Rend. Istit. Mat. Univ. Trieste
Vol. XXXIX, 43–62 (2007)

Gröbner Bases for Submodules of $\mathbb{Z}^n$

Giandomenico Boffi and Alessandro Logar (*)

Dedicated to the memory of Fabio Rossi

Summary. - *We define Gröbner bases for submodules of $\mathbb{Z}^n$ and characterize minimal and reduced bases combinatorially in terms of minimal elements of suitable partially ordered subsets of $\mathbb{Z}^n$. Then we show that Gröbner bases for saturated pure binomial ideals of $K[x_1, \ldots, x_n]$, $char(K) \neq 2$, can be immediately derived from Gröbner bases for appropriate corresponding submodules of $\mathbb{Z}^n$. This suggests the possibility of calculating the Gröbner bases of the ideals without using the Buchberger algorithm.*

1. Introduction

This paper reports on some work related to the computation of Gröbner bases for saturated pure binomial ideals of $K[x_1, \ldots, x_n]$, K a field of characteristic different from 2, with respect to any term order. The idea is to first define Gröbner bases for submodules of $\mathbb{Z}^n$ and then prove that the Gröbner bases for the ideals can be immediately obtained from those of the submodules. Moreover, the minimal and reduced Gröbner bases for submodules are characterized combinatorially in terms of minimal elements of suitable partially ordered subsets of $\mathbb{Z}^n$. Hence the use of the Buchberger algorithm in $K[x_1, \ldots, x_n]$ can be replaced by any algorithm able to find the

(*) Both authors were partially supported by MIUR. The first author is a member of CNR-GNSAGA.
Authors' addresses: Giandomenico Boffi, Dipartimento di Scienze, Università G. D'Annunzio, Viale Pindaro 42, 65127 Pescara, Italy; E-mail: gboffi@unich.it
Alessandro Logar, DMI, Università di Trieste, Via Valerio 12/1, 34127 Trieste, Italy; E-mail: logar@units.it

minimal elements of the above mentioned partially ordered subsets of $\mathbb{Z}^n$. We believe that this replacement may yield a significant reduction in the complexity of computations, but we are still in an initial phase of the investigation. In the last section, an illustration is given in a special case, the case of rank 2 submodules of $\mathbb{Z}^n$ (with respect to a lexicographic term order).

The relevance of pure binomial ideals can be hardly overestimated. Ideals of this kind occur in integer programming and are the defining ideals of toric varieties [7], [10]. More generally, all binomial ideals enjoy nice properties: their Gröbner bases are still given by sets of binomials; the ideals occurring in their primary decompositons are still binomial ideals [8]. Binomial ideals were also involved in the authors' work with Fabio Rossi [3], [4], [5], to whom this article is dedicated.

It was observed long ago that the Buchberger algorithm for toric ideals is a purely combinatorial process involving lattice vectors [12]. Hence our shift from ideals of $K[x_1, \ldots, x_n]$ to submodules of $\mathbb{Z}^n$ is not altogether new, though we develop this point of view to a larger extent. But the shift to lattices has been seen by others as a way to perform the Buchberger algorithm in a more efficient way, while our idea is to avoid using that algorithm. For the problems related to computing toric ideals, see also [2].

The outline of this paper is as follows. Sections 2 and 3 define Gröbner bases for any non-zero submodule M of $\mathbb{Z}^n$ with respect to any term order $<_\tau$. In particular, a minimal (resp., reduced) Gröbner basis is characterized as a subset of M consisting of n-tuples which are minimal with respect to a suitable partial order $\sqsubset$ (resp., $\prec$) of $M \cap \tau(\mathbb{Z}^n)$, where $\tau(\mathbb{Z}^n) := \{a \in \mathbb{Z}^n \ : \ a^+ >_\tau a^-\}$, a^+ and a^- being the only elements of $\mathbb{N}^n$ with disjoint support such that $a = a^+ - a^-$. Section 4 shows how the computation of the (usual) Gröbner bases for saturated pure binomial ideals (with respect to any term order) is equivalent to the computation of the Gröbner bases for corresponding submodules of $\mathbb{Z}^n$. Section 5 shows how one can find minimal and reduced Gröbner bases for rank 2 submodules, with respect to lex, by means of the orders $\sqsubset$ and $\prec$.

The computer algebra system CoCoA [6] has been used for some examples related to this work.

We thank the referee for checking all details very accurately.

After this paper had been accepted for publication, it was pointed out to us that results very similar to the ones appearing in Sections 2 and 3 can be found in [11], an article previously unknown to us. Indeed there is some overlap with [11], particularly in the definition and characterization of the order $\prec$. Our approach, however, is different, for we aim at computing Gröbner bases for submodules of $\mathbb{Z}^n$ in a way completely independent of polynomial ideals, and amenable to new algorithmic strategies.

It was also pointed out to us that interesting recent work on the computation of toric ideals has been done by Hemmecke and his collaborators; see for instance [9].

2. Gröbner bases in $\mathbb{Z}^n$

Given $\alpha := (\alpha_1, \ldots, \alpha_n)$, $\beta := (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$, we say that α divides β (notation: $\alpha \mid \beta$), if $\alpha_i \leq \beta_i$ for all i.

If $a := (a_1, \ldots, a_n) \in \mathbb{Z}^n$, a can be uniquely written as $a = a^+ - a^-$ where a^+, a^- are in $\mathbb{N}^n$ and have disjoint support.

Let $<_\tau$ be a term order in $\mathbb{N}^n$ (that is $<_\tau$ is a total order on $\mathbb{N}^n$ compatible with the additive structure of $\mathbb{N}^n$ and such that $0 \leq_\tau a$ for all $a \in \mathbb{N}^n$) and extend it to $\mathbb{Z}^n$. Let $\tau(\mathbb{Z}^n) := \{a \in \mathbb{Z}^n \mid a^+ >_\tau a^-\}$. Note that $0 \notin \tau(\mathbb{Z}^n)$ and if $a \neq 0$, then either $a \in \tau(\mathbb{Z}^n)$ or $-a \in \tau(\mathbb{Z}^n)$.

Let $a, b \in \mathbb{Z}^n$ and $F := \{f_1, \ldots, f_r\} \subseteq \tau(\mathbb{Z}^n)$. We say that a reduces to b modulo F in one step if there exists $i \in \{1, \ldots, r\}$ such that either f_i^+ divides a^+ and $b = a - f_i$ or f_i^+ divides a^- and $b = a + f_i$. We say that a reduces to b modulo F if there exist $b_1, b_2, \ldots, b_k \in \mathbb{Z}^n$ such that a reduces to b_1 in one step modulo F, b_1 reduces to b_2 in one step modulo F, ..., b_{k-1} reduces to b_k in one step modulo F and $b_k = b$. We say that a is reduced modulo F if f_i^+ does not divide a^+ and a^- for all $i \in \{1, \ldots, r\}$.

