Integer Points in Arbitrary Convex Cones: The Case of the PSD and SOC Cones ⋆

Jesús A. De Loera[1], Brittney Marsters[1], Luze Xu[1], and Shixuan Zhang[2]

[1] University of California, Davis, Davis CA 95616, USA
{jadeloera,bmmarsters,lzxu}@ucdavis.edu
[2] Texas A&M University, College Station TX 77843, USA
shixuan.zhang@tamu.edu

Abstract. We investigate the semigroup of integer points inside a convex cone. We extend classical results in integer linear programming to conic integer programming. We show that the semigroup associated with nonpolyhedral cones can sometimes have a notion of finite generating set. We show this is true for the cone of positive semidefinite matrices (PSD) and the second order cone (SOC). Both cones have a finite generating set of integer points, similar in spirit to Hilbert bases, but require the action of a finitely generated group. We also extend notions of total dual integrality, Gomory-Chvátal closure, and Carathéodory rank to integer points in arbitrary cones.

Keywords: Integer Points · Convex Cones · Semigroups · Hilbert bases · Conic Programming · Positive Semidefinite Cone · Second Order Cone

1 Introduction

A semigroup S is a subset of $\mathbb{Z}^n$ that contains $\mathbf{0}$ and is closed under addition. Given a convex cone $C \subseteq \mathbb{R}^n$, the integer points $S_C := C \cap \mathbb{Z}^n$ form a semigroup which we will call the *conical semigroup* of C. In particular, given any compact convex body $K \subseteq \mathbb{R}^n$, the integer points $\operatorname{cone}(K \times \{1\}) \cap \mathbb{Z}^{n+1}$ form a conical semigroup. Conical semigroups appear not just in optimization [1,6], but also in algebra and number theory [2,3]. Given a convex cone $C \subseteq \mathbb{R}^N$ for $N \geq 1$, we say a subset $B \subseteq S_C$ is a *integral generating set* of S_C if for any $s \in S_C$ there exist $b_1, \ldots, b_m \in B$ and $c_1, \ldots, c_m \in \mathbb{Z}_{\geq 0}$ such that $s = \sum_{i=1}^{m} c_i b_i$, for some $m \geq 1$. Furthermore, we call B a *conical Hilbert basis* if B is an inclusion-minimal integral generating set.

⋆ Due to space limitations, we omit several proofs. These can be found at https://www.math.ucdavis.edu/~deloera/IPCO2024.pdf.
This research is partially based upon work supported by the National Science Foundation under Grant No. DMS-1929284 while the first, third, and fourth authors were in residence at the Institute for Computational and Experimental Research in Mathematics in Providence, RI, during the Discrete Optimization program. We thank Kurt Anstreicher, Renata Sotirov, Pablo Parrilo, Chiara Meroni, and Bento Natura for relevant comments.

When the defining cone C is polyhedral and pointed, there is abundant literature on the topic. It is well-known that we have a unique finite Hilbert basis in this case [11,20]. Historically, Hilbert bases have been fundamental in the theory and algorithms of combinatorial optimization. For example, determining if a rational system $A\mathbf{x} \leq \mathbf{b}$ is totally dual integral (TDI) is equivalent to checking if, for every face F of the polyhedron $P := \{\mathbf{x} : A\mathbf{x} \leq \mathbf{b}\}$, the rows of A which are active in a face F form a Hilbert basis for cone(F)[20].

It is natural to ask, what properties transfer from polyhedral cones to arbitrary convex cones? For instance, *do we preserve any notion of finiteness in generating sets for semigroups when we relax the polyhedral condition and instead consider general conical semigroups? Are there Hilbert bases for general cones?* This paper discusses finite generation for conical semigroups and extends the polyhedral cone theory of Hilbert bases to non-polyhedral convex cones. Our main results will pertain to the semigroups arising from the cone of positive semi-definite matrices and the second order. Both cones play a key role in modern optimization [4,5]. We also discuss some applications of our non-polyhedral point of view.

In what follows, we denote $\mathrm{GL}(N, \mathbb{Z}) := \{U \in \mathbb{Z}^{N\times N} : \ |\det(U)| = 1\}$. Here is a new notion of finite generation for conical semigroups.

Definition 1. *Given a conical semigroup $S_C \subset \mathbb{Z}^N$, we call it (R, G)-finitely generated if there is a finite subset $R \subseteq S_C$ and a finitely generated subgroup $G \subseteq \mathrm{GL}(N, \mathbb{Z})$ acting on S_C such that*

1. *S_C is invariant under the group action, $G \cdot S_C = S_C$, and*
2. *every element $s \in S_C$ can be represented as*

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

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

Note that when C is a (pointed) rational polyhedral cone, then the conical semigroup $S_C = C \cap \mathbb{Z}^N$ is (R, G)-finitely generated by R, its Hilbert basis, and G, the trivial group $\{I_N\}$. Similarly, note that if S_C is an (R, G)-finitely generated semigroup, then $\cup_{r\in R} G \cdot r$ is an integral generating set of S_C, which is a superset of a conical Hilbert basis. We call R the set of *roots* of S_C, and $\cup_{r\in R} G \cdot r$ the set of generators for S_C.

While a non-polyhedral cone cannot be finitely generated in the usual sense, using a possibly infinite (finitely generated) group G allows us to extend our understanding beyond the polyhedral case. Because the possibly infinite generators for S_C can be obtained by group action G on a finite set R and G is finitely generated, this allows for the possibility of algorithmic methods. The well-known Krein-Milman theorem states that any point in a closed pointed cone C can be generated by extreme rays, denoted by $ext(C)$ [4]. When we restrict to the conical semigroup S_C and non-negative integer combinations, the primitive integer point on the extreme rays of C must be contained in the set of generators of S_C, where an integer point $x = (x_1, \dots, x_N) \in \mathbb{Z}^N$ *primitive* if $\gcd(x_1, \dots, x_N) = 1$. We call the integer points of S_C on the extreme rays of C *extreme points*, denoted by $ext(S_C) := \{y : \; y \in ext(C) \cap \mathbb{Z}^N\}$. However, as in the polyhedral case, the generators will often include extra non-extreme boundary points or even interior points. We provide the following definition of *sporadic points* that cannot have an extreme point subtracted from them and still remain within the cone.

Definition 2. *The sporadic points in $S_C = C \cap \mathbb{Z}^N$ are defined to be the points $x \in S_C$ such that there does not exist $y \in ext(S_C)$ such that $x - y \in S_C$.*

If $x \in S$ is sporadic, then x cannot be written as an integer conical combination of extreme points (even though it can be written as a real combination of them). From the definition of sporadic points, we know that all points $x \in S$ can be written as an integer conical combination of primitive extreme points and one sporadic point. To show that a semigroup is (R, G)-finitely generated, it is sufficient to show that the set of primitive extreme points and sporadic points are finite or can be obtained from a finitely generated group G that acts on a finite set of roots, R.

