Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 36 (1995), No. 2, 281-298.

Gröbner Bases of Lattices, Corner Polyhedra, and Integer Programming

Bernd Sturmfels[1], **Robert Weismantel**, and **Günter M. Ziegler**[2]

Department of Mathematics, University of California at Berkeley
Berkeley, CA 94720, USA
bernd@math.berkeley.edu

Konrad-Zuse-Zentrum für Informationstechnik Berlin (ZIB)
Heilbronner Str. 10, D-10711 Berlin, Germany
weismantel@zib-berlin.de

Fachbereich Mathematik, Sekr. 6-1, Technische Universität Berlin
Strasse des 17. Juni 136, D-10623 Berlin, Germany
ziegler@math.tu-berlin.de

Abstract. There are very close connections between the arithmetic of integer lattices, algebraic properties of the associated ideals, and the geometry and the combinatorics of corresponding polyhedra. In this paper we investigate the generating sets ("Gröbner bases") of integer lattices that correspond to the Gröbner bases of the associated binomial ideals. Extending results by Sturmfels & Thomas, we obtain a geometric characterization of the universal Gröbner basis in terms of the vertices and edges of the associated corner polyhedra. In the special case where the lattice has finite index, the corner polyhedra were studied by Gomory, and there is a close connection to the "group problem in integer programming." We present exponential lower and upper bounds for the maximal size of a reduced Gröbner basis. The initial complex of (the ideal of) a lattice is shown to be dual to the boundary of a certain simple polyhedron.

[1]Partially supported by the National Science Foundation and the David and Lucile Packard Foundation
[2]Partially supported by a "Gerhard-Hess-Prize" of the German Science Foundation (DFG)

1. Introduction

For any integer lattice $\mathcal{L} \subseteq \mathbb{Z}^n$ there is an associated binomial ideal

$$I_{\mathcal{L}} \quad := \quad \langle\, \mathbf{x}^{\mathbf{a}^+} - \mathbf{x}^{\mathbf{a}^-} : \, \mathbf{a} \in \mathcal{L} \,\rangle \quad \subset \quad k[x_1, \ldots, x_n].$$

Here k is any field, and, given any lattice point $\mathbf{a} = (a_1, \ldots, a_n)$, we use the abbreviation

$$\mathbf{x}^{\mathbf{a}^+} - \mathbf{x}^{\mathbf{a}^-} \quad := \quad \prod_{i:a_i>0} x_i^{a_i} - \prod_{j:a_j<0} x_j^{-a_j}.$$

Our aim is to study the combinatorics, geometry, and complexity of Gröbner bases for the ideals $I_{\mathcal{L}}$. These occur (under different guises) in quite diverse areas of application:

- optimization and sensitivity analysis in integer programming [9, 24, 25]
- primary decomposition of general binomial ideals [12]
- certain sampling algorithms in computational statistics [11]
- the computation of short lattice vectors in the geometry of numbers [17],
- the "group problem" in integer programming [14, 21].

The quotient $\mathbb{Z}^n/\mathcal{L}$ can be expressed as the direct sum of a finite abelian group and a free abelian group. What happens when either of these constituents is trivial? If $\mathbb{Z}^n/\mathcal{L}$ is free abelian, then the lattice $\mathcal{L}$ is *saturated* and $I_{\mathcal{L}}$ is a prime ideal [12]. Such primes are called *toric ideals*. Gröbner bases for toric ideals and their application to integer programming have been studied by several authors (including Conti & Traverso [9], Moulinet & Pottier [19], Sturmfels [22], Thomas [24, 25]), and what follows is a natural continuation and extension of their results. Our paradigm in this paper, however, is the other extreme case when $\mathcal{L}$ has finite index in $\mathbb{Z}^n$. This index is the order of the finite abelian group $\mathbb{Z}^n/\mathcal{L}$. It is called the *determinant* of the lattice $\mathcal{L}$ and is denoted $\det(\mathcal{L})$. Here the ideal $I_{\mathcal{L}}$ is zero-dimensional, and the k-dimension of $k[x_1, \ldots, x_n]/I_{\mathcal{L}}$ equals $\det(\mathcal{L})$. The study of such binomial ideals arises naturally from the "group problem in integer programming", as will be explained in Section 6.

A main algorithmic step in understanding an integer lattice $\mathcal{L}$ is the computation of a Gröbner basis for the ideal $I_{\mathcal{L}}$, for a term order that refines the partial order given by a linear functional. Such a Gröbner basis can be computed by an adaptation of Buchberger's classical S-pair reduction algorithm [1, 4, 6, 10]. The action of Buchberger's algorithm in our specific setting can be understood in entirely combinatorial terms. This was worked out by Thomas in her "Geometric Buchberger Algorithm" [25].

In the following section we collect basic properties of the ideals $I_{\mathcal{L}}$. Some of them appear in more general form in [12], but we include proofs for completeness. In Section 3 we give an explicit combinatorial characterization of the reduced Gröbner basis of $I_{\mathcal{L}}$ with respect to any term order. In the toric case this characterization is due to Moulinet & Pottier [19]. In Section 4 we estimate the size of reduced Gröbner bases of a lattice of finite index in $\mathbb{Z}^n$. This size can be exponential even for $n = 3$.

In Section 5 we examine the universal Gröbner basis of $I_{\mathcal{L}}$. We characterize it geometrically in terms of the vertices and edges of the associated corner polyhedra. In Section 6 we turn to applications in integer programming. An algebraic localization relates the "global"

Gröbner basis of an integer program (as studied in [1, 9, 25]) and the "local" situation where $\mathcal{L}$ has finite index in $\mathbb{Z}^n$. Finally, in Section 7 we study the simplicial complex associated with the (radical of the) initial ideal $\mathrm{init}_\omega(I_\mathcal{L})$. As an application we obtain a new algebraic method for computing face posets of simple polyhedra.

2. The ideal of a lattice

The symbol $\mathbb{N}$ denotes the positive integers including 0. We write $\mathbf{0}$ for the zero vector in $\mathbb{N}^n$ and $\mathbf{1}$ for the vector with all components equal to 1. The componentwise partial order on $\mathbb{N}^n$ is denoted by "$\leq$". If we write $\mathbf{u} < \mathbf{v}$ for vectors, then this means $\mathbf{u} \leq \mathbf{v}$ and $\mathbf{u} \neq \mathbf{v}$, that is, $\mathbf{v} - \mathbf{u}$ is nonnegative and at least one coordinate of $\mathbf{v} - \mathbf{u}$ is positive. We use the notation $\mathbf{x}^\mathbf{a}$ for the monomial $x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$, and the usual decomposition $\mathbf{a} = \mathbf{a}^+ - \mathbf{a}^-$ into positive and negative part, where $(\mathbf{a}^+)_i = \max\{a_i, 0\}$, and $\mathbf{a}^- = (-\mathbf{a})^+ \geq \mathbf{0}$. The partial order $\mathbf{a} \leq \mathbf{b}$ corresponds to divisibility of monomials, $\mathbf{x}^\mathbf{a}$ divides $\mathbf{x}^\mathbf{b}$. Note that $\mathbf{a} \leq \mathbf{b}$ implies $\omega\mathbf{a} \leq \omega\mathbf{b}$ for every $\omega \geq \mathbf{0}$. (Here ω denotes a row vector, so $\omega\mathbf{a}$ is a scalar product.) We write $\mathrm{supp}(\mathbf{a}) := \{i : a_i \neq 0\} \subseteq \{1, \ldots, n\}$ for the support of a vector, and similarly for monomials $\mathrm{supp}(\mathbf{x}^\mathbf{a}) := \mathrm{supp}(\mathbf{a})$.

Let $\mathcal{L} \subseteq \mathbb{Z}^n$ be an integral lattice. Our basic object of study is the binomial ideal $I_\mathcal{L} = \langle \mathbf{x}^{\mathbf{a}^+} - \mathbf{x}^{\mathbf{a}^-} : \mathbf{a} \in \mathcal{L} \rangle$. Every generating set of binomials for $I_\mathcal{L}$ corresponds to a generating set of $\mathcal{L}$ (this follows from Corollary 2.4), but the converse is not true, unless we impose a certain positivity hypothesis. (For example, $\{\binom{2}{-1}, \binom{-3}{2}\}$ is a basis for $\mathbb{Z}^2$, but the ideal $\langle x^2 - y, y^2 - x^3 \rangle$ is properly contained in $I_{\mathbb{Z}^2} = \langle x - 1, y - 1 \rangle$.)

Lemma 2.1 *Let $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_N\} \subseteq \mathbb{Z}^n$ be a generating set for the lattice $\mathcal{L}$ (i.e., $\mathcal{L} = \{\sum_{i=1}^N \lambda_i \mathbf{a}_i : \lambda_i \in \mathbb{Z}\}$). If the sum of the vectors in $A \cap \mathbb{N}^n$ has all its coordinates positive, then the ideal $I_\mathcal{L}$ coincides with*

$$I_A \quad := \quad \langle \mathbf{x}^{\mathbf{a}_i^+} - \mathbf{x}^{\mathbf{a}_i^-} : 1 \leq i \leq N \rangle.$$

Proof: Clearly we have $I_A \subseteq I_\mathcal{L}$. The following computation will show that the two ideals coincide. For $\mathbf{a}, \mathbf{b} \in A \cap \mathbb{N}^n$ we have $\mathbf{x}^\mathbf{a} - 1, \mathbf{x}^\mathbf{b} - 1 \in I_A$, and thus also

$$\mathbf{x}^{\mathbf{a}+\mathbf{b}} - 1 \quad = \quad \mathbf{x}^\mathbf{a}(\mathbf{x}^\mathbf{b} - 1) \; + \; (\mathbf{x}^\mathbf{a} - 1) \quad \in \quad I_A.$$

