ELSEVIER Linear Algebra and its Applications 295 (1999) 133–144

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

# Semigroup ideals and linear diophantine equations

A. Vigneron-Tenorio *

*Departamento de Matemáticas, Universidad de Cádiz, 11403 Jerez de la Frontera, Cádiz, Spain*

Received 3 November 1997; accepted 8 April 1999

Submitted by J. Dias da Silva

**Abstract**

We give a purely algebraic algorithm to calculate the ideal of a semigroup with torsion. As application and using Gröbner bases, we provide an algorithm to determine whether a linear system of equations with integer coefficients having some of the equations in congruences admits non-negative integer solutions. © 1999 Elsevier Science Inc. All rights reserved.

*Keywords:* Semigroup with torsion; Gröbner basis; Toric ideal; Lattice ideal

## 1. Introduction

Let $S$ be a finitely generated commutative cancelative semigroup with zero element, $0 \in S$. Assume that $S$ is a subsemigroup of an abelian group

$$S \subset \mathbb{Z}^n \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_s\mathbb{Z},$$

where $a_1, \ldots, a_s$ are non-zero and non-unit integers. Let $\{n_1, \ldots, n_r\} \subset S$ be a set of generators for $S$.

Let $k$ be a field, let $k[S]$ be the semigroup $k$-algebra associated to $S$, and let $R = k[X_1, \ldots, X_r]$ be the polynomial ring in $r$ indeterminates. We denote by $X^\alpha$, where $\alpha = (\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^r$, the monomial $X_1^{\alpha_1} \cdots X_r^{\alpha_r}$.

* E-mail: vigneron@cica.es

0024-3795/99/$ – see front matter © 1999 Elsevier Science Inc. All rights reserved.
PII: S0024-3795(99)00087-7

Then $k[S]$ is an $S$-graded ring,

$$k[S] = \bigoplus_{m \in S} k\{m\},$$

with $\{m\}$ being the symbol of $m \in S$ in $k[S]$. We also consider $R$ as an $S$-graded ring, assigning the degree $n_i$ to $X_i$.

The $k$-algebra epimorphism,

$$\varphi : R \to k[S],$$

defined by $\varphi(X_i) = n_i$ is a graded homomorphism of degree zero, and $I = \ker(\varphi)$ is a homogeneous ideal, which we shall call *the ideal of S*.

It is well known [8] that

$$\mathscr{B} = \left\{ X^{\alpha} - X^{\beta} \,\middle|\, \sum_{i=1}^{r} \alpha_i n_i = \sum_{i=1}^{r} \beta_i n_i,\ \alpha_i,\ \beta_i \geqslant 0 \right\}$$

is a set of generators for $I$.

If $S$ is torsion free, i.e. $S \subset \mathbb{Z}^n$ (*toric case*), then there are many algorithms to find a subset of $\mathscr{B}$ which is a finite set of generators for $I$. In [14] there is a good work about these techniques. However, the case $S$ has non-trivial torsion is not considered by these methods.

On the other hand, if the semigroup $S$ is such that $S \cap (-S) = \{0\}$ (*Nakayama case*), then one has the Nakayama lemma for $S$-graded modules. Therefore, in this case it is possible to consider minimal systems of generators for $I$. Besides in this case it is possible to assign a positive degree to $X_i$, $1 \leqslant i \leqslant r$. For more details see [5], where an algorithm method of computing minimal systems of generators for $I$ is provided.

An algorithm to find a subset of $\mathscr{B}$ which is a finite set of generators for $I$, where $S$ has non-trivial torsion appears in [11]. In this paper we provide a faster algorithm than [11] connecting the semigroup ideals with the *lattice ideals*.

Let $\mathscr{L}$ be a lattice in $\mathbb{Z}^r$, we denote

$$I_{\mathscr{L}} = \langle X^u - X^v : u, v \in \mathbb{N}^r,\ u - v \in \mathscr{L} \rangle.$$

The ideal $I_{\mathscr{L}}$ is called a *lattice ideal*. We shall see Lemma 9 that the set of the lattice ideals is equal to the set of ideals of finitely generated commutative cancelative semigroups with zero element. Besides, we reduce the problem of computing the ideal of $S$ to the problem of computing the ideal of the lattice $\ker(S)$ (Note 10).