The two convex cones of interest in this work are positive semidefinite cone (PSD) and second-order cone (SOC). In Sections 2 and 3 of this paper, we will present the following two main results pertaining to integer points in the PSD cone $\mathcal{S}^n_+(\mathbb{Z})$, and those in the SOC $\mathrm{SOC}(n) \cap \mathbb{Z}^n$.

Theorem 1. *The conical semigroup of the cone of positive semidefinite matrices, $\mathcal{S}^n_+(\mathbb{Z})$, is (R, G)-finitely generated by $G \cong \mathrm{GL}(n, \mathbb{Z})$ where G acts on $X \in \mathcal{S}^n_+(\mathbb{Z})$ by $X \mapsto UXU^\intercal$ for each $U \in \mathrm{GL}(n, \mathbb{Z})$, and by R, the union of a single rank-one matrix and a finite subset of the sporadic points. Moreover,*

1. *If $n \leq 5$, then there are no sporadic points. Thus, $R = \{\mathbf{e}_1\mathbf{e}_1^\intercal\}$, where $\mathbf{e}_1$ is the first unit vector.*
2. *If $n = 6$, then $R = \{\mathbf{e}_1\mathbf{e}_1^\intercal, M\}$, where M is a single sporadic point defined in Section 2 Proposition 5.*

Theorem 2. *For dimension $3 \leq n \leq 10$, the conical semigroup $\mathrm{SOC}(n) \cap \mathbb{Z}^n$ is (R, G)-finitely generated. The matrices in G and the set R will be defined in Section 3.*

We say that two matrices X_1, X_2 are unimodularly equivalent if $X_2 = U \cdot X_1$ for some $U \in \mathrm{GL}(n, \mathbb{Z})$. It is easy to see that it defines an equivalence relation for all integer PSD matrices. Note that the equivalence class of $\mathbf{e}_1\mathbf{e}_1^\intercal$ are all rank-1 integer matrix $\mathbf{x}\mathbf{x}^\intercal$ for some primitive integer vector $\mathbf{x} \in \mathbb{Z}^n$. An interpretation of Theorem 1 is that for dimension $n \leq 5$, every integer PSD matrix can be represented as the sum of rank-1 matrices $\mathbf{x}\mathbf{x}^\intercal$ for some primitive integer vector $\mathbf{x} \in \mathbb{Z}^n$. However, the same result fails for dimension $n = 6$. In this case, we will have that every integer PSD matrix can be represented as the sum of rank-1 matrices and one sporadic matrix Y, which is unimodularly equivalent to M (this matrix was first found by [19]). In general, every integer PSD matrix can be represented as the sum of rank-1 matrices and one sporadic matrix, which is unimodularly equivalent to a matrix in the finite set R. Regarding prior work that inspired us, we mention [16] that contains a similar rank-1 decomposition structure for PSD $\{0,1\}$ matrices: a PSD $\{0,1\}$ matrix $X \in \mathcal{S}^n_+(\mathbb{Z}) \cap \{0,1\}^{n\times n}$ satisfies $X = \sum_{i\in K} \mathbf{x}_i\mathbf{x}_i^\mathsf{T}$ for $\mathbf{x}_i \in \{0,1\}^n$, where K is a finite index set. Similarly, [18] extended the results to PSD $\{0,\pm1\}$ matrices: a PSD $\{0,\pm1\}$ matrix $X \in \mathcal{S}^n_+(\mathbb{Z}) \cap \{0,\pm1\}^{n\times n}$ satisfies $X = \sum_{i\in K} \mathbf{x}_i\mathbf{x}_i^\mathsf{T}$ for $\mathbf{x}_i \in \{0,\pm1\}^n$, where K is a finite index set. Our results extend to all integer positive semidefinite matrices. For the second order cone, we extended the construction of the Barning-Hall tree in [8] for the primitive extreme points (or Pythagorean tuples) to classify the sporadic points.

While it might be tempting to believe that these results hint that all conical semigroups are (R,G)-finitely generated for some finite set R and some group G, we conjecture the contrary:

Conjecture 1 *There exists a conical semigroup S that is not (R,G)-finitely generated for any choice of R and G.*

What is the significance of these results beyond their connections to classical geometry of numbers, lattices, and number theory? (see e.g., [14]). We motivate our interest about conical semigroups with two applications in optimization. In what follows, we assume that our cone $C \subset \mathbb{R}^N$ is full-dimensional.

The first application regards the notion of *Chvátal-Gomory cuts* which is useful in the branch-and-cut methods for integer programming. How much of this can be extended to conic integer programming? Given a linear map $\mathcal{A} : \mathbb{R}^m \to \mathbb{R}^N$ and $\mathbf{c} \in \mathbb{R}^N$, we define a *linear conical inequality* (LCI) system as

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

where $\mathbf{c} \in \mathbb{Z}^N$ and $\mathcal{A}(\mathbb{Z}^m) \subseteq \mathbb{Z}^N$. When C is the cone of positive semidefinite matrices in $\mathcal{S}^n(\mathbb{R})$, then $N = \binom{n+1}{2}$ and $\mathcal{A}(\mathbf{x}) = \sum_{i=1}^m x_i A_i$ for some matrices $A_1, \ldots, A_m \in \mathcal{S}^n(\mathbb{Z})$. This is known as a *linear matrix inequality* and defines a *spectrahedron*. An important concept for LCI is called total dual integrality (TDI), which has been well-known for polyhedral cones C [13,12] and recently extended to spectrahedral cones [7,17]. We use C^* to denote the dual cone of C, $\mathcal{A}^*$ to denote the adjoint linear map of $\mathcal{A}$, and give a definition for general cones here.

Definition 3. *An LCI system $\mathbf{c} - \mathcal{A}(\mathbf{x}) \in C$ is totally dual integral, if for any $\mathbf{b} \in \mathbb{Z}^m$, the dual optimization problem*

$$\min \quad y(\mathbf{c}) \quad \text{s.t.} \quad \mathcal{A}^*(y) = \mathbf{b},\ y \in C^*,$$

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

To approximate the convex hull of $Z := \mathrm{LCI}_C(\mathbf{c},\mathcal{A}) \cap \mathbb{Z}^m$, a commonly used approach (quite similar to its polyhedral version) is to add *Chvátal-Gomory* (CG) cuts, which are defined as follows [17]. If $\mathbf{u} \in \mathbb{Z}^m$ is an integral vector and $v \in \mathbb{R}$ a real number such that the linear inequality $\mathbf{u}^\mathsf{T}\mathbf{x} \le v$ is *valid* for all $x \in \mathrm{LCI}_C(c, \mathcal{A})$, then the inequality $\mathbf{u}^\mathsf{T}\mathbf{x} \le \lfloor v \rfloor$ is valid for all $\mathbf{x} \in Z$ and called a CG cut. There are possibly infinitely many CG cuts so we define the (elementary) CG closure as

$$\text{CG-cl}(Z) := \bigcap_{\substack{(\mathbf{u},v)\in\mathbb{Z}^m\times\mathbb{R}:\\ S\subseteq\{\mathbf{x}:\mathbf{u}^\mathsf{T}\mathbf{x}\le v\}}} \left\{\mathbf{x}\in\mathbb{R}^m : \mathbf{u}^\mathsf{T}\mathbf{x} \le \lfloor v \rfloor\right\}. \tag{1}$$

Now take any linear function $w \in C^*$ such that $w(\mathbb{Z}^N) \subseteq \mathbb{Z}$. Then, a CG cut can be generated by

$$w \circ \mathcal{A}(\mathbf{x}) \le \lfloor w(\mathbf{c}) \rfloor,$$

as, by definition, $w \circ \mathcal{A}(\mathbb{Z}^m) \in \mathbb{Z}$. Conversely, if the conical semigroup $S_{C^*} := C^* \cap \mathbb{Z}^N$ is (R, G)-finitely generated, then we can get all CG cuts through R and G for our TDI LCI system. This is one of the nice consequences of this property.