Hence for every integer $M > 0$ the ideal I_A contains an element $\mathbf{x}^\mathbf{m} - 1$ with $m_i \geq M$ for all i. Thus, for $\mathbf{g} = \mathbf{g}^+ - \mathbf{g}^- \in \mathcal{L}$, we can use

$$\mathbf{x}^{\mathbf{g}^+} - \mathbf{x}^{\mathbf{g}^-} \quad = \quad -(\mathbf{x}^{\mathbf{g}^+} - \mathbf{x}^{\mathbf{g}^-})(\mathbf{x}^\mathbf{m} - 1) \quad + \quad \mathbf{x}^\mathbf{m}(\mathbf{x}^{\mathbf{g}^+} - \mathbf{x}^{\mathbf{g}^-})$$

to see that is suffices to show $\mathbf{x}^\mathbf{m}(\mathbf{x}^{\mathbf{g}^+} - \mathbf{x}^{\mathbf{g}^-}) \in I_A$ for large enough $m_i \geq M$. Now since $\mathbf{a}_i$ and $-\mathbf{a}_i$ determine the same binomial (up to a sign), we may assume that $\mathbf{g}$ is written in the form $\mathbf{g} = \sum_{k=1}^K \mathbf{a}_{i_k} \in \mathcal{L}$ (i.e., as a sum of copies of the vectors $\mathbf{a}_i$ with coefficients all 1). With this we write

$$\begin{aligned} \mathbf{x}^\mathbf{m}(\mathbf{x}^{\mathbf{g}^+} - \mathbf{x}^{\mathbf{g}^-}) \quad &= \quad \mathbf{x}^{\mathbf{m}+\mathbf{g}^-}(\mathbf{x}^\mathbf{g} - 1) \quad = \quad \mathbf{x}^{\mathbf{m}+\mathbf{g}^-}(\prod_{k=1}^K \mathbf{x}^{\mathbf{a}_{i_k}} - 1) \\ &= \quad \sum_{k=1}^K (\mathbf{x}^{\mathbf{m}+\mathbf{g}^- - \mathbf{a}_{i_k}^-} \prod_{l=1}^{k-1} \mathbf{x}^{\mathbf{a}_{i_l}})(\mathbf{x}^{\mathbf{a}_{i_k}^+} - \mathbf{x}^{\mathbf{a}_{i_k}^-}), \end{aligned}$$

where the last sum is clearly in I_A, provided $m_i \geq M$ is large enough for all i. □

The "positive vector condition" on A is satisfied in two basic situations: first, if A is a nonnegative basis for the lattice $\mathcal{L}$ (with $\mathbf{a}_i \geq \mathbf{0}$ for all i), and second, if A is *any* basis of $\mathcal{L}$ together with a strictly positive vector in $\mathcal{L}$. Such a positive vector exists if $\mathcal{L}$ has finite index in $\mathbb{Z}^n$ but not in general (see also Proposition 3.7).

We will use $\succ$ to denote *term orders* on $\mathbb{Z}^n$, that is, additive total orders such that $\mathbf{a} \succ \mathbf{0}$ for all $\mathbf{a} \in \mathbb{N}^n \backslash \mathbf{0}$. (We refer to [4] and [10] for the basics about term orders, Gröbner bases, S-pairs, reduction, and the Buchberger algorithm.) It is known (Robbiano [20, Sect. 2]) that every term order can be obtained by refinement of a linear function, that is, for every $\succ$ there exists a nonzero, nonnegative vector $\omega \in (\mathbb{R}_{\geq 0})^n$ such that $\omega\mathbf{a} > \omega\mathbf{b}$ implies $\mathbf{a} \succ \mathbf{b}$. The refinement is in general obtained lexicographically via a sequence of linear functions. However, every Gröbner basis can also be obtained from a "rank one" term order of the form $\succ_\omega$, for some $\omega \in (\mathbb{R}_{>0})^n$ whose components ω_i are linearly independent over the rationals, by Mora & Robbiano [18, Thm. 2.7]. Thus, we do not loose anything when, from now on, we assume that $\succ$ is represented by a positive weight vector ω. We will sometimes write $\text{init}_\omega(f)$ instead of $\text{init}_\succ(f)$ to denote the initial (leading) monomial of a polynomial f with respect to $\succ = \succ_\omega$.

For every nonzero binomial in $I_\mathcal{L}$ the initial monomial is given by

$$\text{init}_\succ(\mathbf{x}^{\mathbf{a}^+} - \mathbf{x}^{\mathbf{a}^-}) \quad := \quad \begin{cases} \mathbf{x}^{\mathbf{a}^+} & \text{if } \mathbf{a}^+ \succ \mathbf{a}^-, \\ \mathbf{x}^{\mathbf{a}^-} & \text{otherwise.} \end{cases}$$

Using the term order $\succ$, we define the *positive part* of the lattice:

$$\mathcal{L}^{\succ \mathbf{0}} \quad := \quad \{\mathbf{a} \in \mathcal{L} : \ \mathbf{a} \succ \mathbf{0}\},$$

where $\mathbf{a} \succ \mathbf{0}$ is equivalent to $\mathbf{a}^+ \succ \mathbf{a}^-$. We can view $\text{init}_\succ$ as a map from $\mathcal{L}^{\succ \mathbf{0}}$ to $\mathbb{N}^n$.

We recall that a subset $\mathcal{F}$ of an ideal I is a *Gröbner basis* of I if and only if the set of initial terms $\{\text{init}_\succ(f) : f \in \mathcal{F}\}$ generates the *initial ideal* $\text{init}_\succ(I) := \langle \text{init}(f) : f \in I \rangle$. If $\mathcal{F}$ is minimal and no trailing term appearing in any $f \in \mathcal{F}$ lies in $\text{init}_\succ(I)$ then $\mathcal{F}$ is unique and is called the *reduced Gröbner basis* of I with respect to $\succ$. Every reduced Gröbner basis of a binomial ideal I consists of binomials. Indeed, starting with a binomial generating set of I, the Buchberger algorithm produces a reduced binomial Gröbner basis, since S-pairs and reduction are binomial-friendly operations.

Proposition 2.2 *The initial ideal of a lattice ideal is given by*

$$\text{init}_\succ(I_\mathcal{L}) \quad = \quad \langle\, \mathbf{x}^{\mathbf{u}^+} \ : \ \mathbf{u} \in \mathcal{L}^{\succ \mathbf{0}}\, \rangle.$$

Proof: Clearly, the right hand side is contained in the left hand side. For the converse let $\mathbf{x}^\mathbf{a}$ be a minimal generator of $\text{init}_\succ(I_\mathcal{L})$. Since the reduced Gröbner basis consists of binomials, there exists a monomial $\mathbf{x}^\mathbf{b}$ with $\omega\mathbf{b} < \omega\mathbf{a}$ such that $\mathbf{x}^\mathbf{a} - \mathbf{x}^\mathbf{b}$ appears in the reduced Gröbner basis of $I_\mathcal{L}$. We have $\mathbf{a} - \mathbf{b} \in \mathcal{L}$ because the operations of forming S-pairs and reduction (of binomials) preserve the lattice spanned by the differences of the exponent vectors. Let $\mathbf{u} := \mathbf{a} - \mathbf{b}$ and write $\mathbf{u} = \mathbf{u}^+ - \mathbf{u}^- \in \mathcal{L}$. Since $\omega\mathbf{u}^+ > \omega\mathbf{u}^-$, we have $\mathbf{x}^{\mathbf{u}^+} \in \text{init}_\succ(I_\mathcal{L})$. By construction $\mathbf{x}^{\mathbf{u}^+}$ divides $\mathbf{x}^\mathbf{a}$, and since $\mathbf{x}^\mathbf{a}$ is a minimal generator of $\text{init}_\succ(I_\mathcal{L})$, we conclude $\mathbf{x}^\mathbf{a} = \mathbf{x}^{\mathbf{u}^+}$, as desired. □

This proposition motives the following definition.

Definition 2.3 *Fix a term order $\succ$ on $\mathbb{N}^n$. A* Gröbner basis of the lattice $\mathcal{L}$ *is a family $\mathcal{G} \subseteq \mathcal{L}^{\succ \mathbf{0}}$ such that $\{\mathbf{x}^{\mathbf{g}^+} - \mathbf{x}^{\mathbf{g}^-} : \mathbf{g} \in \mathcal{G}\}$ is a Gröbner basis of $I_{\mathcal{L}}$. We denote by* $\mathrm{RGB}_{\succ}(\mathcal{L})$ *the set of vectors in $\mathcal{L}^{\succ \mathbf{0}}$ that corresponds to the reduced Gröbner basis of $I_{\mathcal{L}}$.*

Corollary 2.4 *A binomial $\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}}$ is contained in $I_{\mathcal{L}}$ if and only if $\mathbf{a} - \mathbf{b} \in \mathcal{L}$.*

Proof: We must show the only-if direction. Suppose $\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}} \in I_{\mathcal{L}}$. Then the monomials $\mathbf{x}^{\mathbf{a}}$ and $\mathbf{x}^{\mathbf{b}}$ have the same normal form, say $\mathbf{x}^{\mathbf{c}}$, under reduction with respect to the reduced Gröbner basis of $I_{\mathcal{L}}$. A simple calculation shows that reduction of a monomial by lattice binomials preserves the residue class of the exponent vector with respect to the lattice spanned by the binomials in the Gröbner basis. Therefore $\mathbf{a} - \mathbf{c} \in \mathcal{L}$ and $\mathbf{b} - \mathbf{c} \in \mathcal{L}$, and hence $\mathbf{a} - \mathbf{b} \in \mathcal{L}$. $\square$

3. Combinatorics of the reduced Gröbner basis

In this section we present a combinatorial characterization of the reduced Gröbner basis of a lattice $\mathcal{L}$, for a fixed term order $\succ\ =\ \succ_{\omega}$. This characterization was first proved by Moulinet & Pottier [19, Thm. 3] in the toric case. We here extend their result to arbitrary integer lattices.

Fix a term order $\succ$ on $\mathbb{N}^n$. We introduce a new partial order $\sqsupset$ on $\mathbb{Z}^n$ as follows:

$$\mathbf{a} \sqsupset \mathbf{b} \quad :\Longleftrightarrow \quad \begin{array}{ll} \text{either} & \mathbf{a}^+ \geq \mathbf{b}^+ \text{ and } \mathbf{a}^+ \neq \mathbf{b}^+, \\ \text{or} & \mathbf{a}^+ = \mathbf{b}^+ \text{ and } \mathbf{a}^- \succ \mathbf{b}^-. \end{array}$$

Note that this partial order uses and extends the componentwise partial order "$\leq$" on $\mathbb{N}^n$. The extension is different from $\leq$ on $\mathbb{Z}^n$, which is why we need a different symbol. The crucial point is that the partial order $\sqsupset$ depends on the term order $\succ$.