We shall expose different methods of computing lattice ideals. In particular, we shall see how the techniques in [2] become generalized to compute lattice ideals. We use these techniques in our final algorithm (Algorithm 15).

As application of the above algorithm and using Gröbner bases, we solve the classical problem of Integer Linear Programming of knowing if a linear

system of equations with integer coefficients admits non-negative integer solutions. The theorem of Papadimitrious [10, p. 321] solves this problem, and also it is studied in [3,4,13], but the methods presented in these papers are not efficient. In [12] it is treated as homogeneous case.

Our solution is based on the following idea: We associate a semigroup $S$ to a system such that if the system admits non-negative integer solutions then there is a special kind of binomial in $I$ (ideal of $S$) (Proposition 16). To determine whether such binomial lies in $I$, it is enough to compute a generating set for $I$ by using Algorithm 15 and a Gröbner base respect to a suitable monomial order Lemma 17. Since $S$ with torsion is allowed in Algorithm 15, the linear diophantine equations can be congruences.

In Section 2, we expose the different methods of computing lattice ideals and generalize the techniques in [2].

In Section 3, we give the algorithm to calculate the ideal of a semigroup finitely generated commutative cancelative semigroup with zero element.

In Section 4, we use the algorithm above to determine whether a linear system with integer coefficient equations having some equations in congruences admits non-negative integer solutions.

## 2. Lattice ideals

Fix a field $k$, let $R = k[X_1, \ldots, X_r]$ be the polynomial ring in $r$ indeterminates and $\mathscr{L} \subset \mathbb{Z}^r$ a lattice. The problem we want to solve is *how can you compute a set of generators for $I_{\mathscr{L}}$ if you have a set of generators $C$ for $\mathscr{L}$?*

Let $u \in \mathbb{Z}^r$, one can write $u$ uniquely as $u = u^+ - u^-$, where $u^+,\ u^- \in \mathbb{N}^r$ and $\operatorname{supp}(u^+) \cap \operatorname{supp}(u^-) = \emptyset$. For any subset $C \subset \mathscr{L}$ we associate an ideal

$$J_C = \langle X^{u^+} - X^{u^-} : u = u^+ - u^- \in C \rangle.$$

First at all, let $J \subset R$ be a ideal, and $f \in R$ a polynomial, then the following are ideals:

$$(J : f) = \{g \in k[X_1, \ldots, X_r] : fg \in J\},$$

$$(J : f^\infty) = \{g \in k[X_1, \ldots, X_r] : f^s g \in J,\ s \in \mathbb{N}\}.$$

As $R$ is noetherian one knows that there is $s \in \mathbb{N}$ verifying $(J : f^\infty) = (J : f^s)$.

We use the above definitions in Lemma 1.

**Lemma 1.** *If $C$ is a set of generators for the lattice $\mathscr{L}$, then*

$$(J_C : (X_1 \ldots X_r)^\infty) = I_{\mathscr{L}}.$$

**Proof.** See [14, p. 114]. □

There are many algorithms to compute $(J_C : (X_1 \dots X_r)^\infty)$. Our study is based on elimination.

**Proposition 2** [1]. *Let $I = \langle f_1, \dots, f_l \rangle$ be an ideal in $R$, let $0 \neq f \in R$ be a polynomial, and let $J = \langle f_1, \dots, f_l, 1 - Yf \rangle$ be an ideal in $k[X_1, \dots, X_r, Y]$. Then $(I : f^\infty)$ is the elimination ideal for $J_X = J \cap R$. Besides, if $\{g_1, \dots, g_m\}$ is a basis for $J_X$ with*

$$g_i = h_i(1 - Yf) + \sum_{j=1}^{l} h_{ij} f_j \quad (1 \leqslant i \leqslant m,\ h_i,\ h_{ij} \in k[X_1, \dots, X_r,\ Y]),$$