LEMMA 2.1. *Let $a \in \mathbb{Z}^n$ and suppose that $a = u - v$ where $u, v \in \mathbb{N}^n$ (we do not assume that u and v have disjoint support). Then there exists $p \in \mathbb{N}^n$ such that $a^+ = u - p$ and $a^- = v - p$.*

Proof. It suffices to choose $p_i = \min(u_i, v_i)$, where p_i, u_i and v_i denote the i-th components of p, u and v respectively. □

LEMMA 2.2. *Define the following order on the set* $\mathbb{N}^n \times \mathbb{N}^n$*:* $(\alpha, \beta) <_1 (\alpha', \beta')$ *if and only if* $\alpha <_\tau \alpha'$ *or* $\alpha = \alpha'$ *and* $\beta <_\tau \beta'$*. Then* $\mathbb{N}^n \times \mathbb{N}^n$ *is a well ordered set.*

Proof. It is clear that $<_1$ is a total order. It is easy to see that it is a well ordering since $<_\tau$ is a well ordering. □

PROPOSITION 2.3. *Let* F *be as above and let* $a \in \mathbb{Z}^n$*. Then it is possible to construct, in a finite number of steps, an element* $b \in \mathbb{Z}^n$ *such that* a *reduces to* b *modulo* F *and* b *is reduced modulo* F*.*

Proof. To every element $a \in \mathbb{Z}^n$ we associate the element $C(a) := (a^+, a^-) \in \mathbb{N}^n \times \mathbb{N}^n$.

If a is reduced modulo F there is nothing to prove. Otherwise there exists f_i such that $f_i^+ \mid a^+$ or $f_i^+ \mid a^-$. In the first case we have that a reduces, in one step, to $a' := a - f_i$. Since $f_i^+ \mid a^+$, we have that there exists $d \in \mathbb{N}^n$ such that $a^+ = f_i^+ + d$. Hence $a' = a^+ - a^- - f_i^+ + f_i^- = f_i^- + d - a^-$. From Lemma 2.1, we have that there exists a $p \in \mathbb{N}^n$ such that $a'^+ = f_i^- + d - p$ and $a'^- = a^- - p$. Since $<_\tau$ is a term order, we have: $a^+ = f_i^+ + d >_\tau f_i^- + d \geq_\tau f_i^- + d - p$ and $a^- \geq_\tau a^- - p$. This proves that $C(a') <_1 C(a)$. Similarly, suppose $f_i^+ \mid a^-$. In this case a reduces, in one step, to $a' := a + f_i$. Let $d \in \mathbb{N}^n$ be such that $a^- = f_i^+ + d$. Hence $a' = a^+ - a^- + f_i^+ - f_i^- = a^+ - (f_i^- + d)$ and again there exists a $p \in \mathbb{N}^n$ such that $a' = a^+ - p - (f_i^- + d - p)$ and $C(a') = (a^+ - p, f_i^- + d - p)$, so $C(a') <_1 C(a)$. In both cases, the reduction modulo F has produced an element in $\mathbb{N}^n \times \mathbb{N}^n$ smaller than $C(a)$. Lemma 2.2 shows that after a finite number of steps the process produces an element $b \in \mathbb{Z}^n$ reduced modulo F. □

Let $0 \neq M \subseteq \mathbb{Z}^n$ be a $\mathbb{Z}$-submodule (necessarily free, of rank at most n), and let $g_1, \ldots, g_k \in M \cap \tau(\mathbb{Z}^n)$.

DEFINITION 2.4. *We say that* $g_1, \ldots, g_k \in M \cap \tau(\mathbb{Z}^n)$ *is a Gröbner basis for* M *with respect to the given term order* $<_\tau$ *if and only if for all* $a \in M \cap \tau(\mathbb{Z}^n)$ *there exists an index* $i \in \{1, \ldots, k\}$ *such that* $g_i^+ \mid a^+$*.*

PROPOSITION 2.5. *Let* $0 \neq M \subseteq \mathbb{Z}^n$ *and let* $G := \{g_1, \ldots, g_k\} \subseteq M \cap \tau(\mathbb{Z}^n)$*. Then the following statements are equivalent:*

1. *G is a Gröbner basis for M;*

2. *$a \in M$ if and only if a reduces to 0 modulo G.*

Proof. Suppose G is a Gröbner basis. Let $a \in \mathbb{Z}^n$. By Proposition 2.3 there exists a b such that a reduces to b modulo G and b is reduced. Hence $a - b \in M$. If $a \in M$ then $b \in M$ and this shows that $b = 0$. If $b = 0$ then clearly $a \in M$.

Suppose now that *2* holds and let $a \in M \cap \tau(\mathbb{Z}^n)$, so $a^+ >_\tau a^-$. If there exists some $g_i \in G$ such that $g_i^+ \mid a^+$, then we are done. Suppose for a contradiction that this is not the case; hence there exists a suitable g_i such that $g_i^+ \mid a^-$. Adopting the notation of the proof of Proposition 2.3, we have that a reduces to a_1 where $a_1^+ = a^+ - p$ and $a_1^- = g_i^- + d - p$ (where $p,\ d$ are suitable elements in $\mathbb{N}^n$). Note that $a_1^+ >_\tau a_1^-$ (as follows from $a^+ >_\tau a^- = g_i^+ + d \geq_\tau g_i^- + d$). In particular, $a_1^+ = a^+ - p >_\tau 0$. Since a_1 can be reduced modulo G, then either $a^+ - p$ or $g_i^- + d - p$ is a multiple of a suitable g_j^+. In the first case, since $a^+ - p \neq 0$, also a^+ would be a multiple of g_j, against our assumption. Hence we see that in each step of the process of reduction of a to 0 modulo G we produce elements $a_1, a_2, \ldots$ such that $a_i^+ >_\tau 0$ for all $i = 1, 2, \ldots$ and this is a contradiction. □

If $S \subseteq \mathbb{N}^n$, denote by $\langle S \rangle$ the submonoid of $\mathbb{N}^n$ generated by S, namely, $\langle S \rangle := \bigcup_{\alpha \in S}(\alpha + \mathbb{N}^n)$, where $\alpha + \mathbb{N}^n = \{\alpha + \beta : \beta \in \mathbb{N}^n\}$. Clearly, $\langle S \rangle = \{\beta \in \mathbb{N}^n : \exists \alpha \in S \text{ s.t. } \alpha \mid \beta\}$. By Dickson's Lemma (cf. e.g. [1], Corollary 4.48), $\langle S \rangle$ is finitely generated, that is, one can find finitely many elements $\alpha(1), \ldots, \alpha(s)$ of S such that $\langle S \rangle = \bigcup_{i=1}^{s}(\alpha(i) + \mathbb{N}^n)$.

If X is any subset of $\mathbb{Z}^n$, denote by $\mathrm{Lt}_\tau(X)$ the submonoid of $\mathbb{N}^n$ generated by the set $S := \{a^+ \ : \ a \in X \cap \tau(\mathbb{Z}^n)\}$.