Lemma 3.1 *The partial order $\sqsupset$ has no infinite antichains, and no infinite decreasing chains. Thus $\sqsupset$ defines a well-ordering of $\mathbb{Z}^n$, and thus, in particular, of $(\mathbb{Z}^n)^{\succ \mathbf{0}}$.*

Proof: This is immediate from the fact that both $\geq$ and $\succ$ do not have infinite antichains, or infinite decreasing chains, on the positive orthant $\mathbb{N}^n$. $\square$

If P is any subset of $\mathbb{Z}^n$ then $\mathrm{MIN}_{\sqsupset}(P)$ denotes the set of minimal elements in P under the partial order $\sqsupset$. The main result of this section expresses the reduced Gröbner basis of a lattice as the image of its "positive half" under the operator $\mathrm{MIN}_{\sqsupset}$.

Theorem 3.2 *The reduced Gröbner basis of the lattice $\mathcal{L}$ equals the set of all minimal elements of $\mathcal{L}^{\succ \mathbf{0}}$ in the partial order $\sqsupset$:*

$$\mathrm{RGB}_{\succ}(\mathcal{L}) \quad = \quad \mathrm{MIN}_{\sqsupset}(\mathcal{L}^{\succ \mathbf{0}}).$$

Proof: With Proposition 2.2 and Corollary 2.4, we see that $\mathrm{MIN}_{\sqsupset}(\mathcal{L}^{\succ \mathbf{0}})$ is a minimal Gröbner basis, whose elements cannot be reduced. $\square$

Note that in Theorem 3.2 one *cannot* replace $\sqsupset$ by the similar partial order $\sqsupset'$ on $\mathbb{Z}^n$ defined by

$$\mathbf{a} \sqsupset' \mathbf{b} \quad :\Longleftrightarrow \quad \begin{array}{ll} \text{either} & \mathbf{a}^+ > \mathbf{b}^+, \\ \text{or} & \mathbf{a}^+ = \mathbf{b}^+, \text{ and } \mathbf{a}^- > \mathbf{b}^-. \end{array}$$

which is independent of $\succ$. Since the term order $\succ$ is a linear extension of the divisibility order $>$, we see that $\sqsupset'$ is coarser than $\sqsupset$ and hence

$$\mathrm{RGB}_\succ(\mathcal{L}) \;=\; \mathrm{MIN}_\sqsupset(\mathcal{L}^{\succ\mathbf{0}}) \;\subseteq\; \mathrm{MIN}_{\sqsupset'}(\mathcal{L}^{\succ\mathbf{0}}).$$

However, the right hand side may be much larger than the left hand side, as the following example shows. For $N \geq 1$ let $\mathcal{L} \subset \mathbb{Z}^3$ denote the kernel of the 1×3-matrix $[N, 1, 1]$, and let "$\succ$" be the purely lexicographic term order. The reduced Gröbner basis is a lattice basis, $\mathrm{MIN}_\sqsupset(\mathcal{L}^{\succ\mathbf{0}}) \;=\; \{(1,0,-N),(0,1,-1)\}$, while

$$\mathrm{MIN}_{\sqsupset'}(\mathcal{L}^{\succ\mathbf{0}}) \;=\; \mathrm{MIN}_\sqsupset(\mathcal{L}^{\succ\mathbf{0}}) \;\cup\; \{\,(1,-i,-N+i) \,:\, i = 1,2,\ldots,N-1\}.$$

A basic problem in the algorithmic theory of numbers is finding short lattice vectors. Here is a Gröbner basis perspective on this problem.

Corollary 3.3 *The set* $\mathrm{MIN}_\sqsupset(\mathcal{L}^{\succ\mathbf{0}})$ *contains the shortest nonnegative vector in* $\mathcal{L}\cap\mathbb{N}^n$*, that is, the vector that is minimal with respect to the linear ordering on* $\mathcal{L}\cap\mathbb{N}^n$ *given by the term ordering* $\succ$*. In particular, if we take a term order that refines the order of monomials by degrees (like the degree-lexicographic term order), then* $\mathcal{G}$ *contains a vector* $\mathbf{g} \in \mathcal{L}\cap\mathbb{N}^n\backslash\{\mathbf{0}\}$ *that minimizes the sum of coordinates* $\sum_{i=1}^n g_i$.

Proof: If $\mathbf{b}$ is the unique nonzero vector in $\mathcal{L}\cap\mathbb{N}^n$ that minimizes ω, then it cannot be reducible: if we could reduce it by $\mathbf{a} \in \mathcal{L}^{\succ\mathbf{0}}$ with $\mathbf{a} \neq \mathbf{b}$, then we would immediately obtain a nonnegative vector of smaller weight. □

Corollary 3.4 *The nonnegative vectors in a reduced Gröbner basis of* $\mathcal{L}$ *have disjoint supports; in particular,* $\mathrm{RGB}_\succ(\mathcal{L})$ *contains at most n nonnegative vectors. If it contains a strictly positive vector, then it does not contain any other nonnegative vectors.*

Proof: If $\mathbf{b}', \mathbf{b}'' \in \mathrm{RGB}_\succ(\mathcal{L})\cap\mathbb{N}^n$ have $b_i', b_i'' > 0$ for some i, with $\mathbf{b}' \succ \mathbf{b}''$, then we can use the vector $\mathbf{b}' - \mathbf{b}''$ to reduce $\mathbf{b}'$: a contradiction. □

However, although we have just seen that $\mathrm{RGB}_\succ(\mathcal{L}) \cap \mathbb{N}^n$ cannot be large, we will show in Section 4 that the cardinality of $\mathrm{RGB}_\succ(\mathcal{L})$ can be exponentially large. If $\mathcal{L}$ is a lattice of finite index in $\mathbb{Z}^n$, then the complement of the initial ideal has the following geometric interpretation.

Corollary 3.5 *Let* $\mathcal{L}$ *be a lattice of finite index in* $\mathbb{Z}^n$*. Then the set*

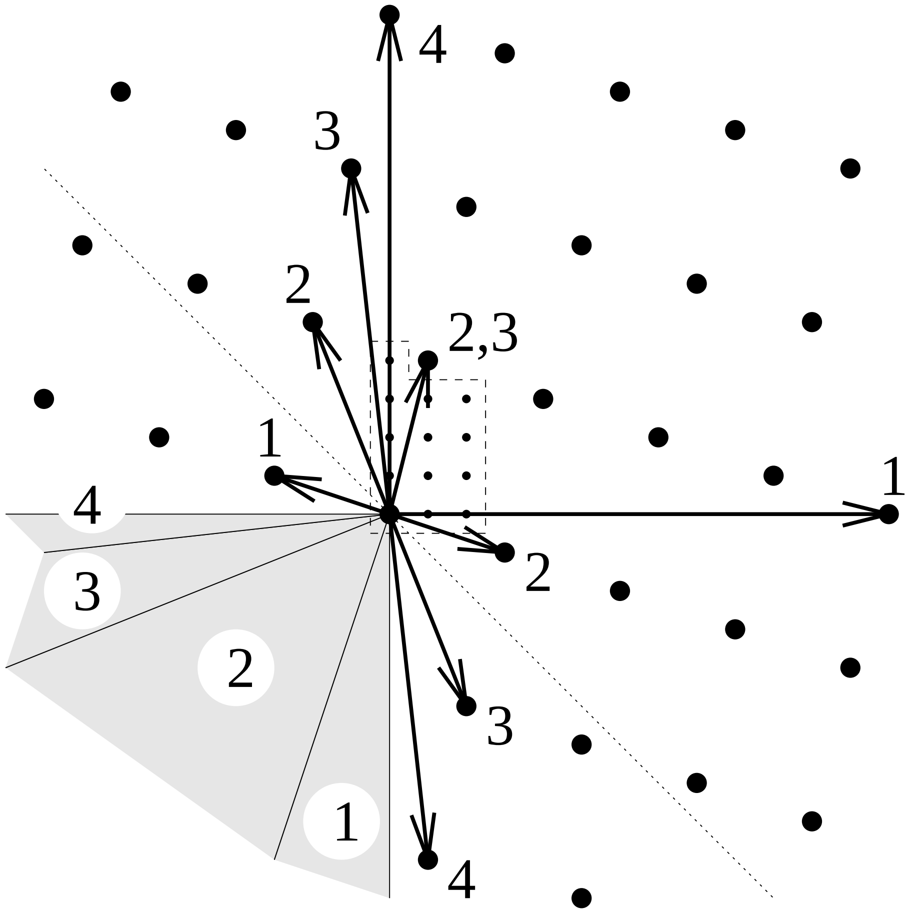
$$\mathbf{S} \;:=\; \Big\{\mathbf{a} \in \mathbb{N}^n : \textit{ there is no } \mathbf{b} \in \mathrm{MIN}_\sqsupset(\mathcal{L}^{\succ\mathbf{0}}) \textit{ with } \mathbf{b}^+ \leq \mathbf{a}\Big\}$$

is a fundamental domain of $\mathcal{L}$*, and thus has cardinality* $\det(\mathcal{L})$.

Proof: A monomial $\mathbf{x}^\mathbf{a}$ is called *standard* if it does not lie in $\mathrm{init}_\succ(I_\mathcal{L})$, that is, if $\mathbf{a}$ lies in the set $\mathbf{S}$.

Every monomial reduces to a standard monomial via Buchberger reduction. Thus every point in $\mathbb{N}^n$ is mapped to a unique point in the fundamental domain by a sequence of steps which correspond to subtraction of lattice vectors. Furthermore, if two monomials $\mathbf{x}^\mathbf{a}$ and $\mathbf{x}^\mathbf{b}$ are in the same equivalence class modulo $\mathcal{L}$ and (without loss of generality) $\mathbf{a}-\mathbf{b} \in \mathcal{L}^{\succ \mathbf{0}}$, then $\mathbf{x}^\mathbf{a}$ is not standard. This proves that there is a bijection between $\mathbb{Z}^n/\mathcal{L}$ and the set $\mathbf{S}$ of standard monomials. ☐

Example 3.6 Let $\mathcal{L}_A \subseteq \mathbb{Z}^2$ be the 2-dimensional lattice of determinant 13 generated by the columns of $A = \begin{pmatrix} 1 & 4 \\ 4 & 3 \end{pmatrix}$.



