Journal of Symbolic Computation 47 (2012) 1297–1308

Contents lists available at SciVerse ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Computing Gröbner bases of pure binomial ideals via submodules of $\mathbb{Z}^n$

Giandomenico Boffi [a], Alessandro Logar [b,1]

[a] *Libera Università LUSPIO, Via Cristoforo Colombo 200, 00145 Roma, Italy*

[b] *Dipartimento di Matematica e Informatica, Università di Trieste, via Valerio 12/1, 34127 Trieste, Italy*

ARTICLE INFO

Article history:
Received 4 April 2011
Accepted 14 June 2011
Available online 29 December 2011

Keywords:
Binomial ideal
Gröbner basis
Polyhedral cone
Buchberger algorithm
Smith normal form
Hilbert basis

ABSTRACT

A binomial ideal is an ideal of the polynomial ring which is generated by binomials. In a previous paper, we gave a correspondence between pure saturated binomial ideals of $K[x_1, \ldots, x_n]$ and submodules of $\mathbb{Z}^n$ and we showed that it is possible to construct a theory of Gröbner bases for submodules of $\mathbb{Z}^n$. As a consequence, it is possible to follow alternative strategies for the computation of Gröbner bases of submodules of $\mathbb{Z}^n$ (and hence of binomial ideals) which avoid the use of Buchberger algorithm. In the present paper, we show that a Gröbner basis of a $\mathbb{Z}$-module $M \subseteq \mathbb{Z}^n$ of rank m lies into a finite set of cones of $\mathbb{Z}^m$ which cover a half-space of $\mathbb{Z}^m$. More precisely, in each of these cones C, we can find a suitable subset $Y(C)$ which has the structure of a finite abelian group and such that a Gröbner basis of the module M (and hence of the pure saturated binomial ideal represented by M) is described using the elements of the groups $Y(C)$ together with the generators of the cones.

0. Introduction

In Boffi and Logar (2007) we have introduced the notion of Gröbner bases of submodules of $\mathbb{Z}^n$. The motivation being the attempt to avoid using Buchberger algorithm in the computation of Gröbner bases of (saturated) pure binomial ideals. It has been known for a long time that the Buchberger algorithm for toric ideals is a purely combinatorial process involving lattice vectors, (Thomas, 1995). And in fact the combinatorics of Boffi and Logar (2007) partly overlaps with that of Sturmfels et al. (1995).

E-mail addresses: giandomenico.boffi@luspio.it (G. Boffi), logar@units.it (A. Logar).
[1] Tel.: +39 040 5582646; fax: +39 040 5582636.

0747-7171/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2011.12.046

But the shift from ideals to lattices (submodules of $\mathbb{Z}^n$ in our language) has been seen by others as a way to perform the Buchberger algorithm in a more efficient way, while we aim at computing Gröbner bases of submodules of $\mathbb{Z}^n$ in a way completely independent of polynomial ideals, and amenable to new algorithmic strategies.

In this paper we extend to submodules of any rank the strategy sketched in Boffi and Logar (2007), Section 5 for the computation of the Gröbner bases of rank 2 submodules of $\mathbb{Z}^n$. It turns out that a variety of ingredients is required and that an interesting role is played by some finite abelian groups.

A further inquiry is still necessary (and planned) in order to mix the ingredients in the most efficient way, and then weigh the pros and cons of our approach. But we think it useful to make our approach known, because it offers a different point of view, even though its practical importance has yet to be ascertained.

An outline of this article goes as follows. Section 1 fixes the notation and recalls some facts, including the relationship with saturated pure binomial ideals given in Boffi and Logar (2007). Section 2 deals with cones in $\mathbb{Q}^n$ and $\mathbb{Z}^n$. Readers acquainted with discrete convex geometry may go over this section in a rather fast way. Section 3 illustrates the general strategy for the computation of the Gröbner bases of submodules of $\mathbb{Z}^n$. Section 4 works out in detail a significant example having all the features discussed in Section 3. The section ends with some final remarks, opening some vistas for future work.

We thank the referees for their suggestions.

The computer algebra system CoCoA (CoCoA Team, 0000) has been used for some examples related to this article.

1. Preliminaries and recollections

Elements of $\mathbb{Z}^n$ (or $\mathbb{Q}^n$) will be considered as row vectors. If $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_n)$ are in $\mathbb{Z}^n$ (or in $\mathbb{Q}^n$), we say that $a <_{\mathrm{Lex}} b$ if the first nonzero coordinate (from the left) of $a - b$ is negative. Let V be an $n \times n$ nonsingular matrix V of integers. Then we can define a linear order on $\mathbb{Z}^n$ by: $a <_V b$ if and only if $aV <_{\mathrm{Lex}} bV$.

If the matrix V is obtained from the $n \times n$ identity matrix after a permutation of the columns, then we say that the corresponding order on $\mathbb{Z}^n$ is of lexicographic type. Clearly, if $V = I_n$, then we get the order Lex defined above.

If $a \in \mathbb{Z}^n$, then we have $a = a^+ - a^-$, where any component of a^+ and of a^- is positive or zero; a^+ and a^- are uniquely determined by a, if we require that they have disjoint support. We associate two subsets of $\mathbb{Z}^n$ with the order $<_V$. The first subset is $P_V(\mathbb{Z}^n)$ (or, simply, $P(\mathbb{Z}^n)$), defined by:

$$P_V(\mathbb{Z}^n) = \{a \in \mathbb{Z}^n \mid a >_V 0\}.$$

Clearly $P_V(\mathbb{Z}^n)$ determines the order on $\mathbb{Z}^n$, for given the set $P_V(\mathbb{Z}^n)$, we can define the order by: $a <_V b$ iff $b - a \in P_V(\mathbb{Z}^n)$. If $<_V$ is a term order on $\mathbb{N}^n$, then $P_V(\mathbb{Z}^n)$ satisfies the further condition: $P_V(\mathbb{Z}^n) \supseteq \mathbb{N}^n$.

The second subset of $\mathbb{Z}^n$, which we associate with the order $<_V$, is the half-space given by

$$\overline{P}_V = \{a \in \mathbb{Z}^n \mid aV_1 \geq 0\},$$

where V_1 is the first column of the order matrix V. Clearly $P_V \subseteq \overline{P}_V$ and $\overline{P}_V \setminus P_V$ is contained in the hyperplane of $\mathbb{Z}^n$ of equation $aV_1 = 0$.

By a cone in $\mathbb{Z}^n$ we mean the intersection of a cone of $\mathbb{Q}^n$ with $\mathbb{Z}^n$.