Theorem 3. *Suppose $C \subset \mathbb{R}^N$ is a full-dimensional convex cone such that $S_{C^*} := C^* \cap \mathbb{Z}^N$ is (R, G)-finitely generated, and $\mathrm{LCI}_C(\mathbf{c}, \mathcal{A})$ is TDI. Then the CG closure for $Z := \mathrm{LCI}_C(\mathbf{c}, \mathcal{A}) \cap \mathbb{Z}^m$ can be described by*

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

The final application has to do with classical notions of integer rank [10]. Just like the notion of (real) rank of a linear system allows us to bound the number of non-zero entries in a solution of a linear system, we want to know how many elements are needed to decompose any element of a conical semigroup as a linear combination of generators with non-negative integer coefficients. Suppose that our conical semigroup $S_C = C \cap \mathbb{Z}^N$ has an integer generating set B. For any element $s \in S_C$, there exist integer generators $b_1, \ldots, b_m \in B$ and $\lambda_1, \ldots, \lambda_m \in \mathbb{Z}_{\ge 1}$ such that $s = \sum_{i=1}^m \lambda_i b_i$, for some $m \ge 1$. The minimum number m needed in the sum is called the *integer Carathéodory rank* (ICR) of s, and the maximum number over all $s \in S_C$ is the ICR of the conical semigroup S_C or the cone C. We show an upper bound on the ICR that depends only on the dimension N. The proof is almost identical to the popular polyhedral result in [10,22] but we must use the extreme point characterization of semi-infinite linear optimization [9] to allow infinite generating sets.

Theorem 4. *Let $C \subset \mathbb{R}^N$ be an arbitrary pointed convex cone and $S_C := C \cap \mathbb{Z}^N$. Then $\mathrm{ICR}(S_C) \le 2N - 2$.*

2 The Positive Semidefinite (PSD) Cone

Let $\mathcal{S}^n(\mathbb{Z})$ (resp. $\mathcal{S}^n(\mathbb{R})$) denote the set of $n \times n$ symmetric matrices of integer (resp. real) entries. For a matrix $X \in \mathcal{S}^n(\mathbb{Z})$, we say that X is PSD (denoted as $X \succeq 0$) if and only if it is so when regarded as a real matrix $X \in \mathcal{S}^n(\mathbb{R})$. We denote $\mathcal{S}^n_+(\mathbb{Z})$ as the set of integer PSD matrices.

The group $\mathrm{GL}(n,\mathbb{Z})$ embeds into $\mathrm{GL}(N,\mathbb{Z})$ as follows. Given a matrix $U \in \mathrm{GL}(n,\mathbb{Z})$ and any $X \in \mathcal{S}^n(\mathbb{Z})$, we define the action $U \cdot X := UXU^\mathsf{T}$. This action is a linear map and takes integer points in $\mathbb{Z}^N$ to integer points, and thus can be represented by the multiplication with a matrix in $\mathrm{GL}(N,\mathbb{Z})$. It is well-known that this group $\mathrm{GL}(n,\mathbb{Z})$ is finitely generated [23]. For the convenience of discussion, we still use the matrix $U \in \mathrm{GL}(n,\mathbb{Z})$ to denote this matrix multiplication in the subgroup of $\mathrm{GL}(N,\mathbb{Z})$.

2.1 Lemmas for $n \le 5$ and $n = 6$

The following *integer rank-1 decomposition* for PSD integer matrices is studied in [19]. 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 1. *If $n \le 5$, 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*

$$X = \sum_{i \in K} \mathbf{x}_i \mathbf{x}_i^\mathsf{T}. \tag{2}$$

To restate Definition 2 in the PSD case, we say an integer 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 $X - \mathbf{x}\mathbf{x}^\mathsf{T} \succeq 0$. Lemma 1 is equivalent to the fact that there is no sporadic point in $\mathcal{S}^n_+(\mathbb{Z})$ when $n \le 5$.

Proposition 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 $Y - \mathbf{x}\mathbf{x}^\mathsf{T} \succeq 0$. 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 $X_i := X_{i-1} - \mathbf{x}_i\mathbf{x}_i^\mathsf{T} \succeq 0$.
2. If $X = 0$, then we have found an integer rank-1 decomposition $X = \sum_{j=1}^{i} \mathbf{x}_j\mathbf{x}_j^\mathsf{T}$; 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 $\mathbf{x}_i\mathbf{x}_i^\mathsf{T}$ contains at least 1 nonzero entry because $\mathbf{x}_i \neq 0$. Thus the trace $\mathrm{tr}(X_i) \le \mathrm{tr}(X_{i-1}) - 1$ for any $i \ge 1$ because the entries are integers. The procedure can repeat no more than $\mathrm{tr}(X)$ times as $\mathrm{tr}(X_i) \ge 0$.

If every $X \in \mathcal{S}^n_+(\mathbb{Z})$ has an integer rank-1 decomposition $X = \sum_{i \in K} \mathbf{x}_i\mathbf{x}_i^\mathsf{T}$, then any of $\mathbf{x}_i, i \in K$ satisfies the requirement $X - \mathbf{x}_i\mathbf{x}_i^\mathsf{T} \succeq 0$. □

For any matrix $X \in \mathcal{S}^n(\mathbb{R})$, we can define a convex set $C(X) := \{\mathbf{x} \in \mathbb{R}^n : X - \mathbf{x}\mathbf{x}^\mathsf{T} \succeq 0\}$. Since $X - \mathbf{x}\mathbf{x}^\mathsf{T} \succeq 0$ if and only if, for any $\mathbf{v} \in \mathbb{R}^n$, $|\mathbf{v}^\mathsf{T}\mathbf{x}|^2 \le \mathbf{v}^\mathsf{T} X \mathbf{v}$, we see that $C(X)$ is a compact convex set that is symmetric about the origin but not necessarily full-dimensional. This provides another equivalent formulation of the integer rank-1 decomposition.