PROPOSITION 2.6. *Let $0 \neq M \subseteq \mathbb{Z}^n$ and let $G := \{g_1, \ldots, g_k\} \subseteq M \cap \tau(\mathbb{Z}^n)$. Then the following statements are equivalent:*

1. *G is a Gröbner basis for M;*

2. *$Lt_\tau(M) = Lt_\tau(G)$.*

Proof. Let G be a Gröbner basis and let $a \in M \cap \tau(\mathbb{Z}^n)$; then clearly $a^+ \in \mathrm{Lt}_\tau(G)$. Conversely, if *2* holds, $a \in M \cap \tau(\mathbb{Z}^n)$ implies $a^+ \in \mathrm{Lt}_\tau(M) = \mathrm{Lt}_\tau(G)$; hence there exists $g_i \in G$ such that $g_i^+ \,|a^+$ and G is a Gröbner basis. □

PROPOSITION 2.7. *If $g_1, \ldots, g_k$ is a Gröbner basis for $0 \neq M \subseteq \mathbb{Z}^n$, then $g_1, \ldots, g_k$ is a system of generators of M.*

Proof. An immediate consequence of Proposition 2.5. □

PROPOSITION 2.8. *If $0 \neq M \subseteq \mathbb{Z}^n$, then M has a Gröbner basis.*

Proof. By Dickson's Lemma, $\mathrm{Lt}_\tau(M)$ is finitely generated by a set of elements $\{g_1^+, \ldots, g_k^+\}$ for suitable $g_1, \ldots, g_k \in M \cap \tau(\mathbb{Z}^n)$. Hence $g_1, \ldots, g_k$ is a Gröbner basis for M by Proposition 2.6. □

3. Minimal and reduced Gröbner bases in $\mathbb{Z}^n$

DEFINITION 3.1. *Let $G := \{g_1, \ldots, g_k\}$ be a Gröbner basis for $0 \neq M \subseteq \mathbb{Z}^n$. We say that G is a minimal Gröbner basis for M if and only if the following condition holds:*
for all $i, j \in \{1, \ldots, k\}$, if $g_i^+ \mid g_j^+$ then $i = j$.

Given a Gröbner basis G for $0 \neq M \subseteq \mathbb{Z}^n$, in order to extract from it a minimal Gröbner basis, it is enough to erase from G those elements g such that g^+ is a multiple of some other h^+ with $h \in G$.

PROPOSITION 3.2. *Suppose $g_1, \ldots, g_k$ and $h_1, \ldots, h_p$ are two minimal Gröbner bases for $0 \neq M \subseteq \mathbb{Z}^n$. Then $k = p$ and the two sets $\{g_1^+, \ldots, g_k^+\}$ and $\{h_1^+, \ldots, h_k^+\}$ are equal.*

Proof. Take an index $i \in \{1, \ldots, k\}$. Since $g_i \in M \cap \tau(\mathbb{Z}^n)$, there exists an h_{j_i} such that $h_{j_i}^+ \mid g_i^+$; but $h_{j_i} \in M \cap \tau(\mathbb{Z}^n)$, then there exists a g_j such that $g_j^+ \mid h_{j_i}^+$, therefore $g_j^+ \mid g_i^+$. This implies that $g_i^+ = g_j^+ = h_{j_i}^+$, and the statement follows immediately. □

DEFINITION 3.3. *Let $G := \{g_1, \ldots, g_k\}$ be a Gröbner basis for $0 \neq M \subseteq \mathbb{Z}^n$. We say that G is a reduced Gröbner basis for M if and only if*

- *G is a minimal Gröbner basis;*

- *for all* $i, j \in \{1, \ldots, k\}$, g_i^+ *does not divide* g_j^-.

Given a minimal Gröbner basis G for $0 \neq M \subseteq \mathbb{Z}^n$, it is possible to construct from it a reduced Gröbner basis. Indeed, if $G = \{g_1, \ldots, g_k\}$, let h_1 be obtained by reduction of g_1 modulo $\{g_2, \ldots, g_k\}$, h_2 be obtained by reduction of g_2 modulo $\{h_1, g_3, \ldots, g_k\}$, ... h_k be obtained by reduction of g_k modulo $\{h_1, \ldots, h_{k-1}\}$. Then it is easy to see that $\{h_1, \ldots, h_k\}$ satisfies Definition 3.3.

PROPOSITION 3.4. *The reduced Gröbner basis for* $0 \neq M \subseteq \mathbb{Z}^n$ *is unique.*

Proof. Suppose that G and H are two reduced Gröbner bases. From Proposition 3.2 we know that G and H have the same number k of elements and we can assume that they are ordered in such a way that $g_i^+ = h_i^+$ for $i = 1, \ldots, k$ (where $G := \{g_1, \ldots, g_k\}$ and $H := \{h_1, \ldots, h_k\}$). Consider $g_i - h_i = h_i^- - g_i^-$. If this element of M is not 0, then it reduces to 0 modulo G and also modulo H, but this contradicts the second condition of a reduced Gröbner basis. □

We define now the following relation on the set $\tau(\mathbb{Z}^n)$: given $a_1, a_2 \in \tau(\mathbb{Z}^n)$, we say that $a_1 \sqsubset a_2$ if $a_1^+ \neq a_2^+$ and $a_1^+ \mid a_2^+$. It is easy to verify that $\sqsubset$ is a partial order on the set $\tau(\mathbb{Z}^n)$.

THEOREM 3.5. *If* $\{g_1, \ldots, g_k\}$ *is a minimal Gröbner basis for* $0 \neq M \subseteq \mathbb{Z}^n$, *then*

1. $g_1, \ldots, g_k$ *are minimal elements of* $M \cap \tau(\mathbb{Z}^n)$ *w.r.t.* $\sqsubset$ *and, if* $i \neq j$, *then* $g_i^+ \neq g_j^+$;
2. $\{g_1, \ldots, g_k\}$ *is maximal w.r.t. the above property.*

Conversely, if we have a set $\{g_1, \ldots, g_k\} \subseteq M \cap \tau(\mathbb{Z}^n)$ *satisfying the two conditions above, then it is a minimal Gröbner basis for* M.

Proof. Let us consider an element g_i of the given minimal Gröbner basis. If g_i is not minimal for $\sqsubset$, then there exists $h \in M \cap \tau(\mathbb{Z}^n)$ such that $h \sqsubset g_i$. Then $h^+ \neq g_i^+$ and $h^+ \mid g_i^+$. Since there exists a g_j such that $g_j^+ \mid h^+$, then $g_j^+ \mid g_i^+$ which gives $i = j$, hence $g_i^+ = h^+$,

a contradiction. If $\{g_1, \ldots, g_k\}$ is not maximal, then there exists an $h \in M \cap \tau(\mathbb{Z}^n)$ minimal w.r.t. $\sqsubset$ such that $g_i^+ \neq h^+$ for all i. Using again the hypothesis, we get that there exists a g_j such that $g_j^+ \mid h^+$, hence $g_j \sqsubset h$, a contradiction.

Suppose now that for the set $\{g_1, \ldots, g_k\}$ the two conditions of the theorem are satisfied; we want to conclude that the set is a minimal Gröbner basis. It is easy to see that any strictly decreasing chain of elements of $M \cap \tau(\mathbb{Z}^n)$ w.r.t. $\sqsubset$ must be finite, hence if $a \in M \cap \tau(\mathbb{Z}^n)$ there exists $b \in M \cap \tau(\mathbb{Z}^n)$ such that $b \sqsubset a$ and b is a minimal element of $M \cap \tau(\mathbb{Z}^n)$. Since $\{g_1, \ldots, g_k\}$ is maximal, there exists g_i such that $g_i^+ = b^+$ hence $g_i^+ \mid a^+$. This shows that the g_i's form a Gröbner basis. If $g_i^+ \mid g_j^+$, since $g_i^+ \neq g_j^+$, then we would have $g_i^+ \sqsubset g_j^+$, a contradiction. Hence the Gröbner basis is minimal. □

Finally we define another relation on $\tau(\mathbb{Z}^n)$ as follows: given $a_1, a_2 \in \tau(\mathbb{Z}^n)$, we say that $a_1 \prec a_2$ if $a_1^+ \neq a_2^+$ and $a_1^+ \mid a_2^+$ or if $a_1^+ = a_2^+$ and $a_1^- <_\tau a_2^-$. It is easy to verify that $\prec$ is a partial order on $\tau(\mathbb{Z}^n)$ which refines $\sqsubset$.