Let $I \subseteq K[x_1, \dots, x_n]$, K a field of characteristic different from 2, be a pure binomial ideal, i.e., an ideal generated by polynomials of the form: $x^a = x^{a^+} - x^{a^-}$ (where $a \in \mathbb{Z}^n$ and x^α denotes $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for every $\alpha \in \mathbb{N}^n$). Let I be the ideal generated by the binomials $x^{a_1}, \dots, x^{a_k}$ (where $a_1, \dots, a_k \in \mathbb{Z}^n$); then we can associate with I the submodule of $\mathbb{Z}^n$ generated by the a_i's. Conversely, if $M \subseteq \mathbb{Z}^n$ is a submodule, we can consider the binomial ideal generated by the binomials x^a, where $a \in M$. In this way (see Boffi and Logar, 2007, Theorem 4.13), we get a one to one correspondence between saturated binomial ideals of $K[x_1, \dots, x_n]$ and submodules of $\mathbb{Z}^n$ (I is said saturated if for any monomial m, if $mf \in I$, then $f \in I$). Moreover, if we start with a pure binomial ideal I, we consider the corresponding submodule M of $\mathbb{Z}^n$ and we construct from M the binomial ideal J as said above, then we get that J is the saturation $\mathrm{Sat}(I)$ of I, where

$$\mathrm{Sat}(I) = \{f \in K[x_1, \dots, x_n] \mid \exists m, \text{ a monomial, s.t. } mf \in I\}.$$

The study of saturated pure binomial ideal is therefore equivalent to the study of submodules of $\mathbb{Z}^n$. In particular, as shown in Boffi and Logar (2007), we can define suitable Gröbner bases for submodules of $\mathbb{Z}^n$ in order to study Gröbner bases of saturated pure binomial ideals of $K[x_1, \dots, x_n]$. One should realize that the saturated binomial ideals I are exactly those such that $I = IL \cap R$, where R stands for the polynomial ring and L is the Laurent polynomial ring $K[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$. See for instance (Eisenbud and Sturmfels, 1996), where L is used a lot in order to study the primary decomposition of the ideals I.

Let $M \subseteq \mathbb{Z}^n$ be a submodule and let $<_V$ be a term order on $\mathbb{Z}^n$ given by a matrix V as above. Following the definition given in Boffi and Logar (2007), a finite set $g_1, \dots, g_k \in M \cap P(\mathbb{Z}^n)$ is a *Gröbner basis* for M (w.r.t. the given term order) if for any $a \in M \cap P(\mathbb{Z}^n)$ there exists an i s.t. $g_i^+ \mid a^+$ (i.e., every coordinate of g_i^+ is not greater than the corresponding coordinate of a^+).

If we define the following partial order on $P(\mathbb{Z}^n)$:

$$a, b \in P(\mathbb{Z}^n), \quad a \sqsubset b \quad \text{if } a \neq b \text{ and } a^+ \mid b^+,$$

we can say that $g_1, \dots, g_k \in M \cap P(\mathbb{Z}^n)$ is a Gröbner basis for M if any element of $M \cap P(\mathbb{Z}^n)$ is preceded (in the partial order $\sqsubset$) by an element g_i.

If $g_1, \dots, g_k$ is a Gröbner basis for M, we say that it is *minimal* if and only if the following condition holds: if $g_i^+ \mid g_j^+$, then $i = j$ (for all $i, j \in \{1, \dots, k\}$). If $g_1, \dots, g_k$ is a minimal Gröbner basis, then $g_1, \dots, g_k$ are minimal elements in $M \cap P(\mathbb{Z}^n)$ w.r.t. $\sqsubset$ (see Boffi and Logar, 2007, Theorem 3.5).

Let m be the rank of M and let $a_1, \dots, a_m$ be a basis of M (as a $\mathbb{Z}$-module). Assume further that the matrix $A = (a_{ij})$ whose rows are the vectors $a_1, \dots, a_m$ is in Hermite normal form (hence, in particular, A is in row echelon form).

Let $F : \mathbb{Z}^m \longrightarrow \mathbb{Z}^n$ be the homomorphism given by $F(\lambda_1, \dots, \lambda_m) = \lambda_1 a_1 + \cdots + \lambda_m a_m$. We define on $\mathbb{Z}^m$ the order induced by $<_V$, i. e.:

$$(\lambda_1, \dots, \lambda_m) <_V (\mu_1, \dots, \mu_m) \quad \text{if and only if} \quad F(\lambda_1, \dots, \lambda_m) <_V F(\mu_1, \dots, \mu_m).$$

Proposition 1. *Let T be the matrix obtained by taking the first m linearly independent columns (over $\mathbb{Q}$) of AV. Then T is the matrix which gives the order on $\mathbb{Z}^m$.*

Proof. Let $C_1, \dots, C_n$ be the columns of AV and suppose that $C_{i_1}, \dots, C_{i_m}$ $(1 \leq i_1 < i_2 < \cdots < i_m)$ are the first m linearly independent columns of AV. If $\lambda = (\lambda_1, \dots, \lambda_m) \in \mathbb{Z}^m$, then $\lambda >_V 0$ if and only if $\lambda C_1 = 0, \dots, \lambda C_{s-1} = 0$ and $\lambda C_s > 0$. If C_j is a column of AV which is linearly dependent on $C_1, \dots, C_{j-1}$ and $j < s$, then $\lambda C_j = 0$. From this the assertion follows. □

If the term order on $\mathbb{Z}^n$ is the Lex term order, defined by the matrix $V = I_n$, then it is easy to see (since A is in Hermite normal form) that the induced order on $\mathbb{Z}^m$ is again the Lex term order induced by the matrix I_m. In general, however, the order induced on $\mathbb{Z}^m$ is not a term order, since $\mathbb{N}^m$ is not contained in the set of positive elements. An easy computation shows that $F(P_V(\mathbb{Z}^m)) \subseteq P_V(\mathbb{Z}^n)$: if $a \in P_V(\mathbb{Z}^m)$, then $aT >_{\text{Lex}} 0$ gives $a(AV) >_{\text{Lex}} 0$; hence $(aA)V >_{\text{Lex}} 0$, so $F(a) = aA \in P_V(\mathbb{Z}^n)$).

Given $u, v \in \mathbb{Z}^m$, $u \neq v$, let

$$u \sqsubset v \quad \text{if } F(u)^+ \mid F(v)^+.$$

This is a partial order on $\mathbb{Z}^m$. Explicitly, it means:
$(u_1, \dots, u_m) \sqsubset (v_1, \dots, v_m)$ if, whenever the i-th component $(u_1 a_1 + \cdots + u_m a_m)_i$ of $(u_1 a_1 + \cdots + u_m a_m)$ is positive, then $(u_1 a_1 + \cdots + u_m a_m)_i \leq (v_1 a_1 + \cdots + v_m a_m)_i$.

An immediate consequence is:

Proposition 2. *Let M, A, V be as above, and let $h_1, \dots, h_k$ be a finite number of elements in $P(\mathbb{Z}^m)$. Then the following are equivalent:*

(1) *$F(h_1), \dots, F(h_k)$ is a Gröbner basis for M;*
(2) *for any $u \in P(\mathbb{Z}^m)$, there exists $i \in \{1, \dots, k\}$ such that $h_i \sqsubset u$.*

Since the image of F is the module M, any Gröbner basis of M is of the form $F(h_1), \dots, F(h_k)$, for suitable $h_1, \dots, h_k \in P(\mathbb{Z}^m)$.

