure of affine semigroups together with the periodic arithmetic constraints imposed by integrality.

1.3.3. Our Contributions: Arithmetic Width. Section 1.3 described the Ehrhart-theoretic principle that lattice-point counts in dilated rational polytopes are eventually quasipolynomial, and showed that this regularity extends to a wide family of related quantities through the closure properties of Theorem 1.3.10. Our second main contribution applies this principle to a new setting: rather than counting lattice points in a dilated polytope, we ask which integer values a linear functional attains on those lattice points, and how the resulting set behaves as the polytope is dilated.

The motivation comes from two earlier observations. From Section 1.1.6, the lattice width $w_c(K)$ measures the continuous span of K in a direction c but is insensitive to gaps in the integer values $c^\top x$ attains on $K \cap \mathbb{Z}^d$. From Section 1.2.4, the set of lengths $\mathsf{L}(n)$ of an element of a numerical semigroup is exactly the set of values of the all-ones functional on $nP_S \cap \mathbb{Z}^k$, and the Structure

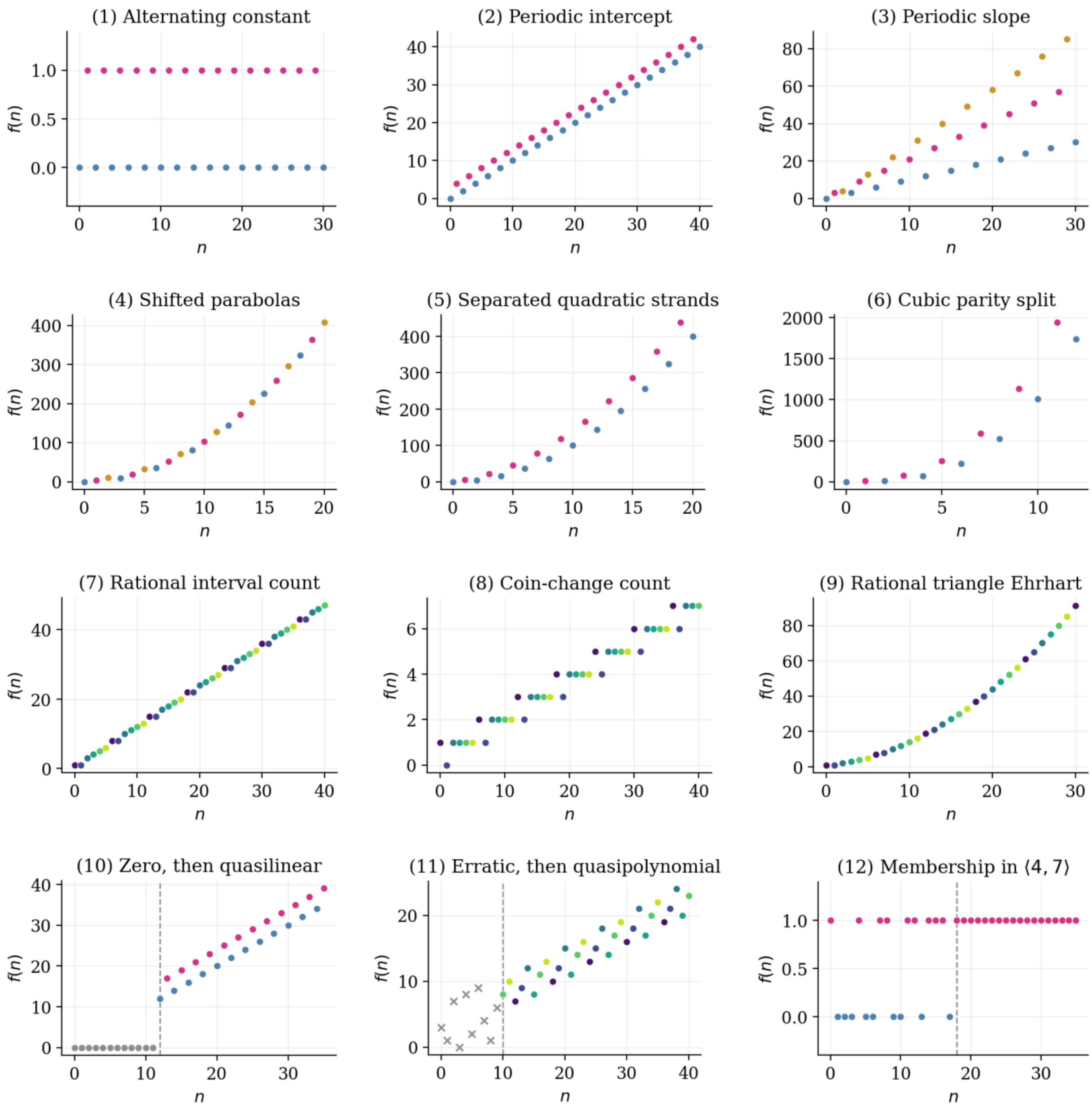


FIGURE 1.15. A zoo of quasipolynomial and eventually quasipolynomial behavior. Each panel is a scatter plot in the variable n. Points are colored by residue class modulo the relevant period. In panels (10)–(12), the dashed vertical line marks the threshold for eventual quasipolynomial behavior.

Theorem for Sets of Lengths (Theorem 1.2.23) shows that these length sets are eventually almost arithmetic progressions in the sense of Definition 1.2.21. Both observations point to the same underlying object: the integer values attained by a linear functional on the lattice points of a convex body.

Panel	*Formula*	*Type*	*Degree*	*Period*	*Threshold*
(1)	$f(n) = \begin{cases} 0 & n \text{ even} \\ 1 & n \text{ odd} \end{cases}$	*QP*	0	2	—
(2)	$f(n) = \begin{cases} n & n \text{ even} \\ n+3 & n \text{ odd} \end{cases}$	*QP*	1	2	—
(3)	$f(n) = \begin{cases} n & n \equiv 0 \pmod 3 \\ 2n+1 & n \equiv 1 \pmod 3 \\ 3n-2 & n \equiv 2 \pmod 3 \end{cases}$	*QP*	1	3	—
(4)	$f(n) = \begin{cases} n^2 & n \equiv 0 \pmod 3 \\ n^2+3 & n \equiv 1 \pmod 3 \\ n^2+7 & n \equiv 2 \pmod 3 \end{cases}$	*QP*	2	3	—
(5)	$f(n) = \begin{cases} n^2 & n \text{ even} \\ n^2+4n+1 & n \text{ odd} \end{cases}$	*QP*	2	2	—
(6)	$f(n) = \begin{cases} n^3+n & n \text{ even} \\ n^3+5n^2+2 & n \text{ odd} \end{cases}$	*QP*	3	2	—
(7)	$f(n) = \lfloor 5n/3 \rfloor - \lceil n/2 \rceil + 1$	*QP*	1	$\mid 6$	—
(8)	$f(n) = \#\{(x,y) \in \mathbb{Z}^2_{\geq 0} : 2x+3y = n\}$	*QP*	1	6	—
(9)	$f(n) = \#\{(x,y) \in \mathbb{Z}^2_{\geq 0} : 2x+3y \leq n\}$	*QP*	2	$\mid 6$	—
(10)	$f(n) = \begin{cases} 0 & n < 12 \\ n & n \geq 12,\ n \text{ even} \\ n+4 & n \geq 12,\ n \text{ odd} \end{cases}$	*EQP*	1	2	12
(11)	$f(n) = \begin{cases} \textit{arbitrary} & n < 10 \\ \lfloor n/2 \rfloor + 1 + 2(n \bmod 3) & n \geq 10 \end{cases}$	*EQP*	1	$\mid 6$	10
(12)	$f(n) = \begin{cases} 1 & n \in \langle 4,7 \rangle \\ 0 & n \notin \langle 4,7 \rangle \end{cases}$	*EQP*	0	1	18

Table 1.3. Summary of the twelve panels in Figure 1.15. Here QP denotes quasipolynomial and EQP denotes eventually quasipolynomial. The notation $\mid 6$ in the period column means that the displayed period divides 6; this does not assert that 6 is minimal.

Definition 1.3.13. *Let $K \subseteq \mathbb{R}^d$ be a convex body and $c \in \mathbb{Z}^d \setminus \{0\}$. The* ***arithmetic range*** *of K in direction c is*

$$\mathrm{AR}_c(K) = \{c^\top x : x \in K \cap \mathbb{Z}^d\},$$

the set of integer values attained by $c^\top x$ on the lattice points of K. The ***arithmetic width*** *of K in direction c is $\mathrm{aw}_c(K) = |\,\mathrm{AR}_c(K)|$, and the* ***arithmetic width*** *of K is*

$$\mathrm{aw}(K) = \min_{c\in\mathbb{Z}^d\setminus\{0\}} \mathrm{aw}_c(K).$$

The two notions of width are related by $\mathrm{aw}_c(K) \le w_c(K) + 1$, with strict inequality precisely when $\mathrm{AR}_c(K)$ has gaps. Unlike lattice width, arithmetic width is insensitive to the magnitude of c: parallel directions yield the same arithmetic width, since $\mathrm{AR}_{\lambda c}(K) = \lambda\,\mathrm{AR}_c(K)$ has the same cardinality as $\mathrm{AR}_c(K)$ for any nonzero $\lambda \in \mathbb{Z}$. The two invariants also need not be minimized in the same directions.

In joint work with De Loera and O'Neill [42], we establish four main results about arithmetic width, proved in Chapter 3. The first is a structure theorem in the Ehrhart spirit: just as the Ehrhart function $|nK \cap \mathbb{Z}^d|$ is eventually quasipolynomial as n grows, the set $\mathrm{AR}_c(nK)$ itself acquires a regular arithmetic structure for n large.

Theorem 1.3.14 (De Loera, Marsters, O'Neill [42]). *Let $K \subseteq \mathbb{R}^d$ be a convex body and $\ell_c : \mathbb{Z}^d \to \mathbb{Z}$ a linear functional. There exist constants t, t', and λ depending only on K such that for all $n \gg 0$,*

$$\mathrm{AR}_c(nK) \cap [nm + t,\, nM - t']$$

is an arithmetic progression of step size λ, where $m = \min_{x\in K} \ell_c(x)$ and $M = \max_{x\in K} \ell_c(x)$.

In other words, for $n \gg 0$ the arithmetic range $\mathrm{AR}_c(nK)$ is an AAP: an arithmetic progression of step λ throughout an interior window whose width grows with n, with all deviations from the AP confined to fixed-size windows of widths t and t' near the endpoints.

Theorem 1.3.14 generalizes the Structure Theorem for Sets of Lengths (Theorem 1.2.23). Taking $K = P_S$ to be the numerical semigroup polytope of $S = \langle g_1, \ldots, g_k\rangle$ and $c = (1, \ldots, 1)$ to be the all-ones functional, the identification $\mathrm{AR}_c(nP_S) = \mathsf{L}(n)$ from Section 1.2.4 immediately recovers the classical statement: there exist t, t', and λ depending only on S such that for $n \gg 0$, $\mathsf{L}(n)$ is an AAP with these parameters. The constants λ, t, t' in Theorem 1.3.14 depend only on $K = P_S$ and hence only on S, matching the conclusion of Theorem 1.2.23. The geometric framework also clarifies the source of the left exceptions: as observed in Example 1.2.17, the non-integer vertex $(0, \frac{40}{3}, 0)$ of $120P_S$ contributes no factorization, and it is precisely such non-integer vertices that distort the AP structure near the endpoints of $\mathsf{L}(n)$. In this sense, the structure theorem for sets of lengths is a corollary of the arithmetic range theorem.

The second main result returns to the quasipolynomial theme of Section 1.3 more directly. The Ehrhart function $L(P, n) = |nP \cap \mathbb{Z}^d|$ counts lattice points in nP; the arithmetic width $\mathrm{aw}_c(nP)$ counts the integer values those lattice points attain under c. Both are functions of n extracted from the same dilation, and both turn out to be eventually quasipolynomial, with $\mathrm{aw}_c(nP)$ a quasilinear function of n regardless of the dimension of P. Whereas lattice width grows linearly in the dilation parameter, the arithmetic width acquires the periodic residue behavior characteristic of quasipolynomials, and remarkably this behavior survives even when one minimizes over directions.

THEOREM 1.3.15 (De Loera, Marsters, O'Neill [42]). *Let $P \subseteq \mathbb{R}^d$ be a rational polytope and $c \in \mathbb{Z}^d \setminus \{0\}$. Then $\mathrm{aw}_c(nP)$ and $\mathrm{aw}(nP)$ are eventually quasilinear functions of n.*

A key step in the proof is showing that the directions achieving the minimum arithmetic width recur periodically: if $n_1 \equiv n_2 \pmod{\mathrm{denom}(P)}$, then $\mathrm{aw}(n_1P)$ and $\mathrm{aw}(n_2P)$ are attained in the same directions for $n_1, n_2 \gg 0$. This periodicity is what allows the eventually quasilinear behavior to survive the minimization over an a priori infinite set of directions, and it places $\mathrm{aw}(nP)$ alongside the Ehrhart function and the other examples of Theorem 1.3.10 as a natural source of quasipolynomial behavior in lattice geometry.

The third result addresses computational complexity. The lattice width is NP-hard to compute and even hard to approximate [14, 114], though it becomes polynomial-time computable in fixed dimension via Lenstra's algorithm. Our analogous results for arithmetic width combine Barvinok's algorithm (Theorem 1.3.8) with the projection theorem of Barvinok and Woods [9] to encode the arithmetic range as a rational generating function whose cardinality can be extracted efficiently.

THEOREM 1.3.16 (De Loera, Marsters, O'Neill [42]). *Let $P \subseteq \mathbb{R}^d$ be a rational polytope with input bit-size L.*

(a) In fixed dimension, given $c \in \mathbb{Z}^d \setminus \{0\}$, there is an algorithm computing $\mathrm{aw}_c(P)$ in time polynomial in L and the bit-size of c.

(b) In fixed dimension, there is an algorithm computing $\mathrm{aw}(P)$ in single-exponential time in L.

The algorithm in part (b) proceeds by first computing a finite test set of directions T, in single-exponential time, such that $\mathrm{aw}(P) = \mathrm{aw}_t(P)$ for some $t \in T$, and then applying the algorithm of part (a) to each $t \in T$.

The fourth result clarifies the distinction between arithmetic and lattice width by exhibiting two extremes: the directions minimizing them can be entirely disjoint, and arithmetic ranges can be arbitrarily irregular as sets.

Theorem 1.3.17 (De Loera, Marsters, O'Neill [42]). *The following hold.*

(a) There exist rational polytopes for which the directions attaining the minimum arithmetic width and the minimum lattice width form disjoint sets.

(b) Every finite subset of $\mathbb{Z}$ occurs as the arithmetic range of some rational simplex.

Part (b) stands in sharp contrast to Theorem 1.3.14: while large dilates of any fixed convex body have arithmetic ranges constrained to be AAPs, no such constraint applies across the family of all rational simplices. The construction in part (b) uses the numerical semigroup polytope P_S together with the classical fact [64] that every finite subset of $\mathbb{N}_{\geq 2}$ arises as the set of lengths of some element of some numerical semigroup; translating nP_S appropriately and applying the translation invariance of arithmetic range extends this to arbitrary finite subsets of $\mathbb{Z}$.

Full proofs of these four theorems appear in Chapter 3.

CHAPTER 2

Generating Conical Semigroups

2.1. Introduction

As established in Chapter 1, the integer points of a rational polyhedral cone admit a finite Hilbert basis: a unique minimal set of integer generators whose nonnegative integer combinations produce all lattice points of the cone. The central question of this chapter is whether any analogous finiteness holds for non-polyhedral cones, and in particular for the positive semidefinite cone $\mathcal{S}^n_+$ and the Lorentz cone $\mathcal{L}^n$, both of which are non-polyhedral and have uncountably many extreme rays.

The significance of this question extends across optimization, algebra, and geometry. In integer programming, Hilbert bases underlie the theory of total dual integrality: a rational system $A\mathbf{x} \leq \mathbf{b}$ is TDI if and only if, for every face of the feasible polyhedron, the active rows of A form a Hilbert basis for their conic span [103]. Extending this theory to conic integer programs, where the feasible region is the intersection of an affine subspace with a non-polyhedral cone such as $\mathcal{S}^n_+$ or $\mathcal{L}^n$, requires an analogous notion of finite generation for the integer points of these cones. Prior work on the integer points of general convex sets is sparse. Hemmecke and Weismantel [71], building on Jeroslow [74], proved that a monoid $M \subseteq \mathbb{Z}^n$ admits a finite integral generating set in the classical sense if and only if $\operatorname{cone}(M)$ is a rational polyhedral cone, so for the conical semigroup $S_C = C \cap \mathbb{Z}^N$ classical finite generation collapses to the polyhedral case. A separate line of work by Dey and Morán [48] characterizes when $\operatorname{conv}(K \cap \mathbb{Z}^n)$ is closed or polyhedral for general convex K, with the cone case showing that closure requires every extreme ray of K to be rational. Both results highlight how restrictive classical notions become outside the polyhedral setting, motivating the relaxation to (R, G)-finite generation.

The difficulty is easy to see: both $\mathcal{S}^n_+$ and $\mathcal{L}^n$ have uncountably many extreme rays, so any finite set of integer points spans at most a finite union of rational rays and cannot generate all of S_C under nonnegative integer combinations. The key idea of this chapter is to circumvent this obstruction by allowing a group G of integer linear maps to act on a finite root set R: the orbit $\bigcup_{r \in R} G \cdot r$ can be infinite, covering all necessary directions, while remaining finitely describable so long as G is finitely generated. The groups that arise are not arbitrary. For the PSD cone, G is $\mathrm{GL}(n, \mathbb{Z})$ acting by congruence $X \mapsto UXU^\top$, the classical action under which two quadratic forms are equivalent. For the Lorentz cone, G is built from the Barning–Hall reflection together with sign-change and permutation matrices, extending the classical generation of primitive Pythagorean triples by a single unimodular matrix. The root set R in each case consists of an extreme-ray representative together with a finite set of *sporadic* integer points: those that cannot be reduced by subtracting a primitive extreme point. Not every conical semigroup admits such a description, as Section 2.5 shows via an irrational planar cone whose only linear symmetry is the identity. The chapter's main results, Theorems 2.2.1 and 2.3.2, establish (R, G)-finite generation for $\mathcal{L}^n$ in dimensions $3 \leq n \leq 10$ and for $\mathcal{S}^n_+$ in all dimensions, with explicit roots in low-dimensional cases.

For the convenience of the reader, we restate the following generalization of the Hilbert basis first introduced in the introduction.

Definition 2.1.1. *Let $C \subseteq \mathbb{R}^N$ be a convex cone and $S_C := C \cap \mathbb{Z}^N$ its conical semigroup. We say S_C is (R, G)-**finitely generated** if there exists a finite set $R \subseteq S_C$ and a finitely generated subgroup $G \subseteq \mathrm{GL}(N, \mathbb{Z})$ acting linearly on C such that*

(1) the cone C and the semigroup S_C are both invariant under G, that is, $G \cdot C = C$ and $G \cdot S_C = S_C$, and

(2) every element $s \in S_C$ can be written as

$$s = \sum_{i \in K} \lambda_i \, g_i \cdot r_i$$

for some finite index set K, with $r_i \in R$, $g_i \in G$, and $\lambda_i \in \mathbb{Z}_{\geq 0}$.

*We call R the **roots** of S_C, and $\bigcup_{r \in R} G \cdot r$ the **generators** of S_C.*

When C is a pointed rational polyhedral cone, (R, G)-finite generation reduces to the classical Hilbert basis by taking R to be the Hilbert basis and $G = \{I_N\}$. The terminology of roots and generators mirrors the polyhedral case while making the role of the group action explicit. In the classical Hilbert basis setting, every generator is a root: the basis elements are both the objects acted on and the objects doing the generating, since the group is trivial. In the (R, G)-finitely generated setting these two roles separate. The roots R are the finitely many seed elements from which all generators are produced, and the generators $\bigcup_{r\in R} G\cdot r$ are the full (potentially infinite) set of integer points whose nonnegative integer combinations produce all of S_C.

The terminology of roots is deliberate. In the Barning–Hall tree (Section 2.2.2), the triple $(3,4,5)$ is literally the root of an infinite ternary tree whose nodes are the primitive Pythagorean triples and whose edges are given by three unimodular matrices. The (R,G)-framework abstracts this picture: R plays the role of the tree's root set, G the role of the branching matrices, and the orbit $\bigcup_{r\in R} G\cdot r$ the role of the tree itself.

An important concept throughout this chapter is that of a sporadic point. By the Krein–Milman theorem, any point in a closed pointed cone C can be written as a real conical combination of its extreme rays [78]. When we restrict to nonnegative integer combinations, the primitive integer points on the extreme rays of C are necessary generators, but they need not suffice: additional interior points may be required. We call these **extreme points** of S_C the set $\mathrm{ext}(S_C) := \mathrm{ext}(C)\cap \mathbb{Z}^N$, and define the obstructions as follows.

Definition 2.1.2. *A point $x\in S_C$ is **sporadic** if there is no $y\in \mathrm{ext}(S_C)$ such that $x-y\in S_C$.*

To show that S_C is (R,G)-finitely generated, it suffices to show that the set of primitive extreme points and sporadic points is either finite or generated by the action of a finitely generated group G on a finite root set R. Our two main results in this chapter show that the PSD and Lorentz cones are finitely generated in this new way and we will begin by the discussion with their sporadic points. From there, we will discuss applications of our theory. Lastly, while it might be tempting to hope that all cones can be finitely generated in this way, we present a simple example to show that not even all cones in the plane can be finitely generated in this way.

2.2. The Lorentz Cone

We work throughout with the Lorentz cone $\mathcal{L}^n$ in ambient dimension n, and write

$$T_n := \mathcal{L}^n \cap \mathbb{Z}^n$$

for its conical semigroup. The last coordinate x_n of a point $\mathbf{x}\in T_n$ is called its **height**. The Lorentz cone has the associated indefinite bilinear form

$$\langle \mathbf{x},\mathbf{y}\rangle := x_1y_1+\cdots+x_{n-1}y_{n-1}-x_ny_n,$$

which plays a central role in the geometry of the extreme points and the group action below. The main result of this section is the following.

THEOREM 2.2.1. *For dimension $3 \leq n \leq 10$, the conical semigroup $\mathcal{L}^n \cap \mathbb{Z}^n$ is (R, G)-finitely generated with G and R defined in Section 2.2.2 and Section 2.2.3.*

The full statement of Theorem 2.2.1, with explicit root sets in each dimension, is given in Section 2.2.4 as Theorem 2.2.8.

2.2.1. Pythagorean Tuples and Extreme Points. The extreme rays of $\mathcal{L}^n$ are the rays $\mathbb{R}_{\geq 0}\mathbf{x}$ for which $\langle \mathbf{x}, \mathbf{x} \rangle = 0$, that is, points on the boundary of the cone satisfying $x_1^2 + \cdots + x_{n-1}^2 = x_n^2$. The primitive integer points on these rays are precisely the primitive integer solutions to this equation. For $n = 3$ this is the classical Pythagorean equation, whose integer solutions have been studied since antiquity [50, 106]; the higher-dimensional generalization connects to the arithmetic of quadratic forms and the geometry of the orthogonal group $O_Q(\mathbb{Z})$ [24].

DEFINITION 2.2.2. *A vector $\mathbf{x} \in \mathbb{Z}^n$ is a **Pythagorean n-tuple** if*

$$x_1^2 + \cdots + x_{n-1}^2 = x_n^2,$$

*and **primitive** if $\gcd(x_1, \ldots, x_n) = 1$. We denote the set of primitive Pythagorean n-tuples in T_n by $\operatorname{ext}^p(T_n)$.*

EXAMPLE 2.2.3. *For $n = 3$, the primitive integer extreme points of $\mathcal{L}^3$ are primitive integer vectors (x_1, x_2, x_3) satisfying $x_1^2 + x_2^2 = x_3^2$, where we allow zero and negative entries in the first two coordinates. The smallest examples with positive entries are $(3, 4, 5)$, $(5, 12, 13)$, and $(8, 15, 17)$; sign changes and permutations of the first two coordinates produce additional primitive extreme points such as $(-3, 4, 5)$ and $(0, 5, 5)$. There are infinitely many such points, and they must all be accounted for in any generating set for T_3.*

As discussed in Definition 2.1.2, the primitive extreme points must appear in any generating set for T_n. The question is whether they suffice, or whether additional sporadic points are required.

2.2.2. The Barning–Hall Tree. The key tool for understanding the structure of $\operatorname{ext}^p(T_n)$ is the Barning–Hall tree, a rooted infinite ternary tree whose vertices are the primitive Pythagorean tuples and whose edges are given by the action of a unimodular matrix. We build up to the general construction by starting with the classical $n = 3$ case.

2.2.2.1. *The Classical Case: Pythagorean Triples.* Every primitive Pythagorean triple with even second coordinate is given by the parametrization $(m^2 - n^2, 2mn, m^2 + n^2)$ for coprime integers $m > n > 0$ of opposite parity [34]. While this describes all primitive triples explicitly, it gives no recursive structure: there is no natural way to organize the triples into a hierarchy or to pass systematically from one to another. Many authors have studied alternative organizational structures for primitive Pythagorean triples, including modular trees, matrix groups, and Gaussian integer factorizations [34, 57]. Barning [6] and Hall [69] independently discovered that three unimodular matrices suffice to generate all primitive Pythagorean triples from the single triple $(3, 4, 5)^\top$ by left multiplication, producing an infinite ternary tree in which every primitive triple appears exactly once. This tree structure is particularly suited to our setting because it reflects the action of the orthogonal group $O_Q(\mathbb{Z})$ of the quadratic form $Q(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$ on its primitive zero set, and the height-reduction argument that proves every triple appears in the tree generalizes directly to the higher-dimensional construction below.

The Pythagorean equation $x_1^2 + x_2^2 = x_3^2$ defines a quadratic form $Q(\mathbf{x}) = x_1^2 + x_2^2 - x_3^2$ whose zero set carries a transitive action of $O_Q(\mathbb{Z})$. The relevant reflections in $O_Q(\mathbb{Z})$ are defined via the bilinear form $\langle \mathbf{x}, \mathbf{y} \rangle_Q = x_1 y_1 + x_2 y_2 - x_3 y_3$: for $\mathbf{w}$ with $Q(\mathbf{w}) \neq 0$, the reflection in $\mathbf{w}$ is

$$s_{\mathbf{w}}(\mathbf{x}) = \mathbf{x} - 2\frac{\langle \mathbf{x}, \mathbf{w} \rangle_Q}{\langle \mathbf{w}, \mathbf{w} \rangle_Q}\mathbf{w}.$$

The reflection in $\mathbf{w} = (1, 1, 1)$ gives Barning's matrix [6]

$$A_3 = \begin{pmatrix} -1 & -2 & 2 \\ -2 & -1 & 2 \\ -2 & -2 & 3 \end{pmatrix}.$$

The three tree-generating matrices are then $A = A_3 s_1$, $B = A_3 s_2$, $C = A_3 s_1 s_2$, where s_1, s_2 are the sign-change reflections in the first and second coordinates:

$$A = \begin{pmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}.$$

Each of A, B, C is unimodular and preserves the Pythagorean equation: if $\mathbf{p}$ is a primitive Pythagorean triple then so are $A\mathbf{p}$, $B\mathbf{p}$, and $C\mathbf{p}$.