THEOREM 3.6. *We have: $\{g_1, \ldots, g_k\}$ is the reduced Gröbner basis for $0 \neq M \subseteq \mathbb{Z}^n$ if, and only if, $\{g_1, \ldots, g_k\}$ is the set of all minimal elements of $M \cap \tau(\mathbb{Z}^n)$ w.r.t. $\prec$.*

Proof. First we show that any g_i is minimal. Since $\prec$ refines $\sqsubset$, from Theorem 3.5 we have that g_i is minimal for $\sqsubset$. Suppose that g_i is not minimal for $\prec$; hence there exists $h \in M \cap \tau(\mathbb{Z}^n)$ such that $h \prec g_i$, so $h^+ = g_i^+$ and $h^- <_\tau g_i^-$. Let $a := h - g_i = g_i^- - h^-$. From Lemma 2.1 we have that there exists $p \in \mathbb{N}^n$ such that $a^+ = g_i^- - p$. Since $a \in M \cap \tau(\mathbb{Z}^n)$, there exists g_j such that $g_j^+ \mid g_i^- - p$, hence $g_j^+ \mid g_i^-$, against the hypothesis. To see that all the minimal elements are among the g_i's, let $h \in M \cap \tau(\mathbb{Z}^n)$ be minimal for $\prec$. Then h is minimal also for $\sqsubset$, hence, from Theorem 3.5, there exists g_i such that $g_i^+ = h^+$. If $h^- <_\tau g_i^-$, then $h \prec g_i$, a contradiction with the minimality of g_i; if $g_i^- <_\tau h^-$, then $g_i \prec h$, a contradiction with the minimality of h; hence $h = g_i$.
Conversely, suppose that $\{g_1, \ldots, g_k\}$ is the set of all the minimal elements of $M \cap \tau(\mathbb{Z}^n)$, and let $a \in M \cap \tau(\mathbb{Z}^n)$. Since $<_\tau$ is a well ordering, it is easy to see that any strictly decreasing chain of elements of $M \cap \tau(\mathbb{Z}^n)$ w.r.t. $\prec$ is finite, hence there exists $b \in$

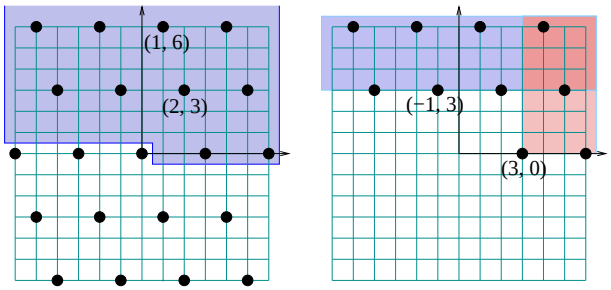

Figure 1: The module M and its first Gröbner basis

$M \cap \tau(\mathbb{Z}^n)$ minimal such that $b \prec a$. Hence there exists g_i such that $g_i = b$, so $g_i^+ \mid a$. □

EXAMPLE 3.7. *Let us consider the module* $M \subseteq \mathbb{Z}^2$ *generated by* $(2,3)$ *and* $(1,6)$. *Let* $<_\tau$ *be the "xel" term order on* $\mathbb{N}^2$ *(i.e.* $(\alpha,\beta) <_\tau (\gamma,\delta)$ *if* $\beta < \delta$ *or* $\beta = \delta$ *and* $\alpha < \gamma$*). The module* M *is represented by the black dots occurring in the left part of Figure 1. The highlighted region represents the set* $M \cap \tau(\mathbb{Z}^2)$. *In this example it is easy to see, from the right part of Figure 1, that* $(3,0)$ *and* $(-1,3)$ *are the only minimal elements w.r.t. the partial order* $\prec$*; hence these two elements are the reduced Gröbner basis for* M *(the hightlighted regions represent the elements* $a \in M \cap \tau(\mathbb{Z}^2)$ *such that* $(-1,3) \prec a$ *or* $(3,0) \prec a$*). Note that we have many different minimal Gröbner bases:* $\{(3,0),(-4,3)\}$ *or* $\{(3,0),(-7,3)\}$ *are two possible examples.*

Fix now on $\mathbb{N}^2$ *the term order* $<_\tau$ *given by the following matrix:* $\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}$, *i.e.,* $(\alpha,\beta) <_\tau (\gamma,\delta)$ *if* $3\alpha+\beta < 3\gamma+\delta$ *or, if* $3\alpha+\beta = 3\gamma+\delta$, *then* $\alpha < \gamma$.

The left part of Figure 2 shows the set $M \cap \tau(\mathbb{Z}^2)$, *while the right part shows the minimal elements of* $M \cap \tau(\mathbb{Z}^2)$ *w.r.t. the partial order* $\prec$. *Hence in this case the reduced Gröbner basis for the module* M *is given by* $(1,-3)$ *and* $(0,9)$.

4. Pure binomial ideals

In this section we shall often apply the usual Gröbner bases techniques of polynomial rings. Hence, if not explicitly stated, the no-

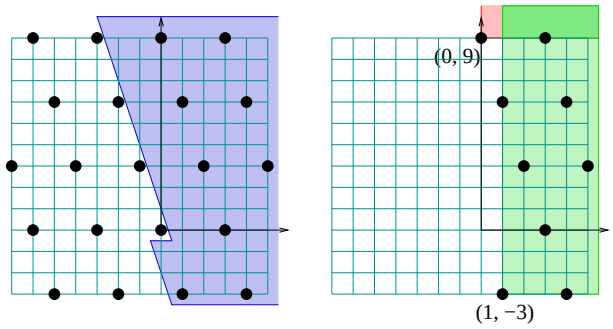

Figure 2: Another Gröbner basis for M

tions of Gröbner basis, reduction, leading term (Lt) etc. will not refer to the definitions of the previous sections.

Let K be any field of characteristic $\neq 2$. By a *pure binomial* (or *binomial*, for short) in $K[x_1, \dots, x_n]$ we mean a polynomial which is the difference of two terms (= monic monomials). Given $b = (b_1, \dots, b_n) \in \mathbb{Z}^n$, we associate to it the binomial f_b such that

$$f_b := x_1^{\max(b_1,0)} \cdots x_n^{\max(b_n,0)} - x_1^{-\min(b_1,0)} \cdots x_n^{-\min(b_n,0)}.$$

If we write $b = b^+ - b^-$, we use the short notation $f_b = x^{b^+} - x^{b^-}$ (where, if $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, x^α denotes $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$).

Let

$$\phi : \mathbb{Z}^n \longrightarrow K[x_1, \dots, x_n]$$

be the injective map given by $\phi(b) = f_b$. (Injectivity follows from $\operatorname{char}(K) \neq 2$).

A binomial $f \in K[x_1, \dots, x_n]$ is called *saturated (with respect to the indeterminates)* if for all $i = 1, \dots, n$, x_i is not a factor of f. If f is any binomial, let $Sat(f)$ be the binomial obtained from f by saturation, i.e., $Sat(f)$ is a saturated binomial such that $f/Sat(f)$ is a monomial.