*then*

$$s = \max\{\deg_Y(h_{ij}) | 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant l\}$$

*satisfies $(I : f^\infty) = (I : f^s)$.*

**Proof.** See [1, p. 266]. □

Then, let $E = \langle f_1, \dots, f_l, 1 - X_1 \cdots X_r Y \rangle$, where $\{f_1, \dots, f_l\}$ is a set of generators for $J_C$, to compute $(J_C : (X_1 \dots X_r)^\infty)$ we shall compute the elimination ideal for $E$. One can compute it using Gröbner bases [1]. Note that with these methods we compute in $k[X_1, \dots, X_r, Y]$.

There are other algorithms which operate in $R$. The first we study appears in [14] but can only use it in special cases. For the lattices, this case is

$$\mathscr{L} \cap \mathbb{N}^r = \{0\}.$$

Then algorithm above is based on the next lemma.

**Lemma 3** [14]. *Fix the graded reverse lexicographic term order induced by $X_1 > \cdots > X_r$, and let $\mathscr{G}$ be the Gröbner basis of a homogeneous ideal $J \subset k[X_1, \dots, X_r]$. Then the set*

$$\mathscr{G}' = \{f \in \mathscr{G} \mid X_r \text{ does not divide } f\} \cup \{f/X_r \mid f \in \mathscr{G}, X_r \text{ divides } f\}$$

*is a Gröbner basis of $(J : X_r)$. A Gröbner basis of $(J : X_r^\infty)$ is obtained by dividing each element $f \in \mathscr{G}$ by the highest power of $X_r$ that divides $f$.*

**Proof.** See [14, p. 113]. □

Then by applying the above lemma, one can compute $(J_C : (X_1 \dots X_r)^\infty)$:

$$(J : (X_1 \dots X_r)^\infty) = (((\cdots (J : X_1^\infty) : X_2^\infty) \cdots) : X_r^\infty),$$

and we have the following algorithm.

**Algorithm 4.** With the above notations.

*Input*: A set of generators C for a lattice $\mathscr{L}$ verifying $\mathscr{L} \cap \mathbb{N}^r = \{0\}$.

*Output*: A set of generators for $I_{\mathscr{L}}$.

1. (Optional) Replace C by a reduced lattice basis (see [7, p. 85]).
2. Let $J_0 = \langle X^{u^+} - X^{u^-} : u \in C \rangle$.
3. For $i = 1, \ldots, r$, compute $J_i = (J_{i-1} : X_i^{\infty})$ using Lemma 3.
4. $J_r = I_{\mathscr{L}}$.

The last method we expose is obtained from [2], and it is based on the following lemma about lattices.

**Lemma 5.** *Let C be a set of generators for the lattice $\mathscr{L}$. If $C \subset \mathbb{N}^r$, then $I_{\mathscr{L}} = J_C$.*

**Proof.** Analogously to [2, p. 230]. □

The algorithm is based on two steps:

**1.P.** Compute recursively any lattices

$$\mathscr{L} = \mathscr{L}_1, \ldots, \mathscr{L}_t$$

such that $\mathscr{L}_t$ verify Lemma 5.

**2.P.** Compute using Gröbner basis the ideal $I_{\mathscr{L}_i}$ from $I_{\mathscr{L}_{i+1}}$.

For **1.P.** we use the following lemma.

**Lemma 6.** *Let C be a set of generators for $\mathscr{L}$, then there is another set of generators C′ having the property that for all $u, v \in C'$: either* $\operatorname{supp}(u^-) = \operatorname{supp}(v^-)$, *or if $i_0$ is in* $\operatorname{supp}(u^-)$ *but not in* $\operatorname{supp}(v^-)$, *then $v_{i_0} = 0$.*

**Proof.** See [2, p. 231]. □

The above lemma guarantees that by changing the signs of some coordinates of any elements in $C'$, one can obtain a lattice satisfying Lemma 5. This changes will be done using the map

$$\begin{array}{rccc} \phi_i : & \mathbb{Z}^r & \to & \mathbb{Z}^r \\ & (a_1, \ldots, a_r) & \mapsto & (a_1, \ldots, -a_i, \ldots, a_r) \end{array}$$

and the lattices and their basis will be defined by $C_i = \phi_{j(i)}(C_{i-1})$ and $\mathscr{L}_i$ will be the lattice generated by $C_i$.