2. Subdivision of $\mathbb{Q}^m$ into cones

Hereinafter, it will be convenient to consider $\mathbb{Z}^m$ and $\mathbb{Z}^n$ embedded in $\mathbb{Q}^m$ and $\mathbb{Q}^n$, respectively. The map F can be extended to a map $F : \mathbb{Q}^m \longrightarrow \mathbb{Q}^n$ given again by $F(u) = uA$. Moreover, we shall consider $\mathbb{Q}^m$ as an affine space, with coordinates $u_1, \ldots, u_m$. From the matrix $A = (a_{ij})$ we get n linear forms $l_1, \ldots, l_n$ in $\mathbb{Q}[u_1, \ldots, u_m]$, by means of:

$$l_i(u_1, \ldots, u_m) = a_{1i}u_1 + \cdots + a_{mi}u_m. \tag{1}$$

In other words, $l_1(u), \ldots, l_n(u)$ are the components of $F(u)$. The linear forms $l_1, \ldots, l_n$ identify n hyperplanes in $\mathbb{Q}^m$, all passing through the origin. Given l_i, let $l_i^{\geq 0}$ be the linear half-space of $\mathbb{Q}^m$ given by the points $u = (u_1, \ldots, u_m)$ such that $l_i(u_1, \ldots, u_m) \geq 0$; $l_i^{\leq 0}$ is defined similarly. Hence for any point $u \in l_i^{\geq 0} \cap \mathbb{Z}^m$, it holds: $F(u)_i \geq 0$, where $F(u)_i$ stands for the i-th coordinate of $F(u)$.

The hyperplanes $l_1, \ldots, l_n$ subdivide $\mathbb{Q}^m$ into polyhedral cones (each of them with vertex in the origin). One way to describe them is the following: let $u \in \mathrm{C}$, where

$$\mathrm{C} = \mathbb{Q}^m \setminus \bigcup_i \{l_i = 0\},$$

then consider:

$$C_u = \bigcap_{i,\ l_i^{\geq 0} \ni u} l_i^{\geq 0} \cap \bigcap_{i,\ l_i^{\geq 0} \not\ni u} l_i^{\leq 0}. \tag{2}$$

Note that the same C_u can be obtained by many other $v \in \mathrm{C}$. Indeed: $v \in C_u \cap \mathrm{C}$ if and only if $C_u = C_v$.

Proposition 3. *For any $v \in C_u$, and for any $i = 1, \ldots, n$, it holds: if $F(v)_i \neq 0$, then $F(u)_i$ and $F(v)_i$ have the same sign.*

Proof. Immediate, from the definition of C_u and the hyperplanes l_i. □

Let

$$\mathcal{C} = \{C_u \mid u \in \mathrm{C}\}. \tag{3}$$

Proposition 4. *The set $\mathcal{C}$ is a finite set of polyhedral cones and*

$$\mathbb{Q}^m = \bigcup_{C \in \mathcal{C}} C.$$

Proof. We can associate with any cone C_u ($u \in \mathrm{C}$) an n-tuple given by the signs of $F(u)_i$, $i = 1, \ldots, n$; if C_u and C_v ($u, v \in \mathrm{C}$) have the same n-tuple of signs, then $C_u = C_v$. Therefore the number of elements of $\mathcal{C}$ is bounded by 2^n, the number of different n-tuples of signs. □

If we define the dimension of a cone of $\mathbb{Q}^m$ as the dimension of the linear space generated by the cone itself, we have:

Proposition 5. *Any cone $C \in \mathcal{C}$ has dimension m.*

Proof. Let $u \in \mathrm{C}$ be such that $C = C_u$ and let $i \in \{1, \ldots, m\}$. Then $F(u)_i > 0$ (or $F(u)_i < 0$). Hence there exists $\epsilon_i > 0$ such that $F(v)_i > 0$ (or $F(v)_i < 0$) for all $v \in B(u, \epsilon_i)$, where $B(u, \epsilon_i)$ denotes the ball of center u and radius ϵ_i. Therefore it follows from Proposition 3 that there exists $\epsilon > 0$ such that $B(u, \epsilon) \subseteq C$. Since the ball $B(u, \epsilon)$ contains a basis of $\mathbb{Q}^m$, we are done. □

Any polyhedral cone is finitely generated (see Schrijver, 1986, Corollary 7.1 a); the generators of a cone C_u (as expressed in (2)) can be obtained from intersections of some of the hyperplanes $\{l_i = 0\}$: if the vector $p \in \mathbb{Q}^m$ is a generator of C_u, there exist indexes $i_1, \ldots, i_k$ such that $\cap_{j=1}^k \{l_{i_j} = 0\}$ is a line and p is on this line. Since the hyperplanes l_i have integer coefficients, it is possible to choose on each of these lines the vector p with integer coordinates and with no common factors, so that in particular $p \in \mathbb{Z}^m$. In this way we can obtain that the generators of C_u are in $\mathbb{Z}^m$. Moreover, if ℓ is a line obtained from an intersection $\cap_{j=1}^k \{l_{i_j} = 0\}$, then ℓ contains two vectors, p and $-p$, which have integer coordinates with no common factors, and which are among the generators of the cones of $\mathcal{C}$. Let us consider therefore the set W of all the above vectors p and $-p$. W is a finite set.

Recall that the (integral) Hilbert basis of a cone is a finite set of integral vectors such that each integral vector of the cone is a nonnegative integral combination of them. By Schrijver (1986), Theorem 16.4, each cone C_u has a Hilbert basis, uniquely determined. Hence we may suppose that W contains the Hilbert bases of the cones C_u.

Example. Let $M \subseteq \mathbb{Z}^3$ be the module generated by the two vectors $a_1 = (2, 1, 4)$, $a_2 = (0, 3, -1)$. The matrix A whose rows are a_1 and a_2 is in Hermite normal form and the map $F : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^3$ is given by: $F(u_1, u_2) = (2u_1, u_1 + 3u_2, 4u_1 - u_2)$. The hyperplanes l_1, l_2, l_3 are therefore $l_1 = 2u_1$, $l_2 = u_1 + 3u_2$, and $l_3 = 4u_1 - u_2$. The set W is given by the six points: $p_1 = (0, 1)$, $p_2 = (0, -1)$, $p_3 = (3, -1)$, $p_4 = (-3, 1)$, $p_5 = (1, 4)$, $p_6 = (-1, -4)$. Take for instance $u = (1, 1)$; then $F(1, 1) = (2, 4, 3)$; here the coordinates are all nonzero (and all positive), hence the corresponding cone C_u is: $l_1^{\geq 0} \cap l_2^{\geq 0} \cap l_3^{\geq 0}$. This cone is also described by the generators p_3, p_5. Analogously we get the cones: $l_1^{\geq 0} \cap l_2^{\leq 0} \cap l_3^{\geq 0}$ (generators: p_2, p_3); $l_1^{\leq 0} \cap l_2^{\leq 0} \cap l_3^{\geq 0}$ (generators: p_2, p_6); $l_1^{\leq 0} \cap l_2^{\leq 0} \cap l_3^{\leq 0}$ (generators: p_4, p_6); $l_1^{\leq 0} \cap l_2^{\geq 0} \cap l_3^{\leq 0}$ (generators: p_1, p_4); $l_1^{\geq 0} \cap l_2^{\geq 0} \cap l_3^{\leq 0}$ (generators: p_1, p_5).

Suppose now that the set W is known (indeed, it can be computed by taking suitable intersections of the hyperplanes l_i). Then it is possible to reconstruct all the cones C_u from W and from the map F, in the following way. Given two points $p, q \in W$, we say that p and q are *tied* if there exists a cone C_u such that they are among the generators of it.