Let B_{sat} be the set of all saturated binomials.

LEMMA 4.1. *We have:*

1. *for all $b \in \mathbb{Z}^n$, $\phi(b)$ is a saturated binomial;*
2. *ϕ gives a bijection between $\mathbb{Z}^n$ and B_{sat}.*

Proof. An immediate computation. □

In this section we shall consider *pure binomial ideals*, i.e., (non-zero) ideals generated by pure binomials. In the sequel we shall call them binomial ideals, for short. If I is a binomial ideal generated by $f_1, \ldots, f_r$, let $m_1 := \phi^{-1}(Sat(f_1))$, ..., $m_r := \phi^{-1}(Sat(f_r))$; we denote by $M(f_1, \ldots, f_r) \subseteq \mathbb{Z}^n$ the $\mathbb{Z}$-module generated by $m_1, \ldots, m_r$.

By $Sat(I)$ we denote the saturation of the ideal I with respect to the indeterminates, i.e.,

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

Finally, given two binomials $f = x^a - x^b$ and $g = x^c - x^d$, we define $\sigma(f, g)$ as the binomial $x^c f - x^a g$.

LEMMA 4.2. *Let b_1, b_2 be in $\mathbb{Z}^n$. Then:*

1. $\phi(b_1 - b_2) = Sat(\sigma(\phi(b_1), \phi(b_2)))$;
2. $\phi(b_1 + b_2) = Sat(\sigma(\phi(b_1), \phi(-b_2)))$.

Let I be a binomial ideal as above. Then:

3. *if $\phi(b_1), \phi(b_2) \in Sat(I)$, then $\phi(b_1 - b_2), \phi(b_1 + b_2) \in Sat(I)$;*
4. *if $\phi(b_1) \in Sat(I)$ and $\lambda \in \mathbb{Z}$, then $\phi(\lambda b_1) \in Sat(I)$.*

Proof. Let $b_1 = b_1^+ - b_1^-$ and $b_2 = b_2^+ - b_2^-$; then $\phi(b_1) = x^{b_1^+} - x^{b_1^-}$ and $\phi(b_2) = x^{b_2^+} - x^{b_2^-}$. We have: $b_1 - b_2 = u - v$ where $u = (b_1^+ + b_2^-)$ and $v = (b_1^- + b_2^+)$ and, from Lemma 2.1, there exists a $p \in \mathbb{N}^n$ such that $(b_1 - b_2)^+ = u - p$ and $(b_1 - b_2)^- = v - p$. Hence $\phi(b_1 - b_2) = x^{u-p} - x^{v-p}$, so $x^p \phi(b_1 - b_2) = x^u - x^v$. Since $\sigma(\phi(b_1), \phi(b_2)) = x^u - x^v$, we get that $\phi(b_1 - b_2) = Sat(x^p \phi(b_1 - b_2)) = Sat(\sigma(\phi(b_1), \phi(b_2)))$.

The second claim follows immediately from the first.

To see the third claim, it is enough to observe that, by definition of σ, $\sigma(\phi(b_1), \phi(b_2)) \in Sat(I)$ and hence the statement follows from *1* and *2*.

The last claim is a consequence of *3*, since $\lambda b_1 = b_1 + \cdots + b_1$ (if $\lambda > 0$) or $\lambda b_1 = -b_1 - \cdots - b_1$ (if $\lambda < 0$). □

PROPOSITION 4.3. *Let I be a binomial ideal generated by binomials $f_1, \ldots, f_r$. If $b \in M(f_1, \ldots, f_r)$, then $\phi(b) \in Sat(I)$.*

Proof. By definition, $M(f_1, \ldots, f_r)$ is generated by the monomials $m_i := \phi^{-1}(f_i)$ and the corresponding $\phi(m_i)(= Sat(f_i))$ are in $Sat(I)$ $(i = 1, \ldots, r)$. If $b \in M$ then b is a linear combination, with coefficients in $\mathbb{Z}$, of $m_1, \ldots, m_r$; hence the statement follows from Lemma 4.2, parts *3* and *4*. □

We recall the following:

PROPOSITION 4.4. *If I is a binomial ideal, then $\mathrm{Sat}(I) \neq (1)$ and is a binomial ideal.*

Proof. First of all, let us prove that $I := (f_1, \ldots, f_r)$ (where the f_i's are pure binomials) does not contain monomials. Fix a term order and let G be the reduced Gröbner basis for I. If I contained monomials, then also G should contain monomials. If we follow the Buchberger algorithm used for computing G, we see that the S-polynomial of two pure binomials is again a pure binomial and the reduction of a pure binomial by a pure binomial, if not 0, is a pure binomial. This shows that all the elements produced in the computation of G are pure binomials. Hence $Sat(I) \neq (1)$. The ideal $Sat(I)$ can be computed by the formula:

$$Sat(I) = K[x_1, \ldots, x_n] \cap (I + (t \cdot x_1 \cdots x_n - 1)),$$

and from this it follows that $Sat(I)$ is a pure binomial ideal. □

PROPOSITION 4.5. *If $I = (f_1, \ldots, f_r)$ is a binomial ideal and $f \in \mathrm{Sat}(I)$ is a saturated binomial, then there exists an element $b \in M(f_1, \ldots, f_r)$ such that $\phi(b) = f$.*

Proof. Fix a term order $<_\tau$ in $K[x_1, \ldots, x_n]$ and let $\{g_1, \ldots, g_k\}$ be the corresponding reduced Gröbner basis for I.

Claim: There exist $p_1, \ldots, p_k \in M(f_1, \ldots, f_r)$ such that $\phi(p_i) = Sat(g_i)$ for $i = 1, \ldots, k$.

To prove this claim, we observe that in order to compute the Gröbner basis for I (with the Buchberger algorithm) we have

to compute S-polynomials and reductions (starting from the binomials $f_1, \ldots, f_r$). Moreover, a one step reduction of a polynomial a w.r.t. a polynomial b can be seen as the computation of the S-polynomial $S(a, b)$. Since $Sat(f_1), \ldots, Sat(f_r)$ are in $\phi(M(f_1, \ldots, f_r))$, it is enough to prove that if $h_1, h_2 \in I$ are two binomials whose saturation is in $\phi(M(f_1, \ldots, f_r))$, then also $Sat(S(h_1, h_2))$ is in $\phi(M(f_1, \ldots, f_r))$. Let then $h_1, h_2 \in I$ and let $b_1, b_2 \in M(f_1, \ldots, f_r)$ be such that $\phi(b_1) = Sat(h_1)$ and $\phi(b_2) = Sat(h_2)$. Let $b_1 = b_1^+ - b_1^-$ and $b_2 = b_2^+ - b_2^-$ and suppose further that $x^{b_1^+} >_\tau x^{b_1^-}$ and $x^{b_2^+} >_\tau x^{b_2^-}$ (if this is not the case, change b_1 and h_1 with $-b_1$ and $-h_1$ or b_2 and h_2 with $-b_2$ and $-h_2$). Then $Sat(S(h_1, h_2)) = Sat(\sigma(\phi(b_1), \phi(b_2)))$. Lemma 4.2 gives that $Sat(S(h_1, h_2)) = \phi(b_1 - b_2)$ is in $\phi(M(f_1, \ldots, f_r))$ and the claim follows.