There are four different reduced Gröbner bases for the corresponding zero-dimensional ideal $I_\mathcal{L}$. For example, if we choose a total degree term order that refines the weight vector $\omega = (1,1)$, then $\mathcal{L}^{\succ \mathbf{0}}$ is the set of lattice points above the dotted line. The corresponding Gröbner basis is

$$\mathcal{G}_{(1,1)} \quad = \quad \{xy^4 - 1,\ x^3 - y,\ y^5 - x^2\}.$$

The corresponding three vectors in the Gröbner basis of $\mathcal{L}$ are marked by "2"; the cone of all vectors $-\omega$ such that ω defines this Gröbner basis is also labelled "2". The dashed line surrounds the integral points corresponding to the standard monomials.

We close this section with a well-known algorithmic technique for computing the reduced Gröbner basis $\mathrm{RGB}_{\succ}(\mathcal{L})$. (For toric ideals this technique was introduced in [9].) We embed $\mathbb{Z}^n$ into $\mathbb{Z}^{n+1}$ by adding a zeroth coordinate, so that $\mathbb{Z}^{n+1} = \mathbb{Z}\mathbf{e}_0 \oplus \mathbb{Z}^n$. Any term order $\succ$ on $\mathbb{Z}^n$ is extended to $\mathbb{Z}^{n+1}$ as follows: if $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^n$ then $a_0\mathbf{e}_0 + \mathbf{a} \succ b_0\mathbf{e}_0 + \mathbf{b}$ if and only if either $a_0 > b_0$, or $a_0 = b_0$ and $\mathbf{a} \succ \mathbf{b}$.

Proposition 3.7 *Given any lattice $\mathcal{L} \subset \mathbb{Z}^n$, we let $\widehat{\mathcal{L}}$ denote the sublattice of $\mathbb{Z}^{n+1}$ spanned by $\mathcal{L}$ and the vector $\mathbf{e} = \sum_{i=0}^n \mathbf{e}_i$. Then*

$$\mathrm{RGB}_{\succ}(\mathcal{L}) \quad = \quad \mathrm{RGB}_{\succ}(\widehat{\mathcal{L}}) \cap \mathbb{Z}^n.$$

To compute $\mathrm{RGB}_{\succ}(\widehat{\mathcal{L}})$ from any basis for $\mathcal{L}$ one can use the remark after the proof of Lemma 2.1: we have $\mathbf{e}$ as a strictly positive vector in $\widehat{\mathcal{L}}$. When computing $\mathrm{RGB}_{\succ}(\mathcal{L})$ in practice, many improvements are possible (and yet to be explored). For instance, the experiments reported in Hosten & Sturmfels [15] show that a significant speed-up can be achieved by precomputing a basis of $\mathcal{L}$ which is reduced in the sense of Lovász [17].

4. On the size of the Gröbner basis

In this section we examine the size of reduced Gröbner bases of a finite index sublattice $\mathcal{L} \subseteq \mathbb{Z}^n$. We provide upper and lower bounds which are exponential in the bit complexity of a basis for $\mathcal{L}$, even for fixed rank $n = 3$.

Proposition 4.1 *The cardinality of any reduced Gröbner basis of an n-dimensional lattice $\mathcal{L} \subseteq \mathbb{Z}^n$ is bounded above by $(n-1)\det(\mathcal{L}) + 1$.*

Proof: At most one of the minimal generators of $\mathrm{init}_\omega(I_{\mathcal{L}})$ has full support $\{1, \ldots, n\}$. All other minimal generators $\mathbf{x}^{\mathbf{a}}$ contain at most $n-1$ variables x_i. The monomial $\mathbf{x}^{\mathbf{a}}/x_i$ is one of the $\det(\mathcal{L})$ many standard monomials. Hence the number of minimal generators of $\mathrm{init}_\omega(I_{\mathcal{L}})$ not having full support is at most the product $(n-1)\det(\mathcal{L})$. □

The slightly weaker upper bound $n\det(\mathcal{L})$ is given by Faugère, Gianni, Lazard & Mora [13, Cor. 2.1]. A similar but more careful argument gives the even better upper bound $(n-2)\det(\mathcal{L}) + n + 1$. Bounds for $|\mathcal{G}|$ in terms of n and $\det(\mathcal{L})$ that are essentially best possible follow from theorems in extremal set theory. The sharp bounds are quite complicated (see Clements [8]), but they imply the following.

Theorem 4.2 *The cardinality #RGB of the reduced Gröbner basis of an n-dimensional lattice $\mathcal{L} \subseteq \mathbb{Z}^n$ is bounded above by the implication*

$$\det(\mathcal{L}) \quad < \quad \binom{k}{n} \qquad \Longrightarrow \qquad \#\mathrm{RGB} \quad < \quad \binom{k}{n-1}$$

for any integer $k \geq n$. In particular, for a fixed number n of variables we have

$$\#\mathrm{RGB} \quad = \quad O\Big((\det(\mathcal{L}))^{1-1/n} \Big).$$

Proof: In the terminology of extremal set theory, see Clements [8], the initial monomials of a reduced Gröbner basis #RGB correspond to an "antichain $\mathcal{A}$ of multisets" on the ground set $\{1, 2, \ldots, n\}$ with unrestricted multiplicities $k_i = \infty$. The associated downset $\underline{\mathcal{A}}$ corresponds to the set of all monomials dividing one of the initial monomials of #RGB, so the standard monomials correspond to $\underline{\mathcal{A}} \backslash \mathcal{A}$, and we have #RGB $= |\mathcal{A}|$ and $\det(\mathcal{L}) = |\underline{\mathcal{A}} \backslash \mathcal{A}|$.

Thus we can apply the results of Clements [7, 8]. Essentially the claim follows from the fact that if $\mathcal{A}$ is the set of *all* multisets of a given fized size, then $\mathcal{A}$ has the smallest downset among all antichains of the same size $|\mathcal{A}|$ (see [7, Theorem on p. 154], [8, p. 256]). Explicitly, we get from [8, Theorem on p. 257] that if #RGB $= |\mathcal{A}| \geq \left\langle {n \atop h-1} \right\rangle = \binom{n+h-2}{n-1}$, then $\det(\mathcal{L}) = |\underline{\mathcal{A}} \backslash \mathcal{A}| \geq \sum_{i=0}^{h-2} \left\langle {n \atop i} \right\rangle = \sum_{i=0}^{h-2} \binom{n+i-1}{i} = \binom{n+h-2}{n}$, using that $\left\langle {n \atop i} \right\rangle = \binom{n-1+i}{i}$ for $k_i = \infty$. Now we set $k = n + h - 2$. □

(One may note that the preceding proposition and theorem are more general: with the same proofs, they give upper bounds for the maximal size of a minimal Gröbner basis of a zero-dimensional ideal in terms of the degree and the number of variables.)

We next present a lower bound which matches the upper bound in Proposition 4.1 up to a factor of 2, provided n is allowed to vary.

Proposition 4.3 *For each integer $n > 1$ there exists a lattice $\mathcal{L}_n \subseteq \mathbb{Z}^n$ with $\det(\mathcal{L}_n) = n+1$ such that the reduced Gröbner basis of $\mathcal{L}_n$ with respect to the total degree order has cardinality $\frac{1}{2}n(n+1) = \frac{1}{2}n \det(\mathcal{L}_n)$.*

Proof: Consider the lattice

$$\mathcal{L}_n \quad := \quad \{ (u_1, u_2, \ldots, u_n) \in \mathbb{Z}^n \, : \, u_1 + 2u_2 + 3u_3 + \cdots + nu_n \equiv 0 \mod n+1 \}.$$

With respect to the total degree ordering on $k[x_1, x_2, \ldots, x_n]$, the reduced Gröbner basis of $\mathcal{L}_n$ equals

$$\{ \underline{x_i x_j} - x_{i+j} \, : \, i+j \leq n \} \; \cup \; \{ \underline{x_i x_j} - 1 \, : \, i+j = n+1 \} \\ \cup \; \{ \underline{x_i x_j} - x_{i+j-n-1} \, : \, i+j \geq n+2 \}.$$

Indeed, there are $\frac{1}{2}n(n+1)$ elements in this set, and each of them is easily seen to lie in $I_{\mathcal{L}_n}$. They form a Gröbner basis because precisely $n+1 = \det(\mathcal{L}_n)$ monomials are not divisible by any of the underlined leading terms. These standard monomials are $1, x_1, x_2, \ldots, x_n$. □

We next present an exponential lower bound for fixed dimension $n = 3$.

Theorem 4.4 *The reduced Gröbner basis of a finite index sublattice $\mathcal{L}$ of $\mathbb{Z}^3$ may have exponential size in the bit complexity of a positive basis of $\mathcal{L}$*

Consider the following family of trivariate ideals:

$$I_r \quad := \quad \langle x^r y^r z^r - 1, \; x^{r-1} y^{r+1} z^{r-1}, \; z^{r-2} - 1 \rangle, \qquad r \geq 4.$$

The bit complexity of this presentation is $O(\log(r))$. The vector space dimension of the residue ring $k[x, y, z]/I_r$ equals $2r(r-2)$, which is the determinant of the corresponding lattice

$$\mathcal{L}_r \quad = \quad \mathbb{Z}\langle (r, r, r), (r-1, r+1, r-1), (0, 0, r-2) \rangle \quad \subset \; \mathbb{Z}^3.$$

Theorem 4.4 is implied by the following lemma:

Lemma 4.5 *The reduced Gröbner basis of I_r with respect to degree lexicographic term order equals the following set of $2r-2$ binomials:*

$$\begin{aligned}\{\, \underline{xz} - y,\ \underline{x^{r-2}} - y^{r-2},\ \underline{y^{2r}} - 1\} \ &\cup\ \{\, \underline{y^i z^{r-2-i}} - x^i \ :\ i = 0,\ldots,r-3\} \\ &\cup\ \{\underline{x^i y^{2r-i}} - z^{r-2-i} \ :\ i = 1,\ldots,r-3\}.\end{aligned}$$

Proof: This set lies in I_r because the vectors

$$(1,-1,1),\ (r-2,0,2-r),\ (0,2r,0),\ (-i,i,r-2-i),\ (i,2r-i,r-2-i)$$

lie in the lattice $\mathcal{L}_r$. It suffices to show that there are precisely $2r(r-2)$ monomials outside the ideal generated by the underlined leading monomials. We give the complete list of these monomials in three disjoint groups:

(a) $x^a y^b$ for $0 \le a \le r-3$, $0 \le b \le r+2$,

(b) $x^b y^a$ for $r+3 \le a \le 2r-1$, $0 \le b \le 2r-a-1$, and

(c) $y^b z^a$ for $1 \le a \le r-3$, $0 \le b \le r-3-a$.