Proposition 6. *Two points $p, q \in W$ are tied if and only if $F(p)_i F(q)_i \geq 0$ for all $i = 1, \ldots, n$.*

Proof. If p and q are tied, let $u \in \mathbb{Q}^m$ be a point such that p and q are among the generators of C_u, and let l_i be one of the hyperplanes. The condition $F(p)_i < 0$ and $F(q)_i > 0$ contradicts Proposition 3. To see the converse, let us suppose (to simplify the notation) that the first s hyperplanes $\{l_i = 0\}$, $i = 1, \ldots, s$, are linearly independent ($s \leq m$). Let $v \in \mathbb{Q}^m$ and let i_0 be an index such that $F(v)_{i_0} = 0$. We can find a point $v' \in \mathbb{Q}^m$ sufficiently close to v, in such a way that:

- $F(v')_{i_0}$ is positive;
- for each $j \neq i_0$, $F(v)_j$ and $F(v')_j$ have the same sign, i.e.,, either they are both positive, or both negative, or both zero.

To see this, let $i_1, \ldots, i_k$ be all the other indices in $\{1, \ldots, s\}$ such that $F(v)_{i_j} = 0$. Let $\epsilon > 0$ and let $B_\epsilon = B(v, \epsilon)$ be the ball centered in v of radius ϵ. Then

$$A_\epsilon = B_\epsilon \cap \{l_{i_1} = 0\} \cap \cdots \cap \{l_{i_k} = 0\} \cap \{l_{i_0} > 0\} \neq \emptyset,$$

since l_{i_0} is linearly independent of $l_{i_1}, \ldots, l_{i_k}$. We can choose a sufficiently small ϵ such that B_ϵ does not meet any of the hyperplanes $\{l_j = 0\}, j \notin \{i_1, \ldots, i_k\}$, so that any $v' \in A_\epsilon$ satisfies the two conditions above.

(Clearly, we can also substitute the first of the two conditions above with the condition "$F(v')_{i_0}$ is negative".)

Suppose now that p and q are such that $F(p)_i F(q)_i \geq 0$ for all i. If the inequality is always strict, then $F(p)_i$ and $F(q)_i$ always have the same sign. Otherwise there exists an index, i_0, such that $F(p)_{i_0} F(q)_{i_0} = 0$. Then we have essentially two possibilities: either $F(p)_{i_0} > 0$ and $F(q)_{i_0} = 0$, or both are zero. In the first case, choose $p' = p$ and $q' \in \mathbb{Q}^m$ such that $F(q')_{i_0} > 0$, and such that $F(q')_j$ and $F(q)_j$ have the same sign for all $j \neq i_0$. In the second case, choose q' as above, and also $p' \in \mathbb{Q}^m$ such that $F(p')_{i_0} > 0$, and $F(p')_j$ and $F(p)_j$ have the same sign for all $j \neq i_0$. Hence p' and q' are such that $F(p')_i F(q')_i \geq 0$ for all i and, moreover, $F(p')_{i_0} F(q')_{i_0} > 0$. Repeating this procedure, we can find two points $p'' \in \mathbb{Q}^m$ and $q'' \in \mathbb{Q}^m$ such that $F(p'')$ and $F(q'')$ have all the coordinates different from zero and of the same sign. So $C_{p''} = C_{q''}$ and $p, q \in C_{p''}$. $\square$

Now we can construct all the cones. We consider the elements of W as the vertices of a graph G_W, and we connect two vertices of G_W precisely when the corresponding points of W are tied. The problem of finding the cones is translated into the problem of finding the maximal complete subgraphs of G_W. This is the maximal clique problem and can be solved with the Bron–Kerbosch algorithm (with pivoting). See, for instance, (Cazals and Karande, 2008) and the references given there.

An alternative approach to construct the cones could be based on the fact that, if C is a polyhedral cone of $\mathbb{Q}^m$ defined by a finite set S of inequalities, and if $\{l = 0\}$ is a hyperplane of $\mathbb{Q}^m$, then $S \cup \{l \geq 0\}$ and $S \cup \{l \leq 0\}$ define two other polyhedral cones (one contained in the half-space $l^{\geq 0}$ and the other contained in $l^{\leq 0}$). Hence, if we start with the cone $l_1^{\geq 0}$, where l_1 is defined as in (1), and we take the hyperplane $\{l_2 = 0\}$, we construct two cones: $l_1^{\geq 0} \cap l_2^{\geq 0}$ and $l_1^{\geq 0} \cap l_2^{\leq 0}$. Similarly, we can construct two more cones if we start with the cone $l_1^{\leq 0}$. Using all the hyperplanes given by (1), we can inductively obtain all the cones of $\mathcal{C}$, described in terms of inequalities. Further work is necessary to obtain their generators.

3. Cones in $P_T(\mathbb{Z}^m)$

We keep the notation of the previous sections. In particular, let $M \subseteq \mathbb{Z}^m$ be a submodule generated by the rows of a matrix A, let V be a nonsingular matrix which gives a term order on $\mathbb{Z}^n$, and let T be the matrix obtained from the first m linearly independent columns of AV, so that T gives a linear order on $\mathbb{Z}^m$, denoted by $<_T$ (see Proposition 1). Furthermore, $P_T(\mathbb{Z}^m)$ $(= iP_T)$ denotes the set of elements of $\mathbb{Z}^m$ which are positive w.r.t. $<_T$, and $\overline{P}_T$ $(=\overline{P}_T(\mathbb{Z}^m))$ is the half-space $T_1^{\geq 0} = \{u \in \mathbb{Z}^m \mid uT_1 \geq 0\}$, where T_1 stands for the first column of T. If C is a finitely generated cone of $\mathbb{Q}^m$, $\gamma(C)$ denotes the finite set $\{q_1, \ldots, q_s\}$ of its generators. We can assume that the generators are in $\mathbb{Z}^m$ and the gcd of the entries of each q_i is 1, i.e., $\gamma(C)$ stands for the Hilbert basis of C. Furthermore, let:

$$X(C) = \left\{ \sum_i \lambda_i q_i \mid \lambda_i \in \mathbb{Q},\ 0 \leq \lambda_i < 1 \right\}; \quad Y(C) = X(C) \cap \mathbb{Z}^m.$$

The set $X(C)$ is bounded and $Y(C)$ is finite.

Proposition 7. *It holds:*

$$C = \left(\bigcup_{q \in \gamma(C)} (q + C) \right) \cup X(C); \tag{4}$$

hence

$$C \cap \mathbb{Z}^m = \left(\bigcup_{q \in \gamma(C)} (q + (C \cap \mathbb{Z}^m)) \right) \cup Y(C). \tag{5}$$

Proof. Let $u \in C$; then $u = \sum \lambda_i q_i$, where $\lambda_i \geq 0$. If $\lambda_i < 1$ for all i, then $u \in X(C)$. Otherwise, there exists j such that $\lambda_j \geq 1$; hence $u = q_j + \sum_i \mu_i q_i$, where $\mu_i = \lambda_i$ if $i \neq j$, and $\mu_j = \lambda_j - 1 \geq 0$. Thus (4) holds. □

The proposition above can be seen as a restatement of (a special case of) Bruns and Gubeladze (2009), Proposition 2.43 d.

The cones considered so far are in the whole space $\mathbb{Z}^m$ (or $\mathbb{Q}^m$). In order to use the cones for the construction of a Gröbner basis of M we need to consider cones which have trace in $P_T(\mathbb{Z}^m)$.