Let now $f \in Sat(I)$ be a saturated binomial; then there exists $a \in \mathbb{N}^n$ s.t. $x^a f \in I$, hence $x^a f$ reduces to 0 w.r.t. $\{g_i\}$. Let $u_1, \ldots, u_s, u_{s+1} = 0$ be the binomials produced in the process of reduction, hence $u_1 = x^a f - x^{t_1} g_{i_1}$, $u_2 = u_1 - x^{t_2} g_{i_2}$, $\ldots$ $u_{s+1} = u_s - x^{t_{s+1}} g_{i_{s+1}}$ where $t_1, \ldots, t_{s+1}$ are suitable elements of $\mathbb{N}^n$, $i_1, \ldots, i_{s+1}$ are suitable indexes in $\{1, \ldots, k\}$ and $\mathrm{Lt}_\tau(u_j) = \mathrm{Lt}_\tau(x^{t_{j+1}} g_{i_{j+1}})$. From $0 = u_{s+1} = u_s - x^{t_{s+1}} g_{i_{s+1}}$ we deduce that $Sat(u_s)$ is in $\phi(M(f_1, \ldots, f_r))$. To see that $f \in \phi(M(f_1, \ldots, f_r))$, it is therefore enough to prove the following:

Let u, v, g be binomials such that $Lt_\tau(v) = Lt_\tau(g)$, $u = v - g$ and $Sat(u), Sat(g) \in \phi(M(f_1, \ldots, f_r))$. Then $Sat(v) \in \phi(M(f_1, \ldots, f_r))$.

Let $b, p \in M(f_1, \ldots, f_r)$ be such that $\phi(b) = Sat(u)$ and $\phi(p) = Sat(g)$. Then $u = x^{b^+ + c} - x^{b^- + c}$, $g = x^{p^+ + d} - x^{p^- + d}$ (for suitable $c, d \in \mathbb{N}^n$) and $b^+ + c = p^- + d$ (since $\mathrm{Lt}_\tau(v) = \mathrm{Lt}_\tau(g)$). Hence $v = x^{p^+ + d} - x^{b^- + c}$. Consider $p + b$: $p + b = (p^+ + b^+) - (p^- + b^-) = (p^+ + b^+ + c) - (p^- + b^- + c) = (p^+ + d) - (b^- + c)$. This shows that $Sat(v) = \phi(p + b)$. □

As a consequence of Proposition 4.4, we can always assume that we have a Gröbner basis for $Sat(I)$ formed by binomials; moreover it is not restrictive to suppose that these binomials are saturated. **Hence from now on, a Gröbner basis for $Sat(I)$ will always**

be meant to consist of saturated binomials. From Proposition 4.3 and Proposition 4.5 we have:

PROPOSITION 4.6. *Given a binomial ideal $I := (f_1, \ldots, f_r)$, the map ϕ gives a bijection between the module $M(f_1, \ldots, f_r)$ and the set of all saturated binomials of $\mathrm{Sat}(I)$. In particular, $\phi(M(f_1, \ldots, f_r))$ contains all the Gröbner bases of $\mathrm{Sat}(I)$.*

Suppose that $I = (f_1, \ldots, f_r) = (h_1, \ldots, h_s)$. The above proposition says that ϕ puts both $M(f_1, \ldots, f_r)$ and $M(h_1, \ldots, h_s)$ in one-to-one correspondence with the set of all saturated binomials of $Sat(I)$. The injectivity of ϕ gives $M(f_1, \ldots, f_r) = M(h_1, \ldots, h_s)$ (since every saturated binomial $f \in Sat(I)$ is equal to both $\phi(b) \in M(f_1, \ldots, f_r)$ and $\phi(b') \in M(h_1, \ldots, h_s)$, whence $b = b'$). Therefore there is just one submodule of $\mathbb{Z}^n$ associated with I. We denote it by M_I.

LEMMA 4.7. *Let $<_\tau$ be a term order, I a binomial ideal. Then $Lt_\tau(I) = Lt_\tau(B(I))$, where $B(I)$ is the set of binomials of I.*

Proof. If G is the Gröbner basis for I w.r.t. $<_\tau$, then $G \subseteq B(I)$. Hence $\mathrm{Lt}_\tau(I) \supseteq \mathrm{Lt}_\tau(B(I)) \supseteq \mathrm{Lt}_\tau(G) = \mathrm{Lt}_\tau(I)$. □

We now link the notion of Gröbner bases for $\mathbb{Z}$-submodules of $\mathbb{Z}^n$, given in the previous sections, to the usual notion of Gröbner bases for binomial ideals in the ring $K[x_1, \ldots, x_n]$.

THEOREM 4.8. *Let I be a binomial ideal. Then the map ϕ induces a bijection between the set of Gröbner bases of M_I (as in Definition 2.4) and the set of Gröbner bases of the ideal $\mathrm{Sat}(I)$. More precisely, if $<_\tau$ is a term order and G is a Gröbner basis for M_I w.r.t. it, then $\phi(G)$ is a Gröbner basis for $\mathrm{Sat}(I)$ w.r.t. $<_\tau$, and conversely. Furthermore, in this bijection, minimal and reduced Gröbner bases for M_I (as in Definitions 3.1 and 3.3) correspond to minimal and reduced Gröbner bases for the ideal $\mathrm{Sat}(I)$.*

Proof. Let $<_\tau$ be a term order and let G be a Gröbner basis for M_I as in Definition 2.4. We want to prove that $\phi(G)$ is a Gröbner basis for $Sat(I)$ w.r.t. $<_\tau$. From Lemma 4.7, it is enough to see that if $f \in Sat(I)$ is a binomial, then $\mathrm{Lt}_\tau(f) \in \mathrm{Lt}_\tau(\phi(G))$. Let $h \in Sat(I)$ be the saturation of f. Then there exists $b \in M_I$ s.t.

$\phi(b) = h$ and it is not restrictive to assume that $b \in M \cap \tau(\mathbb{Z}^n)$. Hence there exists $g \in G$ such that $g^+ \mid b^+$. Since $\phi(g) = x^{g^+} - x^{g^-}$ and $h = \phi(b) = x^{b^+} - x^{b^-}$, we have that $\mathrm{Lt}(\phi(g))$ divides $\mathrm{Lt}(h)$ and clearly $\mathrm{Lt}(h)$ divides $\mathrm{Lt}(f)$. Conversely, if H is a Gröbner basis for $Sat(I)$, then the same kind of computations shows that $\phi^{-1}(H)$ is a Gröbner basis of M_I. Finally, it is easy to see that, in the given correspondence, minimal (reduced) Gröbner bases of M_I correspond to minimal (reduced) Gröbner bases of $Sat(I)$. □

We end this section by proving that there is a one-to-one correspondence between submodules of $\mathbb{Z}^n$ and saturated pure binomial ideals of $K[x_1, \ldots, x_n]$.