Proposition 2. *For $X \in \mathcal{S}^n_+(\mathbb{Z})$, X is sporadic if and only if $C(X) \cap \mathbb{Z}^n = \{\mathbf{0}\}$.*

This provides a geometric perspective to our problem. Note that the set $C(X)$ is a (possibly degenerate) ellipsoid because

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

by the positive semidefiniteness of Schur complements, where $X^\dagger$ denotes the pseudoinverse of X. In the case where $\det(X) > 0$,

$$C(X) = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x}^\mathsf{T} \operatorname{adj}(X)\mathbf{x} \le \det(X)\} \text{ with } \operatorname{vol}(C(X)) = V_n \sqrt{\det(X)}$$

where $\operatorname{adj}(X)$ is the adjugate of X satisfying $\operatorname{adj}(X) = \det(X)X^{-1}$ and $V_n := \pi^{n/2}/\Gamma(\frac{n}{2}+1)$ is the volume of the unit n-ball. The degenerate case for rank 1 is characterized by the following proposition.

Proposition 3. *Suppose $X \in \mathcal{S}_+^n(\mathbb{Z})$, and $\operatorname{rank}(X) = 1$, then $X = \lambda \mathbf{x}\mathbf{x}^\mathsf{T}$, where $\mathbf{x} \in \mathbb{Z}^n$ and $\lambda \in \mathbb{Z}_{\ge 1}$.*

Proof. As $X \succeq 0$ and $\operatorname{rank}(X) = 1$, we can assume that $X = \mathbf{a}\mathbf{a}^\mathsf{T}$ 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 $k_i := a_i^2 \in \mathbb{Z}_{\ge 0}$. Without loss of generality, we can assume that $k_i \ge 1$, i.e., $a_i \ne 0$, otherwise, we can just consider the submatrix corresponding to the nonzero k_i.

Suppose that there exists some $a_i \in \mathbb{Z} \setminus \{0\}$ and $a_j \in \{\pm\sqrt{k_j}\} \notin \mathbb{Q}$. Then $a_i a_j \notin \mathbb{Q}$, a contradiction. Therefore, $a_i \in \mathbb{Z}$ for all i or $a_i \notin \mathbb{Q}$ for all 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 decomposition of k_i, $i \in [n]$. Assume that $k_i = \prod_{\ell=1}^s p_\ell^{\alpha_\ell^i}$, $\alpha_\ell^i \in \mathbb{Z}_{\ge 0}$. 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 $X = \lambda \mathbf{x}\mathbf{x}^\mathsf{T}$ for $x = a/\sqrt{\lambda}$, where $x_i = \sqrt{k_i/\lambda} \in \mathbb{Z}$. $\square$

From Proposition 3, we can directly prove the case for $n = 2$ using Minkowski's Theorem (for example, see [11]).

Proposition 4. *Lemma 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 $a_{11} \ge 0, a_{22} \ge 0, a_{11}a_{22} - a_{12}^2 \ge 0$. By the rank 1 result, we can consider the case when $X \succ 0$, i.e., $\det(X) = a_{11}a_{22} - a_{12}^2 \ge 1, a_{11} \ge 1, a_{22} \ge 1$. Then $C(X) := \{\mathbf{x} \in \mathbb{R}^2 : X - \mathbf{x}\mathbf{x}^\mathsf{T} \succeq 0\} =$

$$\{\mathbf{x} \in \mathbb{R}^2 : a_{11} - x_1^2 \ge 0, a_{22} - x_2^2 \ge 0, (a_{11} - x_1^2)(a_{22} - x_2^2) - (a_{12} - x_1 x_2)^2 \ge 0\}.$$

We claim that $C(X) = \{\mathbf{x} \in \mathbb{R}^2 : (a_{11} - x_1^2)(a_{22} - x_2^2) - (a_{12} - x_1x_2)^2 \geq 0\}$. We only need to show that $(a_{11} - x_1^2)(a_{22} - x_2^2) - (a_{12} - x_1x_2)^2 \geq 0$ implies that $a_{11} - x_1^2 \geq 0, a_{22} - x_2^2 \geq 0$. Notice that $a_{11}a_{22} - a_{12}^2 > 0$ and

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

We know that $a_{11} - x_1^2 \geq 0$ and $a_{22} - x_2^2 \geq 0$.

$C(X)$ is an centrally symmetric ellipsoid $\{\mathbf{x} \in \mathbb{R}^2 : \det(X) - a_{22}x_1^2 + 2a_{12}x_1x_2 - a_{11}x_2^2 \geq 0\}$ with area $\pi\sqrt{\det(X)}$ (because $C(X) = \{(x_1, x_2) : \frac{x_1^2}{a_{11}} - \frac{a_{11}}{\det(X)}(x_2 - \frac{a_{12}}{a_{11}}x_1)^2 \leq 1\}$).

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

If $\det(X) = 1$, then $C(X) = \{x \in \mathbb{R}^n : a_{22}x_1^2 - 2a_{12}x_1x_2 + a_{11}x_2^2 \leq 1\}$. Because $a_{22}, a_{12}, a_{11} \in \mathbb{Z}$, we have $C(X) \cap \mathbb{Z}^2 = \tilde{C}(X) \cap \mathbb{Z}^2$, where $\tilde{C}(X) = \sqrt{2-\epsilon} \cdot C(X) = \{x \in \mathbb{R}^n : a_{22}x_1^2 - 2a_{12}x_1x_2 + a_{11}x_2^2 \leq 2 - \epsilon\}$. Therefore, $\mathrm{vol}(\tilde{C}(X)) = (2-\epsilon) \cdot \pi > 4$, when $0 < \epsilon < 2 - \frac{4}{\pi}$. Therefore, $C(X) \cap \mathbb{Z}^2 = \tilde{C}(X) \cap \mathbb{Z}^2$ is nonempty by Minkowski Theorem. □

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

Lemma 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 $\mathbf{z} \in \mathbb{Z}^n$ such that $X\mathbf{z} = \mathbf{0}$.

Pick $\mathbf{z}$ to be in a basis of a primitive sublattice $\Lambda = N \cap \mathbb{Z}^n$, where $N := \{\mathbf{y} \in \mathbb{R}^n : X\mathbf{y} = \mathbf{0}\}$. Thus, a basis of Λ containing $\mathbf{z}$ can be extended to a basis of $\mathbb{Z}^n$, $U = [\mathbf{z}, \mathbf{u}_2, \ldots, \mathbf{u}_n]$. Because U is a basis of $\mathbb{Z}^n$, we know that $|\det(U)| = 1$, i.e., U is unimodular. Then

$$U^{\mathsf{T}}XU = \begin{bmatrix} 0 & 0 \\ 0 & \hat{X} \end{bmatrix}.$$

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

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

The scaling of $C(X)$ into $\tilde{C}(X)$ (while preserving the integer points) in the proof for Proposition 4 results in

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

where 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 $\det(X) = 1, 2, 3$, respectively, and greater than 2 for $\det(X) \geq 4$. Thus $\mathrm{vol}(\tilde{C}(X)) > 8$ so $\tilde{C}(X) \cap \mathbb{Z}^3 \neq \{0\}$ by Minkowski's theorem.