PROPOSITION 2.2.1 (Barning [6], Hall [69]). *Every primitive Pythagorean triple $\mathbf{p} = (x_1, x_2, x_3)^\top$ with $x_3 > 1$ is obtained from $(3, 4, 5)^\top$ by a unique product $M_1 M_2 \cdots M_k \cdot (3, 4, 5)^\top$ where each $M_i \in \{A, B, C\}$.*

The proof proceeds by descent on x_3. Given any primitive triple $\mathbf{p}$ with $x_3 > 1$, exactly one of $A^{-1}\mathbf{p}$, $B^{-1}\mathbf{p}$, $C^{-1}\mathbf{p}$ has all positive entries and strictly smaller hypotenuse [33]. Iterating, the hypotenuse strictly decreases at each step until $(3, 4, 5)^\top$ is reached, and the path is unique because exactly one inverse applies at each step. The resulting tree, in which every primitive Pythagorean triple appears as a node at depth equal to the number of matrix applications required to reach it from the root, is the **Barning–Hall tree**; Figure 2.1 shows its first three levels. We later exploit this process to classify sporadic points for the Lorentz cones.

EXAMPLE 2.2.4. *We trace $(9, 40, 41)^\top$ back to the root by descent. At each step we apply A_3 and restore positivity via the sign change Q_1.*

Step 1. $A_3(9, 40, 41)^\top = (-7, 24, 25)^\top$*; applying* Q_1 *gives* $(7, 24, 25)^\top$ *with* $x_3 = 25 < 41$.

Step 2. $A_3(7, 24, 25)^\top = (-5, 12, 13)^\top$*; applying* Q_1 *gives* $(5, 12, 13)^\top$ *with* $x_3 = 13 < 25$.

Step 3. $A_3(5, 12, 13)^\top = (-3, 4, 5)^\top$*; applying* Q_1 *gives* $(3, 4, 5)^\top$.

Reversing, $(9, 40, 41)^\top = A \cdot A \cdot A \cdot (3, 4, 5)^\top$*, so* $(9, 40, 41)^\top$ *sits at depth* 3 *in the A-branch, visible in Figure 2.1.*

2.2.2.2. *The General Case: Pythagorean n-Tuples.* Cass and Arpaia [23] extended Barning's construction to n-tuples for $4 \le n \le 9$. The key insight is that the same height-reduction argument works in higher dimensions, provided the reflection matrix A_n is chosen appropriately. Recall from

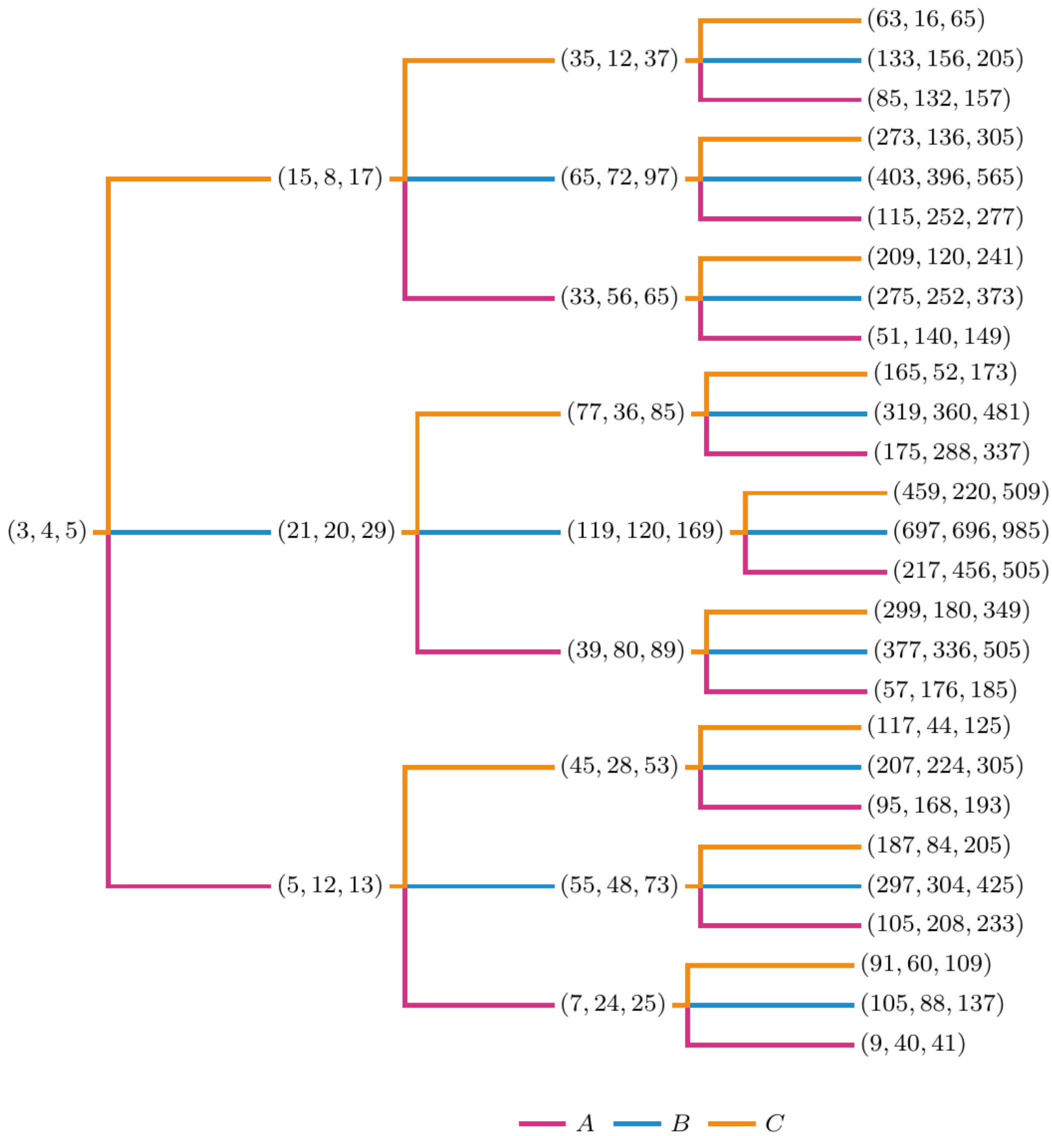


FIGURE 2.1. The Barning–Hall tree for $n = 3$: the first three levels of the infinite ternary tree of primitive Pythagorean triples, rooted at $(3, 4, 5)^\top$. Each triple has exactly three children, generated by left multiplication by A (•), B (•), or C (•). Every primitive Pythagorean triple appears exactly once [6, 69].

Section 2.2 that $T_n = \mathcal{L}^n \cap \mathbb{Z}^n$ is equipped with the bilinear form $\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + \cdots + x_{n-1} y_{n-1} - x_n y_n$, and that $\mathbf{x} \in T_n$ is a Pythagorean n-tuple when $\langle \mathbf{x}, \mathbf{x} \rangle = 0$. The analogous reflection matrix A_n is the reflection in the vector $(1, 1, 1, 0, \ldots, 0, 1)$ with respect to $\langle \cdot, \cdot \rangle$.

Definition 2.2.5. *Let $P_{i,j}$ denote the permutation matrix swapping coordinates i and j, and let Q_k denote the diagonal matrix with -1 in position (k,k) and 1 elsewhere. For $n = 3$, let A_3 be the reflection in $(1,1,1)^\top$ with respect to $\langle\cdot,\cdot\rangle$. For $4 \le n \le 10$, let A_n be the reflection in $(1,1,1,0,\dots,0,1)^\top$ with respect to $\langle\cdot,\cdot\rangle$:*

$$A_n = \begin{pmatrix} 0 & -1 & -1 & & 1 \\ -1 & 0 & -1 & \mathbf{0} & 1 \\ -1 & -1 & 0 & & 1 \\ & \mathbf{0} & & I_{n-4} & \mathbf{0} \\ -1 & -1 & -1 & & 2 \end{pmatrix}.$$

Define $A_n^+ := Q_1 Q_2 \cdots Q_{n-1} A_n$.

The matrix A_n is unimodular and maps T_n to itself; the matrix A_n^+ is its positive-coordinate analogue, obtained by restoring the signs of the first $n-1$ coordinates after the reflection. The height-reduction property generalizes as follows: for any Pythagorean n-tuple $\mathbf{p}$ with $p_n > 1$, the n-th coordinate of $(A_n^+)^{-1}\mathbf{p}$ is strictly less than p_n, except for finitely many $\mathbf{p}$ at each dimension (the stable-height sporadic points of Lemma 2.2.7.4).

Example 2.2.6. *Let $n = 4$ and $\mathbf{p} = (2,1,2,3)^\top$, which satisfies $2^2 + 1^2 + 2^2 = 9 = 3^2$ and is a primitive Pythagorean 4-tuple. Applying $(A_4^+)^{-1}$:*

$$(A_4^+)^{-1}\mathbf{p} = (1,0,0,1)^\top,$$

with height $1 < 3$. Thus $(2,1,2,3)^\top$ is reached from the root $(1,0,0,1)^\top$ by a single application of A_4^+, and it is a depth-1 node in the generalized Barning–Hall tree for $n = 4$.

The following lemma, due to Cass and Arpaia [23] for $3 \le n \le 9$ and extended in [43] to $n = 10$, establishes that the generalized tree structure accounts for all primitive Pythagorean n-tuples.

Lemma 2.2.6.1 (Cass–Arpaia [23]). *For $3 \le n \le 10$, the set $\mathrm{ext}^p(T_n)$ of primitive Pythagorean n-tuples is (R,G)-finitely generated by the group*

$$G = \langle A_n,\ Q_1,\dots,Q_{n-1},\ P_{1,2}, P_{1,3},\dots,P_{1,n-1}\rangle$$

and roots

(1) $R = \{(1, 0, \ldots, 0, 1)^\top\}$ *for* $3 \leq n < 10$,

(2) $R = \{(1, 0, \ldots, 0, 1)^\top,\ (1, 1, \ldots, 1, 3)^\top\}$ *for* $n = 10$.

For $3 \leq n \leq 9$, the entire set $\mathrm{ext}^p(T_n)$ forms a single orbit under G, and the tree is generated from one root by the action of A_n together with the sign-change and permutation matrices in G. The $n = 10$ case requires two roots because the Pythagorean 10-tuples fall into two distinct orbits under G. The obstruction is a parity argument: the tuple $(1, 1, \ldots, 1, 3)^\top \in \mathrm{ext}^p(T_{10})$ has all odd coordinates, and its orthogonal complement in the quadratic space of $\langle \cdot, \cdot \rangle$ is an even lattice, while the orthogonal complement of $(1, 0, \ldots, 0, 1)^\top$ is odd [23]. Since A_{10} preserves this parity invariant, no element of G can carry one root to the other, so both must be included. More generally, for $n = 8k + 2$ with $k \geq 1$, the Pythagorean n-tuples fall into at least $\lfloor (n+6)/8 \rfloor$ distinct orbits.

2.2.3. Sporadic Points of T_n. The Barning–Hall tree accounts for all primitive extreme points of T_n. However, as in the polyhedral case, the extreme points alone need not generate all of T_n under nonnegative integer combinations: additional interior points may be required. Restating Definition 2.1.2 in the language of T_n, we have the following.

Definition 2.2.7. *A point* $\mathbf{s} \in T_n$ *is* ***sporadic*** *if there is no* $\mathbf{p} \in T_n$ *with* $\langle \mathbf{p}, \mathbf{p} \rangle = 0$ *such that* $\mathbf{s} - \mathbf{p} \in T_n$.

The group G of Lemma 2.2.6.1 maps sporadic points to sporadic points, so the set of sporadic points is itself G-invariant. The following two lemmas give partial characterizations of sporadic points that are the main tools in the proof of Theorem 2.2.1.

Lemma 2.2.7.1. *Let* $\mathbf{s} \in T_n$.

(1) *Then,* $A_n^+\mathbf{s}$ *and* $(A_n^+)^{-1}\mathbf{s}$ *are both in* T_n.

(2) *If* $\mathbf{s}$ *is sporadic, then* $A_n^+\mathbf{s}$ *and* $(A_n^+)^{-1}\mathbf{s}$ *are both sporadic.*

Proof. The first claim follows by simply checking the required inequalities directly. For the second claim, we proceed by contradiction. Suppose $\mathbf{s}$ is sporadic but $(A_n^+)\mathbf{s}$ is not. Then, there is some point $\mathbf{p} \in T_n$ such that $\langle \mathbf{p}, \mathbf{p} \rangle = 0$ and $(A_n^+)\mathbf{s} - \mathbf{p} \in T_n$. However, we would then have that

$$(A_n^+)^{-1}(A_n^+\mathbf{s} - \mathbf{p}) = \mathbf{s} - (A_n^+)^{-1}\mathbf{p} \in T_n.$$

As $\mathbf{p} \in \partial T_n$, $(A_n^+)^{-1}\mathbf{p} \in \partial T_n$, which is a contradiction with $\mathbf{s}$ being sporadic. The case of $(A_n^+)^{-1}\mathbf{s}$ being sporadic follows the same argument. $\square$

Next, we will provide some lemmas about sporadic points that are necessary to prove Theorem 2.2.1. Lemmas 2.2.7.2 and 2.2.7.3 show that sporadic points are close to the boundary ∂T_n.

LEMMA 2.2.7.2. *Suppose $\mathbf{s} \in T_n$ is a primitive sporadic with nonnegative entries such that $s_n > 1$ and $s_i \neq 0$ for some $i \in \{1, \ldots, n-1\}$. Then,*

$$s_n = \left\lceil \sqrt{s_1^2 + s_2^2 + \cdots + s_{n-1}^2} \right\rceil$$

.

PROOF. We will show this by proving that

$$\sqrt{s_1^2 + s_2^2 + \cdots + s_{n-1}^2} < s_n < \sqrt{s_1^2 + s_2^2 + \cdots + s_{n-1}^2} + 1$$

where the first inequality is given by membership in T_n. Without loss of generality, we can assume that $s_1 \neq 0$. By way of contradiction, suppose that $\mathbf{s}$ is a primitive sporadic such that $s_n > 1$ and $s_1 > 0$, and that $s_n \geq \sqrt{s_1^2 + s_2^2 + \cdots + s_{n-1}^2} + 1$. Then, we would have that

$$s_n - 1 \geq \sqrt{s_1^2 + s_2^2 + \cdots + s_{n-1}^2} > \sqrt{(s_1 - 1)^2 + s_2^2 + \cdots + s_{n-1}^2}$$

which is equivalent to $\mathbf{s} - (1, 0, \ldots, 0, 1) \in T_n$. This contradicts the assumption that s is sporadic. Thus, we have the desired equality. $\square$

LEMMA 2.2.7.3. *Let $\mathbf{s} \in T_n$. If $\langle \mathbf{s}, \mathbf{s} \rangle = -1$, then $\mathbf{s}$ is sporadic.*

PROOF. By way of contradiction, suppose $\langle \mathbf{s}, \mathbf{s} \rangle = -1$ and that $\mathbf{s}$ is not sporadic. Then, there exists some $\mathbf{p} \in T_n$ such that $\langle \mathbf{p}, \mathbf{p} \rangle = 0$ and $\mathbf{s} - \mathbf{p} \in T_n$. This is equivalent to saying that

$$\langle \mathbf{s} - \mathbf{p}, \mathbf{s} - \mathbf{p} \rangle \leq 0.$$

This gives us that

$$\langle \mathbf{s}, \mathbf{s} \rangle - 2\langle \mathbf{s}, \mathbf{p} \rangle + \langle \mathbf{p}, \mathbf{p} \rangle = -1 - 2\langle \mathbf{s}, \mathbf{p} \rangle \leq 0.$$

Thus, $\langle \mathbf{s}, \mathbf{p} \rangle \geq -\frac{1}{2}$ so $\langle \mathbf{s}, \mathbf{p} \rangle \geq 0$ by its integrality. However, as $\langle \mathbf{s}, \mathbf{s} \rangle = -1$ implies that

$$\sqrt{s_1^2 + \cdots + s_{n-1}^2} < s_n$$

and $\langle \mathbf{p}, \mathbf{p} \rangle = 0$ implies that $\sqrt{p_1^2 + \cdots + p_{n-1}^2} = p_n$, using the Cauchy-Schwarz inequality, we have that

$$s_1p_1 + \cdots + s_{n-1}p_{n-1} \leq \sqrt{(s_1^2 + \cdots + s_{n-1}^2)(p_1^2 + \cdots + p_{n-1}^2)} < s_np_n.$$

Thus, $\langle \mathbf{s}, \mathbf{p} \rangle < 0$, reaching a contradiction. Therefore, $\langle \mathbf{s}, \mathbf{s} \rangle = -1$ implies that $\mathbf{s}$ is sporadic. $\square$

Inspired by the structure of Pythagorean tuples, we analyze the set of sporadic points that remain at the same height in T_n after multiplication by $(A_n^+)^{-1}$. Let $(p)_n$ denote the n^{th} coordinate of p.

Lemma 2.2.7.4. *Let $n \leq 10$. Suppose $\mathbf{s} \in T_n$ is a primitive sporadic such that $s_1 \geq \cdots \geq s_{n-1} \geq 0$ and $s_n > 1$. The following list of tuples are the only such $\mathbf{s}$ where $((A_n^+)^{-1}\mathbf{s})_n = s_n$.*

- *For $n = 7$, we have the following tuple:* $(1, 1, 1, 1, 1, 1, 3)$.
- *For $n = 8$, we have the following tuples:* $(1, 1, 1, 1, 1, 1, 1, 3)$, $(1, 1, 1, 1, 1, 1, 0, 3)$.
- *For $n = 9$, we have the following tuples:*

$$(1, 1, 1, 1, 1, 1, 1, 1, 3), (1, 1, 1, 1, 1, 1, 1, 0, 3), (1, 1, 1, 1, 1, 1, 0, 0, 3), (2, 2, 2, 2, 2, 2, 2, 1, 6).$$

- *For $n = 10$, we have the following tuples:*

$$(1, 1, 1, 1, 1, 1, 1, 1, 0, 3), \quad (1, 1, 1, 1, 1, 1, 1, 0, 0, 3), \quad (1, 1, 1, 1, 1, 1, 0, 0, 0, 3),$$
$$(2, 2, 2, 2, 2, 2, 2, 2, 1, 6), \quad (2, 2, 2, 2, 2, 2, 2, 1, 0, 6).$$

Proof. This is equivalent to showing that these are the only such sporadic points such that $s_1 + s_2 + s_3 = s_n$. Since $\mathbf{s}$ is sporadic, $\mathbf{s} - \mathbf{t} \notin T_n$ for every $\mathbf{t} \in \text{ext}^p(T_n)$. In particular, $\mathbf{s} - (1, 0, \ldots, 0, 1) \notin T_n$, which is equivalent to saying that $(s_n - 1)^2 < (s_1 - 1)^2 + s_2^2 + \cdots + s_{n-1}^2$ or

$$2s_1s_2 + 2s_2s_3 + 2s_1s_3 - 2s_2 - 2s_3 - s_4^2 - \cdots - s_{n-1}^2 < 0. \tag{2.1}$$

We begin by showing that the first six coordinates must be equal. We proceed by contradiction in each of the below arguments.

- Suppose that $s_1 \geq s_2 + 1$. Then, (2.1) implies

$$\begin{aligned}0 &> 2s_2(s_2+1) + 2s_2s_3 + 2(s_2+1)s_3 - 2s_2 - 2s_3 - s_4^2 - \cdots - s_{n-1}^2 \\ &= 2s_2^2 + 4s_2s_3 - s_4^2 - \cdots - s_{n-1}^2 \geq 0.\end{aligned}$$

  As this is a contradiction, we must have that $s_1 = s_2$.

- Suppose that $s_2 \geq s_3 + 1$. Then, (2.1) implies

$$\begin{aligned}0 &> 2s_1(s_3+1) + 2s_3(s_3+1) + 2s_1s_3 - 2(s_3+1) - 2s_3 - s_4^2 - \cdots - s_{n-1}^2 \\ &= 4s_1s_3 + 2s_3^2 - s_4^2 - \cdots - s_{n-1}^2 + 2s_1 - 2s_3 - 2 \\ &\geq 2(s_2 - s_3 - 1) \geq 0.\end{aligned}$$

  As this is a contradiction, we must have that $s_1 = s_2 = s_3$.

- Suppose that $s_3 \geq s_4 + 1$. Then, (2.1) implies

$$\begin{aligned}0 &> 6(s_4+1)^2 - 4(s_4+1) - s_4^2 - \cdots - s_{n-1}^2 \\ &= 5s_4^2 - s_5^2 - \cdots - s_{n-1}^2 + 8s_4 + 2 \geq 0.\end{aligned}$$

  As this is a contradiction, we must have that $s_1 = s_2 = s_3 = s_4$.

- Suppose that $s_4 \geq s_5 + 1$. Then, (2.1) implies

$$\begin{aligned}0 &> 5(s_5+1)^2 - 4(s_5+1) - s_5^2 - \cdots - s_{n-1}^2 \\ &= 4s_5^2 - s_6^2 - \cdots - s_{n-1}^2 + 6s_5 + 1 \\ &\geq 6s_5 + 1 \geq 0.\end{aligned}$$

  As this is a contradiction, we must have that $s_1 = s_2 = s_3 = s_4 = s_5$.

- Suppose that $s_5 \geq s_6 + 1$. Then, (2.1) implies

$$\begin{aligned}0 &> 4(s_6+1)^2 - 4(s_6+1) - s_6^2 - \cdots - s_{n-1}^2 \\ &= 3s_6^2 - s_7^2 - \cdots - s_{n-1}^2 + 4s_6 \geq 0.\end{aligned}$$

  As this is a contradiction, we must have that $s_1 = s_2 = s_3 = s_4 = s_5 = s_6$.

This implies that we have no such sporadic points for $n \leq 6$. Suppose $n = 7$. Then, any candidate tuple must be of the following form:

$$(k, k, k, k, k, k, 3k)$$

where $k \in \mathbb{Z}_{>0}$. As $\mathbf{s}$ is assumed to be primitive, $k = 1$ and the only possible tuple is $(1, 1, 1, 1, 1, 1, 3)$. Suppose $n = 8$. Then, any candidate tuple must be of one of the following forms:

$$(k, k, k, k, k, k, s_7, 3k)$$

$$(k, k, k, k, k, k, k, 3k)$$

where $k \in \mathbb{Z}_{>0}$ and $s_7 \leq k - 1$. As $\mathbf{s}$ is assumed to be primitive, the second possible form only contributes the tuple $(1, 1, 1, 1, 1, 1, 1, 3)$. Suppose $\mathbf{s}$ is of the first form listed. We claim that $k = 1$. By way of contradiction, suppose that $k \geq 2$. Then, $\mathbf{s} - (1, 0, \ldots, 0, 1) \in T_n$ as

$$\begin{aligned}(3k-1)^2 - (k-1)^2 - 5k^2 - s_7^2 &\geq (3k-1)^2 - (k-1)^2 - 5k^2 - (k-1)^2 \\ &= 2k^2 - 2k - 1 \\ &\geq 3 > 0.\end{aligned}$$

Thus, the only tuple satisfying these restrictions is $(1, 1, 1, 1, 1, 1, 0, 3)$.

Suppose $n = 9$. Then, for $k \in \mathbb{Z}_{>0}$, any candidate tuple must be of one of the following forms:

$$(k, k, k, k, k, k, s_7, s_8, 3k) \tag{2.2}$$

$$(k, k, k, k, k, k, k, s_8, 3k) \tag{2.3}$$

$$(k, k, k, k, k, k, k, k, 3k) \tag{2.4}$$

where $s_7, s_8 \leq k - 1$.

Suppose $\mathbf{s}$ is of the form (2.2). By way of contradiction, suppose that $k \geq 2$. We claim that $\mathbf{s} - (1, 0, \ldots, 0, 1) \in T_n$. This follows from the fact that

$$\begin{aligned}(3k-1)^2 - (k-1)^2 - 5k^2 - s_7^2 - s_8^2 &\geq (3k-1)^2 - (k-1)^2 - 5k^2 - 2(k-1)^2 \\ &= k^2 - 2 \\ &\geq 2 > 0.\end{aligned}$$

Thus, $\mathbf{s}$ must not be sporadic and $k = 1$. This gives us the tuple $(1, 1, 1, 1, 1, 1, 0, 0, 3)$.

Suppose $\mathbf{s}$ is of the form (2.3). By way of contradiction, suppose $k \geq 3$. Then, we claim that $\mathbf{s} - (1, 0, \ldots, 0, 1) \in T_n$. This follows from the fact that

$$\begin{aligned}(3k-1)^2 - (k-1)^2 - 6k^2 - s_8^2 &\geq (3k-1)^2 - (k-1)^2 - 6k^2 - (k-1)^2 \\ &= k^2 - 2k - 1 \\ &\geq 2 > 0.\end{aligned}$$

Thus, we only need to consider $k = 1, 2$. If $k = 1$, this gives us the tuple $(1, 1, 1, 1, 1, 1, 1, 0, 3)$. Suppose $k = 2$. This gives us the following possible tuples:

$$(2, 2, 2, 2, 2, 2, 2, 0, 6), \qquad (2, 2, 2, 2, 2, 2, 2, 1, 6).$$

The first tuple listed is not primitive, so this only gives us the tuple $(2, 2, 2, 2, 2, 2, 2, 1, 6)$. Lastly, if $\mathbf{s}$ is of the form (2.4), then $\mathbf{s}$ is only primitive if $k = 1$. This gives us our last tuple, $(1, 1, 1, 1, 1, 1, 1, 1, 3)$.

Suppose $n = 10$. Then, for $k \in \mathbb{Z}_{>0}$, any candidate tuple must be of one of the following forms:

$$(k, k, k, k, k, k, s_7, s_8, s_9, 3k) \tag{2.5}$$

$$(k, k, k, k, k, k, k, s_8, s_9, 3k) \tag{2.6}$$

$$(k, k, k, k, k, k, k, k, s_9, 3k) \tag{2.7}$$

$$(k, k, k, k, k, k, k, k, k, 3k) \tag{2.8}$$

where $s_7, s_8, s_9 \leq k - 1$. Any tuple of form (2.8) is a Pythagorean tuple so we may exclude it. Suppose $\mathbf{s}$ is of the form (2.5). By way of contradiction, suppose $k \geq 2$. Then, we claim that

$\mathbf{s} - (1, 0, \ldots, 0, 1) \in T_n$. This follows from the fact that

$$\begin{aligned}(3k-1)^2 - &(k-1)^2 - 5k^2 - s_7^2 - s_8^2 - s_9^2 \\ &\geq (3k-1)^2 - (k-1)^2 - 5k^2 - 3(k-1)^2 \\ &= 2k - 3 \geq 1 > 0.\end{aligned}$$

Thus, $k = 1$ and the only tuple we have of this form is $(1, 1, 1, 1, 1, 1, 0, 0, 0, 3)$.

Suppose $\mathbf{s}$ is of the form (2.6). By way of contradiction, suppose $k \geq 2$. If $s_9 \geq 1$, then $\mathbf{s} - (1, 1, \ldots, 1, 3) \in T_n$ as

$$\begin{aligned}(3k-3)^2 - 7(k-1)^2 - (s_8 - 1)^2 - (s_9 - 1)^2 &\geq (3k-3)^2 - 7(k-1)^2 - 2(k-2)^2 \\ &= 4k - 6 \geq 2 > 0.\end{aligned}$$

Thus $s_9 = 0$. Suppose $k \geq 3$. Then, $\mathbf{s} - (1, 0, \ldots, 0, 1) \in T_n$ as

$$\begin{aligned}(3k-1)^2 - (k-1)^2 - 6k^2 - s_8^2 &\geq (3k-1)^2 - (k-1)^2 - 6k^2 - (k-1)^2 \\ &= k^2 - 2k - 1 \geq 2 > 0.\end{aligned}$$

Thus, our options are $k = 1, 2$. If $k = 1$, this recovers the tuple $(1, 1, 1, 1, 1, 1, 1, 0, 0, 3)$. If $k = 2$, this gives us potential tuples $(2, 2, 2, 2, 2, 2, 2, 0, 0, 6)$ and $(2, 2, 2, 2, 2, 2, 2, 1, 0, 6)$. The first is not primitive so we exclude it.