An immediate consequence of Proposition 4 is:

Proposition 8. *It holds:*

$$P_T(\mathbb{Z}^m) = \bigcup_{C \in \mathcal{C}} C \cap P_T(\mathbb{Z}^m) \quad \textit{and} \quad \overline{P}_T(\mathbb{Z}^m) = \bigcup_{C \in \mathcal{C}} C \cap \overline{P}_T(\mathbb{Z}^m).$$

If C is a cone of $\mathcal{C}$, we distinguish three cases, according to the position of the generators of C w.r.t. $\overline{P}_T$:

- $\gamma(C) \subseteq \overline{P}_T$.
- $\gamma(C) \cap \overline{P}_T \neq \emptyset$ and $\gamma(C) \cap \left(\mathbb{Z}^m \setminus \overline{P}_T\right) \neq \emptyset$.
- $\gamma(C) \subseteq \mathbb{Z}^m \setminus \overline{P}_T$.

In the first case, $C = C \cap \overline{P}_T$. In the last case $C \cap \overline{P}_T = \{0\}$. In the second case, $C \cap \overline{P}_T$ is a cone, contained in C, given by $C \cap T_1^{\geq 0}$.

In all cases, the set $P(C) = C \cap P_T(\mathbb{Z}^m)$ can be obtained by the formula:

$$C \cap P_T(\mathbb{Z}^m) = \{a \in C \cap \overline{P}_T \mid a >_T 0\}. \tag{6}$$

Hence, in order to find $C \cap P_T(\mathbb{Z}^m)$, it is enough to compute $C \cap \overline{P}_T$ and then select the positive elements w.r.t. $>_T$. Note that $P(C)$ is a cone of $\mathbb{Z}^m$, but it is not necessarily described by a finite number of inequalities: as we see from the above formula, it can be obtained from a cone of $\overline{P}_T$ after omitting some of its faces.

According to Proposition 3, $F(u)$ "does not change the sign" on all the elements $u \in P(C)$.

We can define two partial orders on the set $P(C)$:

- the partial order $\sqsubset$ induced by $P(\mathbb{Z}^m)$, i.e., if $u, v \in P(C)$, $u \neq v$, then $u \sqsubset v$ if $F(u)^+ \mid F(v)^+$;
- the partial order $\prec_+$ defined by: if $u, v \in P(C)$, $u \neq v$, then $u \prec_+ v$ if $v \in u + C$.

Proposition 9. *Let $u, v \in P(C)$; if $u \prec_+ v$, then $u \sqsubset v$.*

Proof. We have: $F(v) = F(u) + F(v - u)$, where v, u and $v - u$ are in C, hence have the same signs. In particular, if the i-th component $F(u)_i$ of $F(u)$ is positive, then $F(v)_i \geq 0$ and $F(v - u)_i \geq 0$. Hence $F(u)^+ \mid F(v)^+$ follows from $F(v)_i = F(u)_i + F(v - u)_i$. □

Proposition 10. *Let $u \in P(\mathbb{Z}^m)$ be minimal among the elements of $P(\mathbb{Z}^m)$ w.r.t. $\sqsubset$. Assume that $u \in P(C)$. Then u is a minimal element of $P(C)$ w.r.t. $\prec_+$.*

Proof. Immediate. □

As a consequence, the set of minimal elements of $P(\mathbb{Z}^m)$ w.r.t. $\sqsubset$ is contained in the set of minimal elements of $P(C)$ w.r.t. $\prec_+$, as C varies in $\mathcal{C}$.

Applying the decomposition (5) to the cones $C \cap \overline{P}_T$, we obtain some information regarding the minimal elements of $(P(C), \prec_+)$:

Proposition 11. *Let C' be the cone $C \cap \overline{P}_T$. The minimal elements of $P(C)$ w.r.t. $\prec_+$ are contained in the finite set $\left(\gamma(C') \cup Y(C')\right) \cap P(\mathbb{Z}^m)$.*

Proof. Since the generators $q_1, \ldots, q_s$ of C' are in $\overline{P}_T$, then $q_i T_1 \geq 0$ for all i. Here $q_i T_1$ denotes the product of the line vector q_i with the column vector given by the first column of T. Assume first that there exists j such that $q_j T_1 > 0$. Let $u \in P(C)$. Hence $u = \sum_i \mu_i q_i$ with $\mu_i \geq 0$ ($\mu_i \in \mathbb{Q}$). If $\mu_i < 1$ for all i, then $u \in Y(C') \cap P(\mathbb{Z}^m)$. Otherwise, there exists k such that $\mu_k \geq 1$. Then $u - q_k = \mu_1 q_1 + \cdots + (\mu_k - 1) q_k + \cdots + \mu_s q_s$. If $u - q_k = 0$, we are done. Else, we have: $(u - q_k) T_1 = \mu_1 q_1 T_1 + \cdots + (\mu_k - 1) q_k T_1 + \cdots + \mu_s q_s T_1 > 0$, since all the summands are nonnegative and at least one of them is positive. Thus $(u - q_k) \in P(\mathbb{Z}^m)$ and $u - q_k \prec_+ u$. Repeating the process, we construct an element of $Y(C') \cap P(\mathbb{Z}^m)$ which precedes u. Next assume that $q_i T_1 = 0$ for all i, and again let $u \in P(C)$ be such that $u = \sum_i \mu_i q_i$ with $\mu_i \geq 0$. Then $u T_1 = 0$ and, by the definition of $P(\mathbb{Z}^m)$, we have that $u T_2 \geq 0$. If $u T_2 > 0$, then there exists j such that $q_j T_2 > 0$ and we can proceed as above. Otherwise, $u T_2 = 0$, hence $u T_3 \geq 0 \ldots$. After a finite number of steps, we are through. □

Let $\mathcal{C}_T$ be the set of the cones $C \cap \overline{P}_T$ (with $C \in \mathcal{C}$). By Proposition 8, $\mathcal{C}_T$ covers $\overline{P}_T$.

As a consequence of the above, and of Proposition 2, we have the following:

Proposition 12. *The (finite) set:*

$$\left(\bigcup_{C\in\mathcal{C}_T}(\gamma(C)\cup Y(C))\right)\cap P(\mathbb{Z}^m)$$

is a Gröbner basis for M w.r.t. the term order $<_V$.

Since any cone $C \in \mathcal{C}_T$ has dimension m, $\gamma(C)$ has at least m elements. If $\gamma(C)$ has precisely m elements, they must be linearly independent; if $\gamma(C)$ has more than m elements, we can find subsets $X_1, \ldots, X_t$ of $\gamma(C)$ such that:

(1) each X_i has m linearly independent elements;
(2) if C_i denotes the cone, whose generators are the vectors of X_i, then $\cup_i C_i = C$;
(3) if $i \neq j$, then $C_i \cap C_j$ is a common face of C_i and C_j.