Each monomial not listed under (a), (b) or (c) is a multiple of one of the underlined terms. The group (a) consists of $(r+3)(r-2)$ monomials, while (b) and (c) consist of $\binom{r-2}{2}$ monomials each. Thus we have $(r+3)(r-2) + 2\binom{r-2}{2} = 2r(r-2)$ in total. □

We close with the observation that $n = 3$ is best possible.

Remark 4.6 *Every reduced Gröbner basis of a sublattice $\mathcal{L} \subset \mathbb{Z}^2$ has at most three elements.*

Proof: Let $\mathcal{G}$ be the reduced Gröbner basis of $I_\mathcal{L}$ with respect to ω. If $\mathrm{rank}(\mathcal{L}) \le 1$ then $I_\mathcal{L}$ is principal and $\mathcal{G}$ is a singleton. If $\mathrm{rank}(\mathcal{L}) = 2$ then the minimal generators of $\mathrm{init}_\omega(I_\mathcal{L})$ must have distinct supports. For the support $\{1,2\}$ this holds by Corollary 3.4, for the supports $\{1\}$ and $\{2\}$ this holds because any two univariate monomials are comparable with respect to divisibility. □

5. Geometry of the universal Gröbner basis

The *universal Gröbner basis* of a sublattice $\mathcal{L} \subseteq \mathbb{Z}^n$ is the union of all reduced Gröbner bases of the ideal $I_\mathcal{L}$ as the cost function varies. In this section we study this set from the point of view of polyhedral geometry. Our results are direct generalizations of Theorem 5.1 in [24], which dealt with the special case where $\mathcal{L}$ is saturated and contains no positive vector. Also the proof techniques in this section are extensions of the techniques in [24]. To begin with, we show that the universal Gröbner basis is a finite set, and we present a method for computing a superset of it.

Given any sublattice $\mathcal{L}$ of $\mathbb{Z}^n$, we define a sublattice $\hat{\mathcal{L}}$ of $\mathbb{Z}^{2n}$ as follows:

$$\hat{\mathcal{L}} \quad := \quad \{\, \mathbf{u} \oplus (-\mathbf{u}) \in \mathbb{Z}^{2n} \ :\ \mathbf{u} \in \mathcal{L}\,\}.$$

Here $\mathbb{Z}^{2n}$ is to be identified with $\mathbb{Z}^n \oplus \mathbb{Z}^n$. Note that any basis of $\mathcal{L}$ lifts immediately to a basis of $\hat{\mathcal{L}}$. However, $\hat{\mathcal{L}}$ has no positive basis, so that one needs the algorithm referred to after Proposition 3.7 to compute a generating set for the corresponding ideal $I_{\hat{\mathcal{L}}}$. We view $I_{\hat{\mathcal{L}}}$ as an ideal in the polynomial ring $k[x_1,\ldots,x_n,y_1,\ldots,y_n]$.

Proposition 5.1 *Let* $\mathbf{x^a} - \mathbf{x^b}$ *be an element of* some *reduced Gröbner basis of* $I_{\mathcal{L}}$*. Then* $\mathbf{x^a y^b} - \mathbf{x^b y^a}$ *appears in* every *reduced Gröbner basis of* $I_{\widehat{\mathcal{L}}}$*. Thus if* $\widehat{\mathcal{G}}$ *is any reduced Gröbner basis of* $I_{\widehat{\mathcal{L}}}$*, then* $\{\mathbf{a} \in \mathbb{Z}^n : \mathbf{x}^{\mathbf{a}^+}\mathbf{y}^{\mathbf{a}^-} - \mathbf{x}^{\mathbf{a}^-}\mathbf{y}^{\mathbf{a}^+} \in \widehat{\mathcal{G}}\}$ *is a finite set that contains the universal Gröbner basis of* $\mathcal{L}$*.*

Proof: Suppose there exists a reduced Gröbner basis of $I_{\widehat{\mathcal{L}}}$ which does not contain $\mathbf{x^a y^b} - \mathbf{x^b y^a}$. Then there exists $\mathbf{x^c y^d} - \mathbf{x^d y^c}$ in $I_{\widehat{\mathcal{L}}}$ such that $\mathbf{x^c y^d}$ divides $\mathbf{x^a y^b}$. This implies $\mathbf{c} \leq \mathbf{a}$ and $\mathbf{d} \leq \mathbf{b}$. Given any term order, the binomial $\mathbf{x^a} - \mathbf{x^b}$ can be reduced by $\mathbf{x^c} - \mathbf{x^d} \in I_{\mathcal{L}}$. □

For our main result in this section we shall need the following lemma.

Lemma 5.2 *Let* $\mathbf{x^a} - \mathbf{x^b}$ *be an element of the reduced Gröbner basis of* $\mathcal{L}$ *with respect to* ω*. If* $\mathbf{c}$ *is a point in* $(\mathbf{a} + \mathcal{L}) \cap \mathbb{N}^n$ *with* $\omega\mathbf{c} \leq \omega\mathbf{a}$ *and* $\mathbf{c} \neq \mathbf{a}$*, then* $\mathrm{supp}(\mathbf{a}) \cap \mathrm{supp}(\mathbf{c}) = \emptyset$*.*

Proof: Suppose $\mathbf{x^a}$ and $\mathbf{x^c}$ have a common factor x_i, and consider the binomial $f := (\mathbf{x^a} - \mathbf{x^c})/x_i = \mathbf{x}^{\mathbf{a}-e_i} - \mathbf{x}^{\mathbf{c}-e_i} \in I_{\mathcal{L}}$. If $\omega\mathbf{c} < \omega\mathbf{a}$, then $\mathbf{x}^{\mathbf{a}-e_i}$ is the leading term of f, which is a contradiction to the hypothesis that $\mathbf{x^a}$ is a minimal generator of $\mathrm{init}_\omega(I_{\mathcal{L}})$. If $\omega\mathbf{a} = \omega\mathbf{c}$, then $\mathbf{a} = \mathbf{c}$. □

For any vector $\mathbf{b} \in \mathbb{Z}^n$ the translate $\mathbf{b} + \mathcal{L}$ is considered as a residue class of the quotient $\mathbb{Z}^n/\mathcal{L}$. With this residue class we associate the polyhedron

$$P[\mathbf{b}] \quad := \quad \mathrm{conv}\Big((\mathbf{b} + \mathcal{L}) \ \cap \ \mathbb{N}^n\Big)$$

If $\mathcal{L}$ has finite index in $\mathbb{Z}^n$ then there are $\det(\mathcal{L})$ residue classes. In that case the polyhedra $P[\mathbf{b}]$ are called the *corner polyhedra* of $\mathcal{L}$. They were introduced and studied by Gomory in connection with the *group problem* in integer programming [14],[21, p. 363]. We shall discuss this problem in Section 6. We also define the polyhedron

$$Q \quad := \quad \mathrm{conv}(\mathcal{L} \ \cap \ \mathbb{N}^n \setminus \{0\}).$$

In [24] and [25] the polyhedra $P[\mathbf{b}]$ were called *fibers*, and it was assumed that they are polytopes (i.e. bounded). This assumption holds if and only if Q is the empty set.

Theorem 5.3 *Let* $\mathcal{L} \subset \mathbb{Z}^n$ *be any integer lattice and* $I_{\mathcal{L}}$ *its ideal. Then the universal Gröbner basis of* $I_{\mathcal{L}}$ *consists of the following two sets:*

- *the binomials* $\mathbf{x^a} - 1$*, where* $\mathbf{a}$ *is a vertex of the polyhedron* $Q = \mathrm{conv}(\mathcal{L} \cap \mathbb{N}^n \setminus \{0\})$*,*
- *the binomials* $\mathbf{x^a} - \mathbf{x^b}$*, where* $\mathbf{a} - \mathbf{b}$ *is a primitive vector in* $\mathcal{L}$*,* $\mathrm{supp}(\mathbf{a}) \cap \mathrm{supp}(\mathbf{b}) = \emptyset$*, and* $\mathrm{conv}\{\mathbf{a}, \mathbf{b}\}$ *is an edge of the corner polyhedron* $P[\mathbf{a}] = P[\mathbf{b}]$*.*

Proof: With our discussion in Section 3, we can see that the two types of binomials listed above have to lie in the universal Gröbner basis. Namely, the binomials of the first kind are needed (for a suitable function ω) by Corollary 3.3. For binomials of the second type we can choose an objective function ω such that $\mathbf{x^a}$ is nonstandard and $\mathbf{x^b}$ is the only monomial of smaller weight in the lattice equivalence class of $\mathbf{a}$. To see that $\mathbf{a} - \mathbf{b}$ is contained in $\mathrm{UGB}(I_{\mathcal{L}})$, it suffices to show that $\mathbf{x^a}$ is a minimal generator of $\mathrm{init}_\omega(I_{\mathcal{L}})$. If not, then there exists $\mathbf{x}^{\mathbf{a}'} - \mathbf{x}^{\mathbf{b}'}$ with leading term $\mathbf{x}^{\mathbf{a}'}$ such that $\mathbf{a}' < \mathbf{a}$. Then $\mathbf{a} - \mathbf{a}' + \mathbf{b}'$ is a lattice point in $P[\mathbf{a}]$ having smaller weight than $\mathbf{a}$, hence it must coincide with $\mathbf{b}$. We conclude that $\mathbf{a}-\mathbf{b}=\mathbf{a}'-\mathbf{b}'$, which gives a contradiction to $\mathrm{supp}(\mathbf{a})\cap\mathrm{supp}(\mathbf{b})=\emptyset$.