To prove Lemma 1, we need to use a more sophisticated method based on the *Hermite constant* [21]

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

Remark 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}

Remark 2. From the volume argument in Minkowski's Theorem, we have

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

which is better than the bound given by $\gamma_n \leq (\frac{4}{3})^{\frac{n(n-1)}{2}}$ when n is large, but it is not enough for the dimension $n = 4, 5$.

Proof (for Lemma 1). The case $n = 1$ follows from Proposition 3. We will show that $C(X) \cap \mathbb{Z}^n \neq \{\mathbf{0}\}$ for $2 \leq n \leq 5$, where $C(X) = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x}^\mathsf{T} \mathrm{adj}(X) \mathbf{x} \leq \det(X)\}$. By the definition of the Hermite constant, we have

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

For $n = 2, 3, 4, 5$, we have $\frac{n^n}{(n-1)^{n-1}} > \gamma_n$. $(\frac{2^2}{1^1} = 4, \frac{3^3}{2^2} \approx 6.75, \frac{4^4}{3^3} \approx 9.48, \frac{5^5}{4^4} \approx 12.21, \frac{6^6}{5^5} \approx 14.93)$ By taking the derivative with respect to $\det(X)$, 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,

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

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

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

which implies that $C(X) \cap (\mathbb{Z}^n \setminus \{\mathbf{0}\}) \neq \emptyset$. Lemma 1 now follows from Propositions 2 and 1, and Lemma 2. $\square$

The argument used to prove Lemma 1 fails for $n \geq 6$, but it implies that the determinant of the sporadic matrices is bounded by a constant only depend 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 1. *If $X \in \mathcal{S}_+^n(\mathbb{Z})$ is sporadic, then $\det(X) < \gamma_n$.*

A sporadic matrix for $n = 6$ was initially found in [19].

Proposition 5. *In $n = 6$, the matrix M is sporadic, i.e., $C(M) \cap \mathbb{Z}^n = \{\mathbf{0}\}$.*

$$M = \begin{bmatrix} 2 & 0 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 1 & 1 & 1 \\ 1 & 0 & 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 & 2 \end{bmatrix} \textit{ with } \det(M) = 3.$$

Proof. We verify that $\min_{\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}} (\mathbf{x}^\mathsf{T} \mathrm{adj}(X) \mathbf{x}) > \det(X) = 3$.

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

Note that $\mathbf{x}^\mathsf{T} \mathrm{adj}(X) \mathbf{x} = [(x_1 + 2x_2 + x_3 - x_4 - x_5 - x_6)^2 + (x_1 + x_2 + x_3 - x_4 - x_5 - x_6)^2 + x_2^2] + [(x_1 - x_3)^2 + x_1^2 + x_3^2] + [(x_4 - x_5)^2 + (x_4 - x_6)^2 + (x_5 - x_6)^2]$. 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 $\mathbf{x}^\mathsf{T} \mathrm{adj}(X) \mathbf{x} = A_2 + A_{13} + A_{456}$.

Suppose, there exists $x \in \mathbb{Z}^6$ such that $\mathbf{x}^\mathsf{T} \mathrm{adj}(X) \mathbf{x} \leq 3$. We are going to show that $x = 0$. Notice that A_2, A_{13}, A_{456} are even, which implies that $A_2 + A_{13} + A_{456} \leq 2$. 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 $A_2 = 6x_2^2 \leq 2$, 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 $A_{13} = 6x_1^2 \leq 2$, 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 $A_{456} = (x_4 - x_5)^2 + (2x_4 + x_5)^2 + (x_4 + 2x_5)^2 = 6(x_4^2 + x_5^2 + x_4 x_5) \leq 2$, we have $x_4 = x_5 = x_6 = 0$.

Therefore, $\min_{\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}} (\mathbf{x}^\mathsf{T} \mathrm{adj}(X) \mathbf{x}) > 3$. For $\mathbf{x} = \mathbf{e}_1$, $\mathbf{x}^\mathsf{T} \mathrm{adj}(X) \mathbf{x} = 4$, i.e., $\min_{\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}} (\mathbf{x}^\mathsf{T} \mathrm{adj}(X) \mathbf{x}) = 4$. $\square$

Moreover, in [15], it is shown that for $n = 6$, M is the unique sporadic matrix under unimodular equivalence. Using this fact, we have the following Lemma.

Lemma 3. *If $n = 6$, then for any $X \in \mathcal{S}_+^n(\mathbb{Z})$,*

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

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

2.2 Proof of Theorem 1

Proof. We know that the primitive extreme points are generated from the group $\mathrm{GL}(n, \mathbb{Z})$ that acts on $\{\mathbf{e}_1\mathbf{e}_1^\mathsf{T}\}$. The finiteness of the index set K follows from similar argument in Proposition 1. We only need to prove that the sporadic points are generated from the group $\mathrm{GL}(n, \mathbb{Z})$ on a finite set R.

Corollary 1 shows that for any sporadic matrix X, $\det(X) < \gamma_n$. By [21, Theorem 2.4], there exists a constant $\alpha_n > 0$ depending only on n, such that for any positive definite matrix $X \in \mathcal{S}^n(\mathbb{Z})$, there is a unimodularly equivalent matrix X' of X with diagonal entries satisfy

$$\prod_{i=1}^n X'_{ii} \le \alpha_n \det(X') = \alpha_n \det(X) < \alpha_n \gamma_n.$$

Because $X' \in \mathcal{S}^n(\mathbb{Z})$ is positive definite, $X'_{ii} \ge 1$ and thus is bounded from above. From this we see that there are only finitely many possibilities for such X' because each off-diagonal entry must satisfy $|X'_{ij}|^2 \le X'_{ii} X'_{jj}$ for any $1 \le i, j \le n$.

The two special cases $n \le 5$ and $n = 6$ follow from Lemma 1 and 3. □

3 The Second-Order Cone (SOC)

In this section, we will let T_n be the conical semigroup $\mathrm{SOC}(n) \cap \mathbb{Z}^n$ where

$$\mathrm{SOC}(n) := \left\{ \mathbf{x} \in \mathbb{R}^n : 0 \le \sqrt{x_1^2 + \cdots + x_{n-1}^2} \le x_n \right\}.$$

Additionally, for $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$, consider the quadratic form

$$\langle \mathbf{a}, \mathbf{b} \rangle := a_1 b_1 + a_2 b_2 + \cdots + a_{n-1} b_{n-1} - a_n b_n.$$

In this quadratic space, the reflection in vector $\mathbf{w}$ is defined as $\mathbf{x} \to \mathbf{x} - 2\frac{\langle \mathbf{x}, \mathbf{w} \rangle}{\langle \mathbf{w}, \mathbf{w} \rangle}\mathbf{w}$.