Lastly, suppose $\mathbf{s}$ is of the form (2.7). If $s_9 \neq 0$, then $\mathbf{s} - (1, 1, \ldots, 1, 3) \in T_n$. This follows from the fact that

$$\begin{aligned}(3k-3)^2 - 8(k-1)^2 - (s_9 - 1)^2 &\geq (3k-3)^2 - 8(k-1)^2 - (k-2)^2 \\ &= 2k - 3 \geq 1 > 0.\end{aligned}$$

Thus, $s_9 = 0$. The only primitive sporadic satisfying these constraints is $(1, 1, 1, 1, 1, 1, 1, 1, 0, 3)$. This completes the proof. $\square$

Then we show that besides the points listed in Lemma 2.2.7.4, every other sporadic points will reduce to a strictly lower height after multiplication by $(A_n^+)^{-1}$.

Lemma 2.2.7.5. *Let* $\mathbf{s} \in T_n$ *be sporadic with nonnegative entries such that* $s_1 \geq s_2 \geq \cdots \geq s_{n-1}$, $s_1 \geq 1$ *and* $3 \leq n \leq 10$. *For* s *not listed in Lemma 2.2.7.4,*

$$((A_n^+)^{-1}\mathbf{s})_n < (\mathbf{s})_n.$$

Proof. This is equivalent to showing that $-s_1 - s_2 - s_3 + 2s_n < s_n$, or rather $s_n < s_1 + s_2 + s_3$. The case of $n = 3$ reduces to the inequality $s_3 < s_1 + s_2$. By Lemma 2.2.7.2, we have that

$$\begin{aligned} s_n &= \left\lceil \sqrt{s_1^2 + s_2^2 + \cdots + s_{n-1}^2} \right\rceil \\ &\leq \left\lceil \sqrt{s_1^2 + s_2^2 + s_3^2 + 2s_1s_2 + 2s_1s_3 + 2s_2s_3} \right\rceil \\ &= \left\lceil \sqrt{(s_1 + s_2 + s_3)^2} \right\rceil = s_1 + s_2 + s_3, \end{aligned} \tag{2.9}$$

where the inequality follows from the order $s_1s_2 \geq s_1s_3 \geq s_2s_3 \geq s_4^2 \geq ... \geq s_{n-1}^2$ and $n \leq 10$. As s is not one of the tuples listed in Lemma 2.2.7.4, the inequality (2.9) can be made strict. Therefore, $s_n < s_1 + s_2 + s_3$, which implies that $(A_n^+)^{-1}\mathbf{s}$ sits at a strictly lower height in the cone than $\mathbf{s}$. □

2.2.4. Proof of Theorem 2.2.1. We now present a complete formulation of Theorem 2.2.1 followed by its proof.

Theorem 2.2.8. *For dimension* $3 \leq n \leq 10$, *the conical semigroup* $\mathcal{L}^n \cap \mathbb{Z}^n$ *is* (R, G)*-finitely generated by*

$$G = \left\langle A_n^+, Q_1, \ldots, Q_{n-1}, P_{1,2}, P_{1,3}, \ldots, P_{1,n-1} \right\rangle$$

and a finite set R. *More specifically,*

(1) *If* $3 \leq n \leq 6$, *then* $R = \left\{(1, 0, \ldots, 0, 1)^\top, (0, \ldots, 0, 1)^\top\right\}$.

(2) *If* $n = 7$, *then*

$$R = \left\{(1, 0, 0, 0, 0, 0, 1)^\top, (0, 0, 0, 0, 0, 0, 1)^\top, (1, 1, 1, 1, 1, 1, 3)^\top\right\}.$$

(3) *If* $n = 8$, *then*

$$R = \left\{(1, 0, 0, 0, 0, 0, 0, 1)^\top, (0, 0, 0, 0, 0, 0, 0, 1)^\top, (1, 1, 1, 1, 1, 1, 1, 3)^\top, (1, 1, 1, 1, 1, 1, 0, 3)^\top\right\}.$$

(4) If $n = 9$, then

$$R = \Big\{(1,0,0,0,0,0,0,0,1)^\top, (0,0,0,0,0,0,0,0,1)^\top, (1,1,1,1,1,1,1,1,3)^\top,$$
$$(1,1,1,1,1,1,1,0,3)^\top, (1,1,1,1,1,1,0,0,3)^\top, (2,2,2,2,2,2,2,1,6)^\top\Big\}.$$

(5) If $n = 10$, then

$$R = \Big\{(1,0,0,0,0,0,0,0,0,1)^\top, (1,1,1,1,1,1,1,1,1,3)^\top, (0,0,0,0,0,0,0,0,0,1)^\top,$$
$$(1,1,1,1,1,1,1,1,0,3)^\top, (1,1,1,1,1,1,1,0,0,3)^\top, (1,1,1,1,1,1,0,0,0,3)^\top,$$
$$(2,2,2,2,2,2,2,2,1,6)^\top, (2,2,2,2,2,2,2,1,0,6)^\top\Big\}.$$

Proof. This follows directly from Lemma 2.2.7.5 and the fact that $(0,0,\dots,0,1)$ is the sporadic of minimal height in this cone. Let $\mathbf{s} \in T_n$. If $\mathbf{s}$ is not sporadic, we can represent it as

$$\mathbf{s} = \lambda_1\mathbf{p}_1 + \lambda_2\mathbf{p}_2 + \cdots + \lambda_k\mathbf{p}_k + \lambda\mathbf{p} \tag{2.10}$$

where $\lambda, \lambda_i \in \mathbb{Z}_{\geq 0}$, each $\mathbf{p}_i$ is a primitive Pythagorean tuple and $\mathbf{p}$ is sporadic. By Lemma 2.2.6.1, each $\mathbf{p}_i$ can be decomposed as $\mathbf{p}_i = G_i(1,0,\dots,0,1)^\top$ when $3 \leq n < 10$ or $\mathbf{p}_i = G_i(1,0,\dots,0,1)^\top + \tilde{G}_i(1,1,\dots,1,3)^\top$ when $n = 10$ where each $G_i, \tilde{G}_i \in G$. It remains to consider the sporadic $\mathbf{p}$. Given any primitive sporadic tuple $\mathbf{s}$, we can recover an element of R as follows:

(1) Multiply $\mathbf{p}$ by the appropriate permutation matrices $P_{i,j}$ and sign changing matrices Q_j so that $\mathbf{p}$ has nonnegative entries and $p_1 \geq \cdots \geq p_{n-1}$. Call this resulting vector $\mathbf{p}'$.
(2) Multiply $\mathbf{p}'$ by $(A_n^+)^{-1}$ and repeat step 1 as necessary. By Lemma 2.2.7.5, the height of the resulting vector will be strictly lower then that of the vector we started with or the resulting vector will belong to R.
(3) Repeat step 2 until the resulting vector $\mathbf{r}$ belongs to R. By Lemma 2.2.7.4, the only possibilities for the resulting vector belong to R.

This process gives the equality $\mathbf{r} = G_1 \dots G_k\mathbf{p}$. If we let $G' = G_1 \dots G_k$, then we have $(G')^{-1}\mathbf{r} = \mathbf{p}$. Therefore, for $3 \leq n \leq 10$, the conical semigroup of $\mathcal{L}^n$ is (R, G)-finitely generated by the claimed R and G. $\square$

When $n = 9$, the primitive sporadic point $(2,2,2,2,2,2,2,1,6)$ can be written as the sum of two sporadic points with smaller heights:

$$(2,2,2,2,2,2,2,1,6) = (1,1,1,1,1,1,1,0,3) + (1,1,1,1,1,1,1,1,3).$$

We can similarly decompose $(2,2,2,2,2,2,2,2,1,6)$ and $(2,2,2,2,2,2,2,1,0,6)$ for $n = 10$. In this sense, these sporadic points fail to be minimal. Thus, if we remove them from the set of roots R, our semigroup S remains (R, G)-finitely generated. However, when we remove these points from our root sets, our decomposition in equality (2.10) requires modification and we must allow for multiple sporadic points in the expression.

Remark 2.2.1. *Lastly, it is worth noting that inequality (2.9) would fail in dimensions larger than 10. Thus, this line of argumentation would fail to produce results for $n > 10$.*

We can use Theorem 2.2.8 to recover a partial converse of Lemma 2.2.7.3.

Corollary 2.2.1. *Let $3 \leq n < 7$ and fix $\mathbf{s} \in T_n$. If $\mathbf{s}$ is a primitive sporadic, then $\langle \mathbf{s}, \mathbf{s} \rangle = -1$.*

Proof. Let $\mathbf{s} \in T_n$ be sporadic. Using Theorem 2.2.8, we can express $\mathbf{s}$ as

$$\mathbf{s} = G'(0, \ldots, 0, 1)^\top$$

for $G' \in G$. As $\langle G'\mathbf{s}, G'\mathbf{s} \rangle = \langle \mathbf{s}, \mathbf{s} \rangle$ for all $G' \in G$, we see that

$$\langle \mathbf{s}, \mathbf{s} \rangle = \langle G'(0, \ldots, 0, 1)^\top, G'(0, \ldots, 0, 1)^\top \rangle = \langle (0, \ldots, 0, 1)^\top, (0, \ldots, 0, 1)^\top \rangle = -1.$$

$\square$

In particular, this converse fails to hold in dimensions ≥ 7 as we have $\mathbf{r} \in R$ such that $\langle \mathbf{r}, \mathbf{r} \rangle \neq -1$.

Example 2.2.9. *The conical semigroup $S = \mathcal{L}^9 \cap \mathbb{Z}^9$ is not (R, G)-finitely generated for*

$$G = \left\langle A_n^+, Q_1, \ldots, Q_{n-1}, P_{1,2}, P_{1,3}, \ldots, P_{1,n-1} \right\rangle$$

and $R = \{(0, \ldots, 0, 1)^\top, (1, 0, \ldots, 0, 1)^\top\}$. In particular, inequality (2.9) in the proof of Lemma 2.2.7.5 is met with equality by sporadic tuples of the form

$$(k, k, \ldots, k, s_n).$$

From Lemma 2.2.7.3, we see that integer solutions to

$$k^2(n-1) - s_n = -1$$

are such tuples. In particular, for $s = (1,1,1,1,1,1,1,1,3)$*, we have that*

$$(A_n^+)^{-1} s^\top = (-1,-1,-1,-1,-1,-1,-1,-1,3)^\top$$

and that all negative sign patterns of s *are taken to a higher height in the cone.*

2.3. The Positive Semidefinite Cone

Let $\mathcal{S}^n(\mathbb{Z})$ denote the set of $n \times n$ symmetric integer matrices and $\mathcal{S}_+^n(\mathbb{Z})$ the integer positive semidefinite matrices. Throughout this section, we view $\mathcal{S}_+^n(\mathbb{Z})$ as a conical semigroup inside $\mathbb{Z}^N$ where $N = \binom{n+1}{2}$, the dimension of $\mathcal{S}^n(\mathbb{R})$. The group $\mathrm{GL}(n,\mathbb{Z})$ acts on $\mathcal{S}_+^n(\mathbb{Z})$ by

$$U \cdot X := UXU^\top, \qquad U \in \mathrm{GL}(n,\mathbb{Z}),\ X \in \mathcal{S}_+^n(\mathbb{Z}).$$

This action is linear, takes integer points to integer points, and is therefore represented by a matrix in $\mathrm{GL}(N,\mathbb{Z})$. It preserves both the cone $\mathcal{S}_+^n$ and its integer lattice. It is well-known that $\mathrm{GL}(n,\mathbb{Z})$ is finitely generated by three matrices [113]:

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ & & & \dots & & \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 1 & 0 & \dots & 0 & 0 \\ & & & \dots & & \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ & & & \dots & & \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix}.$$

For simplicity, we keep the notation $U \cdot X$ for the action of $U \in \mathrm{GL}(n,\mathbb{Z})$ on X without explicitly specifying its representation in $\mathrm{GL}(N,\mathbb{Z})$.

Definition 2.3.1. *Two matrices* $X_1, X_2 \in \mathcal{S}_+^n(\mathbb{Z})$ *are* ***unimodularly equivalent*** *if* $X_2 = UX_1U^\top$ *for some* $U \in \mathrm{GL}(n,\mathbb{Z})$*.*

The equivalence class of $\mathbf{e}_1\mathbf{e}_1^\top$ under this action is the set of all rank-one matrices $\mathbf{x}\mathbf{x}^\top$ for primitive $\mathbf{x} \in \mathbb{Z}^n$: these are the primitive extreme points of $\mathcal{S}_+^n(\mathbb{Z})$. The main result of this section is the following.

THEOREM 2.3.2. *The conical semigroup $\mathcal{S}_+^n(\mathbb{Z})$ is (R, G)-finitely generated by $G \cong \mathrm{GL}(n, \mathbb{Z})$ acting on $X \in \mathcal{S}_+^n(\mathbb{Z})$ by $X \mapsto UXU^\top$ for each $U \in \mathrm{GL}(n, \mathbb{Z})$, and by R, the union of any single rank-one matrix and a finite subset of the sporadic points. Moreover,*

(1) if $n \leq 5$, then there are no sporadic points and $R = \{\mathbf{e}_1\mathbf{e}_1^\top\}$;

(2) if $n = 6$, then $R = \{\mathbf{e}_1\mathbf{e}_1^\top, M\}$, where M is the unique sporadic point (up to unimodular equivalence) defined in Proposition 2.3.5 of Section 2.3.2.

An interpretation of Theorem 2.3.2 is that for $n \leq 5$, every integer PSD matrix can be represented as a sum of rank-one matrices $\mathbf{x}\mathbf{x}^\top$ for some primitive integer vector $\mathbf{x} \in \mathbb{Z}^n$; this fails for $n = 6$, in which case every integer PSD matrix can be represented as a sum of rank-one matrices and one sporadic matrix unimodularly equivalent to M. We refer to a decomposition $X = \sum_{i \in K} \mathbf{x}_i\mathbf{x}_i^\top$ as an **integer rank-1 decomposition**. Prior work has established analogous rank-one decomposition results for restricted classes of integer PSD matrices. In [84], every PSD $\{0, 1\}$-matrix $X \in \mathcal{S}_+^n(\mathbb{Z}) \cap \{0, 1\}^{n \times n}$ is shown to satisfy $X = \sum_{i \in K} \mathbf{x}_i\mathbf{x}_i^\top$ with $\mathbf{x}_i \in \{0, 1\}^n$, and this was extended in [46] to PSD $\{0, \pm 1\}$-matrices. Theorem 2.3.2 extends these results to all integer PSD matrices.

2.3.1. The $K(X)$ Body and Sporadic PSD Matrices. The following *integer rank-1 decomposition* for PSD integer matrices is studied in [89]. We recast their arguments with a modern geometric perspective, and use it to extend the notion of (R, G)-finite generation to the PSD cone.

LEMMA 2.3.2.1. *If $n \leq 5$, then for any $X \in \mathcal{S}_+^n(\mathbb{Z})$, we can find a finite index set K and vectors $\mathbf{x}_i \in \mathbb{Z}^n$, $i \in K$ such that*

$$X = \sum_{i \in K} \mathbf{x}_i\mathbf{x}_i^\top. \tag{2.11}$$

In the PSD case, Definition 2.1.2 reads as follows: a matrix $X \in \mathcal{S}_+^n(\mathbb{Z})$ is sporadic if there does not exist $\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ such that $X - \mathbf{x}\mathbf{x}^\top \succeq 0$. Lemma 2.3.2.1 is then equivalent to the statement that there are no sporadic points in $\mathcal{S}_+^n(\mathbb{Z})$ when $n \leq 5$. The following proposition makes this equivalence precise.

Proposition 2.3.1. *There is no sporadic point in $\mathcal{S}_+^n(\mathbb{Z})$ if and only if every positive semidefinite integer matrix in $\mathcal{S}_+^n(\mathbb{Z})$ has an integer rank-1 decomposition.*

Proof. If there is no sporadic point in $\mathcal{S}_+^n(\mathbb{Z})$, then for every $Y \in \mathcal{S}_+^n(\mathbb{Z})$, there exists $\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ such that $Y - \mathbf{x}\mathbf{x}^\top \succeq 0$. For $X \in \mathcal{S}_+^n(\mathbb{Z})$, we do the following procedure for $X_0 := X$ (with index i initialized to 1).

(1) Take any $\mathbf{x}_i \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$ such that $X_i := X_{i-1} - \mathbf{x}_i\mathbf{x}_i^\top \succeq 0$.
(2) If $X_i = 0$, then we have found an integer rank-1 decomposition $X = \sum_{j=1}^{i} \mathbf{x}_j\mathbf{x}_j^\top$; otherwise set the index $i \leftarrow i+1$ and go back to step 1.

To see that the procedure terminates in finitely many steps, note that the diagonal of $\mathbf{x}_i\mathbf{x}_i^\top$ contains at least 1 nonzero entry because $\mathbf{x}_i \neq 0$. Thus the trace $\mathrm{tr}(X_i) \leq \mathrm{tr}(X_{i-1}) - 1$ for any $i \geq 1$ because the entries are integers. The procedure can repeat no more than $\mathrm{tr}(X)$ times as $\mathrm{tr}(X_i) \geq 0$.
If every $X \in \mathcal{S}_+^n(\mathbb{Z})$ has an integer rank-1 decomposition $X = \sum_{i \in K} \mathbf{x}_i\mathbf{x}_i^\top$, then any of $\mathbf{x}_i, i \in K$ satisfies the requirement $X - \mathbf{x}_i\mathbf{x}_i^\top \succeq 0$. □

For any $X \in \mathcal{S}_+^n(\mathbb{Z})$, define the convex body

$$K(X) := \{\mathbf{x} \in \mathbb{R}^n : X - \mathbf{x}\mathbf{x}^\top \succeq 0\}.$$

Since $X - \mathbf{x}\mathbf{x}^\top \succeq 0$ if and only if $|\mathbf{v}^\top\mathbf{x}|^2 \leq \mathbf{v}^\top X \mathbf{v}$ for all $\mathbf{v} \in \mathbb{R}^n$, the set $K(X)$ is compact, convex, and symmetric about the origin. Equivalently, by positive semidefiniteness of Schur complements,

$$X \succeq \mathbf{x}\mathbf{x}^\top \iff \begin{bmatrix} 1 & \mathbf{x}^\top \\ \mathbf{x} & X \end{bmatrix} \succeq 0 \iff \mathbf{x}^\top X^\dagger \mathbf{x} \leq 1,\ (I - XX^\dagger)\mathbf{x} = 0,$$

where $X^\dagger$ denotes the pseudoinverse of X, so $K(X)$ is an ellipsoid (possibly degenerate when X is rank-deficient). When X has full rank,

$$K(X) = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x}^\top \mathrm{adj}(X)\mathbf{x} \leq \det(X)\} \text{ with } \mathrm{vol}(K(X)) = V_n\sqrt{\det(X)},$$

where $\mathrm{adj}(X)$ is the adjugate of X satisfying $\mathrm{adj}(X) = \det(X)X^{-1}$ and $V_n := \pi^{n/2}/\Gamma(\frac{n}{2}+1)$ is the volume of the unit n-ball. In the language of $K(X)$, the sporadic condition has the following geometric characterization.

Proposition 2.3.2. *For $X \in \mathcal{S}^n_+(\mathbb{Z})$, X is sporadic if and only if $K(X) \cap \mathbb{Z}^n = \{\mathbf{0}\}$.*

The degenerate case for rank one is characterized by the following proposition.

Proposition 2.3.3. *Suppose $X \in \mathcal{S}^n_+(\mathbb{Z})$ with $\operatorname{rank}(X) = 1$, then $X = \lambda \mathbf{x}\mathbf{x}^\top$, where $\mathbf{x} \in \mathbb{Z}^n$ and $\lambda \in \mathbb{Z}_{\geq 1}$.*

Proof. As $X \succeq 0$ and $\operatorname{rank}(X) = 1$, we can assume that $X = \mathbf{a}\mathbf{a}^\top$ for some $\mathbf{a} \in \mathbb{R}^n$. Because $X \in \mathcal{S}^n(\mathbb{Z})$, we have $a_i a_j \in \mathbb{Z}$ for $i, j \in [n]$. In particular, $a_i^2 \in \mathbb{Z}$. Denote $k_i := a_i^2 \in \mathbb{Z}_{\geq 0}$. Without loss of generality, we can assume that $k_i \geq 1$, i.e., $a_i \neq 0$, otherwise, we can just consider the submatrix corresponding to the nonzero k_i.
Suppose that there exists some $a_i \in \mathbb{Z}\backslash\{0\}$ and $a_j \in \{\pm\sqrt{k_j}\} \notin \mathbb{Q}$. Then $a_i a_j \notin \mathbb{Q}$, a contradiction. Therefore, we must have either $a_i \in \mathbb{Z}$ for all i or $a_i \notin \mathbb{Q}$ for any i.
If $a_i \in \mathbb{Z}$ for all i, then the result holds with $\lambda = 1$ and $x = a$.
If $a_i \notin \mathbb{Q}$ for all i, i.e., k_i is not a square. Because $a_i a_j \in \mathbb{Z}$, we have $\sqrt{k_i k_j} \in \mathbb{Z}$, which implies that $k_i k_j = t_{ij}^2$ for some integer t_{ij}. Suppose that $p_1, \ldots, p_s$ are all the prime factors in the decompositions of k_i, $i \in [n]$ such that $k_i = \prod_{\ell=1}^s p_\ell^{\alpha_\ell^i}$, for some $\alpha_\ell^i \in \mathbb{Z}_{\geq 0}$. We have $k_i k_j = \prod_{\ell=1}^s p_\ell^{\alpha_\ell^i + \alpha_\ell^j} = t_{ij}^2$, which implies that $\alpha_\ell^i + \alpha_\ell^j$ is even. Therefore, for a fixed ℓ, either α_ℓ^i is even for all $i \in [n]$ or α_ℓ^i is odd for all $i \in [n]$. Let $I := \{\ell \in [s] : \alpha_\ell^i \text{ is odd}\}$ and $\lambda = \prod_{\ell \in I} p_\ell$. We have k_i/λ is a square, thus $X = \lambda \mathbf{x}\mathbf{x}^\top$ for $x = a/\sqrt{\lambda}$, where $x_i = \sqrt{k_i/\lambda} \in \mathbb{Z}$. □

From Proposition 2.3.3, we can directly prove the case for $n = 2$ using Minkowski's First Theorem (for example, see [40]): if $\operatorname{vol}(K(X)) > 4$, then there is a nonzero integral point in $K(X)$.

Proposition 2.3.4. *Lemma 2.3.2.1 holds for $n = 2$.*

Proof. For $n = 2$. Let $X = \begin{bmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{bmatrix} \succeq 0$, where $a_{11}, a_{12}, a_{22} \in \mathbb{Z}$, which implies that $a_{11} \geq 0, a_{22} \geq 0, a_{11}a_{22} - a_{12}^2 \geq 0$. By Proposition 2.3.3, we only need to consider the case when $X \succ 0$, i.e., $\det(X) = a_{11}a_{22} - a_{12}^2 \geq 1, a_{11} \geq 1, a_{22} \geq 1$. Then,

$$\begin{aligned} K(X) &:= \{\mathbf{x} \in \mathbb{R}^2 : X - \mathbf{x}\mathbf{x}^\top \succeq 0\} \\ &= \{\mathbf{x} \in \mathbb{R}^2 : a_{11} - x_1^2 \geq 0, a_{22} - x_2^2 \geq 0, (a_{11} - x_1^2)(a_{22} - x_2^2) - (a_{12} - x_1 x_2)^2 \geq 0\}. \end{aligned}$$

We claim that $K(X) = \{\mathbf{x} \in \mathbb{R}^2 : (a_{11} - x_1^2)(a_{22} - x_2^2) - (a_{12} - x_1x_2)^2 \geq 0\}$. To see this, note that

$$\begin{aligned} 0 \leq (a_{11} - x_1^2)(a_{22} - x_2^2) - (a_{12} - x_1x_2)^2 &= (a_{11}a_{22} - a_{12}^2) - a_{22}x_1^2 + 2a_{12}x_1x_2 - a_{11}x_2^2 \\ &= \frac{a_{11}a_{22} - a_{12}^2}{a_{11}}(a_{11} - x_1^2) - a_{11}(x_2 - \frac{a_{12}}{a_{11}}x_1)^2 \end{aligned}$$

which together with $a_{11}, a_{22}, a_{11}a_{22} - a_{12}^2 > 0$ implies that $a_{11} - x_1^2 \geq 0$. Similarly,

$$0 \leq (a_{11} - x_1^2)(a_{22} - x_2^2) - (a_{12} - x_1x_2)^2 = \frac{a_{11}a_{22} - a_{12}^2}{a_{22}}(a_{22} - x_2^2) - a_{22}(x_1 - \frac{a_{12}}{a_{22}}x_2)^2$$

implies that $a_{22} - x_2^2 \geq 0$, which shows the claim.

Since X has full rank, $K(X) = \{\mathbf{x} \in \mathbb{R}^2 : \det(X) - a_{22}x_1^2 + 2a_{12}x_1x_2 - a_{11}x_2^2 \geq 0\}$ is a centrally symmetric ellipsoid with area $\pi\sqrt{\det(X)}$.

If $\det(X) \geq 2$, then $\mathrm{vol}(K(X)) \geq \sqrt{2}\pi > 4$, we know that $K(X) \cap \mathbb{Z}^2 \neq \emptyset$ by Minkowski's First Theorem.

If $\det(X) = 1$, then $K(X) = \{x \in \mathbb{R}^n : a_{22}x_1^2 - 2a_{12}x_1x_2 + a_{11}x_2^2 \leq 1\}$. Because $a_{22}, a_{12}, a_{11} \in \mathbb{Z}$, we have $K(X) \cap \mathbb{Z}^2 = \tilde{K}(X) \cap \mathbb{Z}^2$, where $\tilde{K}(X) = \sqrt{2-\epsilon} \cdot K(X) = \{x \in \mathbb{R}^n : a_{22}x_1^2 - 2a_{12}x_1x_2 + a_{11}x_2^2 \leq 2 - \epsilon\}$ for any $0 < \epsilon < 1$. Therefore, $\mathrm{vol}(\tilde{K}(X)) = (2 - \epsilon) \cdot \pi > 4$ when we take any $\epsilon < 2 - \frac{4}{\pi}$. Therefore, $\tilde{K}(X) \cap \mathbb{Z}^2$ is nonempty by Minkowski's First Theorem so neither is $K(X) \cap \mathbb{Z}^2$. $\square$

In the degenerate case, we can reduce the problem to one involving full-rank matrices of some lower dimension.

Lemma 2.3.2.2. *Let $X \in \mathcal{S}^n(\mathbb{Z})$. If $r = \mathrm{rank}(X) < n$, then X is unimodularly equivalent to*

$$\begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \hat{X} \end{bmatrix},$$

for some $\hat{X} \in \mathbb{Z}^{r \times r}$, $\mathrm{rank}(\hat{X}) = r$.

Proof. If $\mathrm{rank}(X) < n$, then there exists a primitive vector $\mathbf{z} \in \mathbb{Z}^n$ in the subspace $N := \{\mathbf{y} \in \mathbb{R}^n : X\mathbf{y} = \mathbf{0}\}$. The sublattice $\Lambda := \mathbb{Z}^n \cap N$ is primitive and thus a basis of Λ containing $\mathbf{z}$ can be extended to a basis of $\mathbb{Z}^n$, which we denote as $U = [\mathbf{z}, \mathbf{u}_2, \ldots, \mathbf{u}_n]$ [92, Chapter 2, Lemma 4].