Using the definitions above and denoting by $\mathbf{X}$ the monomials which do not contain the variable $X_{j(i)}$, then $X_{j(i)}\mathbf{X}^u - \mathbf{X}^v$ lies in $I_{\mathscr{L}_i}$ if and only if $\mathbf{X}^u - \mathbf{X}^v X_{j(i)}$ lies in $I_{\mathscr{L}_{i-1}}$.

The step **2.P.** is based on the following proposition.

**Proposition 7** [14, p. 115]. *Fix an order which eliminates $X_i$. Let*

$$G_{j(i)} = \{X_{j(i)}^{r_j}\mathbf{X}^{u_j} - \mathbf{X}^{v_j} : j = 1, \ldots, m\}$$

*be a Gröbner basis for $I_{\mathscr{L}_i}$. Then*

$$G = \{\mathbf{X}^{u_j} - \mathbf{X}^{v_j}X_{j(i)}^{r_j} : j = 1, \ldots, m\}$$

*is a set of generators for $I_{\mathscr{L}_{i-1}}$.*

To *move the indeterminates* and construct a set of generators for the lattice ideal $I_{\mathscr{L}_i}$, we will use the map $T_i$

$$T_i(X_i^r\mathbf{X}^u - \mathbf{X}^v) = \mathbf{X}^u - \mathbf{X}^vX_i^r.$$

We now expose the algorithm.

**Algorithm 8.** With the above notations.

*Input*: A set of generators $C$ $\mathscr{L}$.

*Output*: A set of generators for $I_{\mathscr{L}}$.

1. Find a set of generators $C'$ for $\mathscr{L}$ verifying six.
2. Let

$$A = \{a_1, \ldots, a_l\} = \{\mathrm{supp}(v^-) \mid v \in C'\},$$

$$C_A = \phi_{a_1}(\phi_{a_2}(\cdots(\phi_{a_l}(C')))),$$

and let

$$G_A = \{X^{v^+} - X^{v^-} : v \in C_A\}.$$

3. While $A \neq \emptyset$ : choose $a \in A$ and let $G_{A\setminus\{a\}}$ be the result to $T_a$ operating on the reduced Gröbner basis for $G_A$ with respect to order $X_a > \cdots$ Now, let $A = A \setminus \{a\}$.
4. At the end, $G_A$ is a set of generators for $I_{\mathscr{L}}$.

This algorithm is more general than Algorithm 4, because it can be used for any lattice, but Algorithm 4 can be only used if the lattice satisfies

$$\mathscr{L} \cap \mathbb{N}^r = \{0\}.$$

A comparison between the last two algorithms appear in [9]. In Section 3 we will use these techniques to compute semigroup ideals.

## 3. Algorithm to calculate the ideal of $S$

Let $S$ be a finitely generated commutative cancelative semigroup with zero element,

$$S \subset \mathbb{Z}^n \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_s\mathbb{Z},$$

where $a_1, \ldots, a_s$ are non-zero and non-unit integers. Let $\{n_1, \ldots, n_r\} \subset S$ be a set of generators for $S$ and $I \subset k[X_1, \ldots, X_r]$ the ideal of $S$. Assume that $S \neq (0)$.

The following lemma connects the lattice ideals with the semigroup ideals.