Definition 4. *Let $P_{i,j}$ be the permutation matrix that swaps the ith and jth columns and define Q_k be the matrix determined by*

$$(Q_k)_{i,j} = \begin{cases} -1 & \text{if } i = j = k \\ 1 & \text{if } i = j \ne k \\ 0 & \text{if } i \ne j. \end{cases}$$

For $n = 3$, let A_3 denote the matrix associated with the reflection in the vector $(1,1,1)$. For $4 \leq n \leq 10$, let A_n denote the matrix associated with the reflection in the vector $(1,1,1,0,\dots,0,1)$ also associated to this bilinear form:

$$A_3 = \begin{pmatrix} -1 & -2 & 2 \\ -2 & -1 & 2 \\ -2 & -2 & 3 \end{pmatrix}, \quad A_n = \left(\begin{array}{ccc|c|c} 0 & -1 & -1 & & 1 \\ -1 & 0 & -1 & \mathbf{0} & 1 \\ -1 & -1 & 0 & & 1 \\ \hline & \mathbf{0} & & I_{n-4} & \mathbf{0} \\ \hline -1 & -1 & -1 & \mathbf{0} & 2 \end{array}\right)$$

We define the matrix $A_n^+ = Q_1 Q_2 \dots Q_{n-1} A_n$.

Elements $\mathbf{s} \in T_n$ such that $\langle \mathbf{s}, \mathbf{s} \rangle = \mathbf{0}$ belong to the boundary of T_n, and we will denote the set of these points as ∂T_n. In number theory, these points are called Pythagorean tuples. In [8], they proved that the set of primitive Pythagorean tuples, denoted as $ext^p(T_n)$, is generated by finitely many matrices acting on a finite set R for $3 \leq n \leq 10$.

Lemma 4 (Theorem 1 in [8]). *For $3 \leq n \leq 10$, $ext^p(T_n) = \cup_{r \in R} G \cdot r$, where the group*

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

and the sets

1. $R = \left\{(1,0,\dots,0,1)^\intercal\right\}$ *for* $3 \leq n < 10$,
2. $R = \left\{(1,0,0,0,0,0,0,0,0,1)^\intercal, (1,1,1,1,1,1,1,1,1,3)^\intercal\right\}$ *for* $n = 10$,

where G acts on R by left multiplication.

We will begin this section by discussing the structural properties of the sporadic points of T_n. Then we use the structural properties of Pythagorean tuples and sporadic points to prove Theorem 2.

3.1 Sporadic Points of $\mathrm{SOC}(n) \cap \mathbb{Z}^n$

In this section, we will begin by restating the definition of sporadic in the case of $\mathrm{SOC}(n)$ and offer two partial characterizations of sporadic elements of $\mathrm{SOC}(n)$.

Definition 5. *Let $T_n = \mathrm{SOC}(n) \cap \mathbb{Z}^n$. We call a point $\mathbf{s} \in T_n$ sporadic if there is no point $\mathbf{p}$ such that $\langle \mathbf{p}, \mathbf{p} \rangle = 0$ and $\mathbf{s} - \mathbf{p} \in T_n$.*

Just as the group G takes elements of ∂T_n to ∂T_n, the group G will take sporadic elements to sporadic elements. This closure ensures that our action by G on the semigroup T_n is well-defined.

Lemma 5. *Let $\mathbf{s} \in T_n$.*

1. *Then, $A_n^+ \mathbf{s}$ and $(A_n^+)^{-1} \mathbf{s}$ are both in S.*
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. There, there is some point $\mathbf{p} \in T_n$ such that $\langle \mathbf{p}, \mathbf{p} \rangle = 0$ and $\mathbf{s} - \mathbf{p} \in T_n$. However, we would then have that

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

As $A_n^+\mathbf{p}$ satisfies $\langle A_n^+\mathbf{p}, A_n^+\mathbf{p} \rangle = 0$, this is a contradiction. The case of the inverse matrices follows similarly. □

Next, we will provide some Lemmas about the properties of sporadic points necessary to prove Theorem 2. For a detailed exposition of the technical proofs, please refer to the extended version. Lemmas 6 and 7 show that sporadic points are close to the boundary, ∂T_n.

Lemma 6. *Suppose $\mathbf{s} \in T_n$ is a primitive sporadic with non-negative entries such that $s_n > 1$ and $s_i \neq 0$ for some $i \in [n-1]$. 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 have the desired equality. □

Lemma 7. *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

$$\begin{aligned} \langle \mathbf{s}, \mathbf{s} \rangle - 2\langle \mathbf{s}, \mathbf{p} \rangle + \langle \mathbf{p}, \mathbf{p} \rangle &\leq 0 \\ -1 - 2\langle \mathbf{s}, \mathbf{p} \rangle &\leq 0 \end{aligned}$$

Thus, $\langle \mathbf{s}, \mathbf{p} \rangle \geq 0$. 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 $\sqrt{p_1^2 + \cdots + p_{n-1}^2} = p_n$, we have that

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

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. □

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 $(p)_n$ denotes the n^{th} coordinate of p,

Lemma 8. *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:*

  $$\begin{array}{lll} (1,1,1,1,1,1,1,1,0,3), & (1,1,1,1,1,1,1,0,0,3), & (1,1,1,1,1,1,0,0,0,3), \\ (2,2,2,2,2,2,2,2,1,6), & (2,2,2,2,2,2,2,1,0,6). & \end{array}$$

Proof. This is equivalent to showing that these are the only such sporadic points such that $s_1 + s_2 + s_3 = s_n$. As $\mathbf{s}$ is sporadic, $\mathbf{s} - (1, 0, \ldots, 0, 1) \notin T_n$. This is equivalent to saying that $(s_n - 1)^2 < (s_1 - 1)^2 + s_s^2 + \cdots + s_{n-1}^2$ or

$$2s_1 s_2 + 2s_2 s_3 + 2s_1 s_3 - 2s_2 - 2s_3 - s_4^2 - \cdots - s_{n-1}^2 < 0. \tag{3}$$

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, (3) implies

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

  As this is a contradiction, we must have that $s_1 = s_2$.
- Suppose that $s_2 \geq s_3 + 1$. Then, (3) implies

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

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

– Suppose that $s_3 \geq s_4 + 1$. Then, (3) implies

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

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, (3) 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, (3) implies

$$\begin{aligned} 0 &> 4(s_6+1)^2 - 4(s_6+1) - s_6^2 - \cdots - s_9^2 \\ &= 3s_6^2 - s_7^2 - \cdots - s_{n-1}^2 + 4s_6 - 4 \geq 0. \end{aligned}$$

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 one 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:

$$\begin{gathered} (k, k, k, k, k, k, s_7, 3k) \\ (k, k, k, k, k, k, k, 3k) \end{gathered}$$