For the converse consider any element $\mathbf{x}^{\mathbf{a}}-\mathbf{x}^{\mathbf{b}}$ with leading term $\mathbf{x}^{\mathbf{a}}$ in the reduced Gröbner basis of $I_{\mathcal{L}}$ with respect to ω. If $\mathbf{b}=\mathbf{0}$ then $\mathbf{a}$ is the unique minimum of the linear functional ω over all nonnegative nonzero elements of $\mathcal{L}$, which means that $\mathbf{a}$ is a vertex of Q. Hence it remains to analyze the case $\mathbf{b}\neq\mathbf{0}$. We must show that $\mathrm{conv}\{\mathbf{a},\mathbf{b}\}$ is an edge of its corner polyhedron. We may assume that all coordinates of ω are positive. Let ω' be the restriction of ω to the complement of $\mathrm{supp}(\mathbf{a})$, that is, $\omega'_i=0$ if $\mathbf{a}_i>0$ and $\omega'_i=\omega_i$ if $\mathbf{a}_i=0$. Our hypotheses imply $0=\omega'\mathbf{a}<\omega'\mathbf{b}=\omega\mathbf{b}<\omega\mathbf{a}$. We define the positive weight vector

$$\omega'' \quad := \quad (\omega(\mathbf{a}-\mathbf{b}))\cdot\omega'+(\omega'(\mathbf{b}-\mathbf{a}))\cdot\omega,$$

which has the property $\omega''(\mathbf{a}-\mathbf{b})=0$ by construction, and thus $\omega''\mathbf{a}=\omega''\mathbf{b}$. In order to prove that $\mathrm{conv}\{\mathbf{a},\mathbf{b}\}$ is an edge, it suffices to show $\omega''\mathbf{a}<\omega''\mathbf{c}$ for all $\mathbf{c}\in\mathbb{N}^n\backslash\{\mathbf{a},\mathbf{b}\}$ with $\mathbf{c}-\mathbf{a}\in\mathcal{L}$.

We distinguish two cases. First suppose that $\omega\mathbf{c}\leq\omega\mathbf{a}$. Then $\mathrm{supp}(\mathbf{a})\cap\mathrm{supp}(\mathbf{c})=\emptyset$ by Lemma 5.2, and hence $\omega\mathbf{c}=\omega'\mathbf{c}$. We also know $\omega\mathbf{c}>\omega\mathbf{b}$, otherwise $\mathbf{x}^{\mathbf{a}}-\mathbf{x}^{\mathbf{b}}$ wouldn't be in the reduced Gröbner basis (by Theorem 3.2). This implies

$$\omega''\mathbf{c} \;=\; (\omega(\mathbf{a}-\mathbf{b})+\omega'(\mathbf{b}-\mathbf{a}))\omega\mathbf{c} \;>\; (\omega(\mathbf{a}-\mathbf{b})+\omega'(\mathbf{b}-\mathbf{a}))\omega\mathbf{b} \;=\; \omega''\mathbf{b} \;=\; \omega''\mathbf{a}.$$

Next consider the case $\omega\mathbf{c}>\omega\mathbf{a}$. Then we have $\omega'\mathbf{c}\geq 0=\omega'\mathbf{a}$, and thus

$$\omega''\mathbf{c} \;=\; (\omega(\mathbf{a}-\mathbf{b}))\omega'\mathbf{c}+(\omega'(\mathbf{b}-\mathbf{a}))\omega\mathbf{c} \;>\; (\omega(\mathbf{a}-\mathbf{b}))\omega'\mathbf{a}+(\omega'(\mathbf{b}-\mathbf{a}))\omega\mathbf{a} \;=\; \omega''\mathbf{a}.$$

This completes the proof. □

For any ideal $I\subset k[x_1,\ldots,x_n]$ there is a natural equivalence relation on the space $\mathbb{R}^n$ of weight vectors: We say that ω and ω' are *equivalent* if $\mathrm{init}_\omega(I)=\mathrm{init}_{\omega'}(I)$. It was shown by Mora & Robbiano [18] that the equivalence classes are the cones of a polyhedral fan in $\mathbb{R}^n$, called the *Gröbner fan* of I. If I is homogeneous then the Gröbner fan is complete, and it was shown by Bayer & Morrison [2] that the Gröbner fan is the normal fan of a polytope in $\mathbb{R}^n$, called the *state polytope* of I. By an extension of the arguments in [2], one can see that for any ideal I (not necessarily homogeneous) there exists a polyhedron in $\mathbb{R}^n$ whose normal fan equals the Gröbner fan. Any such polyhedron will be called a *state polyhedron* for I.

Theorem 5.4 *The Gröbner fan of $I_{\mathcal{L}}$ is the common refinement of the normal fans of the corner polyhedra $P[\mathbf{b}]$, where $\mathbf{b}$ ranges over $\mathbb{Z}^n/\mathcal{L}$.*

Proof: It suffices to show that two sufficiently generic weight vectors $\omega,\omega'\in\mathbb{R}^n_+$ define the same initial ideal of I if and only if they support the same vertex of $P[\mathbf{b}]$ for all $\mathbf{b}$. (See [28] for the basic polyhedral notions used here).

Given a polynomial $f\in k[x_1,\ldots,x_n]$, we write $\mathrm{nf}_\omega(f)$ for its normal form modulo the reduced Gröbner basis of $I_{\mathcal{L}}$ with respect to ω. Note that if $f=\sum_{\mathbf{a}}c_{\mathbf{a}}\mathbf{x}^{\mathbf{a}}$ is the monomial expansion, then $\mathrm{nf}_\omega(f)=\sum_a c_a\mathrm{nf}_\omega(\mathbf{x}^{\mathbf{a}})$; in other words, $\mathrm{nf}_\omega(\cdot)$ is a k-linear map.

Now, given $\omega,\omega'\in\mathbb{R}^n_+$ we have (cf. Mora & Robbiano [18])

$$\begin{aligned}\mathrm{init}_\omega(I)=\mathrm{init}_{\omega'}(I) \quad&\Longleftrightarrow\quad \mathrm{nf}_\omega(f)=\mathrm{nf}_{\omega'}(f)\ \text{ for all } f\in k[x_1,\ldots,x_n] \qquad (1)\\ &\Longleftrightarrow\quad \mathrm{nf}_\omega(\mathbf{x}^{\mathbf{a}})=\mathrm{nf}_{\omega'}(\mathbf{x}^{\mathbf{a}})\ \text{ for all monomials } \mathbf{x}^{\mathbf{a}},\ a\in\mathbb{N}^n.\end{aligned}$$

However, the normal form of a monomial $\mathbf{x}^{\mathbf{a}}$ modulo the binomial ideal I is another monomial, say $\mathbf{x}^{\mathbf{c}}$. The vector $\mathbf{c} \in \mathbb{N}^n$ is characterized by the property that $\mathbf{c} \equiv \mathbf{a} \bmod \mathcal{L}$, and $\mathbf{c}$ has minimum weight $\omega\mathbf{c}$ with this property. Equivalently, $\mathbf{c}$ is the unique vertex of $P[\mathbf{a}]$ supported by ω. Therefore, (1) is equivalent to the statement that ω and ω' support the same vertex of $P[\mathbf{a}]$ for all $\mathbf{a}$ in $\mathbb{N}^n$. □

We recall that the normal fan of a Minkowski sum of two polyhedra is the common refinement of the normal fans of the two polyhedra. This fact extends to the Minkowski sum of any finite number of polyhedra, and it even extends to Minkowski integrals of infinite families of polyhedra (see e.g. [5]). This implies the following corollaries.

Corollary 5.5 *Let $\mathcal{L}$ be a sublattice of finite index in $\mathbb{Z}^n$. Then the Minkowski sum of Gomory's corner polyhedra*

$$\sum_{\gamma \in \mathbb{Z}^n/\mathcal{L}} \mathrm{conv}(\gamma \cap \mathbb{N}^n).$$

is a state polyhedron for the associated zero-dimensional ideal $I_{\mathcal{L}}$.

Corollary 5.6 *Let $\mathcal{L}$ be any sublattice of $\mathbb{Z}^n$, and let $d\mathbf{b}$ be any probability measure with support $\mathbb{N}^n$ such that $\int \mathbf{b} d\mathbf{b}$ is a (finite) point in $\mathbb{R}^n_+$. Then the Minkowski integral $\int P[\mathbf{b}]d\mathbf{b}$ is a state polyhedron for the ideal $I_{\mathcal{L}}$.*

6. Localization in integer programming

The problem to minimize a linear functional over the nonnegative elements in a congruence class of a lattice of finite index in $\mathbb{Z}^m$ was studied by Gomory [14]. It is known as the *group problem* in integer programming (see Schrijver [21, p. 364]). We will show how the group problem appears as a certain algebraic localization from the general integer programming problem. This establishes an algorithmic bridge between the two extreme cases discussed in the introduction, namely, saturated lattices and lattices of finite index.