The construction of the sets $X_1, \ldots, X_t$ can be done using the results of Schrijver (1986), Chapter 7 and in particular Theorem 7.1. Any cone $C \in \mathcal{C}_T$, such that $\gamma(C)$ has more than m elements, can be replaced by a finite collection of new cones, each one of them having m generators. In this way we obtain a new collection of cones $\mathcal{C}'_T$. Clearly it holds:

Proposition 13. *The union of all $(\gamma(C')\cup Y(C'))\cap P(\mathbb{Z}^m)$, $C' \in \mathcal{C}'_T$, is a Gröbner basis for M w.r.t. $<_V$.*

Proposition 13 leads to study cones (contained in $\mathbb{Q}^m$ or $\mathbb{Z}^m$) generated by m linearly independent elements. Hence we focus our attention on this case. Let $q_1, \ldots, q_m$ be m elements of $\mathbb{Z}^m$ linearly independent over $\mathbb{Q}$ and let

$$Y = \left\{\sum_i \lambda_i q_i \mid \lambda_i \in \mathbb{Q},\ 0 \le \lambda_i < 1\right\} \cap \mathbb{Z}^m. \tag{7}$$

We can define a sum on the set Y, in the following way. If $a = \sum_i \lambda_i q_i$ and $b = \sum_i \mu_i q_i$ are elements of Y, we set: $a +_Y b = \sum_i \{\lambda_i + \mu_i\} q_i$, where $\{x\}$ denotes the fractional part of x. Since $a + b = \sum_i (\lambda_i + \mu_i) q_i = \sum_i (n_i + \{\lambda_i + \mu_i\}) q_i$, where $n_i \in \mathbb{N}$, we have that indeed $a +_Y b \in \mathbb{Z}^m$. It is not hard to check that:

Proposition 14. *The set Y, endowed with the above operation $+_Y$, is a finite abelian group. Moreover, it is isomorphic to $\mathbb{Z}^m/\langle q_1, \ldots, q_m\rangle$.*

Proof. Let $\psi : Y \longrightarrow \mathbb{Z}^m/\langle q_1, \ldots, q_m\rangle$ be defined by: $\phi(a) = [a]$. It is easy to see that ψ is a group isomorphism. □

We can use this last isomorphism to compute explicitly the elements of Y, i.e., the integer elements of the set $\left\{\sum_i \lambda_i q_i \mid \lambda_i \in \mathbb{Q},\ 0 \le \lambda_i < 1\right\}$. Let Q be the matrix whose columns are the vectors $q_1, \ldots, q_m$. It can be put in Smith normal form, i.e., we can compute two nonsingular integer matrices, U_1 and U_2, such that $U_1 Q U_2 = \operatorname{diag}(d_1, \ldots, d_m)$, where $d_1, \ldots, d_m \in \mathbb{N}$ are such that $d_1 \mid d_2, \ldots, d_{m-1} \mid d_m$. From this, it follows that:

$$\mathbb{Z}^m/\langle q_1, \ldots, q_m\rangle \simeq \mathbb{Z}/\langle d_1\rangle \oplus \cdots \oplus \mathbb{Z}/\langle d_m\rangle,$$

and the columns of U_1^{-1} give generators of $\mathbb{Z}^m/\langle q_1, \ldots, q_m\rangle$, or of Y, as an abelian group (the first is of order d_1, …, the last is of order d_m). The above construction allows us to describe explicitly the elements of the group Y. In particular, if $C' \in \mathcal{C}'_T$, then $Y(C')$ is a finite abelian group, whose elements can be described according to the above procedure.

Summarizing the claims of this section we have:

Theorem 15. *Given a term order $<_V$ on $\mathbb{Z}^n$ and a module $M \subseteq \mathbb{Z}^n$ of rank m, we can construct a finite set of vectors $\{p_1, \ldots, p_k\}$ in $\overline{P}_T(\mathbb{Z}^m)$ and a collection J of m-tuples of indices $j = (j_1, \ldots, j_m)$, $j_i \in \{1, \ldots, k\}$, such that:*

(1) *to each $j \in J$ we can associate a finite group Y_j obtained from the vectors $p_{j_1}, \ldots, p_{j_m}$ as in (7);*
(2) *a Gröbner basis of M w.r.t. the term order $<_V$ is given by the image, via the map F, of $\{p_1, \ldots, p_k\} \cap P_T(\mathbb{Z}^m)$ and of suitable elements of $Y_j \cap P_T(\mathbb{Z}^m)$, $j \in J$.*

Ideally, the suitable elements mentioned in the theorem should be those minimal w.r.t. $\sqsubset$, because the corresponding Gröbner basis of M would be minimal. But a (big) Gröbner basis is also obtained just taking the whole $Y_j \cap P_T(\mathbb{Z}^m)$, for every $j \in J$. An intermediate Gröbner basis is obtained, if suitable element is intended to mean minimal w.r.t. $\prec_+$, that is, belonging to the appropriate Hilbert basis. In our view, an interesting feature of the theorem lies in the fact that each set Y_j can be investigated by means of an algebraic structure. Unfortunately, we have been unable so far to exploit such a structure in a satisfactory way. We have only gotten partial results in some special cases.

4. An example and some remarks

Let us consider the submodule M of $\mathbb{Z}^5$, whose generators are:

$$a_1 = (2, 1, 3, -3, -1), \qquad a_2 = (0, 5, 2, -3, 0), \qquad a_3 = (0, 0, 4, -1, 9).$$

We want to compute a Gröbner basis of M w.r.t. the term order given by the matrix:

$$V = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 \\ 3 & 0 & 0 & 1 & 0 \\ 4 & 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The order induced on $\mathbb{Z}^3$ (or $\mathbb{Q}^3$) by V is given by the matrix T, which is obtained from AV by taking the first three linearly independent columns, i.e.:

$$T = \begin{pmatrix} -1 & 2 & 1 \\ 4 & 0 & 5 \\ 26 & 0 & 0 \end{pmatrix}.$$

The planes, defined as in (1), are: $l_1, \ldots, l_5 = 2x, 5y + x, 4z + 2y + 3x, -z - 3y - 3x, 9z - x$. Let $F(x, y, z) = (2x, 5y + x, 4z + 2y + 3x, -z - 3y - 3x, 9z - x)$. The set W, formed by the vectors which are generators of the cones, is given by the vectors:

$$(0, 0, 1),\ (0, 2, -1),\ (0, 1, -3),\ (0, 1, 0),\ (20, -4, -13),$$
$$(5, -1, -12),\ (45, -9, 5),\ (10, -9, -3),\ (18, -31, 2),\ (27, -28, 3),$$

and by their opposites. We denote these ten elements by $q_1, \ldots, q_{10}$. In order to compute the set $\mathcal{C}$ of the cones which cover $\mathbb{Q}^3$, we have to compute the signs of $F(q)$ for all $q \in W$. For instance, the signs of $F(q_1)$ are $(0, 0, +, -, +)$, those of $F(q_4)$ are $(0, +, +, -, 0)$, hence q_1 and q_4 are tied. The signs of $F(q_7)$ are $(+, 0, +, -, 0)$, hence q_1, q_4 and q_7 are tied as well. Moreover, this latter set is maximal. The collection of all the maximal cliques (as given by the Bron–Kerbosch algorithm) is:

$$\{q_1, q_4, q_7\}, \{q_1, q_4, -q_6, -q_8, -q_9\}, \{q_1, q_7, q_{10}, -q_3\}, \{q_1, -q_3, -q_6\},$$
$$\{q_2, q_3, q_5, q_6\}, \{q_2, q_3, -q_9, -q_{10}\}, \{q_2, q_4, q_5, q_7\}, \{q_2, q_4, -q_9\}, \{q_3, q_6, -q_1\},$$
$$\{q_3, -q_1, -q_7, -q_{10}\}, \{q_5, q_6, q_8\}, \{q_5, q_7, q_8, -q_{10}\}, \{q_6, q_8, q_9, -q_1, -q_4\},$$
$$\{q_8, q_9, -q_{10}\}, \{q_9, -q_{10}, -q_2, -q_3\}, \{q_9, -q_2, -q_4\}, \{-q_1, -q_4, -q_7\},$$
$$\{-q_2, -q_3, -q_5, -q_6\}, \{-q_2, -q_4, -q_5, -q_7\}, \{-q_5, -q_6, -q_8\},$$
$$\{-q_5, -q_7, -q_8, -q_{10}\}, \{-q_8, -q_9, -q_{10}\}.$$