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

$$(3k-1)^2 - (k-1)^2 - 5k^2 - (k+1) = 3k^2 - 5k + 1 \geq 3 > 0$$

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:

$$(k, k, k, k, k, k, s_7, s_8, 3k) \tag{4}$$

$$(k, k, k, k, k, k, k, s_8, 3k) \tag{5}$$

$$(k, k, k, k, k, k, k, k, 3k) \tag{6}$$

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

Suppose $\mathbf{s}$ is of the form (4). By way of contradiction, suppose that $k \geq 2$. We claim that $\mathbf{s} - (1, 0, \dots, 0, 1) \in T_n$. This follows from that 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 (5). By way of contradiction, suppose $k \geq 3$. Then, we claim that $\mathbf{s} - (1, 0, \dots, 0, 1) \in T_n$. This follows from the fact that

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

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:

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

This first tuple listed is not primitive so this only give us the tuple $(2, 2, 2, 2, 2, 2, 2, 1, 6)$. Lastly, if $\mathbf{s}$ is of the form (6), 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:

$$(k, k, k, k, k, k, s_7, s_8, s_9, 3k) \tag{7}$$
$$(k, k, k, k, k, k, k, s_8, s_9, 3k) \tag{8}$$
$$(k, k, k, k, k, k, k, k, s_9, 3k) \tag{9}$$
$$(k, k, k, k, k, k, k, k, k, 3k) \tag{10}$$

where $s_7, s_8, s_9 \leq k-1$. Any tuple of form (10) is a Pythagorean tuple so we may exclude it. Suppose $\mathbf{s}$ is of the form (7). By way of contradiction, suppose $k \geq 2$. Then, we claim that $\mathbf{s} - (1, 0, \dots, 0, 1) \in T_n$. This follows from the fact that

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

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 (8). By way of contradiction, suppose $k \geq 2$. If $s_9 \geq 1$, then $\mathbf{s} - (1, 1, \dots, 1, 3) \in T_n$ 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, $\mathbf{s} - (1, 0, \dots, 0, 1) \in T_n$ as

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

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 (9). If $s_9 \neq 0$, the $\mathbf{s} - (1, 1, \dots, 1, 3) \in T_n$. This follows from the fact that

$$\begin{aligned}(3k-3)^2 - 8(k-1)^2 - (s_9 - 1)^2 &\geq (3k-3)^2 - 8(k-1)^2 - (k-2)^2 \\ &= 14k - 11 \geq 0\end{aligned}$$

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 8, every other sporadic points will reduce to a strictly lower height after multiplication by $(A_n^+)^{-1}$.

Lemma 9. *Let* $\mathbf{s} \in T_n$ *be sporadic with non-negative entries such that* $s_1 \geq s_2 \geq \dots \geq s_{n-1}$, $s_1 \geq 1$ *and* $3 \leq n \leq 10$. *For* s *not listed in Lemma 8,*

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

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 a similar inequality $s_3 < s_1 + s_2$. By Lemma 6, we have that

$$\begin{aligned}s_n &= \left\lceil \sqrt{s_1^2 + s_2^2 + \dots + s_{n-1}^2} \right\rceil \\ &\leq \left\lceil \sqrt{s_1^2 + s_2^2 + s_3^2 + 2s_1s_2 + 2s_1s_3 + 2s_2s_3} \right\rceil \qquad (11) \\ &= \left\lceil \sqrt{(s_1 + s_2 + s_3)^2} \right\rceil = s_1 + s_2 + s_3,\end{aligned}$$

where the inequality follows from the order $s_1s_2 \geq s_1s_3 \geq s_2s_3 \geq s_4^2 \geq \dots \geq s_{n-1}^2$. As s is not one of the tuples listed in Lemma 8, the inequality (11) 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 $\mathbf{s}$. $\square$

3.2 Proof of Theorem 2

We now present a complete formulation of Theorem 2 followed by its proof.

Theorem 5. *For dimension* $3 \leq n \leq 10$, *the conical semigroup* $\mathrm{SOC}(n) \cap \mathbb{Z}^n$ *is* (R, G)*-finitely generated by*

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

and a finite set R. *More specifically,*

1. *If* $3 \leq n \leq 6$*, then* $R = \left\{(1,0,\dots,0,1)^\intercal, (0,\dots,0,1)^\intercal\right\}$.
2. *If* $n = 7$*, then*
$$R = \left\{(1,0,0,0,0,0,1)^\intercal, (0,0,0,0,0,0,1)^\intercal, (1,1,1,1,1,1,3)^\intercal\right\}.$$
3. *If* $n = 8$*, then*
$$R = \left\{(1,0,0,0,0,0,0,1)^\intercal, (0,0,0,0,0,0,0,1)^\intercal, (1,1,1,1,1,1,1,3)^\intercal, (1,1,1,1,1,1,0,3)^\intercal\right\}.$$
4. *If* $n = 9$*, then*
$$R = \Big\{(1,0,0,0,0,0,0,0,1)^\intercal, (0,0,0,0,0,0,0,0,1)^\intercal, (1,1,1,1,1,1,1,1,3)^\intercal, \\ (1,1,1,1,1,1,1,0,3)^\intercal, (1,1,1,1,1,1,0,0,3)^\intercal, (2,2,2,2,2,2,2,1,6)^\intercal\Big\}.$$
5. *If* $n = 10$*, then*
$$R = \Big\{(1,0,0,0,0,0,0,0,0,1)^\intercal, (1,1,1,1,1,1,1,1,1,3)^\intercal, (0,0,0,0,0,0,0,0,0,1)^\intercal, \\ (1,1,1,1,1,1,1,1,0,3)^\intercal, (1,1,1,1,1,1,1,0,0,3)^\intercal, (1,1,1,1,1,1,0,0,0,3)^\intercal, \\ (2,2,2,2,2,2,2,2,1,6)^\intercal, (2,2,2,2,2,2,2,1,0,6)^\intercal\Big\}.$$

Proof. This follows directly from Lemma 9 and that 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

$$\mathbf{s} = \lambda_1\mathbf{p}_1 + \lambda_2\mathbf{p}_2 + \cdots + \lambda_k\mathbf{p}_k + \lambda\mathbf{p} \tag{12}$$

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 4, each $\mathbf{p}_i$ can be decomposed as $\mathbf{p}_i = G_i(1,0,\dots,0,1)^\intercal$ when $3 \leq n < 10$ or $\mathbf{p}_i = G_i(1,0,\dots,0,1)^\intercal + \tilde{G}_i(1,1,\dots,1,3)^\intercal$ 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 non-negative 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 9, 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 8, 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 $\mathrm{SOC}(n)$ is (R, G)-finitely generated by the claimed R and G. □

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:

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

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 point from our root sets, our decomposition in equality (12) requires modification and we must allow for multiple sporadic points in the expression.

Remark 3. Lastly, it is worth noting that inequality (11) would fail in dimensions larger than 10. Thus, this line of argumentation would fail to produce results for $n > 10$.

We can use Theorem 5 to recover a partial converse of Lemma 7.