PROPOSITION 4.9. *For every binomial ideal I, $Sat(I)$ equals $(\phi(M_I))$, the ideal generated by $\phi(M_I)$.*

Proof. By Proposition 4.3, $(\phi(M_I)) \subseteq Sat(I)$. By Proposition 4.6, $(\phi(M_I)) \supseteq Sat(I)$. □

PROPOSITION 4.10. *For every $0 \neq M \subseteq \mathbb{Z}^n$, let I be the ideal $(\phi(M))$. Then $M_I = M$.*

Proof. Since $K[x_1, \ldots, x_n]$ is Noetherian, I can be generated by a finite number of elements of $\phi(M)$, say $\phi(b_1), \ldots, \phi(b_r)$. By definition, M_I is generated by $b_1, \ldots, b_r$. If $b \in M \setminus M_I$, then $\phi(b)$ is a saturated binomial of I and Proposition 4.3 implies that there exists $b' \in M_I$ such that $\phi(b') = \phi(b)$. But ϕ injective forces $b = b'$, a contradiction. Hence $M = M_I$ as claimed. □

COROLLARY 4.11. *For every $0 \neq M \subseteq \mathbb{Z}^n$, $(\phi(M))$ is a saturated ideal.*

Proof. Let $I := (\phi(M))$. Proposition 4.10 says that $M = M_I$. But Proposition 4.9 says that $(\phi(M_I)) = Sat(I)$. Hence $(\phi(M)) = Sat(I)$. □

COROLLARY 4.12. *For every binomial ideal I, $M_I = M_{Sat(I)}$.*

Proof. Let $J := Sat(I)$. Proposition 4.9 says that $J = (\phi(M_I))$. But then Proposition 4.10 says that $M_J = M_I$. □

THEOREM 4.13. *There exists a one-to-one correspondence between the set, $\mathcal{M}$, of all non-zero submodules M of $\mathbb{Z}^n$ and the set, $\mathcal{J}$, of all saturated pure binomial ideals J of $K[x_1, \ldots, x_n]$.*

Proof. Define $\chi : \mathcal{M} \longrightarrow \mathcal{J}$ by means of $M \mapsto (\phi(M))$, and $\omega : \mathcal{J} \longrightarrow \mathcal{M}$ by means of $J \mapsto M_J$. Then $\phi\omega = \mathrm{Id}$ because Propositon 4.9 implies $(\phi(M_J)) = Sat(J)$, and $Sat(J) = J$ by assumption. $\omega\chi = \mathrm{Id}$ because if $J := (\phi(M))$, then Proposition 4.10 implies $M_J = M$. □

5. Rank 2 submodules of $\mathbb{Z}^n$

As stressed in the Introduction, we believe that, in order to compute Gröbner bases of saturated pure binomial ideals, it is possible to avoid using the Buchberger algorithm by resorting to the calculation of minimal elements in suitable partially ordered subsets of $\mathbb{Z}^n$ (recall the end of Section 3). In this section we implement our point of view in the case of rank 2 submodule of $\mathbb{Z}^n$, w.r.t. lex.

Fix in $K[x_1, \ldots, x_n]$ the pure lexicographic term order $<_\tau$ such that $x_n <_\tau \cdots <_\tau x_1$ (consequently the analogous term order is defined in $\mathbb{Z}^n$). Let $I \subseteq K[x_1, \ldots, x_n]$ be a pure binomial ideal such that the module $M_I \subseteq \mathbb{Z}^n$ is of rank 2 and is generated by $a := (a_1, \ldots, a_n)$ and $b := (b_1, \ldots, b_n)$, say. We can assume that the matrix $\begin{pmatrix} a_1 & \ldots & a_n \\ b_1 & \ldots & b_n \end{pmatrix}$ is in Hermite normal form. Hence it is upper triangular and, in each row, the first non-zero entry from the left is positive; in particular, a and b are in $M_I \cap \tau(\mathbb{Z}^n)$.

Identify M_I with $\mathbb{Z}^2$ by means of the map $\psi : \mathbb{Z}^2 \longrightarrow M_I$ defined by $\psi(u, v) := ua + vb$. Then the set $M_I \cap \tau(\mathbb{Z}^n)$ corresponds to the set $A := \{(u, v) \in \mathbb{Z}^2 \ : \ u > 0 \text{ or } u = 0 \text{ and } v > 0\}$. The partial orders $\sqsubset$ and $\prec$ defined on $\tau(\mathbb{Z}^n)$ can be transferred on A by setting $(u, v) \sqsubset (u', v')$ iff $\psi(u, v) \sqsubset \psi(u', v')$ and $(u, v) \prec (u', v')$ iff $\psi(u, v) \prec \psi(u', v')$. It is clear that $\sqsubset$ and $\prec$ are partial orders on A and that (u, v) is a minimal element in $(A, \sqsubset)$ (resp., in $(A, \prec)$) if and only if $\psi(u, v)$ is minimal in $(M_I \cap \tau(\mathbb{Z}^n), \sqsubset)$ (resp., in $(M_I \cap \tau(\mathbb{Z}^n), \prec)$).

DEFINITION 5.1. *If $(u_0, v_0) \in \mathbb{Z}^2$, we set*

$$C(u_0, v_0) := \{(u, v) \in A \ : \ (u_0, v_0) \sqsubset (u, v)\}.$$

In more detail, $C(u_0, v_0)$ is the set of elements $(u, v) \in A$ such that $u_0a + v_0b \sqsubset ua + vb$ and this last condition (recalling the definition of $\sqsubset$) means that if $u_0a_i + v_0b_i > 0$, then $u_0a_i + v_0b_i \leq ua_i + vb_i$. Hence $C(u_0, v_0)$ is a cone in $\mathbb{Z}^2$ with vertex in (u_0, v_0).

The following proposition is easy to see:

PROPOSITION 5.2. *Let $(u, v), (u', v') \in A$. Then $(u', v') \in C(u, v)$ if and only if $C(u', v') \subseteq C(u, v)$, and $(u, v) \in A$ is minimal w.r.t. $\sqsubset$ if and only if $C(u, v)$ is minimal in the set of cones with vertices in A, ordered by inclusion.*

As an immediate consequence of Theorem 3.5 we have:

PROPOSITION 5.3. *Let $(u_1, v_1), \ldots, (u_k, v_k) \in A$. Then*

$$\psi(u_1, v_1), \ldots, \psi(u_k, v_k) \text{ is a minimal Gröbner basis for } M_I$$

if and only if:

1. *$C(u_1, v_1), \ldots, C(u_k, v_k)$ are minimal elements in the set*

$$\{C(u, v) \ : \ (u, v) \in A\}$$

   ordered by inclusion;

2. *$\{(u_1, v_1), \ldots, (u_k, v_k)\}$ is maximal w.r.t. the above property.*

A consequence of the definition of Gröbner basis given in Definition 2.4 is the following:

PROPOSITION 5.4. *Let $(u_1, v_1), \ldots, (u_k, v_k) \in A$. Then: $\psi(u_1, v_1), \ldots, \psi(u_k, v_k)$ are a Gröbner basis for M_I if and only if $C(u_1, v_1) \cup \cdots \cup C(u_k, v_k) = A$.*

The above propositions suggest an algorithm for computing a minimal Gröbner basis for M_I, and hence for $Sat(I)$:
Let $B_i \subseteq A$ ($i \in \mathbb{N}$) be any family of finite sets giving a partition of A. It is clear that there exists an index $n \in \mathbb{N}$ such that $\cup_{i=0}^{n} B_i$ contains (the subset of A corresponding to) the minimal Gröbner basis for M_I. We can therefore start with the set B_0, construct the cones $C(u, v)$ with $(u, v) \in B_0$ and select those which are minimal. Inductively, if we assume we have constructed the minimal cones with vertices in

$\cup_{i=0}^{r} B_i$, then we can construct new cones with vertices in B_{r+1} and select the minimal ones in the set $\cup_{i=0}^{r+1} B_i$. The process stops when the union of all the constructed cones gives the set A.