Our presentation follows [21, p. 364]. It is informal in the sense that no theorems or propositions are stated. Let A be an integer $d \times n$-matrix of rank d, $\mathbf{b} \in \mathbb{Z}^d$ and $\omega \in \mathbb{R}^n$. The general integer programming problem can be written as follows:

$$\text{minimize } \omega \cdot \mathbf{u} \text{ subject to } \mathbf{u} \in \mathbb{Z}^n,\ A\mathbf{u} = \mathbf{b},\ \mathbf{u} \geq 0. \tag{2}$$

Let $\mathbf{u}^0 \in \mathbb{Z}^n$ be any feasible (but not optimal) solution of (2). Suppose we are also given a basic optimal solution $\mathbf{u}^* \in \mathbb{R}^n$ for the LP-relaxation

$$\text{minimize } \omega \cdot \mathbf{u} \text{ subject to } \mathbf{u} \in \mathbb{R}^n,\ A\mathbf{u} = \mathbf{b},\ \mathbf{u} \geq 0. \tag{3}$$

There exists a column basis $\{i_1, \ldots, i_d\} \subset \{1, 2, \ldots, n\}$ of A such that $\mathrm{supp}(\mathbf{u}^*) \subseteq \{i_1, \ldots, i_d\}$. We replace ω by the unique vector $\tilde{\omega} \in \mathbb{R}^n$ with support in $[n] \backslash \{i_1, \ldots, i_d\}$ such that $\omega - \tilde{\omega}$ lies in the row space of A. Let $\pi : \mathbb{Z}^n \to \mathbb{Z}^{n-d}$ denote the projection onto the nonbasic coordinates. The lattice $\mathcal{L} := \pi(\ker_{\mathbb{Z}}(A))$ has finite index in $\mathbb{Z}^{n-d}$. Identify $\tilde{\omega}$ with its image in $\mathbb{Z}^{n-d}$, set $\tilde{\mathbf{b}} := \pi(\mathbf{u}^0)$, and consider the group problem:

$$\text{minimize } \tilde{\omega} \cdot \mathbf{v} \text{ subject to } \mathbf{v} \in \mathbb{Z}^{n-d},\ \mathbf{v} \geq 0,\ \mathbf{v} \equiv \tilde{\mathbf{b}} \ (\mathrm{mod} \mathcal{L}). \tag{4}$$

This problem is a relaxation of (2). Indeed, if $\mathbf{v}^1$ is an optimal solution to (4), then we can choose $\mathbf{u}^1 \in \mathbb{Z}^n$ with $\pi(\mathbf{u}^1) = \mathbf{v}^1$ and $A\mathbf{u}^1 = \mathbf{b}$. If $\mathbf{u}^1 \geq 0$ then $\mathbf{u}^1$ is an optimal solution to (2), otherwise $\omega\mathbf{u}^1 \geq \omega\mathbf{u}^*$ is a new lower bound for the optimum value of (2).

These transformations have a natural reformulation in the setting of Gröbner bases. We recall the Gröbner basis approach to integer programming as presented in [1, 9, 25, 15, 23, 27, 26]. Let $\mathcal{L}' \subset \mathbb{Z}^n$ be the kernel of A. Then $\mathcal{L}'$ is saturated and its ideal $I_{\mathcal{L}'} \subset k[x_1, \ldots, x_n]$ is the *toric ideal of* A. The optimal solution of the integer program (2) is obtained by reducing the monomial $\mathbf{x}^{\mathbf{u}^0}$ with respect to the reduced Gröbner basis $\mathrm{RGB}_\omega(\mathcal{L}')$.

Let $X = \{x_1, \ldots, x_n\} \setminus \{x_{i_1}, \ldots, x_{i_d}\}$ and consider the homomorphism

$$\rho \, : \, k[x_1, \ldots, x_n] \; \rightarrow \; k[X]$$

which maps the variables $x_{i_1}, \ldots, x_{i_d}$ to 1 and leaves the other variables unchanged. (This amounts to localizing at the prime ideal $\langle x_j \, : \, j \notin \{i_1, \ldots, i_d\}\rangle$, whence the title of this section.) We have the following relation among the toric ideal and the zero-dimensional ideal:

$$\rho(\, I_{\mathcal{L}'}\,) \quad = \quad I_{\mathcal{L}}.$$

The punchline of our discussion is that, instead of computing $\mathrm{RGB}_\omega(\mathcal{L}')$, it is much easier to compute $\mathrm{RGB}_{\tilde{\omega}}(\mathcal{L})$, the reduced Gröbner basis of a zero-dimensional binomial ideal. Indeed, the "local Gröbner basis" $\mathrm{RGB}_{\tilde{\omega}}(\mathcal{L})$ has typically much smaller cardinality than the "global Gröbner basis" $\mathrm{RGB}_\omega(\mathcal{L}')$. The solution to the relaxation (4) is obtained by reducing the monomial $x^{\tilde{\mathbf{b}}}$ modulo $\mathrm{RGB}_{\tilde{\omega}}(\mathcal{L})$.

That the relaxation (4) may fail to have the same optimum as (2) can be explained by the fact that the "global" initial ideal $\mathrm{init}_\omega(I_{\mathcal{L}'})$ is smaller than the preimage in $k[x_1, \ldots, x_n]$ of the "localized" initial ideal

$$\mathrm{init}_{\tilde{\omega}}(I_{\mathcal{L}}) \;\; = \;\; \mathrm{init}_{\tilde{\omega}}(\rho(I_{\mathcal{L}'})) \;\; = \;\; \rho(\mathrm{init}_{\tilde{\omega}}(I_{\mathcal{L}'})). \tag{5}$$

More precisely, the set of right hand sides $\mathbf{b}$ for which (4) fails to solve (2) corresponds to embedded primary components of the ideal $\mathrm{init}_\omega(I_A)$. This correspondence is studied in [23, Chapter 12].

We remark that, in spite of the identity (5), the <u>reduced</u> Gröbner basis $\mathrm{RGB}_{\tilde{\omega}}(\mathcal{L})$ is generally <u>not</u> a subset of $\rho(\mathrm{RGB}_\omega(\mathcal{L}'))$. For instance, take $n = 4, d = 1$, $A = [13, 19, 21, 29]$ and $\omega = \tilde{\omega} = (41, 50, 10, 0)$. Here ρ maps the basic variable x_4 to 1, and $\mathcal{L}$ is a sublattice of index 29 in $\mathbb{Z}^3$. In binomial notation, we have

$$\mathrm{RGB}_\omega(\mathcal{L}) \quad = \quad \{x_3^{17} - x_2^2, x_2 x_3^6 - 1, x_2^3 - x_3^{11}, x_1 - x_3^2\}.$$

The global Gröbner basis $\mathrm{RGB}_\omega(\mathcal{L}')$ has 14 elements. The local Gröbner basis element $x_2^3 - x_3^{11}$ does not appear in $\rho(\mathrm{RGB}_\omega(\mathcal{L}'))$.

7. The initial complex of a lattice

For any ideal $I \subseteq k[x_1, \ldots, x_n]$ and any term order $\omega \in \mathbb{R}^n$ there is an associated simplicial complex $\Delta_\omega(I)$ with vertex set $\{1, 2, \ldots, n\}$. It is called the *initial complex* [16] and is defined as follows: a subset $F \subseteq \{1,\ldots,n\}$ is a face of $\Delta_\omega(I)$ if there is no polynomial $f \in I$ whose initial monomial $\mathrm{init}_\omega(f)$ has support F. Equivalently, $\Delta_\omega(I)$ is the simplicial complex whose Stanley-Reisner ideal is the radical of $\mathrm{init}_\omega(I)$.

It is our objective to determine the *initial complex of a lattice* $\mathcal{L} \subset \mathbb{Z}^n$. By this we mean $\Delta_\omega(\mathcal{L}) := \Delta_\omega(I_\mathcal{L})$. Let $\mathcal{L}_\mathbb{R} := \mathcal{L} \otimes \mathbb{R}$ be the real vector space spanned by $\mathcal{L}$, and let $\mathcal{L}_\mathbb{R}^\perp$ be its orthogonal complement in $\mathbb{R}^n$. We define the closed convex polyhedron

$$\mathcal{P}_\omega \quad := \quad \mathbb{R}^n_+ \ \cap \ (\omega + \mathcal{L}_\mathbb{R}^\perp).$$

Lemma 7.1 *If the weight vector $\omega \in \mathbb{R}^n$ defines a term order for the ideal $I_\mathcal{L}$ then the polyhedron $\mathcal{P}_\omega$ is simple.*

Proof: Let $d = \mathrm{rank}(\mathcal{L})$ and suppose $\mathcal{P}_\omega$ is not simple. Then there exists a point $\mathbf{u} \in \mathcal{P}_\omega$ such that $|\mathrm{supp}(\mathbf{u})| \leq d-1$. This implies the existence of a nonzero vector $\mathbf{a} \in \mathcal{L}$ with $\mathrm{supp}(\mathbf{a}) \cap \mathrm{supp}(\mathbf{u}) = \emptyset$. Moreover, we may choose $\mathbf{a}$ to have minimal support (i.e., $\mathbf{a}$ is a *circuit* of $\mathcal{L}_\mathbb{R}$). This implies $\mathbf{u}\mathbf{a}^+ = \mathbf{u}\mathbf{a}^- = 0$. Moreover, since $\mathbf{u} - \omega \in \mathcal{L}_\mathbb{R}^\perp$, we have $\omega\mathbf{a} = \mathbf{u}\mathbf{a} = 0$. Therefore both $\mathbf{x}^{\mathbf{a}^+}$ and $\mathbf{x}^{\mathbf{a}^-}$ are contained in the monomial ideal $\mathrm{init}_\omega(I)$. Hence there exists $\mathbf{b} \in \mathcal{L}$ such that $\omega\mathbf{b} = \mathbf{u}\mathbf{b} > 0$ and $\mathbf{x}^{\mathbf{b}^+}$ divides $x^{\mathbf{a}^+}$. Since $\mathbf{u}$ is nonnegative we conclude $0 < \mathbf{u}\mathbf{b}^+ \leq \mathbf{u}\mathbf{a}^+$. This is a contradiction. □

Our main result in this section gives an algebraic expression for the combinatorial structure of the polyhedron $\mathcal{P}_\omega$. In the special case where $I_\mathcal{L}$ is a homogeneous prime ideal this theorem was proved in [22]. The following version is considerably more general and its proof more direct. We thank Serkan Hosten for suggesting the use of LP-duality in proving Theorem 7.2.

Theorem 7.2 *The initial complex $\Delta_\omega(\mathcal{L})$ equals the simplicial complex that is polar to the boundary complex of the simple polyhedron $\mathcal{P}_\omega$.*

Corollary 7.3 *The initial complex of a lattice is either a sphere or a ball.*

Proof: Our assertion is equivalent to the following statement: A subset $F \subseteq \{1,\ldots,n\}$ is a face of $\Delta_\omega(\mathcal{L})$ if and only if there exists $\mathbf{u} \in \mathcal{P}_\omega$ such that $\mathrm{supp}(\mathbf{u}) = \{1,\ldots,n\}\backslash F$. We write $\mathbf{e}_F := \sum_{i\in F} \mathbf{e}_i$ for the incidence (row) vector of a subset F.