Corollary 2. *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 5, we can express $\mathbf{s}$ as

$$\mathbf{s} = G'(0, \ldots, 0, 1)^\mathsf{T}$$

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

$$\langle \mathbf{s}, \mathbf{s} \rangle = \langle G'(0, \ldots, 0, 1)^\mathsf{T}, G'(0, \ldots, 0, 1)^\mathsf{T} \rangle = \langle (0, \ldots, 0, 1)^\mathsf{T}, (0, \ldots, 0, 1)^\mathsf{T} \rangle = -1.$$

□

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

4 Applications: Total Dual Integrality, Chvátal-Gomory Closures, and Integer Rank of vectors.

Proof (for Theorem 3). The containment $\subseteq$ is obvious as discussed above. To see the other containment, take any halfspace $H := \{\mathbf{x} \in \mathbb{R}^m : u^\mathsf{T}\mathbf{x} \leq v\}$ 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

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

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 $\lambda_1, \ldots, \lambda_k \in \mathbb{Z}_{\geq 0}$ such that

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

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

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

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

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

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

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

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

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

To prove Theorem 4, we use the notation $\mathbb{R}^{\oplus I}$ (or simply $\mathbb{R}^I$) to denote an $\mathbb{R}$-vector space where each vector $(a_i)_{i \in I} \in \mathbb{R}^I$ has all but finitely many $a_i = 0$.

Proof (for Theorem 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

$$\begin{aligned} \max \quad & \sum_{i \in I} \lambda_i \\ \text{s.t.} \quad & \sum_{i \in I} \lambda_i b_i = s, \\ & (\lambda_i)_{i \in I} \in \mathbb{R}^{\oplus I}_{\geq 0}. \end{aligned} \tag{13}$$

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 [9, Theorem 2], we know that (13) has an extreme point solution, denoted as $(\lambda_i^*)_{i \in I}$ with $J := \{i \in I : \lambda_i^* > 0\}$. By [9, 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 $0 < \gamma_1, \ldots, \gamma_N < 1$, $\sum_{i=1}^N \gamma_i = 1$, 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 $\iota \in \operatorname{argmin}\{\frac{\lambda_i^*}{\gamma_i} : i = 1, \ldots, N\}$. 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 (13). 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 $\sum_{i=1}^N y_i < N-1$. □

Remark 4. If we apply the theorem to the case $S_C = \mathcal{S}_+^n(\mathbb{Z})$, then $N = \dim \mathcal{S}^n(\mathbb{R}) = \binom{n+1}{2}$. The bound on the ICR in this case is $2N - 2 = n^2 + n - 2$, which grows *quadratically* with n as opposed to the linear growth in the case of the usual Carathéodory rank of positive semidefinite matrices. If we apply the theorem to the case $T_n = \mathrm{SOC}(n) \cap \mathbb{Z}^n$, then $N = \dim \mathrm{SOC}(n) = n$. The ICR in this case is $2N - 2 = 2n - 2$.

References

1. Aliev, I., De Loera, J.A., Eisenbrand, F., Oertel, T., Weismantel, R.: The support of integer optimal solutions. SIAM J. Optim. **28**(3), 2152–2157 (2018)

2. Aliev, I., Averkov, G., De Loera, J.A., Oertel, T.: Sparse representation of vectors in lattices and semigroups. Math. Program. **192**(1-2), 519–546 (2022)
3. Aliev, I., De Loera, J.A., Oertel, T., O'Neill, C.: Sparse solutions of linear Diophantine equations. SIAM J. Appl. Algebra Geom. **1**(1), 239–253 (2017)
4. Barvinok, A.: A course in convexity, vol. 54. American Mathematical Soc. (2002)
5. Ben-Tal, A., Nemirovski, A.: Lectures on modern convex optimization: analysis, algorithms, and engineering applications. SIAM (2001)
6. Berndt, S., Brinkop, H., Jansen, K., Mnich, M., Stamm, T.: New support size bounds for integer programming, applied to makespan minimization on uniformly related machines. ArXiv:2305.08432 (2023)
7. de Carli Silva, M.K., Tuncel, L.: A notion of total dual integrality for convex, semidefinite, and extended formulations. SIAM Journal on Discrete Mathematics **34**(1), 470–496 (2020)
8. Cass, D., Arpaia, P.J.: Matrix generation of Pythagorean n-tuples. Proceedings of the American Mathematical Society **109**(1), 1–7 (1990)
9. Charnes, A., Cooper, W.W., Kortanek, K.: Duality in semi-infinite programs and some works of Haar and Carathéodory. Management Science **9**(2), 209–228 (1963)
10. Cook, W., Fonlupt, J., Schrijver, A.: An integer analogue of Caratheodory's theorem. Journal of Combinatorial Theory, Series B **40**(1), 63–70 (1986)
11. De Loera, J., Hemmecke, R., Köppe, M.: Algebraic and Geometric Ideas in the Theory of Discrete Optimization. MOS-SIAM Series on Optimization, Society for Industrial and Applied Mathematics (2013)
12. Edmonds, J., Giles, R.: Total dual integrality of linear inequality systems. In: Progress in combinatorial optimization, pp. 117–129. Elsevier (1984)
13. Giles, F.R., Pulleyblank, W.R.: Total dual integrality and integer polyhedra. Linear algebra and its applications **25**, 191–196 (1979)
14. Kaveh, K., Khovanskii, A.G.: Newton-Okounkov bodies, semigroups of integral points, graded algebras and intersection theory. Ann. of Math. (2) **176**(2), 925–978 (2012)
15. Ko, C.: On the decomposition of quadratic forms in six variables (dedicated to professor LJ Mordell on his fiftieth birthday). Acta Arithmetica **3**(1), 64–78 (1939)
16. Letchford, A.N., Sørensen, M.M.: Binary positive semidefinite matrices and associated integer polytopes. Mathematical Programming **131**(1-2), 253–271 (Feb 2012)
17. de Meijer, F., Sotirov, R.: The Chvátal-Gomory procedure for integer SDPs with applications in combinatorial optimization. ArXiv:2201.10224 (2022)
18. de Meijer, F., Sotirov, R.: On integrality in semidefinite programming for discrete optimization. ArXiv:2306.09865 (2023)
19. Mordell, L.J.: The representation of a definite quadratic form as a sum of two others. The Annals of Mathematics **38**(4), 751 (Oct 1937)
20. Schrijver, A.: Theory of Linear and Integer Programming. Wiley Series in Discrete Mathematics & Optimization, Wiley (1998)
21. Schürmann, A.: Computational geometry of positive definite quadratic forms: polyhedral reduction theories, algorithms, and applications, vol. 48. American Mathematical Soc. (2009)
22. Sebö, A.: Hilbert bases, Caratheodory's theorem and combinatorial optimization. In: Proceedings of the 1st Integer Programming and Combinatorial Optimization Conference. pp. 431–455 (1990)
23. Trott, S.M.: A pair of generators for the unimodular group. Canadian Mathematical Bulletin **5**(3), 245–252 (1962)