Some of these cones (such as the first one, for instance) are already contained in $\overline{P}_T(\mathbb{Z}^3)$. Other cones (such as $\{q_2, q_3, q_5, q_6\}$ and $\{-q_1, -q_4, -q_7\}$, for instance) have all their generators outside of $P_T(\mathbb{Z}^3)$, and hence we do not need to consider them. Further cones (like $\{q_3, -q_1, -q_7, -q_{10}\}$, say) are not contained in $\overline{P}_T(\mathbb{Z}^3)$, but do have a nontrivial trace in it, which has to be computed. For instance, the trace of $\{q_3, -q_1, -q_7, -q_{10}\}$ in $\overline{P}_T(\mathbb{Z}^3)$ is the cone generated by: $-q_{10}$, $(-74, 79, -15)$ and $(-36, 17, -4)$).

Finally, we need to decompose the cones of $\overline{P}_T(\mathbb{Z}^3)$, which are generated by more then 3 vectors, into cones with precisely three (linearly independent) generators. For instance, the cone $\{q_1, q_4, -q_6, -q_8, -q_9\}$ can be split into the following three cones: $\{q_1, q_4, -q_6\}$, $\{q_4, -q_6, -q_8\}$ and $\{q_4, -q_8, -q_9\}$ (clearly, there are other possible choices).
In order to express all the cones thus obtained, we need to add five more vectors to the list $q_1, \ldots, q_{10}$. Namely: $q_{11} = (74, -79, 15)$, $q_{12} = (-36, 17, -4)$, $q_{13} = (130, -26, 9)$, $q_{14} = (0, 13, -2)$ and $q_{15} = (18, -41, 7)$. The set $\mathcal{C}'_T$ of cones with 3 generators, able to cover $\overline{P}_T(\mathbb{Z}^3)$, is summarized by the table in Fig. 1. Let us see an example of computation of the generators of the group $Y(C)$. Take for instance $C = C_7$, whose generators are $-q_3, -q_5, -q_6$. The Smith normal form of the 3×3 matrix, whose columns are the three vectors above, yields:

$$\begin{pmatrix} 0 & -20 & -5 \\ -1 & 4 & 1 \\ 3 & 13 & 12 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 3 & -4 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 35 \end{pmatrix} \cdot \begin{pmatrix} 1 & -4 & -1 \\ 0 & 4 & 1 \\ 0 & -3 & -1 \end{pmatrix}.$$

From this equality we get that:

$$Y(C_7) = \{\lambda(0, -1, 3) + \mu(-20, 4, 13) + \nu(-5, 1, 12) \mid 0 \le \lambda, \mu, \nu < 1\} \cap \mathbb{Z}^3$$

is (isomorphic to) the group $\mathbb{Z}_5 \oplus \mathbb{Z}_{35}$. Moreover, let $y_1 = (-1, 0, 4)$ and $y_2 = (0, 0, -1)$ be the last two columns of the matrix which multiplies the diagonal matrix diag(1, 5, 35) on the left. If we express y_1 and y_2 as linear combinations of $-q_3$, $-q_5$ and $-q_6$, the corresponding weights λ, μ, ν are recorded by the triplets $x_1 = (1/5, 1/5, 2/5)$ and $x_2 = (0, 1/35, 31/35)$, respectively. x_1 and x_2 are the generators of $Y(C_7)$; the former has order 5, the latter has order 35. Therefore

$$Y(C_7) = \left\{ \left\{ \frac{i}{5} \right\} (-q_3) + \left\{ \frac{i}{5} + \frac{j}{35} \right\} (-q_5) + \left\{ \frac{2i}{5} + \frac{31j}{35} \right\} (-q_6) \right\},$$

where it is enough to take $i = 0, \ldots, 4$ and $j = 0, \ldots, 34$.

In conclusion, a Gröbner basis of the module M is already given by the generators of the cones, and by those elements of each of the groups of Fig. 1, which turn out to lie in $P_T(\mathbb{Z}^m)$. A smaller basis is given by selecting in each group the elements lying in $P_T(\mathbb{Z}^m)$ and minimal with respect to $\prec_+$ (they relate to the appropriate Hilbert bases). A minimal Gröbner basis is given by further selecting the elements which are minimal with respect to $\sqsubset$. Just to give an idea of the huge selection process that can take place, we record that a minimal Gröbner basis of this example is given by the following 29 vectors of $\mathbb{Z}^3$:

(-1, 0, 0)	(-1, 1, 0)	(0, 1, 0)	(0, -1, 1)	(-1, 0, 1)	(0, 0, 1)
(1, -1, 1)	(1, -2, 1)	(-2, 1, 1)	(2, -3, 1)	(2, -2, 1)	(3, -4, 1)
(3, -3, 1)	(4, -5, 1)	(4, -4, 1)	(-5, 6, -1)	(5, -5, 1)	(-6, 6, -1)
(-5, 6, -1)	(5, -5, 1)	(-6, 6, -1)	(6, -5, 1)	(-7, 6, -1)	(-7, 5, -1)
(7, -4, 1)	(-8, 5, -1)	(8, -4, 1)	(-9, 5, -1)	(9, -4, 1).	

Several different strategies can be devised to reduce the number of elements. For instance, given $C \in \mathcal{C}'_T$, we can try to use the group structure of $Y(C)$ to collect the minimal elements of the cone $P(C)$ with respect to the partial orders. A good selection strategy is clearly crucial if we want to improve the efficiency of the algorithm. At this stage, we are nowhere near competitive with algorithms such as `4ti2` (see 4ti2 team, 0000), which is based on Hemmecke and Malkin (2009), or `Normaliz` Bruns et al. (0000), which already deals with Hilbert bases via triangulation and enumeration of the fundamental parallelotope. And even if we find a good selection strategy, and streamline the whole procedure, it is not clear whether the end result is competitive. Nevertheless, since the knowledge of a Gröbner basis of a $\mathbb{Z}$-module, and hence of a saturated pure binomial ideal, although far from minimal, is sufficient to solve several computational problems, such as the membership problem, it could be interesting to see how to use the peculiar structure of the Gröbner bases of Theorem 15 in order to decide some of those problems, e.g., whether a polynomial belongs to a binomial ideal. As a further comment, we note that there are submodules of $\mathbb{Z}^n$ (which come from special classes of binomial ideals) for which the hyperplanes given by (1) have many symmetries, so that the construction of the cones can be simplified. Use of symmetries has already proven effective in the literature, see for instance the recent (Bruns et al., 0000).