Because U is a basis of $\mathbb{Z}^n$, we know that $|\det(U)| = 1$, i.e., U is unimodular. Then

$$U^\top X U = \begin{bmatrix} 0 & 0 \\ 0 & \hat{X} \end{bmatrix}.$$

Iterating this process until $\hat{X}$ is positive definite, i.e., $\text{rank}(\hat{X}) = r$. $\square$

Notice that if X_1, X_2 are unimodularly equivalent, then $K(X_1) \cap \mathbb{Z}^n \neq \{\mathbf{0}\}$ if and only if $K(X_2) \cap \mathbb{Z}^n \neq \{\mathbf{0}\}$. Thus our problem expects an answer under the unimodular equivalence of integer matrices in $\mathcal{S}_+^n(\mathbb{Z})$.

The scaling of $K(X)$ into $\tilde{K}(X)$ (while preserving the integer points) in the proof for Proposition 2.3.4 results in

$$\text{vol}(\tilde{K}(X)) < V_n \sqrt{\det(X)} \cdot \left(\frac{\det(X) + 1}{\det(X)}\right)^{n/2}$$

where V_n is a constant dependent only on the dimension n, and the right-hand side can be approached arbitrarily. When $n = 3$, $V_n \approx 4.189$, the right-hand side becomes $2^{3/2} \approx 2.828$, $\sqrt{2} \cdot (3/2)^{3/2} \approx 2.598$, $\sqrt{3} \cdot (4/3)^{3/2} \approx 2.667$ for $\det(X) = 1, 2,$ and 3, respectively, and greater than 2 for $\det(X) \geq 4$. Thus $\text{vol}(\tilde{K}(X)) > 8$ so $\tilde{K}(X) \cap \mathbb{Z}^3 \neq \{0\}$ by Minkowski's First Theorem.

To prove Lemma 2.3.2.1, we need to use a more sophisticated method based on the *Hermite constant* [104]

$$\gamma_n := \left(\max_{A \succ 0} \frac{\lambda_1(A)}{(\det(A))^{\frac{1}{n}}}\right)^n, \text{ where } \lambda_1(A) = \min_{\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}} (\mathbf{x}^\top A \mathbf{x}).$$

Remark 2.3.1. *Hermite gives a bound $\gamma_n \leq (\frac{4}{3})^{\frac{n(n-1)}{2}}$. The exact value of γ_n is only known for $n \leq 8$ and $n = 24$.*

n	2	3	4	5	6	7	8	24
γ_n	$\frac{4}{3}$	2	2	8	$\frac{64}{3}$	64	256	4^{24}

Table 2.1. Known exact values of the Hermite constant γ_n.

Remark 2.3.2. *From a volume argument by Minkowski's First Theorem, we have*

$$\min_{\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}} (\mathbf{x}^\top A \mathbf{x}) \leq \frac{4}{\pi} \Gamma(1 + \frac{n}{2})^{\frac{2}{n}} \det(A)^{\frac{1}{n}} \sim \frac{2n}{\pi e} \det(A)^{\frac{1}{n}},$$

which is better than the bound given by $\gamma_n \leq (\frac{4}{3})^{\frac{n(n-1)}{2}}$ *when* n *is large. But this estimation on* γ_n *is not enough to prove Lemma 2.3.2.1 for the dimension* $n = 4, 5$.

Proof of Lemma 2.3.2.1. The case $n = 1$ follows from Proposition 2.3.3. We will show that $K(X) \cap \mathbb{Z}^n \neq \{\mathbf{0}\}$ for $2 \leq n \leq 5$, where $K(X) = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x}^\top \mathrm{adj}(X)\mathbf{x} \leq \det(X)\}$. By the definition of the Hermite constant, we have

$$\min_{\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}} (\mathbf{x}^\top \mathrm{adj}(X)\mathbf{x}) \leq (\gamma_n \det(\mathrm{adj}(X)))^{\frac{1}{n}} = (\gamma_n (\det(X))^{n-1})^{\frac{1}{n}}.$$

For $n = 2, 3, 4, 5$, we have $\frac{n^n}{(n-1)^{n-1}} > \gamma_n$ as $\frac{2^2}{1^1} = 4$, $\frac{3^3}{2^2} \approx 6.75$, $\frac{4^4}{3^3} \approx 9.48$, $\frac{5^5}{4^4} \approx 12.21$, and $\frac{6^6}{5^5} \approx 14.93$. By taking the derivative with respect to $\det(X)$ for finding extremum value, we know that $\frac{(\det(X)+1)^n}{(\det(X))^{n-1}} \geq \frac{n^n}{(n-1)^{n-1}}$. Thus, $\gamma_n < \frac{(\det(X)+1)^n}{\det(X)^{n-1}}$. Therefore,

$$\min_{\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}} (\mathbf{x}^\top \mathrm{adj}(X)\mathbf{x}) \leq (\gamma_n \det(\mathrm{adj}(X)))^{\frac{1}{n}} = (\gamma_n \det(X)^{n-1})^{\frac{1}{n}} < \det(X) + 1.$$

Because $x^\top \mathrm{adj}(X)x, \det(X) \in \mathbb{Z}$ for any $x \in \mathbb{Z}^n$, we have

$$\min_{\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}} (\mathbf{x}^\top \mathrm{adj}(X)\mathbf{x}) \leq \det(X),$$

which implies that $K(X) \cap (\mathbb{Z}^n \setminus \{\mathbf{0}\}) \neq \emptyset$. Lemma 2.3.2.1 now follows from Propositions 2.3.2 and 2.3.1, and Lemma 2.3.2.2. □

The argument used to prove Lemma 2.3.2.1 fails for $n \geq 6$, but it implies that the determinant of the sporadic matrices is bounded by a constant only dependent on n. For example, in the case of $n = 6$, the argument only fails when $3 \leq \det(X) \leq 14$; for $n = 7$, it only fails when $2 \leq \det(X) \leq 56$, and for $n = 8$, it only fails when $1 \leq \det(X) \leq 247$. We summarize this observation in the following corollary.

Corollary 2.3.1. *If* $X \in \mathcal{S}^n_+(\mathbb{Z})$ *is sporadic, then* $\det(X) < \gamma_n$.

2.3.2. The Mordell Matrix and the $n = 6$ Obstruction. Corollary 2.3.1 gives us a finite handle on the sporadic points: rather than searching the infinite cone $\mathcal{S}^n_+(\mathbb{Z})$, we only need to inspect integer PSD matrices of bounded determinant, and only up to unimodular equivalence. For $n \leq 5$ the bound is strong enough to exclude all sporadics entirely, as Lemma 2.3.2.1 shows. For $n = 6$, the bound gives $\det(X) \leq 21$, leaving finitely many equivalence classes to check by hand.

The classical theory of *extreme quadratic forms*, going back to Korkine and Zolotareff [80], provides the right perspective for this enumeration: every positive definite quadratic form is unimodularly equivalent to one whose successive minima can be read off the diagonal, and in low rank with small determinant, the number of such reduced forms is small. Carrying out the check for $n = 6$, $\det(X) \le 21$, yields exactly one equivalence class of sporadic matrices, the Mordell matrix.

The matrix is most naturally understood as a quadratic form. Recall that $X \in \mathcal{S}_+^n(\mathbb{Z})$ defines the form $f_X(\mathbf{x}) = \mathbf{x}^\top X \mathbf{x}$ on $\mathbb{Z}^n$, and that X admits an integer rank-1 decomposition $X = \sum_i \mathbf{x}_i \mathbf{x}_i^\top$ if and only if f_X is a sum of squares of integer linear forms: $f_X(\mathbf{y}) = \sum_i (\mathbf{x}_i^\top \mathbf{y})^2$. Mordell [89] asked exactly this question: when does a positive definite integer quadratic form admit such a decomposition? He proved that this is always possible for $n \le 5$ and exhibited a concrete obstruction at $n = 6$. Ko [79] subsequently extended the analysis at $n = 6$ and established uniqueness up to unimodular equivalence. We present below the matrix M in a formulation unimodularly equivalent to Mordell's original form.

Proposition 2.3.5 ([89]). *The matrix*

$$M = \begin{pmatrix} 2 & 0 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 1 & 1 & 1 \\ 1 & 0 & 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 & 2 \end{pmatrix}, \qquad \det(M) = 3,$$

is sporadic in $\mathcal{S}_+^6(\mathbb{Z})$, and is the unique sporadic element of $\mathcal{S}_+^6(\mathbb{Z})$ up to unimodular equivalence [79].

Proof. We verify that $\min_{\mathbf{x}\in\mathbb{Z}^6\setminus\{\mathbf{0}\}}(\mathbf{x}^\top \mathrm{adj}(M)\mathbf{x}) > \det(M) = 3$.

$$\mathrm{adj}(M) = (\det(M))M^{-1} = \begin{bmatrix} 4 & 3 & 1 & -2 & -2 & -2 \\ 3 & 6 & 3 & -3 & -3 & -3 \\ 1 & 3 & 4 & -2 & -2 & -2 \\ -2 & -3 & -2 & 4 & 1 & 1 \\ -2 & -3 & -2 & 1 & 4 & 1 \\ -2 & -3 & -2 & 1 & 1 & 4 \end{bmatrix}$$

Note that $\mathbf{x}^\top \mathrm{adj}(M)\mathbf{x} = [(x_1+2x_2+x_3-x_4-x_5-x_6)^2+(x_1+x_2+x_3-x_4-x_5-x_6)^2+x_2^2]+[(x_1-x_3)^2+x_1^2+x_3^2]+[(x_4-x_5)^2+(x_4-x_6)^2+(x_5-x_6)^2]$. Let $A_2 := (x_1+2x_2+x_3-x_4-x_5-x_6)^2+(x_1+x_2+x_3-x_4-x_5-x_6)^2+x_2^2$, $A_{13} := (x_1-x_3)^2+x_1^2+x_3^2$ and $A_{456} := (x_4-x_5)^2+(x_4-x_6)^2+(x_5-x_6)^2$. Then $\mathbf{x}^\top \mathrm{adj}(M)\mathbf{x} = A_2 + A_{13} + A_{456}$.

Suppose there exists $\mathbf{x} \in \mathbb{Z}^6$ such that $\mathbf{x}^\top \mathrm{adj}(M)\mathbf{x} \le 3$. We are going to show that $\mathbf{x} = 0$. Notice that A_2, A_{13}, A_{456} are even, which implies that $A_2 + A_{13} + A_{456} \le 2$. Then at most one of A_2, A_{13}, A_{456} is nonzero.

We consider the following three cases:

(1) if $A_{13} = 0, A_{456} = 0$, then $x_1 = x_3 = 0, x_4 = x_5 = x_6 = 0$. Because $A_2 = 6x_2^2 \le 2$, we have $x_2 = 0$.

(2) if $A_2 = 0, A_{456} = 0$, then $x_4 = x_5 = x_6 = 0$, $x_2 = 0$, $x_1 + x_3 = 0$. Because $A_{13} = 6x_1^2 \le 2$, we have $x_1 = 0$.

(3) if $A_2 = 0, A_{13} = 0$, then $x_1 = x_3 = 0$, $x_2 = 0$, $x_4 + x_5 + x_6 = 0$. Because $A_{456} = (x_4-x_5)^2 + (2x_4+x_5)^2 + (x_4+2x_5)^2 = 6(x_4^2+x_5^2+x_4x_5) \le 2$, we have $x_4 = x_5 = x_6 = 0$.

Therefore, we have that $\min\limits_{\mathbf{x}\in\mathbb{Z}^6\setminus\{\mathbf{0}\}}(\mathbf{x}^\top \mathrm{adj}(M)\mathbf{x}) > 3$. For $\mathbf{x} = \mathbf{e}_1$, we see that $\mathbf{x}^\top \mathrm{adj}(M)\mathbf{x} = 4$, i.e., $\min\limits_{\mathbf{x}\in\mathbb{Z}^6\setminus\{\mathbf{0}\}}(\mathbf{x}^\top \mathrm{adj}(M)\mathbf{x}) = 4$. □

The determinant $\det(M) = 3$ is no accident: it is the smallest determinant compatible with the bound $\det(X) < \gamma_6 = 64/3$ that admits a sporadic configuration in dimension 6. The associated ellipsoid $K(M)$ contains no nonzero integer points despite having volume $V_6\sqrt{3} \approx 8.95$, well below the Minkowski threshold of $2^6 = 64$. This is why Minkowski-type volume arguments fail for $n \ge 6$

and why the Hermite constant is needed. The geometry also clarifies what is special about $n = 6$. The Hermite constant grows fast enough that for $n \leq 5$, the inequality $\gamma_n < n^n/(n-1)^{n-1}$ gives the bound needed for Lemma 2.3.2.1, but at $n = 6$ the inequality reverses: $\gamma_6 = 64/3 \approx 21.33$ while $6^6/5^5 \approx 14.93$. The sporadic matrix M realizes this gap.

Combining Proposition 2.3.5 with Ko's uniqueness result [79] yields the following decomposition for arbitrary $X \in \mathcal{S}^6_+(\mathbb{Z})$.

Lemma 2.3.2.3. *If $n = 6$, then for any $X \in \mathcal{S}^n_+(\mathbb{Z})$,*

$$X = \sum_{i \in K} \mathbf{x}_i \mathbf{x}_i^\top + Y$$

for $\mathbf{x}_i \in \mathbb{Z}^n$ and Y unimodularly equivalent to M, where K is a finite index set.

Every integer PSD matrix in dimension 6 decomposes as a sum of rank-one matrices plus at most one "Mordell piece": a copy of M, suitably transformed. Either X has an honest rank-one decomposition, or it has one modulo a single unimodular copy of M. This is the smallest possible failure of pure rank-one decomposability for integer PSD matrices, and (R, G)-finite generation is precisely the language that captures this structured failure.

2.3.3. Proof of Theorem 2.3.2.

Proof of Theorem 2.3.2. The primitive extreme points of $\mathcal{S}^n_+(\mathbb{Z})$ are the rank-one matrices $\mathbf{x}\mathbf{x}^\top$ for primitive $\mathbf{x} \in \mathbb{Z}^n$, all of which lie in the $\mathrm{GL}(n, \mathbb{Z})$-orbit of $e_1 e_1^\top$. It therefore suffices to show that the sporadic points form finitely many orbits under $\mathrm{GL}(n, \mathbb{Z})$.

By Corollary 2.3.1, any sporadic X satisfies $\det(X) < \gamma_n$. By ♣ [citation], any positive definite $X \in \mathcal{S}^n(\mathbb{Z})$ is unimodularly equivalent to a matrix X' whose diagonal entries satisfy $\prod_i X'_{ii} \leq \alpha_n \det(X') < \alpha_n \gamma_n$ for a constant α_n depending only on n. Since $X'_{ii} \geq 1$ are bounded integers and $|X'_{ij}|^2 \leq X'_{ii} X'_{jj}$, there are only finitely many possibilities for X', hence finitely many sporadic orbits.

The cases $n \leq 5$ and $n = 6$ follow from Lemmas 2.3.2.1 and 2.3.2.3 respectively, giving the explicit root sets stated in Theorem 2.3.2. For $n \geq 7$ the argument is existential: the root set R is finite but not explicitly enumerated. ∎

2.4. Applications

The (R, G)-finite generation results of the preceding sections have consequences beyond the classification of integer points in the PSD and Lorentz cones. In this section we develop three applications: an extension of total dual integrality to conic integer programs, a finite description of Chvátal–Gomory closures for TDI conic systems, and an upper bound on the integer Carathéodory rank of arbitrary pointed cones. All three results hold at the level of a general cone C, not specific to the PSD or Lorentz setting.

Throughout this section, $C \subset \mathbb{R}^N$ is a full-dimensional pointed convex cone and $S_C := C \cap \mathbb{Z}^N$ its conical semigroup.

2.4.1. Total Dual Integrality and Chvátal–Gomory Closures.

A central problem in integer programming is approximating the convex hull of integer points in a feasible region by linear inequalities. The classical Chvátal–Gomory cut construction is the simplest tool for this: given any inequality $\mathbf{u}^\top \mathbf{x} \le v$ with $\mathbf{u} \in \mathbb{Z}^m$ that is valid for the relaxation, the strengthened inequality $\mathbf{u}^\top \mathbf{x} \le \lfloor v \rfloor$ is valid for all integer feasible points. The set of all such cuts produces the *Chvátal–Gomory closure* of the feasible region. In the polyhedral setting, total dual integrality and Hilbert bases give a finite description of this closure: a rational system $A\mathbf{x} \le \mathbf{b}$ is TDI if and only if, for each face F of the corresponding polyhedron, the active rows of A form a Hilbert basis for the cone they generate [103]. We extend this picture to conic integer programs, where the role of the Hilbert basis is played by an (R, G)-finitely generated semigroup.

Given a linear map $\mathcal{A} : \mathbb{R}^m \to \mathbb{R}^N$ and $\mathbf{c} \in \mathbb{Z}^N$ with $\mathcal{A}(\mathbb{Z}^m) \subseteq \mathbb{Z}^N$, define the **linear conical inequality** (LCI) system

$$\mathrm{LCI}_C(\mathbf{c}, \mathcal{A}) := \{\mathbf{x} \in \mathbb{R}^m : \mathbf{c} - \mathcal{A}(\mathbf{x}) \in C\}.$$

When $C = \mathcal{S}^n_+$ and $\mathcal{A}(\mathbf{x}) = \sum_{i=1}^m x_i A_i$ for symmetric integer matrices A_i, this is a linear matrix inequality and LCI_C is a spectrahedron.

Definition 2.4.1. *The LCI system $\mathbf{c} - \mathcal{A}(\mathbf{x}) \in C$ is **totally dual integral** (TDI) if for every $\mathbf{b} \in \mathbb{Z}^m$, the dual problem*

$$\min \; y(\mathbf{c}) \quad \textit{subject to} \quad \mathcal{A}^*(y) = \mathbf{b}, \; y \in C^*,$$

has an integer optimal solution $y^* \in C^* \cap \mathbb{Z}^N$ whenever it is feasible.

Total dual integrality is well-studied for polyhedral cones [51, 66] and has been recently extended to spectrahedral cones [38, 47]. For polyhedral cones the role of (R, G)-finite generation reduces to the existence of a Hilbert basis; for non-polyhedral C the (R, G)-finite generation of S_{C^*} plays the analogous role.

To approximate the convex hull of $Z := \mathrm{LCI}_C(\mathbf{c}, \mathcal{A}) \cap \mathbb{Z}^m$, one adds **Chvátal–Gomory cuts**: if $\mathbf{u} \in \mathbb{Z}^m$ and the inequality $\mathbf{u}^\top \mathbf{x} \le v$ is valid for all $\mathbf{x} \in \mathrm{LCI}_C(\mathbf{c}, \mathcal{A})$, then $\mathbf{u}^\top \mathbf{x} \le \lfloor v \rfloor$ is valid for all $\mathbf{x} \in Z$. The **CG closure** is

$$\text{CG-cl}(Z) := \bigcap_{\substack{(\mathbf{u},v)\in\mathbb{Z}^m\times\mathbb{R}:\\ Z\subseteq\{\mathbf{x}:\mathbf{u}^\top\mathbf{x}\le v\}}} \left\{\mathbf{x} \in \mathbb{R}^m : \mathbf{u}^\top \mathbf{x} \le \lfloor v \rfloor\right\}.$$

In general there are infinitely many CG cuts. When S_{C^*} is (R, G)-finitely generated, Theorems 2.3.2 and 2.2.1 imply that the CG closure admits a finite description.

THEOREM 2.4.2 (De Loera, Marsters, Xu, Zhang [43]). *Suppose $S_{C^*} := C^* \cap \mathbb{Z}^N$ is (R, G)-finitely generated and $\mathrm{LCI}_C(\mathbf{c}, \mathcal{A})$ is TDI. Then*

$$\text{CG-cl}(Z) = \left\{\mathbf{x} \in \mathbb{R}^m : (g \cdot r)^\top \mathcal{A}(\mathbf{x}) \le \lfloor (g \cdot r)^\top \mathbf{c} \rfloor,\ \forall\, r \in R,\ g \in G\right\}.$$

PROOF OF THEOREM 2.4.2. The containment $\subseteq$ is obvious as discussed above. To see the other containment, take any halfspace $H := \{\mathbf{x} \in \mathbb{R}^m : u^\top \mathbf{x} \le v\}$ for some $(\mathbf{u}, v) \in \mathbb{Z}^m \times \mathbb{R}$ such that $C \subseteq H$. Then by the full dimensionality of C, we have

$$v \ge \sup_x \left\{\mathbf{u}^\top \mathbf{x} : \mathbf{c} - \mathcal{A}(\mathbf{x}) \in C\right\} = \inf_y \left\{y(\mathbf{c}) : \mathcal{A}^*(y) = \mathbf{u},\ y \in C^*\right\}.$$

Using the TDI assumption, the infimum is attained by some $y^* \in C^* \cap \mathbb{Z}^N$. As S is (R, G)-finitely generated, $r_1, \ldots, r_k \in R$, $g_1, \ldots, g_k \in G$, and $\lambda_1, \ldots, \lambda_k \in \mathbb{Z}_{\ge 0}$ such that

$$y^* = \sum_{j=1}^k \lambda_j (g_j \cdot r_j),$$

for some $k \ge 1$. Consequently, we have

$$\lfloor v \rfloor \ge \lfloor y^*(\mathbf{c}) \rfloor = \left\lfloor \sum_{j=1}^k \lambda_j (g_j \cdot r_j)^\top \mathbf{c} \right\rfloor \ge \sum_{j=1}^k \lambda_j \lfloor (g_j \cdot r_j)^\top \mathbf{c} \rfloor.$$

Note that $(\lambda_1, \ldots, \lambda_k)$ is a feasible solution to the following (semi-infinite) linear optimization problem

$$\begin{aligned} \inf_{\lambda} \quad & \sum_{r \in R, g \in G} \lfloor (g \cdot r)^\top \mathbf{c} \rfloor \lambda_{r,g} \\ \text{s.t.} \quad & \mathcal{A}^* \Bigg(\sum_{r \in R, g \in G} \lambda_{g,r} (g \cdot r) \Bigg) = \mathbf{u}, \\ & \lambda \in \bigoplus_{r \in R, g \in G} \mathbb{R}_{\geq 0}. \end{aligned}$$

By weak duality of the semi-infinite optimization problem, we also have

$$\sum_{j=1}^{k} \lambda_j \lfloor (g_j \cdot r_j)^\top \mathbf{c} \rfloor \geq \sup_{x} \left\{ \mathbf{u}^\top \mathbf{x} : \mathcal{A}^*(g \cdot r)^\top \mathbf{x} \leq \lfloor (g \cdot r)^\top \mathbf{c} \rfloor, \ \forall r \in R, g \in G \right\}.$$

Therefore, the inequality $\mathbf{u}^\top \mathbf{x} \leq \lfloor v \rfloor$ is implied by the inequalities $(g \cdot r)^\top \mathcal{A}(\mathbf{x}) = \mathcal{A}^*(g \cdot r)^\top \mathbf{x} \leq \lfloor (g \cdot r)^\top \mathbf{c} \rfloor$ for $r \in R, g \in G$. Since the halfspace H is arbitrary, we conclude that

$$\square \qquad \text{CG-cl}(Z) \supseteq \left\{ \mathbf{x} \in \mathbb{R}^m : (g \cdot r)^\top \mathcal{A}(\mathbf{x}) \leq \lfloor (g \cdot r)^\top \mathbf{c} \rfloor, \quad \forall r \in R, g \in G \right\}.$$

$\square$

2.4.2. Integer Carathéodory Rank. The classical theorem of Carathéodory states that any point in a d-dimensional convex cone $C \subseteq \mathbb{R}^d$ generated by vectors $\{a_1, \ldots, a_k\}$ can be written as a nonnegative real combination of at most d of these generators. The integer analogue asks the same question with nonnegative integer combinations and a Hilbert basis as the generating set. The **integer Carathéodory rank** $\text{ICR}(C)$ of a pointed rational cone $C \subseteq \mathbb{R}^n$ is the smallest integer k such that every integer point in C is a nonnegative integer combination of at most k Hilbert basis elements. A cone has the *integer Carathéodory property* (ICP) if $\text{ICR}(C) = n$, the smallest possible value for an n-dimensional cone.

The problem of bounding $\text{ICR}(C)$ has remained active since its introduction, with renewed progress in the past few years. The history of bounds on $\text{ICR}(C)$ is as follows.

1986. Cook, Fonlupt, and Schrijver [36] introduced $\text{ICR}(C)$, proved the upper bound $\text{ICR}(C) \leq 2n - 1$, and conjectured the ICP for all pointed rational cones.

1990. Sebő [105] improved the upper bound to $\mathrm{ICR}(C) \le 2n-2$ for $n \ge 2$ and proved that the ICP holds for $n \le 3$.

1999. Bruns, Gubeladze, Henk, Martin, and Weismantel [19] constructed a 6-dimensional cone with $\mathrm{ICR}(C) = 7$, refuting the Cook–Fonlupt–Schrijver conjecture and showing the ICP fails in general for $n \ge 6$.

2007. Bruns [17] produced further counterexamples in higher dimensions, with asymptotic constructions yielding $\mathrm{ICR}(C) \ge \lfloor 7n/6 \rfloor$ for some cones in each dimension $n \ge 6$.

2024. Aliev, Henk, Hogan, Kuhlmann, and Oertel [1] proved the asymptotic bound $\mathrm{ICR}^{\mathrm{a}}(C) \le \lfloor 3n/2 \rfloor$, where $\mathrm{ICR}^{\mathrm{a}}$ measures the rank for "most" integer vectors in the cone, and gave sharper bounds in terms of Δ, the maximal absolute $n \times n$ subdeterminant of an integer polyhedral representation of C: when $\Delta \in \{1, 2\}$, the ICP holds.

2025. Kuhlmann [81] showed that simplicial cones with multiplicity at most 5 have the ICP and proved $\mathrm{ICR}(C) \le n + |\det| - 3$ for simplicial cones with multiplicity $6 \le |\det| \le n$, improving Sebő's bound whenever the multiplicity is bounded by the dimension.

The cases $n \in \{4, 5\}$ remain open: it is not known whether the ICP holds in these dimensions, and Sebő's $2n-2$ bound has not been improved for general cones in over thirty years. The work of this chapter sits at the boundary of this program: rather than improving the bound on $\mathrm{ICR}(C)$ for a polyhedral cone, we ask what survives of the Carathéodory picture when C is non-polyhedral and no finite Hilbert basis exists. Theorems 2.3.2 and 2.2.1 provide an answer: every integer point in $\mathcal{S}^n_+(\mathbb{Z})$ or T_n is a nonnegative integer combination of group-orbit elements drawn from a finite root set.

First, we define the key notions in this new non-polyhedral setting.

Definition 2.4.3. *Let $B \subseteq S_C$ be an integer generating set. The **integer Carathéodory rank** of $s \in S_C$ with respect to B is the minimum m such that $s = \sum_{i=1}^m \lambda_i b_i$ for some $b_i \in B$ and $\lambda_i \in \mathbb{Z}_{\ge 1}$. The **ICR** of S_C is $\mathrm{ICR}(S_C) = \sup_{s \in S_C} \mathrm{ICR}(s)$.*

Theorem 2.4.4 (De Loera, Marsters, Xu, Zhang [43]). *Let $C \subset \mathbb{R}^N$ be an arbitrary pointed convex cone and $S_C := C \cap \mathbb{Z}^N$. Then $\mathrm{ICR}(S_C) \le 2N - 2$.*

The strategy of the proof is to reformulate the integer decomposition problem as a linear program: we ask for the optimal real-valued solution, round it down to obtain an integer part, and then control the leftover fractional part using a second LP. In the polyhedral setting this LP has finitely many variables; in our setting the integer generating set may be infinite (recall that for non-polyhedral cones, $B = \bigcup_{r \in R} G \cdot r$ contains infinitely many points), so we use the semi-infinite LP duality of Charnes, Cooper, and Kortanek [28] to extract an extreme point solution supported on at most N generators. The remainder of the argument is combinatorial, tracking how the fractional parts of the optimal solution can be absorbed into a second decomposition.