**Lemma 9.** *$I$ is the ideal of a finitely generated commutative cancelative semigroup with zero element, $S$, if and only if $I$ is a lattice ideal.*

**Proof.** Let $S = \langle n_1, \ldots, n_r \rangle$ be a semigroup and $I$ its ideal in $k[X_1, \ldots, X_r]$. By [8, p. 177] it is known that $I$ is generated by

$$\mathscr{B} = \left\{ X^{\alpha} - X^{\beta} \middle| \sum_{i=1}^{r} \alpha_i n_i = \sum_{i=1}^{r} \beta_i n_i,\ \alpha_i,\ \beta_i \geqslant 0 \right\}.$$

Besides, since $S$ is cancelative we know that $I$ is generated by

$$\mathscr{B}' = \left\{ X^{\alpha^+} - X^{\alpha^-} \middle| \sum_{i=1}^{r} \alpha_i n_i = 0,\ \alpha_i \in \mathbb{Z} \right\}.$$

then, if we take the lattice $\mathscr{L}$ generated by $\alpha^+ - \alpha^-$ *in* $\mathscr{B}'$,

$$I = \langle X^{\alpha^+} - X^{\alpha^-} | \alpha^+ - \alpha^- \in \mathscr{L} \rangle,$$

then $I$ is a lattice ideal.

Conversely [6], let $\mathscr{L} \subset \mathbb{Z}^r$ be a lattice. We define the map

$$\pi : \mathbb{N}^r \to \frac{\mathbb{Z}^r}{\mathscr{L}},$$

$$e_i \mapsto e_i + \mathscr{L},$$

where the $e_i$ are the unit vectors in $\mathbb{N}^r$.

Let $S$ be the semigroup $\langle e_1 + \mathscr{L}, \ldots, e_r + \mathscr{L} \rangle$ and $I$ its ideal. It is easy to see that $I = I_{\mathscr{L}}$. □

**Note 10.** We have proved that $I = I_{\ker(S)}$, where $\ker(S) \subset \mathbb{Z}^r$ is the lattice

$$\left\{ (x_1, \ldots, x_r) \in \mathbb{Z}^r : (x_1, \ldots, x_r) \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = 0 \right\}.$$

To calculate the ideal of $S$ we take a new torsion free semigroup $S'$ in $\mathbb{Z}^{n+s}$ associated to $S$.

Let $n_i' = n_i$ in $\mathbb{Z}^{n+s}$, $\forall i \in \{1, \ldots, r\}$, and let

$$n'_i = (\underbrace{0,\ldots,0}_{n},\underbrace{0,\ldots,0,a_{i-r},0,\ldots,0}_{s})$$

for $i \in \{r+1,\ldots,r+s\}$.

Now, let $S' = \langle n'_1,\ldots,n'_{r+s}\rangle$ be a subsemigroup of $\mathbb{Z}^{n+s}$, and $\ker(S') \subset \mathbb{Z}^{r+s}$ the lattice

$$\left\{ (x_1,\ldots,x_{r+s}) \in \mathbb{Z}^{n+s} : (x_1,\ldots,x_{r+s}) \begin{pmatrix} n'_1 \\ \vdots \\ n'_{r+s} \end{pmatrix} = 0 \right\}.$$

We have the following lemma concerning the lattices $\ker(S)$ and $\ker(S')$.

**Lemma 11.** *Let $C'$ be a set of generators for* $\ker(S') \subset \mathbb{Z}^{r+s}$, *then*

$$C = \left\{ (x_1,\ldots,x_r) \in \mathbb{Z}^r : (x_1,\ldots,x_r,x_{r+1},\ldots x_{r+s}) \in C' \right\}$$

*is a set of generators for* $\ker(S) \subset \mathbb{Z}^r$.

**Proof.** Trivial. □

Then, to calculate $I$, we only need calculate the lattice ideal $I_{\ker(S)}$. This computation can be done by using Algorithm 8.

The following example shows that the irreducible sets of generators for $I$ have not always the same cardinal.

**Example 12.** Let $S$ be the semigroup

$$S = \langle (0,\overline{0},\overline{1}),(2,\overline{1},\overline{1}),(1,\overline{0},\overline{3}),(-2,-\overline{1},\overline{3})\rangle \subset \mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}.$$

Then we have that the ideal of $S$ is generated by

$$\begin{aligned} I &= \langle x_4^2x_3^4 - x_1^2, x_2 - x_4^3x_3^8, x_4^4x_3^8 - 1\rangle \\ &= \langle x_4x_2 - 1, 1 - x_1^4, x_3^8 - x_1^8x_2^4, x_3^{12} - x_1^{10}x_2^6\rangle, \end{aligned}$$

where both are irreducible systems.