Let A be an integer $d \times n$-matrix whose rows form a basis for the lattice $\mathcal{L}$, and let $\mathbf{b} := A\omega$. By linear programming duality [21, Cor. 7.1.g],

$$\min\{\,\mathbf{e}_F \cdot \mathbf{u} \ : \ \mathbf{u} \in \mathbb{R}^n, \mathbf{u} \geq 0, A\mathbf{u} = \mathbf{b}\,\} \quad = \quad \max\{\,\mathbf{v}\cdot\mathbf{b} \ : \ \mathbf{v} \in \mathbb{R}^d, \mathbf{v}A \leq \mathbf{e}_F\,\}.$$

This translates into the equivalent statement

$$\min\{\,\mathbf{e}_F \cdot \mathbf{u} \ : \ \mathbf{u} \in \mathcal{P}_\omega\,\} \quad = \quad \max\{\,\mathbf{a}\cdot\omega \ : \ \mathbf{a} \in \mathcal{L}_\mathbb{R}, \, \mathbf{a} \leq \mathbf{e}_F\,\}.$$

Clearly, the left hand side is nonnegative. It is zero if and only if there is a point $\mathbf{u} \in \mathcal{P}_\omega$ whose support is contained in $\{1,\ldots,n\}\backslash F$. By Lemma 7.1, the family $\{\mathrm{supp}(\mathbf{u}) \colon \mathbf{u} \in \mathcal{P}_\omega\}$ is closed under taking supersets, so that "is contained in" can be replaced by "equals" in the previous sentence. The maximum on the right hand side is positive if and only if there exists $\mathbf{a} = \mathbf{a}^+ - \mathbf{a}^- \in \mathcal{L}$ with $\mathbf{a}^+\omega > \mathbf{a}^-\omega$ and $\mathrm{supp}(\mathbf{a}^+) \subseteq F$. This holds if and only if there exists $f \in I_\mathcal{L}$ with $\mathrm{supp}(\mathrm{init}_\omega(f)) \subseteq F$, which is equivalent to F not being a face of $\Delta_\omega(\mathcal{L})$. □

As an application we obtain the following algebraic method for computing the minimal nonfaces of a simple polytope.

Corollary 7.4 *Let $A = (a_{ij})$ be a nonnegative integer $d \times n$-matrix with no zero column, and let $\mathbf{b} \in \mathbb{R}^d$ be a general point in the cone spanned by the columns of A. Then $P = \{\mathbf{u} \in \mathbb{R}^n : \mathbf{u} \geq 0, A\mathbf{u} = \mathbf{b}\}$ is a simple polytope. Its boundary complex is polar to the initial complex, with respect to any weight vector $\omega \in P$, of the ideal*

$$I \quad = \quad \langle \prod_{j=1}^{n} x_{ij}^{a_{ij}} \; - \; 1 \;\; : \;\; i = 1, \ldots, d \rangle.$$

Proof: The assumption that A is nonnegative and has no zero column implies (using Lemma 2.1) that $I = I_{\mathcal{L}}$ where $\mathcal{L}$ is the lattice spanned by the rows of A. Corollary 7.4 now follows from Theorem 7.2 by identifying $\mathbf{u} = \omega$. □

In order to compute the (supports of the) vertices of the polytope P, we need to find the minimal associated primes of the initial ideal $\mathrm{init}_\omega(I)$.

Corollary 7.5 *Using the notation above, we have the prime decomposition*

$$\mathrm{Rad}(\mathrm{init}_\omega(I)) \quad = \quad \bigcap_{\mathbf{v}\,\mathrm{vertex\,of}\,P} \langle x_i : i \in \mathrm{supp}(\mathbf{v}) \rangle.$$

Naturally these corollaries are most useful for practical computations when the ideal $\mathrm{init}_\omega(I)$ is square-free to begin with. A sufficient condition for this property can be given using [24, Thm. 3.17]: if $\mathcal{L}$ is the row span of a *unimodular* matrix then $\mathrm{init}_\omega(I)$ is a radical ideal. We illustrate our techniques for such a unimodular example.

Example 7.6 *(A Simple 3×5-Transportation Polytope)*
Let $X = (x_{ij})$ be a 3×5-matrix of indeterminates, and let $\mathcal{L}$ be the sublattice of $\mathbb{Z}^{15} \cong \mathbb{Z}^3 \otimes \mathbb{Z}^5$ defined by the binomial ideal

$$\begin{aligned} I_{\mathcal{L}} \quad = \quad & \langle x_{11}x_{12}x_{13}x_{14}x_{15} - 1, x_{21}x_{22}x_{23}x_{24}x_{25} - 1, x_{31}x_{32}x_{33}x_{34}x_{35} - 1, \\ & x_{11}x_{21}x_{31} - 1, x_{12}x_{22}x_{32} - 1, x_{13}x_{23}x_{33} - 1, x_{14}x_{24}x_{34} - 1, x_{15}x_{25}x_{35} - 1 \rangle. \end{aligned}$$

Let ω be the 3×5-matrix with all entries equal to 1. This weight matrix defines the total degree term order for $I_{\mathcal{L}}$. The polytope P_ω is the set consisting of all real nonnegative 3×5-matrices with all row sums equal to 5 and all column sums equal to 3. In order to compute this *transportation polytope*, we compute the reduced Gröbner basis of $I_{\mathcal{L}}$ with respect to ω. It consists of 50 binomials of degrees three and four. Since $\mathcal{L}$ is unimodular, the initial ideal is square-free:

$$\mathrm{init}_\omega(I_{\mathcal{L}}) \;=\; \langle x_{11}x_{12}x_{13}x_{14}, x_{11}x_{12}x_{13}x_{15}, x_{11}x_{12}x_{14}x_{15}, \ldots, x_{32}x_{33}x_{34}x_{35} \rangle.$$

Using a computer algebra system such as MACAULAY [3] it takes a fraction of a second to determine the prime decomposition as in Corollary 7.5. We find that the simple polytope P_ω has dimension 7 and has 360 vertices. By computing the numerator of the Hilbert series of $\mathrm{init}_\omega(I_{\mathcal{L}})$, we find its h-vector to be $h(P_\omega) = (1, 7, 28, 79, 130, 79, 28, 7, 1)$.

References

[1] W. W. Adams & P. Loustaunau: *An Introduction to Gröbner Bases,* American Mathematical Society, Graduate Studies in Math., Vol. III, 1994.

[2] D. Bayer & I. Morrison: *Gröbner bases and geometric invariant theory I, J. Symbolic Computation* **6** (1988), 209-217.

[3] D. Bayer & M. Stillman: *Macaulay: a computer algebra system for algebraic geometry,* available by anonymous ftp from `zariski.harvard.edu`.

[4] T. Becker & V. Weispfenning: *Gröbner Bases: A Computational Approach to Commutative Algebra,* Graduate Texts in Mathematics **141**, Springer-Verlag 1993.

[5] L. J. Billera & B. Sturmfels: *Fiber polytopes, Annals of Mathematics* **135** (1992), 527-549.

[6] B. Buchberger: *Gröbner bases: an algorithmic method in polynomial ideal theory,* in: N.K. Bose (ed.), "Multidimensional Systems Theory", D. Reidel 1985, 184-232.

[7] G. F. Clements: *The minimal number of basic elements in a multiset antichain J. Combinatorial Theory*, Ser. A **25** (1978), 153-162.

[8] G. F. Clements: *Multiset antichains having minimal downsets, J. Combinatorial Theory*, Ser. A **48** (1988), 255-258.

[9] P. Conti & C. Traverso: *Buchberger algorithm and integer programming,* Proceedings AAECC-9 (New Orleans), Springer LNCS **539**, 1991, pp. 130-139.

[10] D. A. Cox, J. B. Little & D. O'Shea: *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra, Undergraduate Texts in Mathematics*, Springer-Verlag, New York 1992.

[11] P. Diaconis, B. Sturmfels: *Algebraic algorithms for sampling from conditional distributions, Annals of Statistics*, to appear.

[12] D. Eisenbud & B. Sturmfels: *Binomial ideals,* preprint 1994, 44 pages.

[13] J. C. Faugère, P. Gianni, D. Lazard & T. Mora: *Efficient computation of zero-dimensional Gröbner bases by change of ordering, J. Symbolic Computation* **16** (1993), 329-344.

[14] R. E. Gomory: *Some polyhedra related to combinatorial problems, Linear Algebra and its Applications* **2** (1969), 451-455.

[15] S. Hosten & B. Sturmfels: *GRIN: An implementation of Gröbner bases for integer programming,* Proceedings IPCO IV (Copenhagen), Springer LNCS, 1995, to appear.

[16] M. Kalkbrener & B. Sturmfels: *Initial complexes of prime ideals, Advances in Mathematics*, to appear.

[17] A. K. Lenstra, H. W. Lenstra & L. Lovász: *Factoring polynomials with rational coefficients, Math. Annalen* **261** (1982), 513–534.

[18] T. Mora & L. Robbiano: *The Gröbner fan of an ideal, J. Symbolic Computation* **6** (1988), 183-208.

[19] C. Moulinet & L. Pottier: *Gröbner bases of toric ideals: properties, algorithms, and applications,* preprint, INRIA Sophia Antipolis, 10 pages.

[20] L. Robbiano: *On the theory of graded structures, J. Symbolic Computation* **2** (1986), 139-170.

[21] A. Schrijver: *Theory of Linear and Integer Programming,* Wiley-Interscience, Chichester 1986.

[22] B. Sturmfels: *Gröbner bases of toric varieties, Tôhoku Math. Journal* **43** (1991), 249-261.

[23] B. Sturmfels: *Gröbner Bases and Convex Polytopes,* American Mathematical Society, Providence, R.I., to appear in 1996.

[24] B. Sturmfels & R. R. Thomas: *Variation of cost functions in integer programming,* preprint, Cornell University 1994, 31 pages.

[25] R. R. Thomas: *A geometric Buchberger algorithm for integer programming, Mathematics of Operations Research*, to appear.

[26] R. R. Thomas & R. Weismantel: *A multivariate grading and truncated Gröbner bases for toric ideals in integer programming,* Preprint SC 95-09, ZIB-Berlin, March 1995, 13 pages.

[27] R. Urbaniak, R. Weismantel & G. M. Ziegler: *A variant of the Buchberger algorithm for integer programming,* Preprint SC 94-29, ZIB-Berlin, January 1995, 19 pages.

[28] G. M. Ziegler: *Lectures on Polytopes,* Graduate Texts in Mathematics **152**, Springer-Verlag, New York 1995.

Received April 28, 1995