Proof of Theorem 2.4.4. Suppose $B = \{b_i\}_{i \in I} \subset S_C$ for some possibly infinite index set I is an integer generating set for S_C. Consider a semi-infinite linear optimization problem

$$
\begin{aligned}
& \max && \sum_{i \in I} \lambda_i \\
& \text{s.t.} && \sum_{i \in I} \lambda_i b_i = s, \\
& && (\lambda_i)_{i \in I} \in \mathbb{R}^{\oplus I}_{\geq 0}.
\end{aligned} \tag{2.12}
$$

Since C is pointed, B satisfies the "opposite sign condition," meaning that whenever $\sum_{i \in I} \mu_i b_i = 0$ for some nonzero $(\mu_i)_{i \in I} \in \mathbb{R}^{\oplus I}$, we have $\mu_i < 0 < \mu_j$ for some $i, j \in I$. Thus by [28, Theorem 2], we know that (2.12) has an extreme point solution, denoted as $(\lambda_i^*)_{i \in I}$ with $J := \{i \in I : \lambda_i^* > 0\}$. By [28, Theorem 1], the vectors $\{\lambda_i\}_{i \in J} \subset S_C$ associated with the extreme point solution must be linearly independent. Thus $|J| \leq N$.

For each $i \in J$, let $z_i := \lfloor \lambda_i^* \rfloor$ and $y_i := \lambda_i^* - z_i$. We claim that $\sum_{i \in J} y_i < N - 1$. Given this claim, the theorem is proved as follows. The vector $s' := s - \sum_{i \in J} z_i b_i \in C \cap \mathbb{Z}^N = S_C$ can be written as integer combination of B by definition, that is, there exists an index set $J' \subset I$ with $b_i' \in B$, $\lambda_i' \in \mathbb{Z}_{\geq 1}$ for each $i \in J'$ such that $s' = \sum_{i \in J'} \lambda_i' b_i'$. This implies that

$$
s = s' + \sum_{i \in J} z_i b_i = \sum_{i \in J} z_i b_i + \sum_{j \in J'} \lambda_i' b_i'.
$$

We see that $\sum_{i \in J} z_i + \sum_{j \in J'} \lambda_i' \leq \sum_{i \in J} \lambda_i^*$ by the optimality of $(\lambda_i^*)_{i \in I}$. Consequently, $\sum_{j \in J'} \lambda_j' \leq \sum_{i \in J} y_i < N - 1$, and thus s can be written as an integer sum of at most $|J| + N - 2 \leq 2N - 2$ generators from B.

It remains to prove the claim, $\sum_{i \in J} y_i < N - 1$. Note that if $|J| \leq N - 1$ this is trivially true because $y_i < 1$ by definition. So we may assume that $|J| = N$ and denote $J = \{1, \ldots, N\}$ without loss of generality. Moreover, if the convex hull $V := \operatorname{conv}\{b_1, \ldots, b_N\}$ has a nonempty intersection with B, say $b_{N+1} \in V \cap B$ with $b_{N+1} = \sum_{i=1}^N \gamma_i b_i$ for some $0 < \gamma_1, \dots, \gamma_N < 1$, $\sum_{i=1}^N \gamma_i = 1$, then we can write s as

$$s = \epsilon b_{N+1} + \sum_{i=1}^{N} (\lambda_i^* - \epsilon\gamma_i) b_i,$$

where $\epsilon := \frac{\lambda_\iota^*}{\gamma_\iota}$ for some $\iota \in \operatorname{argmin}\{\frac{\lambda_i^*}{\gamma_i} : i = 1, \dots, N\}$. This shows that $(\mu_i^*)_{i\in I}$ with $\mu_i^* := \lambda_i^* - \epsilon\gamma_i$ for each $i \in J \setminus \{\iota\}$, $\mu_{N+1}^* := \epsilon$, and $\mu_i^* = 0$ for any $i \notin J_1 := J \cup \{N+1\} \setminus \{\iota\}$, is also an optimal solution to (2.12). Thus by replacing J with J_1, we can assume that the intersection $V \cap B = \varnothing$. Under this assumption, let $s'' := \sum_{i=1}^N (1 - y_i) b_i = \sum_{i=1}^N b_i - s' \in C \cap \mathbb{Z}^N$. Again by the definition of B, we can write $s'' = \sum_{j\in J''} \lambda_j'' b_j''$, for some finite subset $J'' \subset I$, $b_j'' \in B$ and $\lambda_j'' \in \mathbb{Z}_{\geq 1}$ for each $j \in J''$. Note that

$$s = \delta s'' + \sum_{i\in J} (\lambda_i^* - \delta(1 - y_i)) b_i = \delta \sum_{i\in J''} \lambda_i'' b_i + \sum_{i\in J} (\lambda_i^* - \delta(1 - y_i)) b_i,$$

for some sufficiently small $\delta > 0$, so by the optimality of $(\lambda_i^*)_{i\in I}$, we must have $1 \leq \sum_{i\in J''} \lambda_i'' \leq \sum_{i\in J} (1 - y_i)$. If $\sum_{i=1}^N y_i \geq N - 1$, then this implies that $\sum_{i\in J} (1 - y_i) = 1$, which is a contradiction with our assumption $V \cap B = \varnothing$. Thus we must have $\sum_{i=1}^N y_i < N - 1$. $\square$

For the PSD cone $\mathcal{S}_+^n(\mathbb{Z})$, the ambient dimension is $N = \binom{n+1}{2}$, so Theorem 2.4.4 gives

$$\mathrm{ICR}(\mathcal{S}_+^n(\mathbb{Z})) \leq n^2 + n - 2.$$

For Lorentz cones $T_n = \mathcal{L}^n \cap \mathbb{Z}^n$, the ambient dimension is $N = n$, so the bound becomes

$$\mathrm{ICR}(T_n) \leq 2n - 2.$$

These bounds are notable because they grow with the ambient dimension N rather than the eigenvector dimension n. For PSD matrices, the contrast is striking: the real Carathéodory rank is at most n via the spectral decomposition $X = \sum_i \mathbf{x}_i \mathbf{x}_i^\top$ with $\mathbf{x}_i \in \mathbb{R}^n$, but an integer analogue of this decomposition need not exist, and the corrections needed to reach an integer decomposition are bounded by the ambient dimension $\binom{n+1}{2}$ rather than the eigenvector dimension n. The result is a quadratic upper bound where the real-valued problem admits a linear one. Whether either of the two bounds is tight remains open.

The bound $2N - 2$ is independent of the choice of integer generating set B: it holds simultaneously for every integer generating set of S_C, including the Hilbert basis (when one exists) and the set

$\bigcup_{r\in R} G\cdot r$ produced by an (R,G)-finite generating description. In particular, every $X \in \mathcal{S}_+^n(\mathbb{Z})$ can be written as a sum of at most n^2+n-2 rank-one and Mordell-type pieces, although finding the shortest such decomposition is computationally nontrivial.

2.5. Not All Conical Semigroups Are (R,G)-Finitely Generated

The results of Sections 2.2 and 2.3 might suggest that (R,G)-finite generation is a general phenomenon for conical semigroups. This is not the case. In this section we give an example of a planar cone whose conical semigroup admits no (R,G)-finite generating set for any choice of finite R and finitely generated G. The obstruction is irrationality: the cone has an irrational boundary ray, and any group action preserving the cone and its integer points is forced to be trivial.

Example 2.5.1. *Let $\alpha > 0$ be irrational and define the planar cone*

$$C := \{(x,y) \in \mathbb{R}^2 : 0 \le y \le \alpha x\},$$

generated by the vectors $\mathbf{v}_1 := (1,0)$ and $\mathbf{v}_2 := (1,\alpha)$. We claim that the conical semigroup $S_C := C \cap \mathbb{Z}^2$ is not (R,G)-finitely generated for any finite set $R \subset S_C$ and any finitely generated group G acting linearly on C.

The argument has two parts. First, we show that any $g \in G$ acting linearly on C and preserving S_C must be the identity. Second, since $\mathbf{v}_2$ is not a rational direction, S_C itself is not finitely generated, so no finite set R generates S_C even under the trivial group action.

Part 1: $G = \{I\}$. Since $\mathbf{v}_1$ and $\mathbf{v}_2$ are linearly independent, C is simplicial and every $\mathbf{v} \in C$ has a unique expression as a nonnegative real combination of $\mathbf{v}_1$ and $\mathbf{v}_2$. Any linear action of $g \in G$ on C is therefore represented by a matrix

$$U_g = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix} \in \mathbb{R}^{2\times 2}$$

with $\det(U_g) = u_{11}u_{22} - u_{21}u_{12} \neq 0$, and inverse

$$U_g^{-1} = \tfrac{1}{\det(U_g)} \begin{bmatrix} u_{22} & -u_{12} \\ -u_{21} & u_{11} \end{bmatrix}.$$

Since $\mathbf{v}_1 = (1,0) \in S_C$*, we have*

$$U_g \mathbf{v}_1 = \begin{bmatrix} u_{11} \\ u_{21} \end{bmatrix} \in S_C,$$

which forces $u_{11}, u_{21} \in \mathbb{Z}$ *and*

$$0 \le u_{21} \le \alpha u_{11}. \tag{2.13}$$

Setting $\mathbf{w} := (\lceil 1/\alpha \rceil, 1) \in S_C$*, the condition* $U_g \mathbf{w} \in S_C$ *gives*

$$U_g \mathbf{w} = \begin{bmatrix} \lceil 1/\alpha \rceil u_{11} + u_{12} \\ \lceil 1/\alpha \rceil u_{21} + u_{22} \end{bmatrix} \in S_C,$$

which forces $u_{12}, u_{22} \in \mathbb{Z}$*. Thus* $U_g \in \mathbb{Z}^{2\times 2}$*.*

Now take a sequence $\mathbf{w}_k := (x_k, y_k) \in S_C$ *with* $\lim_{k\to\infty} y_k/x_k = \alpha$*, whose existence is guaranteed by Dirichlet's approximation theorem. Since* $U_g \mathbf{w}_k \in S_C$*, we have* $0 \le u_{21}x_k + u_{22}y_k \le \alpha(u_{11}x_k + u_{12}y_k)$*, and dividing by* x_k *and taking* $k \to \infty$ *yields*

$$0 \le u_{21} + \alpha u_{22} \le \alpha(u_{11} + \alpha u_{12}). \tag{2.14}$$

Applying the same reasoning to $U_g^{-1}\mathbf{v}_1 \in S_C$*, we have*

$$U_g^{-1}\mathbf{v}_1 = \tfrac{1}{\det(U_g)} \begin{bmatrix} u_{22} \\ -u_{21} \end{bmatrix} \in S_C,$$

which gives

$$0 \le \tfrac{1}{\det(U_g)}(-u_{21}) \le \alpha \tfrac{1}{\det(U_g)} u_{22}, \tag{2.15}$$

and therefore $\frac{1}{\det(U_g)}(\alpha u_{22} + u_{21}) \ge 0$*. By* (2.14)*,* $u_{21} + \alpha u_{22} \ge 0$*, and the inequality is strict by the irrationality of* α *(otherwise* $\alpha = -u_{21}/u_{22} \in \mathbb{Q}$*, a contradiction). Consequently,* $\det(U_g) > 0$*, and* (2.15) *now gives* $u_{21} \le 0$*, which combined with* (2.13) *yields* $u_{21} = 0$*.*

For the remaining entries, consider

$$U_g^{-1}\mathbf{w}_k = \tfrac{1}{\det(U_g)}\begin{bmatrix} u_{22}x_k - u_{12}y_k \\ \\ u_{11}y_k \end{bmatrix} \in S_C.$$

Taking $k \to \infty$ gives $0 \leq \alpha u_{11} \leq \alpha(u_{22} - \alpha u_{12})$. Combined with (2.14), which now reads $u_{22} \leq u_{11} + \alpha u_{12}$, we obtain $u_{22} = u_{11} + \alpha u_{12}$. Irrationality of α forces $u_{12} = 0$, and hence $u_{11} = u_{22}$. Finally, $U_g^{-1}\mathbf{v}_1 = (1/u_{11}, 0) \in S_C$ forces $1/u_{11} \in \mathbb{Z}$, so $u_{11} = \pm 1$, and (2.13) rules out $u_{11} = -1$. Therefore $U_g = I$, and $G = \{I\}$.

Part 2: S_C is not finitely generated. With G trivial, (R, G)-finite generation reduces to the existence of a finite Hilbert basis for S_C. For any nonzero $(x, y) \in S_C$ with $x > 0$, the slope y/x lies in $[0, \alpha)$, with strict inequality because α is irrational. Given a finite set $R \subset S_C$, the slopes of its elements form a finite subset of $[0, \alpha)$, so there exists $\varepsilon > 0$ with $y/x \leq \alpha - \varepsilon$ for every $(x, y) \in R$ with $x > 0$. Nonnegative integer combinations preserve this slope bound: any $\sum_i \lambda_i(x_i, y_i)$ with $\lambda_i \in \mathbb{Z}_{\geq 0}$ has slope at most $\alpha - \varepsilon$. On the other hand, Dirichlet's approximation theorem produces lattice points $(x_k, y_k) \in S_C$ with $y_k/x_k \to \alpha$, so for k large enough (x_k, y_k) has slope exceeding $\alpha - \varepsilon$ and therefore cannot be expressed in the integer cone over R. Hence S_C is not finitely generated, completing the argument.

Example 2.5.1 shows that (R, G)-finite generation is a genuine constraint, not automatic. The obstruction here is purely arithmetic: the boundary slope α is irrational, and any integer-invertible linear map respecting the cone is forced to fix that slope, hence to be trivial. The construction extends to higher dimensions by taking products $C \times \mathbb{R}^{N-2}_{\geq 0}$, so non-$(R, G)$-finitely generated cones exist in every dimension $N \geq 2$. We close with the natural classification question, which we leave open.

Question 2.5.2. *Which convex cones $C \subseteq \mathbb{R}^N$ have (R, G)-finitely generated conical semigroups? Can such cones be characterized, at least in dimension 2?*

Substantial progress on this question has been made in recent work of Blekherman, De Loera, Xu, and Zhang [15], where the two-dimensional case is fully resolved. They prove that a pointed cone $C \subseteq \mathbb{R}^2$ with extreme rays $[u_1], [u_2]$ has (R, G)-finitely generated conical semigroup if and only if either both extreme rays are rational, or u_1, u_2 are eigenvectors with positive eigenvalues of a non-identity unimodular matrix $A \in \mathrm{GL}(2, \mathbb{Z})$. They give an analogous characterization for half-spaces. In higher dimensions, they establish a structural necessary condition for nonpolyhedral cones: any nonpolyhedral cone with (R, G)-finitely generated conical semigroup must either have infinitely many rational extreme rays or have all rational extreme rays contained in a proper subspace. A full characterization is still open.

CHAPTER 3

Arithmetic Width

Convex bodies admit several different width measurements, most notably the Euclidean and lattice (or integer) widths. These invariants have proven useful in many areas of mathematics. In integer optimization, lattice width has been instrumental in the development of algorithms, such as Lenstra's algorithm, shortest vector computation, and other lattice algorithms [83, 93]. Moreover, in computer graphics, lattice width is used to describe straightness in digital spaces [56]. In convex geometry, lattice width appears in Borsuk-type partitioning and lattice-based sphere-packing and covering problems [7, 85].

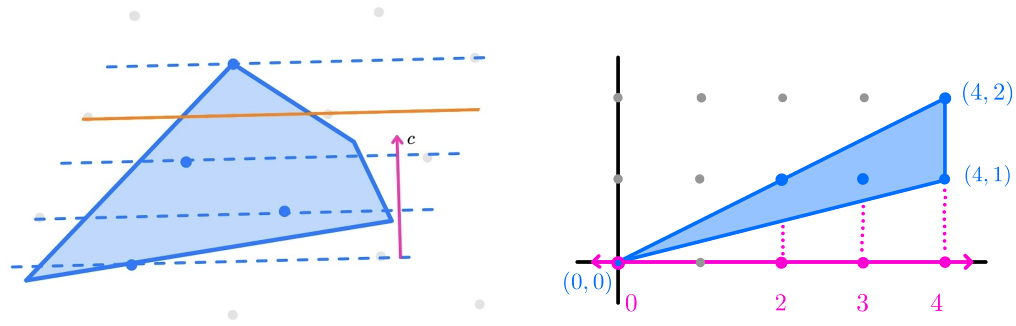
In this chapter, we will present our results from [42] that proposes a new alternative notion of width for convex bodies, called the *arithmetic width*, that seeks to address limitations of lattice width and provides alternative lower bounds for estimation. In order to be self-contained, we will repeat some of the discussion presented in the introduction. Before we introduce our new definition, let us briefly recall established notions of width. The lattice width of a convex body $K \subseteq \mathbb{R}^d$ is

$$w(K) = \min_{c \in \mathbb{Z}^d \setminus \{0\}} w_c(K), \qquad \text{where} \qquad w_c(K) = \max_{x,y \in K} c^T(x-y).$$

Geometrically, the lattice width measures the minimum of the Euclidean distance between two hyperplanes with normal $c \in \mathbb{Z}^d$, scaled by the length $||c||$ of that integer vector. In some sense, the lattice width measures the thinness of the convex body in integer directions. In Figure (3.1a), each of the dashed lines contain a lattice point of the polytope. However, the solid line contains no lattice points. If K "slips through" the integer lattice – i.e., if there are gaps between lattice-supporting hyperplanes that intersect $\mathbb{Z}^d \cap K$ – then $w(K)$ remains blind to those gaps. In contrast, the arithmetic width is a finer invariant than the integer or Euclidean widths as it accounts for these missing lattice points in our polytope in fixed directions.

Definition 3.0.1. *Fix a nonzero* $c \in \mathbb{Z}^d$. *The* hyperplane cover of $K \cap \mathbb{Z}^d$ in direction c *is*

$$h_c(K) = \{H : H \textit{ is a hyperplane with normal } c \textit{ and } H \cap K \cap \mathbb{Z}^d \neq \emptyset\}.$$



(a) (b)

FIGURE 3.1. A convex body K depicted with a hyperplane contributing to lattice width but containing no lattice points in K (left), and the polytope P in Example **??** (right).

The arithmetic width of K in direction c *is* $\mathrm{aw}_c(K) = |h_c(K)|$.

Lattice and arithmetic width satisfy the following inequality:

$$\mathrm{aw}_c(K) = |h_c(K)| \leq w_c(K) + 1.$$

Whenever there are gaps, the arithmetic width and lattice width must differ.

Few results are known on lower bounds for lattice width, which makes arithmetic width a valuable new tool in the study of widths [**76**,**86**]. Moreover, it is clear that $\mathrm{aw}_c(K) = 0$ precisely when there are no lattice points inside K. In contrast, Khintchine's celebrated flatness theorem [**76**] guarantees that for every dimension d there exists a positive constant which upper-bounds the lattice width of convex bodies which have no lattice points inside. The exact value of the so-called *flatness constant* is generally not known, even in dimension $d = 3$ (see [**31**,**98**] and references therein), but is conjectured to be roughly proportional to d.

Lattice and arithmetic widths also differ in ways beyond their sensitivity to empty slices of the convex body. While it is clear that the optimal values of lattice and arithmetic widths can differ, we will see in Example 3.1.2 that even the optimal directions for these notions of width can differ. The distinguishing properties of the arithmetic width and the lattice width are summarized in Table 1.2.

There are other width-adjacent notions with clear connections to the arithmetic width, namely the layer-number and k-level of a lattice polytope. In [**49**], while investigating diameters of graphs of lattice polytopes, Deza and Onn introduced the *layer-number in direction* c as the number of distinct values the linear functional $c^T x$ takes over the vertices of a lattice polytope. They defined the layer-number of P as the minimum over all non-zero directions and showed that there is a constant C that bounds the layer number of any d-dimensional convex polytope by Cd^2. As the layer-number only considers vertices in its count, the layer-number serves as a lower bound for the arithmetic width. Similarly, a lattice polytope P is *k-level* if every facet-defining linear function of P takes at most k distinct values on the vertices of the polytope. Thus, for any k-level polytope, the arithmetic width in facet defining directions is at most k. The importance of k-level polytopes stems from their connections to optimization. It is well-known that if P is k-level, then it admits a spectrahedral lift of polynomial size (for fixed k). Notably, being k-level is used to give efficient semidefinite programming representations for stable set polytopes of perfect graphs [**55**].

A complementary perspective comes from additive combinatorics, via the notion of P-free sets, inspired by the classical Sidon problem of Erdös. For a given convex polyhedron P, one can ask what is the largest subset of integers A such that $P \cap (\mathbb{Z}^d \cap A^d) = \emptyset$? In other words, a subset $A \subseteq \{0, \ldots, n\}$ is called P-free if no lattice point of P has all its coordinates in A. This question generalizes classical questions in additive combinatorics related to Sidon and Salem-Spencer sets [**5**, **102**]. For example, consider the polyhedron $P \subseteq \mathbb{R}^3$ defined by $x_1 + x_3 = 2x_2$ and $x_1, x_2, x_3 \geq 0$. In this case, a set A is P-free if it contains no three-term arithmetic progression. This combinatorial perspective motivates us to study which integer values appear as coordinates, informing possibilities for the P-free sets A. We will discuss this further in Section 3.5

To make the above precise, we introduce the notion of the arithmetic range.

Definition 3.0.2. *Let $K \subseteq \mathbb{R}^d$ be a convex body and let $\ell_c : \mathbb{Z}^d \to \mathbb{Z}$ be a linear functional given by $\ell_c(x) = c^T x$. The* arithmetic range *of K with respect to the direction ℓ_c is*

$$\mathrm{AR}_c(K) = \{n \in \mathbb{Z} : n = \ell_c(x) \text{ for some } x \in K \cap \mathbb{Z}^d\}.$$

See Example 1.1.17 for an example.

We will soon prove (see Proposition 3.1.1(3.1.1)) that

$$\mathrm{aw}_c(K) = |AR_c(K)|.$$

3.1. Arithmetic width: properties and examples

To provide intuition and necessary tools to prove our main results, we collect in this short section several basic properties of arithmetic width and give further examples. These results clarify how arithmetic width behaves under common geometric operations, demonstrate the variety of possible arithmetic ranges, and continue the discussion of the distinction between arithmetic width and lattice width. In all that follows, we denote $[n] = \{1, \ldots, n\} \subseteq \mathbb{Z}_{>0}$.

PROPOSITION 3.1.1. *Let $K \subset \mathbb{R}^d$ be a convex body.*

(a) The arithmetic width $\operatorname{aw}_c(K)$ for a nonzero integer vector c is invariant under integer translations of K. Specifically, if $t \in \mathbb{Z}^d$, then $\operatorname{aw}_c(K) = \operatorname{aw}_c(t + K)$.

(b) Let c_1 and c_2 be nonzero parallel integer vectors. Then, $\operatorname{aw}_{c_1}(K) = \operatorname{aw}_{c_2}(K)$.

(c) For a nonzero integer direction c,

$$\operatorname{aw}_c(K) = |\operatorname{AR}_c(K)| = |h_c(K)|.$$

(d) The maximal arithmetic width of K is $|K \cap \mathbb{Z}^d|$.

PROOF. Fix a nonzero integer vector c. As $|K \cap \mathbb{Z}^d| = |(K+t) \cap \mathbb{Z}^d|$ and $\ell_c(x_1) = \ell_c(x_2)$ if and only if $\ell_c(x_1 + t) = \ell_c(x_2 + t)$ for $x_1, x_2 \in K \cap \mathbb{Z}^d$, we have claim (a):

$$\operatorname{aw}_c(K) = |\operatorname{AR}_c(K)| = |\operatorname{AR}_c(K + t)| = \operatorname{aw}_c(K + t).$$

Now fix two non-zero, parallel, integer vectors c_1 and c_2. This means there is some $\lambda \in \mathbb{Q}_{\neq 0}$ with $c_1 = \lambda c_2$. For $x \in K \cap \mathbb{Z}^d$, as $\ell_{c_1}(x) = \lambda \ell_{c_2}(x)$, we see that $\operatorname{AR}_{c_1}(K) = \lambda \operatorname{AR}_{c_2}(K)$. This gives us claim (b).

We can partition $K \cap \mathbb{Z}^d$ by their images under ℓ_c. Letting $K_j = \{x \in K \cap \mathbb{Z}^d : \ell_c(x) = j\}$, we have that

$$K \cap \mathbb{Z}^d = \bigcup_{j \in \operatorname{AR}_c(K)} K_j.$$

To each K_j, there is a corresponding $H \in h_c(K)$ given by $c^T x = j$. This proves claim (c).

Now, for claim (d), consider the moment curve $g(x) = (1, x, \ldots, x^{d-1})$ and let $n = |K \cap \mathbb{Z}^d|$. For each pair of distinct lattice points $x, y \in K \cap \mathbb{Z}^d$, consider the polynomial given by $f_{x,y}(z) = g(z)^T (x - y)$. For each pair x, y, this polynomial is of degree at most $d-1$ and thus has at most $d-1$ roots. Let Z

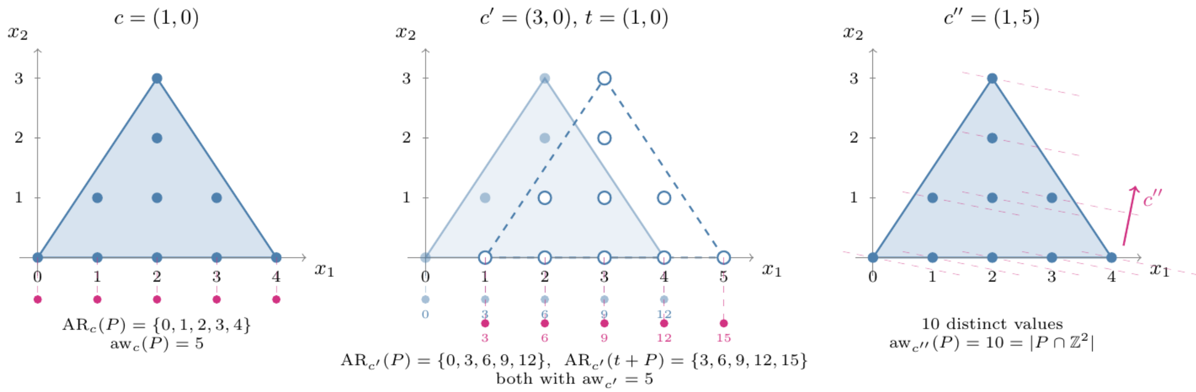


FIGURE 3.2. The polytope $P = \mathrm{conv}((0,0),(4,0),(2,3))$ illustrating Proposition 3.1.1 as discussed in Example 3.1.1.

be the union of the sets of all roots of each possible $f_{x,y}(z)$. Thus, $|Z| \le (d-1)\binom{n}{2}$. Choosing any integer $z \in \{0,1,\dots,(d-1)\binom{n}{2}+1\} \setminus Z$ gives us that $\ell_{g(z)}(x) \ne \ell_{g(z)}(y)$ for all distinct $x, y \in K \cap \mathbb{Z}^d$. Thus, no two lattice points of K map to the same place in the arithmetic range, giving us our final claim. $\square$

EXAMPLE 3.1.1. *Let* $P = \mathrm{conv}((0,0),(4,0),(2,3)) \subset \mathbb{R}^2$*, with* $|P \cap \mathbb{Z}^2| = 10$*, as in Figure 3.2. In direction* $c = (1,0)$*, we have* $\mathrm{AR}_c(P) = \{0,1,2,3,4\}$*, illustrating (c) since the hyperplane cover* $h_c(P)$ *consists of the five vertical lines* $x_1 = 0,1,\dots,4$*, each meeting* $P \cap \mathbb{Z}^2$*. The parallel direction* $c' = (3,0)$ *rescales the arithmetic range to* $\{0,3,6,9,12\}$ *and the translate* $t+P$ *for* $t = (1,0)$ *shifts it to* $\{3,6,9,12,15\}$*, both preserving the size* 5 *and illustrating (b) and (a). Finally, the generic direction* $c'' = (1,5)$ *separates all ten lattice points, taking values* $\{0,1,2,3,4,6,7,8,12,17\}$*, so* $\mathrm{aw}_{c''}(P) = 10$ *achieves the maximum in (d).*

To conclude this section, we provide two examples: the first makes it clear that the arithmetic and lattice widths are truly distinct notions of width; and the second allows us to realize arbitrary finite sets as arithmetic ranges of certain simplices.