But, when $S$ satisfies

$$S \cap (-S) = \{0\},$$

one can affirm that all the irreducible systems of generators have the same cardinality. In that case, we call an irreducible system of generators a *minimal generator system*. We say that $S$ is a *Nakayama* semigroup.

To detect if $S$ is Nakayama, we can use the following lemma.

**Lemma 13.** *Let $S$ be a semigroup and let $I$ be its ideal in $k[X_1,\dots,X_r][X_1,\dots,X_r]$. Then $S$ is not Nakayama semigroup if and only if there is a polynomial of the form $X^\alpha - 1$ in $I$.*

**Proof.** See [11, p. 148]. □

**Note 14.** As an application of the above lemma, we will be able to determine whether a semigroup $S$ is Nakayama or not: $S$ is Nakayama if we can find a binomial $\pm(X^\alpha - 1)$ in a system of generators of $I$, otherwise it is not.

Now we have an algorithm to calculate the ideal of a finitely generated commutative cancelative semigroup with zero element.

**Algorithm 15.** With the notations above:
*Input*: A set of generators $\{n_1,\dots,n_r\}$ of $S$, $n_i \neq 0$ for any $i$.
*Output*: A set of generators for $I$ and we know if $S$ is (or not) Nakayama.
1. Calculate the set $S'$.
2. Take a set of generators for the lattice $\ker(S')$, $C'$.
3. Take $C$ the $C' \subset \mathbb{Z}^{r+s}$ projection onto the first $r$ coordinates. So, we have a set of generators for the lattice $\ker(S)$.
4. Compute the lattice ideal $I_{\ker(S)}$ $(I = I_{\ker(S)})$.
5. Determine whether $I$ contains a binomial $X^\alpha - 1$. If such a binomial is in $I$, then $S$ is Nakayama. Otherwise, it is not.

## 4. Application

Now, we want to determine whether a system of equations such as:

$$(\text{Sist})\begin{cases} n_{11}x_1 + n_{12}x_2 + \cdots + n_{1r}x_r = b_1 \pmod{d_1} \\ n_{21}x_1 + n_{22}x_2 + \cdots + n_{2r}x_r = b_2 \pmod{d_2} \\ \vdots \quad\quad \vdots \quad\quad \vdots \\ n_{l1}x_1 + n_{l2}x_2 + \cdots + n_{lr}x_r = b_l \pmod{d_l} \\ n_{(l+1)1}x_1 + n_{(l+1)2}x_2 + \cdots + n_{(l+1)r}x_r = b_{l+1} \\ \vdots \quad\quad \vdots \quad\quad \vdots \quad\quad \vdots \\ n_{m1}x_1 + n_{m2}x_2 + \cdots + n_{mr}x_r = b_m \end{cases}$$

admits solutions in $\mathbb{N}^r$.

We are going to transform the problem above into a problem about semigroup ideals.

We consider $n_i = (n_{1i}, \ldots, n_{mi})$ with $1 \leqslant i \leqslant r$ and $b = (b_1, \ldots, b_m)$ in $\mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_l\mathbb{Z} \oplus \mathbb{Z}^{m-l}$. We may assume, without loss of generality, that $n_i \neq 0$ for any $i$.

If (Sist) is a homogeneous system, then using Lemma 13 we only need to take $S = \langle n_1, \ldots, n_r \rangle$, and ask if $S$ is Nakayama, i.e. $X^\alpha - 1 \in I_S$ (ideal of $S$). If $S$ is Nakayama, then the system admits a solution in $\mathbb{N}^r$, and $\alpha$ is a solution. Otherwise, (Sist) does not admit solutions in $\mathbb{N}^r$.