More precisely, the algorithm can be described as follows:
Input: $a, b \in M_I$, generators of M_I in Hermite normal form.
Output: a minimal Gröbner basis for M_I w.r.t. $<_\tau$.
$i := 0$;
$\mathcal{C} := \emptyset$;
while $(\cup_{C \in \mathcal{C}} C \neq A)$ do
    for $(u, v) \in B_i$ do
        compute the cone $C(u, v)$;
        erase the cones of $\mathcal{C}$ contained in $C(u, v)$;
        if $C(u, v)$ is not contained in any cone of $\mathcal{C}$, add it to $\mathcal{C}$;
    end for
    $i := i + 1$;
end while;
return $\{\psi(u, v)\}$ where (u, v) are the vertices of the cones of $\mathcal{C}$.

It is clear that the algorithm terminates, because A is covered by a finite number of cones.

REMARK 5.5. *In order to get the reduced Gröbner basis for the module M_I, it is enough to slightly modify the above algorithm: each time we add a new cone C to the collection $\mathcal{C}$ of cones produced in the algorithm, we have to choose C minimal w.r.t. $\prec$.*

It is clear that the choice of the partition $\{B_i\}$ of A can be crucial in order to speed up the algorithm.

EXAMPLE 5.6. *Let* $I := (x_1^2 x_3 - x_2^3 x_4^4, x_1^3 x_2^6 - x_3^3 x_4^2) \subseteq K[x_1, \ldots, x_4]$. *We want to compute the minimal (reduced) lex Gröbner basis for* $\mathrm{Sat}(I)$. *The module M_I is generated by:* $(2, -3, 1, -4)$, $(3, 6, -3, -2)$*; the Hermite normal form is:* $a := (1, 9, -4, 2)$, $b := (0, 21, -9, 8)$.

Choose $B_0 := \{(0, 1)\}$. *Hence we compute the first cone and get*

$$C_1 := C(0, 1) = \{(u, v) \in A \ : \ v \geq -3/7u + 1\}.$$

Choose $B_1 := \{(1, 0), (1, -1)\}$. *The corresponding cones are*

$$C_2 := C(1, 0) = \{(u, v) \in A \ : u \geq 1, \ v \geq -3/7u + 3/7\},$$

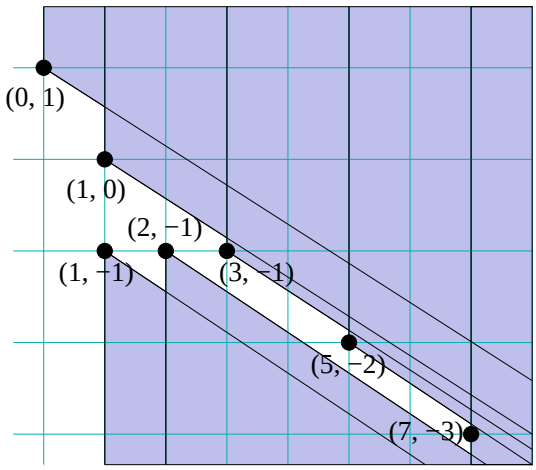

Figure 3: The Gröbner basis for $Sat(I)$

$$C_3 := C(1,-1) = \{(u,v) \in A \ : u \geq 1,\ v \leq -4/9u - 5/9\}.$$

Choose $B_2 := \{(2,-1),(3,-1)\}$. *The corresponding cones are*

$$C_4 := C(2,-1) = \{(u,v) \in A \ : u \geq 2,\ v \leq -4/9u - 1/9\},$$

$$C_5 := C(3,-1) = \{(u,v) \in A \ : u \geq 3,\ v \geq -3/7u + 2/7\}.$$

Choose $B_3 := \{(5,-2)\}$. *The corresponding cone is*

$$C_6 := C(5,-2) = \{(u,v) \in A \ : u \geq 5,\ v \geq -3/7u + 1/3\}.$$

Choose $B_4 := \{(7,-3)\}$. *The corresponding cone is*

$$C_7 := C(7,-3) = \{(u,v) \in A \ : u \geq 7\}.$$

Since $\cup_{i=1}^{7} C_i = A$, *we have that the minimal (actually reduced) Gröbner basis for* M_I *is:*

$$(0,21,-9,8),\ (1,9,-4,2),\ (1,-12,5,-6),\ (2,-3,1,-4),$$
$$(3,6,-3,-2),\ (5,3,-2,-6),\ (7,0,-1,-10),$$

which corresponds to the reduced Gröbner basis for Sat(I) *(w.r.t. the lexicographic term order in which* $x_1 > \cdots > x_4$*) given by:*

$$x_2^{21}x_4^8 - x_3^9,\ x_1x_2^9x_4^2 - x_3^4,\ x_1x_3^5 - x_2^{12}x_4^6,\ x_1^2x_3 - x_2^3x_4^4,$$
$$x_1^3x_2^6 - x_3^3x_4^2,\ x_1^5x_2^3 - x_3^2x_4^6,\ x_1^7 - x_3x_4^{10}.$$

Figure 3 shows the graphical aspect of the Gröbner basis.

References

[1] T. Becker and V. Weispfenning, *Gröbner bases. A computational approach to commutative algebra* **141**, Springer-Verlag, New York, U.S.A. (1993), in cooperation with Heinz Kredel.

[2] A. Bigatti, R La Scala, and L. Robbiano, *Computing toric ideals*, J. Symbolic Comput. **27**, no. 4 (1999), 351–365.

[3] G Boffi and F. Rossi, *Lexicographic Gröbner bases of 3-dimensional transportation problems*, Contemp. Math. Amer. Math. Soc., Providence, RI **286** (2001), 145–168, Symbolic computation: solving equations in algebra, geometry, and engineering (South Hadley, MA, 2000).

[4] G Boffi and F. Rossi, *Lexicographic Gröbner bases for transportation problems of format* $r \times 3 \times 3$, J. Symbolic Comput. **41**, nos. 3 and 4 (2006), 336–356.

[5] G Boffi and F. Rossi, *On a family of projective toric varieties*, Int. J. Pure Appl. Math. **31**, no. 4 (2006), 537–553.

[6] CoCoATeam, CoCoA*: a system for doing Computations in Commutative Algebra*, Available at `http://cocoa.dima.unige.it`.

[7] P Conti and C Traverso, *Buchberger algorithm and integer programming*, Applied algebra, algebraic algorithms and error-correcting codes (New Orleans, LA, 1991), Lecture Notes in Comput. Sci., **539**, Springer, Berlin, 1991, pp. 130–139.

[8] D Eisenbud and B. Sturmfels, *Binomial ideals*, Duke Math. J. **84** (1996), 1–45.

[9] R. Hemmecke and P. Malkin, *Computing generating sets of lattice ideals*, e-print arXiv: math.CO/0508359 (2006).

[10] B. Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series, no. 8, American Mathematical Society, Providence, RI, 1996.

[11] B. Sturmfels, R. Weismantel, and G. Ziegler, *Gröbner bases of lattices, corner polyhedra, and integer programming*, Beiträge Algebra Geom. **36**, no. 2 (1995), 281–298.

[12] R. Thomas, *A geometric Buchberger algorithm for integer programming*, Math. Oper. Res. **4** (1995), 864–884.

Received November 5, 2007.