EXAMPLE 3.1.2. *Let* $P = \mathrm{conv}((0,0),(1,0),(\frac{3}{5},\frac{14}{5}))$*. Since* $P \cap \mathbb{Z}^2 = \{(0,0),(1,0)\}$*, the optimal arithmetic width is obtained in the directions* $c^* = \pm(0,1)$ *that collapse* $(0,0)$ *and* $(1,0)$*, giving us* $\mathrm{aw}(P) = 1$*. The lattice width in this direction is*

$$w_{\pm(0,1)}(P) = \tfrac{14}{5}.$$

Additionally, for the lattice width, we have that $w(P) = 1$. However, the only directions that obtain the lattice width for P are $\pm(1, 0)$. From this, we can conclude that the directions where the optimal arithmetic width is obtained can differ from the directions where the optimal lattice width is obtained. In particular, the sets where the respective minimal widths are obtained can form disjoint sets.

EXAMPLE 3.1.3. *Sets arising as the images of lattice points under a linear functional appear in several areas of combinatorics and algebra [3, 9, 110]. One such area is in the study of numerical semigroups, that is, sets of the form*

$$S = \langle g_1, \dots, g_k \rangle = \{n \in \mathbb{Z}_{\geq 0} : n = a_1 g_1 + \cdots + a_k g_k,\, a_i \in \mathbb{Z}_{\geq 0} \text{ for } i \in [k]\}.$$

The numerical semigroup polytope of S is

$$P_S = \operatorname{conv}\left(\tfrac{1}{g_1} e_1, \dots, \tfrac{1}{g_k} e_k\right),$$

where e_i is the standard i-th basis vector. The lattice points in nP_S correspond to the factorizations *of n in S; that is, each $(x_1, \dots, x_k) \in nP_S \cap \mathbb{Z}^k$ corresponds to a nonnegative integer solution to $n = g_1 x_1 + \cdots + g_k x_k$. Applying the linear functional $c = (1, \dots, 1)$ to such a lattice point yields its* factorization length, *and as such, $\mathrm{AR}(nP_S)$ coincides with the set of lengths of $n \in S$. As stated in [64, Theorem 3.3], any finite nonempty set $L \subseteq \mathbb{N}_{\geq 2}$ occurs as the set of lengths of some element n of some numerical semigroup S. By translating nP_S appropriately and applying Proposition 3.1.1(3.1.1), we conclude that every finite subset of $\mathbb{Z}$ occurs as the arithmetic range of some rational simplex.*

These examples give us our first main result of this chapter.

THEOREM 3.1.4. *The following hold:*

(a) the directions that obtain the minimum lattice width and the minimum arithmetic width can differ; and

(b) any finite set of integers occurs as the arithmetic range of some rational simplex.

3.2. The arithmetic range of convex bodies

In this section, we prove our first main result: for sufficiently large dilates of convex bodies, the arithmetic range is "almost" an arithmetic progression. We first make this notion precise.

DEFINITION 3.2.1. *We say a finite, nonempty set $S \subset \mathbb{Z}$ is an* almost arithmetic progression *with step size λ, left bound t, and right bound t' if*

$$S = \{m, m+\lambda, \ldots, M-\lambda, M\} \setminus (A \cup A')$$

for some $A \subseteq [m, m+t] \cap (\lambda\mathbb{Z}+m)$ and $A' \subseteq [M-t', M] \cap (\lambda\mathbb{Z}+m)$, where $m = \min(S)$ and $M = \max(S)$. Said another way,

$$(\lambda\mathbb{Z}+m) \supseteq S \supseteq [m+t, M-t'] \cap (\lambda\mathbb{Z}+m).$$

We call

$$\mathrm{gaps}(S) = A \cup A', \qquad \mathrm{gaps}_l(S) = A, \qquad \text{and} \qquad \mathrm{gaps}_r(S) = A'$$

the gaps, left gaps, *and* right gaps *of S, respectively.*

EXAMPLE 3.2.2. *Returning to Example 3.1.3, for $S = \langle 22, 79, 91, 190\rangle$ and $n = 4180$, we have*

$$\mathrm{AR}(nP_S) = \{22\} \cup \{28, 31, 34, \ldots, 172\} \cup \{178, 190\},$$

which is an almost arithmetic progression with step size $\lambda = 3$, left bound $t = 3$, and right bound $t' = 15$. It turns out for any $n \in S$, the arithmetic range $\mathrm{AR}(nP_S)$ is an almost arithmetic progression with identical step size and left and right bounds. This phenomenon is known to occur for any numerical semigroup; see the discussion in Remark 3.3.1.

In what follows, we say $K \subseteq \mathbb{R}^d$ is a convex body if it is a compact, convex set. We do not require that K has a non-empty interior, allowing $\dim(K) < d$. Additionally, let $B_r(c) \subset \mathbb{R}^d$ be the Euclidean ball of radius $r > 0$ centered at $c \in \mathbb{R}^d$.

THEOREM 3.2.3. *Let K be a convex body in $\mathbb{R}^d$ whose affine span contains a lattice point, and let $\ell_c : \mathbb{Z}^d \to \mathbb{Z}$ be a linear functional. For $n \gg 0$, the arithmetic range of nK is an almost arithmetic progression whose step size, left bound, and right bound depend only on K.*

PROOF. Let $m = \min_{x\in K} \ell_c(x)$ and $M = \max_{x\in K} \ell_c(x)$. Let

$$\mathcal{L} = \operatorname{aff}(K) \cap \mathbb{Z}^d \qquad \text{and} \qquad J = K \cap \operatorname{aff}(\mathcal{L}).$$

Since $\operatorname{aff}(K)$ contains a lattice point, by Proposition 3.1.1(3.1.1) we may assume $\operatorname{aff}(K)$ contains the origin, so in particular $\mathcal{L}$ is a sublattice of $\mathbb{Z}^d$. Pick $\lambda \in \mathbb{Z}$ such that $\lambda\mathbb{Z} = \ell_c(\mathcal{L})$. We claim

$$nJ \cap \mathbb{Z}^d = nK \cap \mathbb{Z}^d$$

for all $n \in \mathbb{Z}_{\geq 0}$. The inclusion $nJ \cap \mathbb{Z}^d \subseteq nK \cap \mathbb{Z}^d$ follows immediately from $J \subseteq K$. For the other direction, suppose $z \in nK \cap \mathbb{Z}^d$. Then $z = nx$ for some $x \in K$. As $z \in \operatorname{aff}(K) \cap \mathbb{Z}^d = \mathcal{L}$, we have $z \in \operatorname{aff}(\mathcal{L})$. If $x \notin \operatorname{aff}(\mathcal{L})$, then $nx \notin \operatorname{aff}(\mathcal{L})$, a contradiction. Thus, $x \in \operatorname{aff}(\mathcal{L})$, so $x \in J$ and $z \in nJ$, proving the claimed equality. When considering $nK \cap \mathbb{Z}^d$, we may therefore replace K with J and assume without loss of generality that the affine span of K has the same dimension as the rank of its lattice, that is, $\dim(\operatorname{aff}(K)) = \operatorname{rank}(\operatorname{aff}(K) \cap \mathbb{Z}^d)$.

Without loss of generality, we can assume c is primitive, since if $c = \mu c_0$ for $\mu \in \mathbb{Z}$ and $c_0 \in \mathbb{Z}^d$, then $\operatorname{AR}_c(K) = \mu \operatorname{AR}_{c_0}(K)$ as shown in Proposition 3.1.13.1.1. Let $H = \ker(\ell_c) \cap \operatorname{aff}(K)$. If $H = \operatorname{aff}(K)$, then $\operatorname{AR}_c(nK) \subseteq \{0\}$ for all n, and all desired conclusions immediately follow. As such, we may assume $\dim H = \dim \operatorname{aff}(K) - 1$.

Choose $r > 0$ such that any translate of $B = B_r(0) \cap H$ in H will contain a lattice point. Now, dilate K until K contains a lattice point x such that $\widetilde{B} \cap H \subseteq K$ for $\widetilde{B} = B_r(x) \cap \operatorname{aff}(K)$. Call this dilation factor N. Note that $\dim(B) = \dim(\widetilde{B}) - 1$, and that $\widetilde{B}$ contains a translate of B, namely $\widetilde{B} \cap (H + x)$. Let $p_m, p_M \in K$ attain the minimum value m and maximum values M respectively. Define

$$t := c^T(x - Np_m) \quad \text{and} \quad t' := c^T(Np_M - x)$$

as the lengths of the intervals $[\ell_c(x), \ell_c(Np_m)]$ and $[\ell_c(x), \ell_c(Np_M)]$, respectively. Now, for each n, let $\hat{p}_m(n)$ and $\hat{p}_M(n)$ denote the unique points on the line containing np_m and np_M such that

$$t = \ell_c(\hat{p}_m(n)) - \ell_c(np_m) \quad \text{and} \quad t' = \ell_c(np_M) - \ell_c(\hat{p}_M(n)),$$

i.e., the images of $\hat{p}_m(n)$ and $\hat{p}_M(n)$ are distances t and t' from the images of np_m and np_M, respectively. Note that for $n \gg N$, we have $\hat{p}_m(n), \hat{p}_M(n) \in K$. More precisely, any point on the

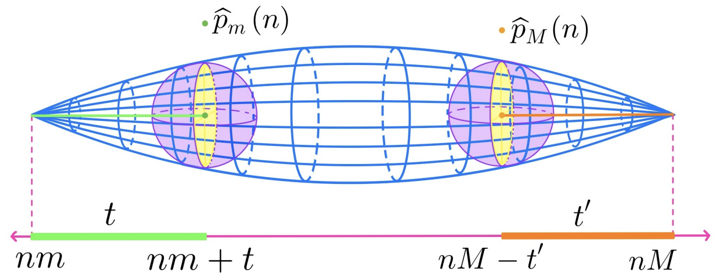


FIGURE 3.3. Illustration of the proof of Theorem 3.2.3.

line containing np_m in direction c can be written as $x_\gamma = np_m + \gamma c$ for $\gamma \in \mathbb{R}$. Writing the desired $\hat{p}_m(n)$ as $\hat{p}_m(n) = np_m + \gamma c$ for some $\gamma \in \mathbb{R}$ gives us that

$$\ell_c(\hat{p}_m(n)) = \ell_c(np_m) + t = \ell_c(np_m + \gamma c) = \ell_c(np_m) + \gamma ||c||^2.$$

Solving for $\gamma = \frac{t}{||c||^2}$, and applying a similar argument for $\hat{p}_M(n)$, gives us that

$$\hat{p}_m(n) = np_m + \frac{t}{||c||^2}c \qquad \text{and} \qquad \hat{p}_M(n) = np_M - \frac{t'}{||c||^2}c.$$

By Bézout's identity, since c is primitive, for any integer j, there exists $x \in \mathbb{Z}^d$ such that $c^T x = j$. Thus, for any $j \in \lambda\mathbb{Z}$ we have $\ell_c^{-1}(j) \cap \mathbb{Z}^d \neq \emptyset$. In particular, for any $j \in [\ell_c(\hat{p}_m(n)), \ell_c(\hat{p}_M(n))] \cap \lambda\mathbb{Z}$, we have that $\ell_c^{-1}(j) \cap \operatorname{aff}(K) = H + w$ for some $w \in \mathcal{L}$. Moreover, since K is convex and $B_r(\hat{p}_m(n)), B_r(\hat{p}_M(n)) \subseteq K$, we have $B_r(z) \cap \operatorname{aff}(K) \subseteq K$ for any $z \in [\hat{p}_m(n), \hat{p}_M(n)]$. Particularly, if we additionally assume $z \in \ell_c^{-1}(j)$, then the ball $B_r(z) \cap \ell_c^{-1}(j) \cap \operatorname{aff}(K)$ is a translate of B in $H + w$. As such, by the choice of r and the fact that $w \in \mathbb{Z}^d$, we see $B_r(z) \cap \ell_c^{-1}(j) \cap \operatorname{aff}(K)$ contains an integer point in nK. Thus, we have found constants t, t', λ dependent only on K such that, for $n \gg 0$, the set $AR_c(nK) \cap [nm + t, nM - t']$ is an arithmetic progression of step size λ. $\square$

3.3. The arithmetic width of rational polytopes

In this section, we will build upon our results from Theorem 3.2.3 for our analysis of the arithmetic width of dilates of convex polytopes. We begin this section with definitions that explore the complement of the arithmetic range: the sets of gaps. From there, we compare gaps across subsequent dilates of polytopes, which gives enough tools to prove Theorems 3.3.2 and 3.3.5. In what follows, we say P is a *rational polytope* if $P = \operatorname{conv}(v_1, \ldots, v_k) \subset \mathbb{R}^d$ where k is finite and each $v_i \in \mathbb{Q}^d$ for

$i \in [k]$. If each $v_i \in \mathbb{Z}^d$, we say that P is *integral*. The *denominator of* P, denoted $\operatorname{denom}(P)$, is the smallest positive dilation factor n such that nP is an integral polytope [117].

3.3.1. Arithmetic width in fixed directions. In the previous section, we found that gaps of the arithmetic range of large dilates of a convex body occur near the extremes, motivating us to examine the behavior of the gaps as we dilate a polytope. Recall that the *vertex tangent cone* at a vertex v of a rational polytope P is the intersection of all halfspaces containing P whose boundaries contain v; see [11].

LEMMA 3.3.0.1. *Let P be a rational polytope in $\mathbb{R}^d$ with denominator D, and fix a linear functional $\ell_c : \mathbb{Z}^d \to \mathbb{Z}$. Then, for any $n \gg 0$ for which $\operatorname{aff}(nP)$ contains a lattice point,*

$$|\operatorname{gaps}(AR_c(nP))| = |\operatorname{gaps}(AR_c((n+D)P))|.$$

PROOF. Let $m = \min_{x \in P} \ell_c(x)$ and $M = \max_{x \in P} \ell_c(x)$. For sufficiently large n, Theorem 3.2.3 provides constants $t, t' > 0$ and step size λ such that

$$\operatorname{AR}_c(nP) \cap [nm + t', nM - t]$$

is a gap-free arithmetic progression of step size λ, and any gaps in $\operatorname{AR}_c(nP)$ may only occur in the regions $[nm, nm + t']$ or $[nM - t, nM]$.

Define the region near the minimum as

$$P_{m,n} = nP \cap \ell_c^{-1}([nm, nm + t']) \subset \mathbb{Z}^d$$

and for $(n + D)P$ as

$$P_{m,n+D} = (n + D)P \cap \ell_c^{-1}([(n + D)m, (n + D)m + t']) \subset \mathbb{Z}^d.$$

Similarly, define the region near the maximum as

$$P_{M,n} = nP \cap \ell_c^{-1}([nM - t, nM]) \subset \mathbb{Z}^d$$

and for $(n + D)P$ as

$$P_{M,n+D} = (n + D)P \cap \ell_c^{-1}([(n + D)M - t, (n + D)M]) \subset \mathbb{Z}^d.$$

Let $p_m \in P$ satisfy $\ell_c(p_m) = m$ and $p_M \in P$ satisfy $\ell_c(p_M) = M$. Note, as we are optimizing a linear functional on a rational polytope, we may take p_m, p_M as vertices of P. In the proof of Proposition 3.1.1(3.1.1), we established that for any integral vector v and convex set $K \subset \mathbb{R}^d$, we have $\mathrm{AR}_c(K+v) = \mathrm{AR}_c(K) + \ell_c(v)$. In particular, since P is a rational polytope, translation by Dp_m or Dp_M will be integer translations. Moreover, letting C_m and C_M denote the vertex tangent cones of P at p_m and p_M, respectively, we have

$$nC_m \cap \ell_c^{-1}([nm, nm+t']) = n(C_m \cap \ell_c^{-1}([m, m+t']))$$

and

$$nC_M \cap \ell_c^{-1}([nM-t, nM]) = n(C_M \cap \ell_c^{-1}([M-t, M])).$$

Since for each $x \in C_m$ and $y \in C_M$, all sufficiently large n have $nx, ny \in nP$, we have

$$\ell_c(P_{m,n+D}) = \ell_c(P_{m,n} + Dp_m) \qquad \text{and} \qquad \ell_c(P_{M,n+D}) = \ell_c(P_{M,n} + Dp_M)$$

for $n \gg 0$. So,

$$\mathrm{AR}_c(P_{m,n+D}) = \mathrm{AR}_c(P_{m,n}) + Dm \qquad \text{and} \qquad \mathrm{AR}_c(P_{M,n+D}) = \mathrm{AR}_c(P_{M,n}) + DM.$$

Thus, we see that

$$\mathrm{gaps}_l(\mathrm{AR}_c((n+D)P)) = \mathrm{gaps}_l(\mathrm{AR}_c(nP)) + Dm \qquad \text{and}$$
$$\mathrm{gaps}_r(\mathrm{AR}_c((n+D)P)) = \mathrm{gaps}_r(\mathrm{AR}_c(nP)) + DM.$$

Since $\mathrm{gaps}(\mathrm{AR}_c(P)) = \mathrm{gaps}_l(\mathrm{AR}_c(P)) \cup \mathrm{gaps}_r(\mathrm{AR}_c(P))$, the proof is now complete. □

EXAMPLE 3.3.1. *Continuing Example 3.2.2, recall that for* $S = \langle 22, 79, 91, 190 \rangle$ *and* $c = (1,1,1,1)$,

$$\mathrm{AR}_c(4180P_S) = \{22\} \cup \{28, 31, 34, \ldots, 172\} \cup \{178, 190\}$$

has step $\lambda = 3$, *with gaps decomposing as*

$$\mathrm{gaps}_l = \{25\}, \qquad \mathrm{gaps}_r = \{175, 181, 184, 187\}$$

relative to the full AP $\{22, 25, 28, \ldots, 187, 190\}$*. The denominator of* P_S *is* $D = \mathrm{lcm}(22, 79, 91, 190)$*, and the extremal values of* c *on* P_S *are* $m = 1/190$ *and* $M = 1/22$*, attained at* $\frac{1}{190}e_4$ *and* $\frac{1}{22}e_1$ *respectively. At the next dilation* $n + D = 4180 + D$ *in the same residue class, the arithmetic range has gap sets*

$$\{25 + D/190\}, \qquad \{175 + D/22,\ 181 + D/22,\ 184 + D/22,\ 187 + D/22\},$$

again with $|\,\mathrm{gaps}\,| = 5$*, illustrating Lemma 3.3.0.1.*

Having proved Lemma 3.3.0.1, we now have the tools to proceed with the proof of Theorem 3.3.2. The proof also identifies the linear coefficient of the resulting quasilinear function.

THEOREM 3.3.2. *Let* P *be a rational polytope in* $\mathbb{R}^d$*. Then, for a fixed direction* $c \in \mathbb{Z}^d$*, the arithmetic width* $\mathrm{aw}_c(nP)$ *is an eventually quasilinear function of* $n \in \mathbb{Z}_{\geq 0}$*.*

PROOF. Let $m = \min_{x \in P} \ell_c(x)$ and $M = \max_{x \in P} \ell_c(x)$. Let λ be the step size given by Theorem 3.2.3. Lastly, let $D = \mathrm{denom}(P)$. We will prove that $\mathrm{aw}_c(nP)$ is eventually quasilinear by proving that

$$\mathrm{aw}_c((n + D)P) = \mathrm{aw}_c(nP) + \tfrac{1}{\lambda} D(M - m) \tag{3.1}$$

for all $n \gg 0$ for which $\mathrm{aff}(nP)$ contains a lattice point. Fix $k \in \{0, 1, \ldots, D-1\}$ for which $\mathrm{aff}(kP)$ contains a lattice point. Fix $t_k \in \mathbb{R}_{\geq 0}$ such that

$$\max \mathrm{AR}_c(kP) = \max_{x \in kP} c^T x - t_k = kM - t_k.$$

Then, for all $n \equiv k \bmod D$ with $n > k$, we have

$$\max \mathrm{AR}_c(nP) = nM - t_k.$$

Similarly, fix $t'_k \in \mathbb{R}_{\geq 0}$ such that for all $n \in \mathbb{Z}_{>0}$ with $n \equiv k \bmod D$,

$$\min \mathrm{AR}_c(nP) = nm + t'_k.$$

As such, if $n \equiv k \bmod D$, then

$$\mathrm{aw}_c(nP) = \tfrac{1}{\lambda}\big((nM - t_k) - (nm + t'_k) + 1\big) - |\,\mathrm{gaps}(\mathrm{AR}_c(nP))|.$$

By an analogous argument, we obtain

$$\mathrm{aw}_c((n+D)P) = \tfrac{1}{\lambda}\big(((n+D)M - t_k) - ((n+D)m + t'_k) + 1\big) - |\operatorname{gaps}(\mathrm{AR}_c((n+D)P))|.$$

Applying Lemma 3.3.0.1, we obtain

$$\mathrm{aw}_c((n+D)P) - \mathrm{aw}_c(nP) = \tfrac{1}{\lambda}D(M-m).$$

This proves equality (3.1), so we conclude $\mathrm{aw}_c(nP)$ is indeed eventually quasilinear in n. $\square$

This theorem has implications in discrete optimization. Integer linear programs (ILPs) are concerned with finding integral solutions to maximizing or minimizing linear functionals over polyhedra. As these problems are often more difficult than their real linear programming counterparts (LPs), to approximate solutions to ILPs, one often first solves the real relaxation and then rounds. The additive integrality gap is a way of measuring the accuracy of this approximation method [52, 73]. Here we present a different construction.

Definition 3.3.3. *Let P be a rational polytope in $\mathbb{R}^d$ and fix linear functional ℓ_c for $c \in \mathbb{Z}^d$. We define the (additive) maximum and minimum integrality gaps as*

$$I_M(P,c) = \max_{x\in P} c^T x - \max_{x \in P\cap\mathbb{Z}^d} c^T x \qquad \textit{and} \qquad I_m(P,c) = \min_{x \in P\cap\mathbb{Z}^d} c^T x - \min_{x\in P} c^T x.$$

Corollary 3.3.1. *Let P be a rational polytope in $\mathbb{R}^d$ and fix linear functional ℓ_c for $c \in \mathbb{Z}^d$. Then, for integers $t_1, t_2 \gg 0$ such that $t_1 \equiv t_2 \bmod D$ we have that*

$$I_M(t_1P,c) = I_M(t_2P,c) \qquad \textit{and} \qquad I_m(t_1P,c) = I_m(t_2P,c).$$

This follows immediately from Theorem 3.3.2, since for each congruence class $t_1 \equiv t_2 \bmod D$, we have that $I_M(t_1P,c) = I_M(t_2P,c) = t_k$ and $I_m(t_1P,c) = I_m(t_2P,c) = t'_k$ where t_k, t'_k are given in the proof of Theorem 3.3.2. Thus, the integrality gap is eventually a periodic sequence (that is, quasi-constant) with period dividing D.

Corollary 3.3.1 is closely related to themes in parametric integer programming. Earlier work by Hosten and Sturmfels [73] and by Eisenbrand and Shmomin [52] studies the maximal additive integrality gap as you vary the data of the integer program, showing that it is always finite and computable in fixed dimension. This is often framed as varying the right-hand side of the constraints, which is equivalent to individually translating the facet-defining hyperplanes of a polytope. Dilating a polytope is one way to vary the constraints of a linear program. Their results establish that, in their more general framework, the additive integrality gap is eventually quasipolynomial.

Remark 3.3.1. *Returning to the setting of Examples 3.1.3 and 3.2.2, one of the cornerstones of factorization theory is the* structure theorem for sets of length*, which states that for certain families of semigroups, the set of factorization lengths of large elements are almost arithmetic sequences [**61**, **62**]. For numerical semigroups specifically, the sets of length of large elements were recently shown in [**90**] to satisfy a periodicity reminiscent of Theorem 3.3.2. In fact, applying Lemma 3.3.0.1, and the main ideas of its proof, to the numerical semigroup polytope P_S from Example 3.1.3 yields an alternative proof of their main result [**90**, Theorem 4.2].*

3.3.2. Arithmetic width in minimizing directions. In order to use Theorem 3.3.2 to prove the same eventually quasilinear behavior of the arithmetic width, we first examine the minimizing directions across varying dilates of our polytope. This allows us to prove our second main result, Theorem 3.3.5.

Lemma 3.3.3.1. *Let $P \subset \mathbb{R}^d$ be a rational polytope with denominator D. If $n_1 \equiv n_2 \bmod D$, then $\mathrm{aw}(n_1P)$ and $\mathrm{aw}(n_2P)$ are obtained in the same directions for $n_1, n_2 \gg 0$.*

Proof. Without loss of generality, assume $n_1 > n_2$ such that $n_1, n_2 \gg 0$, and fix $k \in \mathbb{Z}_{>0}$ such that $n_1 = n_2 + kD$. Then, applying the recurrence relationship in Equation (3.1), we see

$$\mathrm{aw}_c(n_2 + (k+1)D)P = \mathrm{aw}_c(n_2P) + \tfrac{1}{\lambda}D(k+1)(M-m).$$

As we also have that

$$\mathrm{aw}_c((n_1 + D)P) = \mathrm{aw}_c(n_1P) + \tfrac{1}{\lambda}D(M-m),$$

setting these expressions equal gives us that

$$\mathrm{aw}_c(n_1P) - \mathrm{aw}_c(n_2P) = \tfrac{1}{\lambda}kD(M-m). \tag{3.2}$$

Assume $c_* \in \mathbb{Z}^d \setminus \{0\}$ is such that $\mathrm{aw}(n_1P) = \mathrm{aw}_{c_*}(n_1P)$. By way of contradiction, assume $\mathrm{aw}(n_2P) \neq \mathrm{aw}_{c_*}(n_2P)$, so $\mathrm{aw}(n_2P) = \mathrm{aw}_{d_*}(n_2P) < \mathrm{aw}_{c_*}(n_2P)$ for some $d_* \in \mathbb{Z}^d \setminus \{0\}$. However,

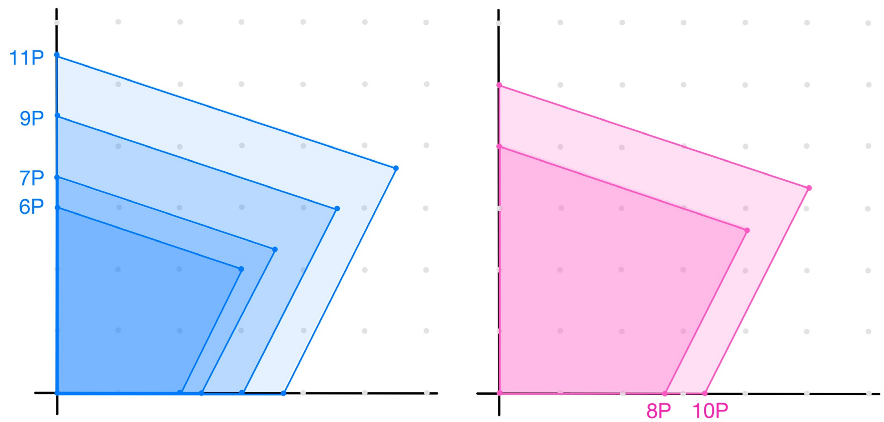


FIGURE 3.4. Dilations of the polytope P from Example 3.3.4, partitioned based on their optimal directions.

adding $\frac{1}{\lambda}kD(M-m)$ to both sides of the inequality and applying Equation (3.2) yields $\mathrm{aw}_{d_*}(n_1P) < \mathrm{aw}_{c_*}(n_1P)$ which is a contradiction. This proves that if $\mathrm{aw}(n_1P) = \mathrm{aw}_{c_*}(n_1P)$, then $\mathrm{aw}(n_2P) = \mathrm{aw}_{c_*}(n_2P)$.