With the above notations, assume $b \neq 0$. Let $S$ be the semigroup

$$S = \langle n_1, \ldots, n_r, b \rangle \subset \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_l\mathbb{Z} \oplus \mathbb{Z}^{m-l},$$

and let $I_S$ be its ideal.

**Proposition 16.** *The system* (*Sist*) *admits solutions in* $\mathbb{N}^r$ *if and only if there is a binomial like* $X_{r+1} - \mathbf{X}^\beta$ *in* $I_S \subset k[X_1, \ldots, X_{r+1}]$, *where* $\mathbf{X}$ *does not contain the variable* $X_{r+1}$.

**Proof.** Suppose $(a_1, \ldots, a_r) \in \mathbb{N}^r$ is a solution for (Sist). Then $a_1 n_1 + \cdots + a_r n_r = b$ and trivially $X_{r+1} - \mathbf{X}^{(a_1, \ldots, a_r)} \in I_S$. The reciprocal is analogous. □

To see if $I_S$ satisfies the proposition above, we can use the following lemma.

**Lemma 17.** *Fix a monomial order satisfying* $X_{r+1} > \cdots$ *Let* $I_S$ *be the ideal above and denote by* $\mathscr{B}$ *the reduced Gröbner basis of* $I_S$. *The following are equivalent*:
1. *There is a binomial* $X_{r+1} - \mathbf{X}^\beta$ *in* $I_S$.
2. *There is a binomial* $\pm(X_{r+1} - \mathbf{X}^{\beta'})$ *in* $\mathscr{B}$.

**Proof.** Trivial by Gröbner Bases Theory. □

If the semigroup $S$ is Nakayama, to determine whether there is a binomial $X_{r+1} - \mathbf{X}^\alpha$ in $I_S$, we do not need to use Lemma 17. We can use the following lemma and so we do not need to find a Gröbner basis for $I_S$.

**Lemma 18.** *Let* $S$ *be Nakayama semigroup, and let* $\mathscr{C}$ *be any binomial set of generators with coefficients* $\pm 1$ *for* $I_S$. *Then there is a binomial* $X_{r+1} - \mathbf{X}^\beta$ *in* $I_S$ *if and only if there is a binomial* $\pm(X_{r+1} - \mathbf{X}^{\beta'})$ *in* $\mathscr{C}$.

**Proof.** Trivial. □

Then, we have an algorithm to determine whether the system (Sist) admits solutions in $\mathbb{N}^r$.

**Algorithm 19.** With the above notations:

*Input*: A set of equations like (Sist) with $n_i \neq 0$.

*Output*: We know if (Sist) admits, or not, solutions in $\mathbb{N}^r$. In the affirmative case, we have a solution.

1. If $b = 0$ :
   1.1. Take $S = \langle n_1, \ldots, n_r \rangle$.
   1.2. Compute $I_S$ by using Algorithm 15.
   1.3. If $S$ is not Nakayama, i.e. $\exists X^\alpha - 1 \in I_S$, then (Sist) admits solutions in $\mathbb{N}^r$ and $\alpha$ is a solution. Otherwise, (Sist) does not admit solutions in $\mathbb{N}^r$.
2. If $b \neq 0$ :
   2.1. Take $S = \langle n_1, \ldots, n_r, b \rangle$.
   2.2. Compute $I_S$ by using Algorithm 15.
   2.3. If $S$ is Nakayama, let $\mathscr{C}$ be a generating set of $I_S$. Otherwise, fix a monomial order verifying $X_{r+1} > \cdots$, and take a Gröbner bases for $I_S$, $\mathscr{C}$.
   2.4. If there is a binomial $\pm(X_{r+1} - \mathbf{X}^\beta)$ in $\mathscr{C}$, then (Sist) admits solutions in $\mathbb{N}^r$, and $\beta$ is a solution. Otherwise, (Sist) does not admit solutions in $\mathbb{N}^r$.