cone	generators	abelian group	group generators
C_1	q_1, q_4, q_7	$\mathbb{Z}_{45}$	$(\frac{8}{9}, \frac{1}{5}, \frac{1}{45})$
C_2	$q_4, q_1, -q_6$	$\mathbb{Z}_5$	$(\frac{4}{5}, \frac{3}{5}, \frac{1}{3})$
C_3	$q_4, -q_6, -q_8$	$\mathbb{Z}_{105}$	$(\frac{1}{3}, \frac{61}{105}, \frac{1}{105})$
C_4	$q_4, -q_8, -q_9$	$\mathbb{Z}_{74}$	$(\frac{1}{2}, \frac{1}{37}, \frac{3}{74})$
C_5	$q_1, -q_3, -q_6$	$\mathbb{Z}_5$	$(0, \frac{1}{5}, \frac{1}{5})$
C_6	$-q_3, -q_2, -q_5$	$\mathbb{Z}_5 \oplus \mathbb{Z}_{20}$	$(\frac{2}{5}, \frac{1}{5}, \frac{1}{5}), (\frac{7}{10}, \frac{1}{4}, \frac{1}{20})$
C_7	$-q_3, -q_5, -q_6$	$\mathbb{Z}_5 \oplus \mathbb{Z}_{35}$	$(\frac{1}{5}, \frac{1}{5}, \frac{2}{5}), (0, \frac{1}{35}, \frac{31}{35})$
C_8	$-q_5, -q_6, -q_8$	$\mathbb{Z}_{35} \oplus \mathbb{Z}_{35}$	$(\frac{33}{35}, \frac{34}{35}, \frac{1}{35}), (\frac{34}{35}, \frac{4}{35}, 0)$
C_9	$-q_8, -q_9, -q_{10}$	$\mathbb{Z}_{37} \oplus \mathbb{Z}_{37}$	$(\frac{1}{37}, 0, \frac{1}{37}), (\frac{36}{37}, \frac{17}{37}, 0)$
C_{10}	$-q_{10}, -q_{11}, q_{12}$	$\mathbb{Z}_{61} \oplus \mathbb{Z}_{61}$	$(\frac{18}{61}, \frac{1}{61}, \frac{59}{61}), (\frac{42}{61}, 0, \frac{60}{61})$
C_{11}	$q_4, -q_9, -q_{15}$	$\mathbb{Z}_{90}$	$(\frac{1}{2}, \frac{83}{90}, \frac{1}{45})$
C_{12}	$q_4 - q_{15}, q_{14}$	$\mathbb{Z}_{36}$	$(\frac{3}{4}, \frac{17}{18}, \frac{7}{36})$
C_{13}	$-q_2, q_{15}, -q_{14}$	$\mathbb{Z}_9 \oplus \mathbb{Z}_{18}$	$(\frac{5}{18}, \frac{17}{18}, \frac{1}{18}), (\frac{7}{9}, 0, \frac{1}{9})$
C_{14}	$-q_9, -q_{10}, -q_{11}$	$\mathbb{Z}_{2257}$	$(\frac{3}{37}, \frac{1950}{2257}, \frac{1}{61})$
C_{15}	$-q_9, -q_{11}, -q_{15}$	$\mathbb{Z}_{5580}$	$(\frac{43}{90}, \frac{1}{124}, \frac{5519}{5580})$
C_{16}	q_4, q_7, q_{13}	$\mathbb{Z}_{245}$	$(\frac{1}{5}, \frac{236}{245}, \frac{1}{49})$
C_{17}	q_4, q_{13}, q_{14}	$\mathbb{Z}_{260}$	$(\frac{1}{4}, \frac{129}{130}, \frac{251}{260})$
C_{18}	$q_7, q_{13}, -q_{12}$	$\mathbb{Z}_{49} \oplus \mathbb{Z}_{49}$	$(\frac{1}{49}, 0, \frac{11}{49}), (0, \frac{48}{49}, \frac{39}{49})$
C_{19}	$-q_2, -q_3, q_{11}$	$\mathbb{Z}_{370}$	$(\frac{2}{5}, \frac{49}{370}, \frac{1}{74})$
C_{20}	$-q_2, q_{11}, q_{15}$	$\mathbb{Z}_{1116}$	$(\frac{11}{18}, \frac{69}{124}, \frac{485}{1116})$
C_{21}	$-q_2, -q_5, -q_{13}$	$\mathbb{Z}_2 \oplus \mathbb{Z}_{1870}$	$(\frac{1}{2}, \frac{1}{2}, 0), (\frac{3}{5}, \frac{61}{1870}, \frac{1}{374})$
C_{22}	$-q_2, -q_{13}, -q_{14}$	$\mathbb{Z}_{1170}$	$(\frac{17}{18}, \frac{57}{130}, \frac{293}{585})$
C_{23}	$-q_5, -q_8, -q_{10}$	$\mathbb{Z}_{1295}$	$(\frac{9}{35}, \frac{1182}{1295}, \frac{1}{37})$
C_{24}	$-q_5, -q_{10}, q_{12}$	$\mathbb{Z}_{8357}$	$(\frac{100}{137}, \frac{1}{8357}, \frac{1021}{8357})$
C_{25}	$-q_5, q_{12}, -q_{13}$	$\mathbb{Z}_{18326}$	$(\frac{101}{374}, \frac{43}{49}, \frac{1}{18326})$
C_{26}	$q_1, q_7, -q_{12}$	$\mathbb{Z}_{441}$	$(\frac{1}{9}, \frac{424}{441}, \frac{1}{49})$
C_{27}	$q_1, -q_{12}, q_{11}$	$\mathbb{Z}_{1586}$	$(\frac{23}{26}, \frac{835}{1586}, \frac{1}{1586})$
C_{28}	$q_1, q_{11}, -q_3$	$\mathbb{Z}_{74}$	$(0, \frac{59}{74}, \frac{1}{74})$

Fig. 1. An example.

Acknowledgements

This research was partly supported by MIUR (Italian Government PRIN "Algebra commutativa e combinatorica con applicazioni alla geometria algebrica"), by the universities UdA (Pescara) and LUSPIO (Rome) (first author) and by the university of Trieste (second author).

References

4ti2 team 4ti2—a software package for algebraic, geometric and combinatorial problems on linear spaces. Available at www.4ti2.de.

Boffi, G., Logar, A., 2007. Gröbner bases for submodules of $\mathbb{Z}^n$. Rend. Istit. Mat. Univ. Trieste XXXIX, 43–62.

Bruns, W., Gubeladze, J., 2009. Polytopes, Rings and K-theory. In: Springer Monographs in Mathematics, Springer.

Bruns, W., Hemmecke, R., Ichim, B., Köppe, M., Söger, C., Challenging computations of Hilbert bases of cones associated with algebraic statistics. arXiv:1001.4145v1 [math.CO].

Bruns, W., Ichim, B., Söger, C., Normaliz. Available at www.mathematik.uni-osnabrueck.de/normaliz/.

Cazals, F., Karande, C., 2008. A note on the problem of reporting maximal cliques. Theoretical Computer Science 407, 564–568.

CoCoA Team. CoCoA: a system for doing Computations in Commutative Algebra. Available at http://cocoa.dima.unige.it.

Eisenbud, D., Sturmfels, B., 1996. Binomial ideals. Duke Math. J. 84, 1–45.

Hemmecke, R., Malkin, P., 2009. Computing generating sets of lattice ideals and Markov bases of lattices. Journal of Symbolic Computation 1463–1476.

Schrijver, A., 1986. Theory of Linear and Integer Programming. John Wiley and Sons.

Sturmfels, B., Weismantel, R., Ziegler, G., 1995. Gröbner bases of lattices, corner polyhedra, and integer programming. Beiträge Algebra Geom. 36 (2), 281–298.

Thomas, R., 1995. A geometric Buchberger algorithm for integer programming. Math. Oper. Res. 4, 864–884.