Conversely, assume $c_* \in \mathbb{Z}^d \setminus \{0\}$ is such that $\mathrm{aw}(n_2P) = \mathrm{aw}_{c_*}(n_2P)$. As $n_2 = n_1 - kD$, we rewrite Equation (3.1) as

$$\mathrm{aw}_c(n_2P) = \mathrm{aw}_c(n_1P) - \tfrac{1}{\lambda}kD(M-m).$$

By way of contradiction, assume $\mathrm{aw}(n_1P) \neq \mathrm{aw}_{c_*}(n_1P)$. Thus, there is some $d_* \in \mathbb{Z}^d \setminus \{0\}$ such that $\mathrm{aw}(n_1P) = \mathrm{aw}_{d_*}(n_1P) < \mathrm{aw}_{c_*}(n_1P)$. However, subtracting $\frac{1}{\lambda}kD(M-m)$ from both sides of this inequality yields $\mathrm{aw}_{d_*}(n_2P) < \mathrm{aw}_{c_*}(n_2P)$ which gives us the same contradiction. Therefore, when $n_1 \equiv n_2 \bmod D$, we have that $\mathrm{aw}(n_1P)$ and $\mathrm{aw}(n_2P)$ are obtained in the same directions for $n_1, n_2 \gg 0$. $\square$

EXAMPLE 3.3.4. *Consider the polytope*

$$P = \mathrm{conv}\left((0,0), \left(\tfrac{1}{3}, 0\right), \left(0, \tfrac{1}{2}\right), \left(\tfrac{1}{2}, \tfrac{1}{3}\right)\right).$$

The optimal directions are oscillating periodically. In Figure 3.4, the polytopes given in the right image have arithmetic width minimized in the same directions. Similarly, the polytopes given in the left image have their arithmetic widths minimized in the same directions. More specifically, let

c_n be a direction obtaining the arithmetic width of nP. Then,

$$c_n = \begin{cases} (1,0) \text{ or } (0,1) & \text{for } n \equiv 0,1,3,5 \bmod 6, \\ (0,1) & \text{for } n \equiv 2,4 \bmod 6. \end{cases}$$

As ensured by Lemma 3.3.3.1, when n is restricted to the same residue class modulo 6, the polytopes nP have the same optimal directions.

THEOREM 3.3.5. *Let $P \subset \mathbb{R}^d$ be a rational polytope. The arithmetic width $aw(nP)$ is an eventually quasilinear function of n for $n \in \mathbb{Z}_{\geq 0}$.*

PROOF. Recall, from the proof of Theorem 3.3.2, we have that

$$aw_c((n+D)P) = aw_c(nP) + \tfrac{1}{\lambda}D(M_c - m_c),$$

where $M_c = \max_{x\in P} c^T x$ and $m_c = \min_{x\in P} c^T x$. By Lemma 3.3.3.1, for each equivalence class i modulo the denominator D of P, there is a direction c_i^* on which $aw(nP)$ is attained for all sufficiently large $n \equiv i \bmod D$. Letting $M_i = M_{c_i^*}$ and $m_i = m_{c_i^*}$ for each i for ease of display, this yields, for all $n \gg 0$,

$$\mathrm{aw}(nP) = \begin{cases} \frac{1}{\lambda}(M_0 - m_0)n + a_0 & \text{for } n \equiv 0 \bmod D, \\ \frac{1}{\lambda}(M_1 - m_1)n + a_1 & \text{for } n \equiv 1 \bmod D, \\ \qquad \vdots & \qquad \vdots \\ \frac{1}{\lambda}(M_{D-1} - m_{D-1})n + a_{D-1} & \text{for } n \equiv (D-1) \bmod D, \end{cases}$$

for some $a_0, a_1, \ldots, a_{D-1}$, which proves our claim. □

3.4. Computing arithmetic width: algorithms and complexity

How do we compute the arithmetic width? Here, we will use an algebraic technique wherein we encode lattice points as exponent vectors of monomials, the rational generating functions of the lattice points in a polytope. From there, we will rely on Barvinok's theory for the efficient encoding of the lattice points of polyhedra as short sums of rational functions. For details on the theory and implementations of Barvinok's theorem, see [8, 9, 41]. The results that follow assume a fixed dimension d, and all stated running times are in the input bit-size of the rational polytope. For rational polytopes, we provide a polynomial time algorithm to compute the arithmetic width in fixed direction and a singly-exponential time algorithm to compute the arithmetic width. We will now state the key facts needed for our main results.

Given a rational polyhedron P, the associated generating function of its lattice points is the Laurent series

$$g_P(x) = \sum_{\alpha \in P \cap \mathbb{Z}^d} x^\alpha.$$

Barvinok's theory shows that, in fixed dimension d, this (generally exponential) sum admits a polynomial-size representation as a sum of rational functions of the form

$$g_P(x) = \sum_{i \in I} E_i \frac{x^{u_i}}{\prod\limits_{j=1}^{d} (1 - x^{v_{ij}})}, \tag{3.3}$$

where I is a polynomial-size indexing set, $E_i \in \{1, -1\}$ and $u_i, v_{ij} \in \mathbb{Z}^d$ for all i and j.

The key idea is that Barvinok's compact representation of the lattice points supports efficient computations. For example, substituting $x_i = 1$ for all $i \in [d]$ yields the number of lattice points in P. More generally, the following lemma shows us that such substitutions can be done in polynomial time. This tool will later be used to compute the arithmetic range and arithmetic width.

Lemma 3.4.0.1 ([9, Theorem 2.6]). *Let*

$$g(x) = \sum_{i \in I} \alpha_i \frac{x^{u_i}}{\prod_{j=1}^{k} (1 - x^{v_{ij}})},$$

where $u_i, v_{ij} \in \mathbb{Z}^d$, $\alpha_i \in \mathbb{Q}$, and k is fixed. Given integer vectors $\ell_1, \ldots, \ell_d \in \mathbb{Z}^n$, let $\psi : \mathbb{C}^n \to \mathbb{C}^d$ be the monomial map defined by $z = (z_1, \ldots, z_n) \mapsto (x_1, \ldots, x_d)$ where $x_i = z_1^{\ell_{i1}} z_2^{\ell_{i2}} \ldots z_n^{\ell_{in}}$. Additionally, assume $\psi(\mathbb{C}^n)$ is not contained in the pole set of $g(x)$. Then, $g(\psi(z))$ can be computed in polynomial time (in the input bit size) as a short rational generating function of the same form as $g(z)$.

Having obtained a compact rational generating function for the lattice points of P, the next step is to compute the arithmetic width in a fixed direction is a projection step. This is achieved using the Projection Theorem of Barvinok and Woods [9].

LEMMA 3.4.0.2 ([9, Theorem 1.7]). *Fix the dimension d. Let $P \subset \mathbb{R}^d$ be a rational polytope and let $T : \mathbb{Z}^d \to \mathbb{Z}^k$ be a linear map. Then, there is a polynomial-time algorithm that computes a short rational generating function for $f\big(T(P \cap \mathbb{Z}^d); z\big)$.*

Having gathered the appropriate machinery, we are now prepared to prove that $\mathrm{aw}_c(P)$ can be computed in polynomial time when the dimension is fixed.

THEOREM 3.4.1. *Let $P \subset \mathbb{R}^d$ be a rational polytope and let L be the input bit-size of P. In fixed dimension, given a nonzero integer vector $c \in \mathbb{Z}^d \setminus \{0\}$, there is an algorithm to compute $\mathrm{aw}_c(P)$ that runs in polynomial time in L and the input bit-size of c.*

PROOF. By Barvinok's algorithm, the generating function $g_P(x) = \sum_{\alpha \in P \cap \mathbb{Z}^d} x^\alpha$ can be computed in polynomial time and expressed in the short rational form of Equation (3.3). Applying Lemma 3.4.0.1 to the linear map $\ell_c : \mathbb{Z}^d \to \mathbb{Z}$ defined by $\ell_c(x) = c^T x$, we obtain a univariate rational generating function $h(t)$ whose monomials correspond bijectively to $\mathrm{AR}_c(P)$. Note that h is computed in compact rational form, not as an explicit list of monomials. Finally, the arithmetic width in direction c is the number of distinct monomials in h. By Lemma 3.4.0.2, this quantity can be determined in polynomial time. Evaluating $h(t)$ at $t = 1$ produces the desired count. $\square$

In order to extend the results of Theorem 3.4.1 to the minimum arithmetic width, we first exhibit a finite set of test directions that suffices to check to compute the arithmetic width.

LEMMA 3.4.1.1. *Let $P \subset \mathbb{R}^d$ be a rational polytope. There is a finite set of directions T, computable in single-exponential time in the input bit-size of P, that serves as a sufficient test set to compute $\mathrm{aw}(P)$.*

PROOF. Without loss of generality, we may assume $\dim(P) = d$, and moreover that the affine span of $P \cap \mathbb{Z}^d$ equals $\mathbb{R}^d$, as otherwise the arithmetic width is 1 with respect to any vector perpendicular to this affine span. If c is a direction that minimizes the arithmetic width, then there are at least two distinct lattice points $x, y \in P \cap \mathbb{Z}^d$ such that $\ell_c(x) = \ell_c(y)$, i.e., $c^T(x - y) = 0$. Thus, it suffices to consider directions c that collapse lattice points in P. In fact, we claim there must be at least $d - 1$ such vector pairs whose differences are linearly independent. Indeed, letting

$$A_c = \mathrm{span}\{x - y : x, y \in P \cap \mathbb{Z}^d \text{ and } \ell_c(x) = \ell_c(y)\},$$

any vector c' for which $A_c \subseteq \ker(\ell_{c'})$ will have $\mathrm{aw}_{c'}(P) \leq \mathrm{aw}_c(P)$, and this inequality will be strict whenever $\dim A_{c'} > \dim A_c$. If $\dim(A_c) < d-1$, then since the affine span of $P \cap \mathbb{Z}^d$ equals $\mathbb{R}^d$, we may locate such a c' by ensuring its kernel contains at least one additional difference $x - y \notin A_c$ with $x, y \in P \cap \mathbb{Z}^d$.

As a consequence of the preceding paragraph, to determine T, it suffices to consider directions c that are orthogonal to $d-1$ linearly independent differences of lattice points in P. We may use this to determine T as follows:

1. Compute $N = (P - P) \cap \mathbb{Z}^d$. For rational polytopes, $|N|$ can be computed in polynomial time in fixed dimension using methods such as Barvinok's algorithm. However, the number of lattice points in P, and thus N, can be exponentially large in the bit-length L of the input data, even for fixed d.
2. Enumerate all linearly independent subsets of N of size $d-1$. For each such subset $T' = \{v_1, \dots, v_{d-1}\}$, form the matrix $V = (v_1|\dots|v_{d-1})$.
3. For each such V, compute a primitive integer vector $c \in \ker(V^T)$. Add each c to T. □

THEOREM 3.4.2. *Let $P \subset \mathbb{R}^d$ be a rational polytope with input bit-size L. In fixed dimension, there is a single-exponential time algorithm in L to compute the arithmetic width of P.*

PROOF. Using Lemma 3.4.1.1 to compute T and then apply the algorithm from Theorem 3.4.1 to each $t \in T$ to determine the minimizing direction and value. □

With this, we have proved our third main result.

THEOREM 3.4.3. *Let $P \subset \mathbb{R}^d$ be a rational polytope and let L be the input bit-size of P.*

(a) In fixed dimension, given a nonzero integer vector $c \in \mathbb{Z}^d \setminus \{0\}$, there is an algorithm to compute $\mathrm{aw}_c(P)$ that runs in polynomial time in L and the input bit-size of c.

(b) There is a finite set of directions T, computable in single-exponential time in L, that serve as a sufficient test set to compute $\mathrm{aw}(P)$ (i.e., $\mathrm{aw}(P) = \mathrm{aw}_t(P)$ for some $t \in T$). Thus, in fixed dimension, there is an algorithm to compute the arithmetic width of P that runs in single-exponential time in L.

PROOF OF MAIN THEOREM 3.4.3. Theorems 3.4.1 and 3.4.2 and Lemma 3.4.1.1 prove this claim. □

3.5. Factors for elements of semigroups

As is often the case in combinatorics, we began our exploration of arithmetic width by considering a benign, seemingly unrelated question. *If you consider the set of coordinates that appear in factorizations of an element n in the numerical semigroup S, how big is the largest subset of these that do not form a factorization (when coordinates are allowed to repeat)?* For those with a background in additive combinatorics, this question should feel familiar: it is in the spirit of Sidon sets (where all pairwise sums are distinct), Erdős-type problems, and more broadly the study of solution-free sets, that is, large subsets of integers avoiding additive patterns such as arithmetic progressions [53, 54, 99, 100]. In our setting, we are also looking for large subsets that avoid a specified additive configuration, namely one that assembles into a valid factorization of $n \in S$. This places our problem squarely in the realm of extremal combinatorics. See [111] for a more complete introduction to the field of arithmetic combinatorics.

Definition 3.5.1. *Let S be a numerical semigroup. For $n \in S$, define the **factor set** of n to be*

$$\mathsf{F}_S(n) := \{a_i : (a_1, \ldots, a_k) \in \mathsf{Z}_S(n) \text{ and } 1 \leq i \leq k\},$$

the set of all coordinate values appearing in some factorization of n. When the semigroup S is clear from context, we write $\mathsf{F}(n)$.

In particular, the arithmetic width invariant arose in our examination of this set as

$$\mathsf{F}_S(n) = \bigcup_{i=1}^{k} \mathrm{AR}_{e_i}(nP_S)$$

for the semigroup $S = \langle g_1, \ldots, g_k \rangle$ where e_i is the i-th standard basis vector and P_S is the numerical semigroup polytope.

Example 3.5.2. *Fix the element $n = 97$ in the numerical semigroup $S = \langle 6, 9, 20 \rangle$. Its set of factorizations is*

$$\mathsf{Z}_S(97) = \{(8, 1, 2),\ (5, 3, 2),\ (2, 5, 2)\},$$

*and its set of factors, the coordinates appearing across all factorizations, is $\{1, 2, 3, 5, 8\}$. We now ask which subsets of $\{1, 2, 3, 5, 8\}$ are **non-factorizing**: no selection of values from the subset,* *used as coordinates with repetition allowed, produces a valid factorization of* 97*. A subset* A *is non-factorizing if and only if for every* $(a_1, a_2, a_3) \in \mathsf{Z}_S(n)$*, at least one* a_i *is absent from* A*. Observe that the coordinate* 2 *appears in every factorization of* 97*, so any subset omitting* 2 *is immediately non-factorizing. Among subsets containing* 2*, one checks that* $\{1,2,3\}$ *and* $\{2,3,8\}$ *are non-factorizing: the former omits both* 5 *and* 8*, blocking* $(8,1,2)$ *and* $(5,3,2)$ *and* $(2,5,2)$ *respectively, while the latter omits both* 1 *and* 5*, blocking all three factorizations for the same reason. The complete list of non-factorizing subsets is*

$$\begin{aligned}&\emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{5\},\ \{8\},\\ &\quad\{1,2\},\ \{1,3\},\ \{1,5\},\ \{1,8\},\ \{2,3\},\ \{2,8\},\ \{3,5\},\ \{3,8\},\ \{5,8\},\\ &\quad\{1,2,3\},\ \{1,3,5\},\ \{1,3,8\},\ \{1,5,8\},\ \{2,3,8\},\ \{3,5,8\},\\ &\quad\{1,3,5,8\}.\end{aligned}$$

The three maximal non-factorizing subsets are $\{1,2,3\}$*,* $\{2,3,8\}$*, and* $\{1,3,5,8\}$*.*

A geometrically inclined reader might notice that the non-factorizing subsets form a simplical complex. The collection of non-factorizing subsets of $\mathsf{Z}_S(97)$ is closed under taking subsets: if A is non-factorizing and $B \subseteq A$, then B is non-factorizing as well, since removing elements from A can only reduce the set of factorizations it contains. This is precisely the defining property of a simplicial complex.

Definition 3.5.3. *The* ***factorization avoidance complex*** *of* $n \in S$*, denoted* $\mathsf{BB}_S(n)$*, is the simplicial complex on the ground set* $\mathsf{F}_S(n)$ *whose faces are the non-factorizing subsets of* $\mathsf{F}_S(n)$*. The facets of* $\mathsf{BB}_S(n)$ *are the maximal non-factorizing subsets.*

Note that not every element of $\mathsf{F}_S(n)$ need appear as a vertex: if some factorization (a,a,a) has all coordinates equal, then $\{a\}$ is itself factorizing, and a belongs to the ground set but not to any face of the complex. We refer to such elements as **ghost vertices** [32].

The first natural question to ask here is about the dimension of the simplical complex as $n \in S$ grows. In order to have any hope answering this, we must first understand the size of the factor set grows as $n \to \infty$ as it's the ground set of the complex. Unsurprisingly, we once again present partial results stating that this growth is eventually quasipolynomial in fixed cases and present

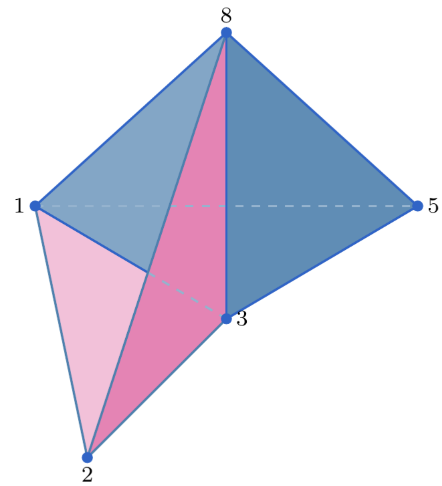


FIGURE 3.5. The factorization avoidance complex $\mathsf{BB}_S(97)$ in Example 3.5.2 has maximal simplices $\{1,2,3\}$, $\{2,3,8\}$, and $\{1,3,5,8\}$.

a conjecture for the more general case. The following proposition, which describes the complete factorization structure of a two-generator semigroup via its unique minimal trade, will be useful in what follows.

PROPOSITION 3.5.1. *Let $S = \langle g_1, g_2\rangle$ with $\gcd(g_1, g_2) = 1$ and $n \in S$. Then there exists a unique $r \in \{0, 1, \ldots, g_2 - 1\}$ with $n \equiv g_1 r \pmod{g_2}$, and the factorizations of n are*

$$\mathsf{Z}(n) = \left\{ \left(r + ig_2,\ \frac{n - g_1(r + ig_2)}{g_2} \right) : i = 0, 1, \ldots, \left\lfloor \frac{n/g_1 - r}{g_2} \right\rfloor \right\},$$

ordered by the unique minimal trade $(-g_2, g_1)$. In particular, $|\mathsf{Z}(n)| = \lfloor (n/g_1 - r)/g_2 \rfloor + 1$.

PROOF. A factorization $(a, b) \in \mathsf{Z}(n)$ satisfies $g_1 a + g_2 b = n$, so $g_1 a \equiv n \pmod{g_2}$. Since $\gcd(g_1, g_2) = 1$, the integer g_1 is invertible mod g_2, and $a \equiv g_1^{-1} n \pmod{g_2}$. Let r be the unique representative of this residue class in $\{0, 1, \ldots, g_2 - 1\}$. Then $a = r + ig_2$ for some $i \geq 0$, and $b = (n - g_1(r + ig_2))/g_2$. The requirement $b \geq 0$ gives $i \leq (n/g_1 - r)/g_2$, so i ranges over $\{0, 1, \ldots, \lfloor (n/g_1 - r)/g_2 \rfloor\}$. Consecutive factorizations in this enumeration differ by $(g_2, -g_1)$ in the first and second coordinates, respectively, which is the unique minimal trade. $\square$

This is essentially the classical method for solving linear Diophantine equations: fixing the residue class of one variable forces the other, and the full solution set is then an arithmetic progression.

Example 3.5.4. *Let* $S = \langle 2, 3\rangle$ *and* $n = 50$*. Since* $\gcd(2,3) = 1$*, we apply Proposition 3.5.1 with* $g_1 = 2$ *and* $g_2 = 3$*. We seek* $r \in \{0, 1, 2\}$ *with* $50 \equiv 2r \pmod 3$*; since* $50 \equiv 2 \pmod 3$*, we have* $r = 1$*. The factorizations are then*

$$\mathsf{Z}(50) = \left\{ \left(1 + 3i,\ \frac{50 - 2(1 + 3i)}{3}\right) : i = 0, 1, \ldots, \left\lfloor \frac{50/2 - 1}{3} \right\rfloor \right\} = \{(1 + 3i,\ 16 - 2i) : i = 0, \ldots, 8\},$$

giving the nine factorizations $(1, 16), (4, 14), (7, 12), (10, 10), (13, 8), (16, 6), (19, 4), (22, 2), (25, 0)$*, each obtained from the previous by the trade* $(-g_2, g_1) = (-3, 2)$*.*

Now we are prepared to look at the growth of the factor set.

Notation 2. *In what follows, let* $v(n) := |\mathsf{F}_S(n)|$*.*

Theorem 3.5.5. *Fix a numerical semigroup semigroup* $S = \langle g_1, g_2\rangle$*. For* $n \gg 0$*,*

$$v(n + g_1 g_2^2) = v(n) + (2g_2 - 1).$$

Proof. By Proposition 3.5.1, we can order the factorizations of n as $(a_1, b_1), \ldots, (a_k, b_k)$ in decreasing order of first coordinate, so $a_{i+1} = a_i - g_2$ and $b_{i+1} = b_i + g_1$. Applying Proposition 3.5.1 to $n + g_1 g_2^2$ gives a chain of $k + g_2$ factorizations, which we denote $(a'_1, b'_1), \ldots, (a'_{k+g_2}, b'_{k+g_2})$, with $a'_i = a_1 + g_2^2 - (i - 1)g_2$ and $b'_i = b_1 + (i - 1)g_1$. We call a factor in $\mathsf{F}(n + g_1 g_2^2)$ *new* if it does not appear in $\mathsf{F}(n)$. For $n \geq g_1^2 g_2^2/(g_2 - g_1)$, we have $k > g_2$, so the following partition of $\mathsf{Z}(n + g_1 g_2^2)$ into three blocks is well defined.

To begin, we observe that $\mathsf{F}(n) \subseteq \mathsf{F}(n + g_1 g_2^2)$. Indeed, for any $(a_i, b_i) \in \mathsf{Z}(n)$, both $(a_i + g_2^2, b_i)$ and $(a_i, b_i + g_1 g_2)$ are factorizations of $n + g_1 g_2^2$. The former preserves b_i and the latter preserves a_i, so every element of $\mathsf{F}(n)$ appears in $\mathsf{F}(n + g_1 g_2^2)$.

Next, partition $\mathsf{Z}(n + g_1 g_2^2)$ into three blocks and count the new factors in each:

(i) Block 1: the first g_2 factorizations $(a'_1, b'_1), \ldots, (a'_{g_2}, b'_{g_2})$, each obtained from a factorization of n by adding $(g_2^2, 0)$;

(ii) Block 2: the middle $k - g_2$ factorizations $(a'_{g_2+1}, b'_{g_2+1}), \ldots, (a'_k, b'_k)$, each obtainable from a factorization of n by adding *either* $(g_2^2, 0)$ or $(0, g_1 g_2)$;

(iii) Block 3: the last g_2 factorizations $(a'_{k+1}, b'_{k+1}), \ldots, (a'_{k+g_2}, b'_{k+g_2})$, each obtained from a factorization of n by adding $(0, g_1 g_2)$.

For block 1, we claim that each of the g_2 factorizations contributes exactly one new factor. For $1 \le i \le g_2$, the i-th factorization satisfies $(a_i', b_i') = (a_i, b_i) + (g_2^2, 0)$, so the second coordinate $b_i' = b_i$ already belongs to $\mathsf{F}(n)$, and only a_i' can be new. Since the smallest value among $a_1', \ldots, a_{g_2}'$ is $a_1 + g_2 > a_1 = \lfloor n/g_1 \rfloor$, each exceeds the largest first coordinate of $\mathsf{Z}(n)$. Moreover, $b_k \le \lfloor n/g_2 \rfloor < a_1 + g_2$ for $n \ge g_1^2 g_2^2/(g_2 - g_1)$, so these values do not appear as second coordinates of $\mathsf{Z}(n)$ either. Thus block 1 contributes g_2 new factors.

For block 2, we claim that no factorization contributes a new factor. Indeed, for $g_2 < i \le k$, the i-th factorization admits two representations:

$$(a_i', b_i') = (a_i, b_i) + (g_2^2, 0) = (a_{i-g_2}, b_{i-g_2}) + (0, g_1 g_2).$$

The first shows $b_i' = b_i \in \mathsf{F}(n)$ and the second shows $a_i' = a_{i-g_2} \in \mathsf{F}(n)$, so neither coordinate is new. Thus block 2 contributes no new factors.

For block 3, we claim that exactly $g_2 - 1$ of the g_2 factorizations contribute a new factor. For $k < i \le k + g_2$, we have $(a_i', b_i') = (a_{i-g_2}, b_{i-g_2}) + (0, g_1 g_2)$, so $a_i' = a_{i-g_2} \in \mathsf{F}(n)$ and only the second coordinate b_i' can be new. These second coordinates are $b_k + g_1, b_k + 2g_1, \ldots, b_k + g_2 g_1$, which represent all residue classes mod g_2 since $\gcd(g_1, g_2) = 1$. Since the first coordinates of $\mathsf{Z}(n)$ are all congruent to $a_1 \pmod{g_2}$, exactly one of these second coordinates, say $b_k + jg_1$, satisfies $b_k + jg_1 \equiv a_1 \pmod{g_2}$.

It remains to show that $b_k + jg_1$ already appears in $\mathsf{F}(n)$. Since $a_k < g_2$ and $b_k = (n - g_1 a_k)/g_2$,

$$b_k + jg_1 \le \frac{n}{g_2} + g_1 g_2 \le \frac{n}{g_1} = a_1$$

for $n \ge g_1^2 g_2^2/(g_2 - g_1)$, so $b_k + jg_1$ lies in the arithmetic progression $a_1, a_1 - g_2, \ldots, a_k$ and is therefore already an element of $\mathsf{F}(n)$. The remaining $g_2 - 1$ second coordinates are not congruent to $a_1 \pmod{g_2}$, so they cannot appear as first coordinates of $\mathsf{Z}(n)$, and they each exceed b_k, so they do not appear as second coordinates either. Thus block 3 contributes $g_2 - 1$ new factors.

Combining the counts from all three blocks gives

$$v(n + g_1 g_2^2) = v(n) + g_2 + (g_2 - 1) = v(n) + (2g_2 - 1). \qquad \square$$

EXAMPLE 3.5.6. *Let $S = \langle 2, 3 \rangle$ and $n = 50$ so $n + g_1 g_2^2 = 68$. The top row is $\mathsf{Z}(50)$ and the bottom row is $\mathsf{Z}(68)$, with a blue E_1 edge from f to $f + (g_2^2, 0)$ and a pink E_2 edge from f to $f + (0, g_1 g_2)$.*

Block 1 vertices receive only a blue edge, Block 3 vertices only a pink edge, and Block 2 vertices receive one of each and contribute no new factors. New factors are highlighted; Block 1 contributes $g_2 = 3$ *and Block 3 contributes* $g_2 - 1 = 2$.