**Example 20.** Given the following system of equations

$$\begin{cases} 3x + 2y + 7z + 12t &= 4 \pmod{20}, \\ x + y - z &= 1 \pmod{3}. \end{cases}$$

To use the algorithm above, we must take

$$S = \langle (\overline{3}, \overline{1}), (\overline{2}, \overline{1}), (\overline{7}, -\overline{1}), (\overline{12}, \overline{0}), (\overline{4}, \overline{1}) \rangle$$

in $\mathbb{Z}/20\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Fix the monomial order $x_5 > x_1 > x_2 > x_3 > x_4$, then we have the reduced Gröbner bases of $I_S$

$$\left[x_5 - x_3^8 x_4^4, x_1 - x_4^4 x_3^5, -x_4^4 x_3^2 + x_2, x_3^{12} - x_4^2, -1 + x_4^5\right].$$

Since $x_5 - x_3^8 x_4^4$ lies in $I_S$, the system admits a solution in $\mathbb{N}^4$, for example, $(0, 0, 8, 4)$.

**Example 21.** Next, consider the homogeneous system of equations:

$$\begin{cases} x + y - z + t &= 0, \\ -11x + 2y + 2z + t &= 0. \end{cases}$$

We take

$$S = \langle (1, -11), (1, 2), (-1, 2), (1, 1) \rangle,$$

and then we have a set of generators for $I_S$

$$\left[ - x_1^2 x_3^7 x_4^2 x_2^3 + 1, x_1 x_4^3 x_3^4 - 1 \right].$$

We can see that the binomial $x_1x_4^3x_3^4 - 1$ lies in $I_S$ and then the system admits a solution in $\mathbb{N}^4$, for example, $(1, 0, 4, 3)$.

All the algorithm above are implemented in MapleV, and are available by `ftp` at

`ftp.uca.es/pub/matematicas/semigroul.zip`

## Acknowledgement

I would like to thank P. Pisón for her help in the preparation of this paper.

## References

[1] T. Becker, V. Weispfenning, Gröbner bases, A Computational Approach to Commutative Algebra, Springer, Berlin, 1993.
[2] F. Dibiase, R. Urbanke, An algorithm to calculate the kernel of certain polynomial ring homomorphisms, Exp. Math. 4 (3) (1995) 227–234.
[3] I. Borosh, A sharp bound for positive solutions of homogeneous linear diophantine equations, Proc. Amer. Math. Soc. 60 (1976) 19–21.
[4] I. Borosh, M. Flahive, D. Rudin, B. Treybig, A sharp bound for solutions of linear diophantine equations, Proc. Amer. Math. Soc. 105 (1989) 844–846.
[5] E. Briales, A. Campillo, C. Marijuán, P. Pisón, Minimal systems of generators for ideals of semigroups, J. Pure Appl. Algebra, 127 (1998) 7–30.
[6] A. Campillo, P. Giménez, Syzygies of affine toric varieties, preprint.
[7] H. Cohen, A course in computational algebraic number theory, Graduate Texts in Mathematics, Springer, Berlin, 1993, p. 138.
[8] J. Herzog, Generators of relations of abelian semigroups and semigroups ring, Manuscripta Math. 3 (1970) 175–193.
[9] S. Hosten, B. Sturmfels, GRIN: An implementation of Gröbner bases for integer programming, Manuscript, Cornell University.
[10] C.H. Papadimitriou, Combinatorial Optimization: Algorithms and Complexity, Prentice-Hall, Englewood Cliffs, NJ, 1982.
[11] P. Pisón-Casares, A. Vigneron-Tenorio, Ideales de semigroups con torsión: Cálculos mediante MapleV, in: Proceedings of the EACA'96, September, 1996, Sevilla (Spain).
[12] J.C. Rosales, On finitely generated submomoids of $\mathbb{N}^k$, Semigroup Forum 50 (1995) 251–262.
[13] J.C. Rosales, P.A. García-Sánchez, Non-negative elements of subgroups of $\mathbb{Z}^n$, Linear Algebra Appl. 270 (1998) 351–357.
[14] B. Sturmfels, Gröbner Bases and Convex Polytopes, University Lecture Series, vol. 8, American Mathematical Society, Providence, RI, 1995.