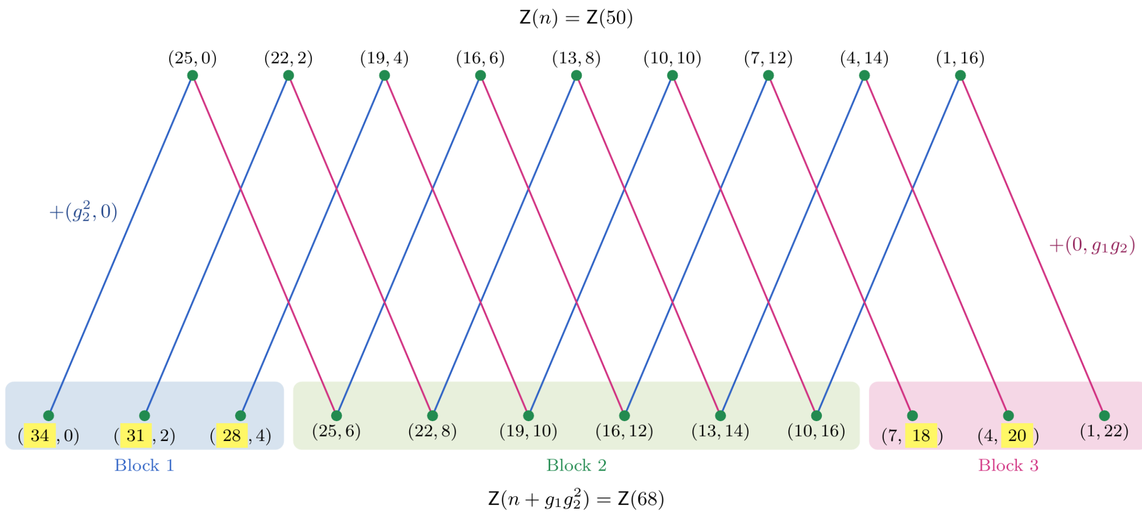


FIGURE 3.6. The edge structure of $\mathsf{Z}(50)$ and $\mathsf{Z}(68)$ in $S = \langle 2, 3\rangle$, illustrating the proof of Theorem 3.5.5.

Once we move into the case with three generators, we require additional constraints and care about pairwise GCDs.

THEOREM 3.5.7. *Fix a semigroup* $S = \langle g_1, g_2, g_3\rangle$ *such that* $\gcd(g_2, g_3) = 1$. *Then, for* $n \gg 0$,

$$v(n + g_1) = v(n) + 1.$$

PROOF. Let $F_{23} = F(\langle g_2, g_3\rangle) = g_2g_3 - g_2 - g_3$ denote the Frobenius number of $\langle g_2, g_3\rangle$, and define

$$A_n = \left\lfloor \frac{n - F_{23}}{g_1} \right\rfloor.$$

We call a factor in $\mathsf{F}(n + g_1)$ *new* if it does not appear in $\mathsf{F}(n)$.

To begin, we observe that $\mathsf{F}(n)+1 \subseteq \mathsf{F}(n+g_1)$. Indeed, if $(a, b, c) \in \mathsf{Z}(n)$, then $(a+1, b, c) \in \mathsf{Z}(n+g_1)$, so every factor of n gives rise to the factor one larger in $\mathsf{F}(n + g_1)$.

Next, we show that every integer $0 \le a \le A_n$ belongs to $\mathsf{F}(n)$. If a satisfies $n - g_1a > F_{23}$, then $n - g_1a$ lies in $\langle g_2, g_3\rangle$ since $\gcd(g_2, g_3) = 1$. Hence there exist $b, c \ge 0$ with $n - g_1a = g_2b + g_3c$, so $(a,b,c) \in \mathsf{Z}(n)$ and $a \in \mathsf{F}(n)$. By definition of A_n, the condition $n - g_1 a > F_{23}$ holds for all $0 \le a \le A_n$.

We now claim that for $n \gg 0$, no new factors arise from the second or third coordinates. Any $(a,b,c) \in \mathsf{Z}(n+g_1)$ satisfies $g_2 b \le n + g_1$ and $g_3 c \le n + g_1$, so since $g_2 \le g_3$,

$$b,\, c \le \left\lfloor \frac{n+g_1}{g_2} \right\rfloor .$$

Since $g_1 < g_2$, for $n \gg 0$ we have

$$\left\lfloor \frac{n+g_1}{g_2} \right\rfloor \le A_n,$$

and since every integer between 0 and A_n already lies in $\mathsf{F}(n)$, every second and third coordinate of every factorization of $n + g_1$ is already a factor of n. Thus any new factor must occur as a first coordinate.

It remains to show that exactly one new first coordinate appears. We have

$$A_{n+g_1} = \left\lfloor \frac{n + g_1 - F_{23}}{g_1} \right\rfloor = A_n + 1,$$

so $A_n + 1 \in \mathsf{F}(n+g_1)$ by the second observation above. Since $A_n + 1 \notin \mathsf{F}(n)$, this is a new factor. To see that it is the only new factor, we show that no first coordinate larger than $A_n + 1$ is new. Suppose $a > A_n + 1 = A_{n+g_1}$ is a first coordinate of some factorization of $n + g_1$. Then $n + g_1 - g_1 a \le F_{23}$, so $n + g_1 - g_1 a \notin \langle g_2, g_3 \rangle$ in general, meaning a need not be a factor of $n + g_1$ at all. More precisely, if a is a gap of $\mathsf{F}(n+g_1)$, then $a > A_{n+g_1} = A_n + 1$, so $a - 1 > A_n$, which means $a - 1$ is also a gap of $\mathsf{F}(n)$. Thus no new gaps are introduced, and the only change between $\mathsf{F}(n)$ and $\mathsf{F}(n+g_1)$ in the first coordinate is the addition of $A_n + 1$. We conclude that

$$v(n+g_1) = v(n) + 1$$

for all sufficiently large n. $\square$

For the remaining cases, where $\gcd(g_2, g_3) > 1$, the situation is more subtle. Computational evidence suggests an analogous quasipolynomial growth pattern, with period and increment determined by the gcd structure of the generators.

Conjecture 1. *Fix a semigroup* $S = \langle g_1, g_2, g_3 \rangle$ *such that* $\gcd(g_1, g_2) = \gcd(g_1, g_3) = 1$ *and* $\gcd(g_2, g_3) = d > 1$. *Then for* $n \gg 0$,

$$v(n + g_1g_2g_3d) = v(n) + g_1g_3(d-1) + g_2g_3.$$

A proof of this conjecture would proceed via slice decomposition of $\mathsf{Z}_S(n)$ by the third coordinate: each c-slice is a factorization set in the two-generator semigroup $\langle g_1, g_2 \rangle$ at level $n - g_3c$, and the shift $g_1g_2g_3d$ introduces g_1g_2d new slices whose contribution to $\mathsf{F}_S(n + g_1g_2g_3d) \setminus \mathsf{F}_S(n)$ can in principle be tracked via Theorem 3.5.5. The combinatorics of overlap between these new slices remains an obstacle.

The general case, where the remaining pairwise gcds may also exceed 1, appears to follow a similar slice-based pattern but with a more intricate dependence on the full gcd structure. We leave this as an open problem.

Open Problem 3.5.8. *Given any numerical semigroup* $S = \langle g_1, \ldots, g_k \rangle$, *determine the eventual linear recurrence describing the growth of* $|\mathsf{F}_S(n)|$ *as* $n \to \infty$.

Bibliography

[1] I. Aliev, M. Henk, M. Hogan, S. Kuhlmann, and T. Oertel, *New bounds for the integer Carathéodory rank*, SIAM J. Optim., 34 (2024), pp. 190–200.

[2] A. Assi and P. A. García-Sánchez, *Numerical semigroups and applications*, vol. 1 of RSME Springer Series, Springer, [Cham], 2016.

[3] E. Bajo, R. Davis, J. A. De Loera, A. Garber, S. Garzón Mora, K. Jochemko, and J. Yu, *Weighted Ehrhart theory: Extending Stanley's nonnegativity theorem*, Advances in Mathematics, 444 (2024), p. 109627.

[4] V. Baldoni, N. Berline, J. A. De Loera, B. E. Dutra, M. Köppe, and M. Vergne, *Coefficients of Sylvester's denumerant*, Integers, 15 (2015), pp. Paper No. A11, 32.

[5] J. Balogh, Z. Füredi, and S. Roy, *An upper bound on the size of Sidon sets*, The American Mathematical Monthly, 130 (2023), pp. 437–445.

[6] F. J. M. Barning, *On Pythagorean and quasi-Pythagorean triangles and a generation process with the help of unimodular matrices*, Math. Centrum Amsterdam Afd. Zuivere Wisk., 1963 (1963), p. 37.

[7] A. Barvinok, *A course in convexity*, vol. 54 of Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 2002.

[8] A. Barvinok and J. E. Pommersheim, *An algorithmic theory of lattice points in polyhedra*, in New perspectives in algebraic combinatorics (Berkeley, CA, 1996–97), vol. 38 of Math. Sci. Res. Inst. Publ., Cambridge Univ. Press, Cambridge, 1999, pp. 91–147.

[9] A. Barvinok and K. Woods, *Short rational generating functions for lattice point problems*, J. Amer. Math. Soc., 16 (2003), pp. 957–979.

[10] M. Beck, S. Elia, and S. Rehberg, *Rational Ehrhart theory*, Integers, 23 (2023), pp. Paper No. A60, 31.

[11] M. Beck, C. Haase, and F. Sottile, *Formulas of Brion, Lawrence, and Varchenko on rational generating functions for cones*, Math. Intelligencer, 31 (2009), pp. 9–17.

[12] M. Beck and S. Robins, *Computing the continuous discretely*, Undergraduate Texts in Mathematics, Springer, New York, 2007. Integer-point enumeration in polyhedra.

[13] A. Ben-Tal and A. Nemirovski, *Lectures on modern convex optimization*, MPS/SIAM Series on Optimization, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA; Mathematical Programming Society (MPS), Philadelphia, PA, 2001. Analysis, algorithms, and engineering applications.

[14] H. Bennett, *The complexity of the shortest vector problem*, SIGACT News, 54 (2023), pp. 37–61.

[15] G. Blekherman, J. A. De Loera, L. Xu, and S. Zhang, *Semigroups of integer points in convex cones*, 2025.

[16] S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan, *Linear matrix inequalities in system and control theory*, vol. 15 of SIAM Stud. Appl. Math., SIAM, Philadelphia, PA, 1994.

[17] W. Bruns, *On the integral Carathéodory property*, Experiment. Math., 16 (2007), pp. 359–365.

[18] W. Bruns and J. Gubeladze, *Polytopes, rings, and K-theory*, Springer Monographs in Mathematics, Springer, Dordrecht, 2009.

[19] W. Bruns, J. Gubeladze, M. Henk, A. Martin, and R. Weismantel, *A counterexample to an integer analogue of Carathéodory's theorem*, J. Reine Angew. Math., 510 (1999), pp. 179–185.

[20] W. Bruns, J. Gubeladze, and N. V. Trung, *Problems and algorithms for affine semigroups*, Semigroup Forum, 64 (2002), pp. 180–212.

[21] W. Bruns and B. Ichim, *On the coefficients of Hilbert quasipolynomials*, Proc. Amer. Math. Soc., 135 (2007), pp. 1305–1308.

[22] M. Caboara and C. Mascia, *A partial characterization of Hilbert quasi-polynomials in the non-standard case*, J. Symbolic Comput., 99 (2020), pp. 165–190.

[23] D. Cass and P. J. Arpaia, *Matrix generation of Pythagorean n-tuples*, Proc. Amer. Math. Soc., 109 (1990), pp. 1–7.

[24] J. W. S. Cassels, *Rational quadratic forms*, vol. 13 of London Mathematical Society Monographs, Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978.

[25] S. T. Chapman, E. B. Dugan, S. Gaskari, E. Lycan, S. Mendoza, C. O'Neill, and V. Ponomarenko, *Some asymptotic results on p-lengths of factorizations for numerical semigroups and arithmetical congruence monoids*, Houston J. Math., 50 (2025). to appear.

[26] S. T. Chapman, R. Garcia, and C. O'Neill, *Beyond coins, stamps, and Chicken McNuggets: an invitation to numerical semigroups*, in A Project-Based Guide to Undergraduate Research in Mathematics, P. Harris, E. Insko, and A. Wootton, eds., Foundations of Undergraduate Research in Mathematics, Birkhäuser, Cham, 2020.

[27] S. T. Chapman, P. A. García-Sánchez, D. Llena, V. Ponomarenko, and J. C. Rosales, *The catenary and tame degree in finitely generated commutative cancellative monoids*, Manuscripta Math., 120 (2006), pp. 253–264.

[28] A. Charnes, W. W. Cooper, and K. Kortanek, *Duality in semi-infinite programs and some works of Haar and Carathéodory*, Management Sci., 9 (1962/63), pp. 209–228.

[29] E. Charrier, L. Buzer, and F. Feschet, *Efficient lattice width computation in arbitrary dimension*, in Discrete Geometry for Computer Imagery. DGCI 2009, S. Brlek, C. Reutenauer, and X. Provençal, eds., vol. 5810 of Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2009, pp. 91–102.

[30] S. Chen, N. Li, and S. V. Sam, *Generalized Ehrhart polynomials*, Trans. Amer. Math. Soc., 364 (2012), pp. 551–569.

[31] G. Codenotti, T. Hall, and J. Hofscheier, *Generalised flatness constants: A framework applied in dimension* 2, 2021.

[32] P. Conceição, *The homotopy type of the moment-angle complex associated to the complex of injective words*, 2026.

[33] K. Conrad, *Pythagorean descent*. Expository note, available at https://kconrad.math.uconn.edu/blurbs/linmultialg/descentPythag.pdf. Accessed: 2026-05-03.

[34] ———, *Pythagorean triples*. Expository note, available at https://kconrad.math.uconn.edu/blurbs/ugradnumthy/pythagtriple.pdf. Accessed: 2026-05-03.

[35] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, vol. 290 of Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, New York, third ed., 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[36] W. Cook, J. Fonlupt, and A. Schrijver, *An integer analogue of Carathéodory's theorem*, J. Combin. Theory Ser. B, 40 (1986), pp. 63–70.

[37] H. Dao, E. Miller, J. Montaño, C. O'Neill, and K. Woods, *Quasipolynomial behavior via constructibility in multigraded algebra*, 2025.

[38] M. K. de Carli Silva and L. Tun¸cel, *A notion of total dual integrality for convex, semidefinite, and extended formulations*, SIAM J. Discrete Math., 34 (2020), pp. 470–496.

[39] E. de Klerk and F. Vallentin, *On the Turing model complexity of interior point methods for semidefinite programming*, SIAM Journal on Optimization, 26 (2016), pp. 1944–1961.

[40] J. A. De Loera, R. Hemmecke, and M. Köppe, *Algebraic and geometric ideas in the theory of discrete optimization*, vol. 14 of MOS-SIAM Series on Optimization, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA; Mathematical Optimization Society, Philadelphia, PA, 2013.

[41] J. A. De Loera, R. Hemmecke, J. Tauzer, and R. Yoshida, *Effective lattice point counting in rational convex polytopes*, Journal of Symbolic Computation, 38 (2004), pp. 1273–1302. Symbolic Computation in Algebra and Geometry.

[42] J. A. De Loera, B. Marsters, and C. O'Neill, *An arithmetic measure of width for convex bodies*, 2025. To appear, Beiträge zur Algebra und Geometrie.

[43] J. A. De Loera, B. Marsters, L. Xu, and S. Zhang, *Integer points in arbitrary convex cones: The case of the psd and soc cones*, in Integer Programming and Combinatorial Optimization, J. Vygen and J. Byrka, eds., Cham, 2024, Springer Nature Switzerland, pp. 99–112.

[44] J. A. De Loera, J. Rambau, and F. Santos, *Triangulations*, vol. 25 of Algorithms and Computation in Mathematics, Springer-Verlag, Berlin, 2010. Structures for algorithms and applications.

[45] J. A. De Loera and B. Sturmfels, *Algebraic unimodular counting*, Math. Program., 96 (2003), pp. 183–203.

[46] F. de Meijer and R. Sotirov, *On integrality in semidefinite programming for discrete optimization*, SIAM J. Optim., 34 (2024), pp. 1071–1096.

[47] ———, *The Chvátal-Gomory procedure for integer SDPs with applications in combinatorial optimization*, Math. Program., 209 (2025), pp. 323–395.

[48] S. S. Dey and D. A. Morán R., *Some properties of convex hulls of integer points contained in general convex sets*, Math. Program., 141 (2013), pp. 507–526.

[49] M. Deza and S. Onn, *Lattice-free polytopes and their diameter*, Discrete & Computational Geometry, 13 (1995), pp. 59–76.

[50] L. E. Dickson, *History of the theory of numbers. Vol. II: Diophantine analysis*, Chelsea Publishing Co., New York, 1966.

[51] J. Edmonds and R. Giles, *Total dual integrality of linear inequality systems*, in Progress in combinatorial optimization (Waterloo, Ont., 1982), Academic Press, Toronto, ON, 1984, pp. 117–129.

[52] F. Eisenbrand and G. Shmonin, *Parametric integer programming in fixed dimension*, Math. Oper. Res., 33 (2008), pp. 839–850.

[53] P. Erd˝ os, *Some problems in number theory, combinatorics and combinatorial geometry*, Math. Pannon., 5 (1994), pp. 261–269.

[54] P. Erdös and P. Turán, *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc., 16 (1941), pp. 212–215.

[55] H. Fawzi, J. ao Gouveia, P. A. Parrilo, J. Saunderson, and R. R. Thomas, *Lifting for simplicity: Concise descriptions of convex sets*, Foundations of Computational Mathematics, 15 (2015), pp. 119–153.

[56] F. Feschet, *The lattice width and quasi-straightness in digital spaces*, in 19th International Conference on Pattern Recognition (ICPR 2008), December 8-11, 2008, Tampa, Florida, USA, IEEE Computer Society, 2008, pp. 1–4.

[57] V. E. Firstov, *A special matrix transformation semigroup of primitive pairs and the genealogy of Pythagorean triples*, Mat. Zametki, 84 (2008), pp. 281–299.

[58] J. I. García-García, M. Omar, C. O'Neill, and S. Yih, *Factorization length distribution for affine semigroups II: asymptotic behavior for numerical semigroups with arbitrarily many generators*, J. Combin. Theory Ser. A, 178 (2021), pp. Paper No. 105358, 34.

[59] P. A. García-Sánchez, I. Ojeda, and J. C. Rosales, *Affine semigroups having a unique Betti element*, J. Algebra Appl., 12 (2013), pp. 1250177, 11.

[60] P. A. García-Sánchez, C. O'Neill, and G. Webb, *The computation of factorization invariants for affine semigroups*, Journal of Algebra and its Applications, 18 (2019), pp. 1950019, 21 pp.

[61] A. Geroldinger, *A structure theorem for sets of lengths*, Colloq. Math., 78 (1998), pp. 225–259.

[62] ———, *Sets of lengths*, Amer. Math. Monthly, 123 (2016), pp. 960–988.

[63] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations*, vol. 278 of Pure and Applied Mathematics (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006. Algebraic, combinatorial and analytic theory.

[64] A. Geroldinger and W. A. Schmid, *A realization theorem for sets of lengths in numerical monoids*, Forum Math., 30 (2018), pp. 1111–1118.

[65] F. R. Giles and W. R. Pulleyblank, *Total dual integrality and integer polyhedra*, Linear Algebra Appl., 25 (1979), pp. 191–196.

[66] F. R. Giles and W. R. Pulleyblank, *Total dual integrality and integer polyhedra*, Linear Algebra Appl., 25 (1979), pp. 191–196.

[67] M. X. Goemans, *Semidefinite programming in combinatorial optimization*, Math. Programming, 79 (1997), pp. 143–161. Lectures on mathematical programming (ismp97) (Lausanne, 1997).

[68] M. X. Goemans and D. P. Williamson, *Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming*, J. ACM, 42 (1995), pp. 1115–1145.

[69] A. Hall, *232. Genealogy of Pythagorean triads*, The Mathematical Gazette, 54 (1970), pp. 377–379.

[70] L. G. Ha ˇ cijan, *A polynomial algorithm in linear programming*, Dokl. Akad. Nauk SSSR, 244 (1979), pp. 1093–1096.

[71] R. Hemmecke and R. Weismantel, *Representation of sets of lattice points*, SIAM J. Optim., 18 (2007), pp. 133–137.

[72] J. Herzog, S. Moradi, and M. Rahimbeigi, *Numerical Semigroups: A Commutative Algebra Approach*, Compact Textbooks in Mathematics, Birkhäuser, Cham, 2026.

[73] S. Ho¸sten and B. Sturmfels, *Computing the integer programming gap*, Combinatorica, 27 (2007), pp. 367–382.

[74] R. G. Jeroslow, *Some basis theorems for integral monoids*, Math. Oper. Res., 3 (1978), pp. 145–154.

[75] K. Kaveh and A. G. Khovanskii, *Newton-Okounkov bodies, semigroups of integral points, graded algebras and intersection theory*, Ann. of Math. (2), 176 (2012), pp. 925–978.

[76] A. Khintchine, *A quantitative formulation of Kronecker's theory of approximation*, Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya, 12 (1948), pp. 113–122.

[77] N. U. Kiran, *An algebraic approach to q-partial fractions and Sylvester denumerants*, Ramanujan J., 59 (2022), pp. 671–712.

[78] V. L. Klee, Jr., *Extremal structure of convex sets*, Arch. Math. (Basel), 8 (1957), pp. 234–240.

[79] C. Ko, *On a Waring's Problem with Squares of Linear Forms*, Proc. London Math. Soc. (2), 42 (1936), pp. 171–185.

[80] A. Korkine and G. Zolotareff, *Sur les formes quadratiques*, Math. Ann., 6 (1873), pp. 366–389.

[81] S. Kuhlmann, *Integer Carathéodory results with bounded multiplicity*, Beitr. Algebra Geom., 66 (2025), pp. 275–292.

[82] J. B. Lasserre, *Global optimization with polynomials and the problem of moments*, SIAM J. Optim., 11 (2001), pp. 796–817.

[83] H. W. Lenstra, Jr., *Integer programming with a fixed number of variables*, Math. Oper. Res., 8 (1983), pp. 538–548.

[84] A. N. Letchford and M. M. Sø rensen, *Binary positive semidefinite matrices and associated integer polytopes*, Math. Program., 131 (2012), pp. 253–271.

[85] L. Lovász, *Geometry of numbers and integer programming*, in Mathematical programming (Tokyo, 1988), vol. 6 of Math. Appl. (Japanese Ser.), SCIPRESS, Tokyo, 1989, pp. 177–201.

[86] L. Mayrhofer, J. Schade, and S. Weltge, *Lattice-free simplices with lattice width 2d - o(d)*, in Integer Programming and Combinatorial Optimization - 23rd International Conference, IPCO 2022, Eindhoven, The Netherlands, June 27-29, 2022, Proceedings, K. I. Aardal and L. Sanità, eds., vol. 13265 of Lecture Notes in Computer Science, Springer, 2022, pp. 375–386.

[87] D. Micciancio and S. Goldwasser, *Complexity of lattice problems*, vol. 671 of The Kluwer International Series in Engineering and Computer Science, Kluwer Academic Publishers, Boston, MA, 2002. A cryptographic perspective.

[88] E. Miller and B. Sturmfels, *Combinatorial commutative algebra*, vol. 227 of Graduate Texts in Mathematics, Springer-Verlag, New York, 2005.

[89] L. J. Mordell, *The representation of a definite quadratic form as a sum of two others*, Ann. of Math., 38 (1937), p. 751.

[90] G. Moskowitz and C. O'Neill, *The structure theorem for sets of lengths for numerical semigroups*, J. Commut. Algebra, 17 (2025), pp. 31–43.

[91] Y. Nesterov and A. Nemirovskii, *Interior-point polynomial algorithms in convex programming*, vol. 13 of SIAM Studies in Applied Mathematics, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1994.

[92] P. Q. Nguyen and B. Vallée, eds., *The LLL Algorithm: Survey and Applications*, Information Security and Cryptography, Springer, Berlin, Heidelberg, 2010.

[93] P. Q. Nguyen and B. Vallée, *Lll and applications in integer programming*, The LLL Algorithm: Survey and Applications, (2010), pp. 649–678.

[94] C. O'Neill, *On factorization invariants and Hilbert functions*, Journal of Pure and Applied Algebra, 221 (2017), pp. 3069–3088.

[95] C. O'Neill and R. Pelayo, *How do you measure primality?*, American Mathematical Monthly, 122 (2015), pp. 121–137.

[96] M. Padberg and G. Rinaldi, *A branch-and-cut algorithm for the resolution of large-scale symmetric traveling salesman problems*, SIAM Rev., 33 (1991), pp. 60–100.

[97] G. Pataki and A. Touzov, *How do exponential size solutions arise in semidefinite programming?*, SIAM Journal on Optimization, (2024). arXiv:2103.00041, v2 (2023).

[98] V. Reis and T. Rothvoss, *The subspace flatness conjecture and faster integer programming*, in 2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS), IEEE, 2023, pp. 974–988.

[99] K. F. Roth, *On certain sets of integers*, J. London Math. Soc., 28 (1953), pp. 104–109.

[100] ———, *On certain sets of integers. II*, J. London Math. Soc., 29 (1954), pp. 20–26.

[101] B. Y. Rubinstein and L. G. Fel, *Restricted partition functions as Bernoulli and Euler polynomials of higher order*, Ramanujan J., 11 (2006), pp. 331–347.

[102] R. Salem and D. C. Spencer, *On sets of integers which contain no three terms in arithmetical progression*, Proceedings of the National Academy of Sciences of the United States of America, 28 (1942), pp. 561–563.

[103] A. Schrijver, *Theory of linear and integer programming*, Wiley-Interscience Series in Discrete Mathematics, John Wiley & Sons, Ltd., Chichester, 1986. A Wiley-Interscience Publication.

[104] A. Schürmann, *Computational geometry of positive definite quadratic forms*, vol. 48 of University Lecture Series, American Mathematical Society, Providence, RI, 2009. Polyhedral reduction theories, algorithms, and applications.

[105] A. Sebö, *Hilbert bases, Caratheodory's theorem and combinatorial optimization*, in Proceedings of the 1st Integer Programming and Combinatorial Optimization Conference, 1990, pp. 431–455.

[106] W. a. Sierpiński, *Pythagorean triangles*, vol. no. 9 of Scripta Mathematica Studies, Yeshiva University, Graduate School of Science, New York, 1962. Translated by Ambikeshwar Sharma.

[107] R. P. Stanley, *Combinatorics and commutative algebra*, vol. 41 of Progress in Mathematics, Birkhäuser Boston, Inc., Boston, MA, second ed., 1996.

[108] B. Sturmfels, *On vector partition functions*, J. Combin. Theory Ser. A, 72 (1995), pp. 302–309.

[109] ———, *Gröbner bases and convex polytopes*, vol. 8 of University Lecture Series, American Mathematical Society, Providence, RI, 1996.

[110] B. Sturmfels and S. Sullivant, *Combinatorial secant varieties*, Pure and Applied Mathematics Quarterly, 2 (2006), pp. 867–891. Special Issue in Honor of Robert MacPherson.

[111] T. Tao and V. Vu, *Additive combinatorics*, vol. 105 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 2006.

[112] S. Trandafir, *External columns and chambers of vector partition functions*, Discrete Comput. Geom., (2025). Online first.

[113] S. M. Trott, *A pair of generators for the unimodular group*, Canad. Math. Bull., 5 (1962), pp. 245–252.

[114] P. van Emde Boas, *Another NP-complete partition problem and the complexity of computing short vectors in a lattice*, Tech. Rep. Report 81-04, Department of Mathematics and Computer Science, University of Amsterdam, 1981.

[115] L. Vandenberghe and S. Boyd, *Semidefinite programming*, SIAM Rev., 38 (1996), pp. 49–95.

[116] K. Woods, *The unreasonable ubiquitousness of quasi-polynomials*, Electron. J. Combin., 21 (2014), pp. Paper 1.44, 23.

[117] G. M. Ziegler, *Lectures on polytopes*, vol. 152 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1995.