First Syzygies of Toric Varieties and Diophantine Equations in Congruence*

P. Pisón-Casares †
Departamento de Álgebra, Facultad de Matemáticas,
Apartado 1160, 41080 Sevilla (Spain)
Fax: + 34 95 4556938. E-mail: pilar@algebra.us.es

A. Vigneron-Tenorio ‡
Departamento de Matemáticas, E.U.E. Empresariales,
Por-Vera 54, 11403 Jerez de la Frontera (Cádiz, Spain)
Fax: + 34 956 345104. E-mail: vigneron@cica.es

Abstract

We compute the first syzygies of a subclass of lattice ideals by means of some abstract simplicial complexes. This subclass includes the ideals defining toric varieties. A finite check set containing the minimal first syzygy degrees is determined, and a singly-exponential bound for these degrees is explicited. Integer Programming techniques are used, precisely the Hilbert bases for diophantine equations in congruences.

Key Words: Toric varieties, syzygies, simplicial complexes, diophantine equations.

Introduction

Let S be a finitely generated commutative semigroup with zero element. Let $\{n_1, \dots, n_r\} \subset S$ 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 $R = k[X_1, \dots, X_r]$ be the polynomial ring in r indeterminates.

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

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

where $k[S]_m = k\{m\}$ and $\{m\}$ is the symbol of $m \in S$ in $k[S]$. We also consider R as an $S-$graded ring, by assigning the degree $\{n_i\}$ to X_i. We write $\mathbf{m} = \oplus_{m \in S-\{0\}} R_m$ for the irrelevant maximal ideal in R.

The $k-$algebra epimorphism,

$$\varphi_0 : R \longrightarrow k[S],$$

defined by $\varphi_0(X_i) = \{n_i\}$, is a graded homomorphism of degree zero. Thus, the ideal $I_S = ker(\varphi_0)$ is a homogeneous ideal that it is called a *semigroup ideal.*

On the other hand, given $\mathcal{L} \subset \mathbf{Z}^r$ a $\mathbf{Z}$-submodule or *lattice*, the ideal

$$I(\mathcal{L}) := \langle \mathbf{X}^u - \mathbf{X}^v \ \mid \ u, v \in \mathbf{N}^r, \ u - v \in \mathcal{L} \rangle,$$

*1991 *Mathematics Subject Classification* [13DO2], [13P1O]

†Supported by Plan Propio de la Universidad de Sevilla

‡Partially supported by Plan Propio de la Universidad de Sevilla and Plan Propio de la Universidad de Cádiz

is called a *lattice ideal*.

If S is cancellative there exists a group $G(S)$, unique disregarding isomorphism, with $S \subset G(S)$. $G(S)$ is finitely generated and commutative group, because S is finitely generated and commutative semigroup. Then, we can suppose that

$$G(S) = \mathbf{Z}^h \oplus \mathbf{Z}/a_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/a_s\mathbf{Z},$$

with $a_1, \ldots a_s \in \mathbf{Z}$.

It is known (see [28]) that the class of semigroup ideals considered above, it is equal to the class of lattice ideals. Precisely, S has associated the lattice

$$ker(S) := \{u \in \mathbf{Z}^r \quad | \quad \sum_{i=1}^{r} u_i n_i = 0\}.$$

We also require the condition $S \cap (-S) = \{0\}$ on the semigroup. It corresponds to the property $\mathcal{L} \cap \mathbf{N}^r = \{0\}$. This condition guarantees the Nakayama's lemma for S-graded R-modules (Proposition 1.4 in [4]). If S has not got torsion, the obtained ideal defines a toric variety (see [26] and the references therein).

By Nakayama's lemma, all of the minimal generating set of I_S have the same cardinality equal to

$$\beta_0 := \dim_k(I_S/\mathbf{m}I_S) = \sum_{m \in S} \dim_k(I_S/\mathbf{m}I_S)_m,$$

and every one has exactly $\dim_k(I_S/\mathbf{m}I_S)_m$ elements of degree m.

Set

$$V_0(m) := (I_S/\mathbf{m}I_S)_m.$$

Then, the notherian property on R guarantees that the set of minimal degrees of I_S,

$$C_0 := \{m \in S \quad | \quad V_0(m) \neq 0\},$$

is finite.

The k-vector space $V_0(m)$ is related with the reduced homology of an abstract simplicial complex associated to the element $m \in S$, The origin of this relation can be found in [20] and [7]. This relation is used in [9] to give a combinatorial description of the minimal generating set of I_S in the particular case $r \leq 5$ and S a numerical semigroup (i.e. a monomial curve in the affine space of dimension less or equal than 5). An arithmetical characterization for the elements in C_0 appears in [10]. Using Integer Programming, this characterization provides an algorithm for computing the set C_0 and a minimal generating set of I_S, [4].

This paper is a continuation of this working scheme. We are interested in progressing in the combinatorial understanding about the first syzygies of I_S. We employ the same abstract simplicial complexes Δ_m (see section 1 for definition). These combinatorial objects also appear in [1], [5], [6], [8] and [16].

Fix a minimal generating set of I_S, $\{f_1, \ldots, f_{\beta_0}\}$. Suppose that $f_i \in R_{p_i}$, for any i, $1 \leq i \leq \beta_0$. Consider the S-graded morphism of R-modules

$$\varphi_1 : R^{\beta_0} \longrightarrow R,$$

defined by $\varphi_1(g_1, \ldots, g_{\beta_0}) = \sum_{i=1}^{\beta_0} g_i f_i$. Let $N_1 := ker(\varphi_1)$ be the first module of syzygies associated to $\{f_1, \ldots, f_{\beta_0}\}$. N_1 is an S-graded module with

$$(N_1)_m := \{(g_1, \ldots, g_{\beta_0}) \quad | \quad g_i \in R_{m-p_i}, \text{ for any } i\}.$$

Again, by Nakayama's lemma all of the minimal generating set of N_1 have the same cardinality. This cardinality is

$$\beta_1 := \dim_k(N_1/\mathbf{m}N_1) = \sum_{m \in S} \dim_k(N_1/\mathbf{m}N_1)_m.$$

Set

$$V_1(m) := \frac{(N_1)_m}{(\mathbf{m}N_1)_m}.$$

A minimal generating set of N_1 consists exactly of $dim_k(V_1(m))$ elements of degree m, for each m. In particular, since R is noetherian, one has $V_1(m) = 0$ for all m but finitely many values. Therefore, the set of minimal first syzygy degrees,

$$C_1 := \{m \in S \;\mid\; V_1(m) \neq 0\},$$

is finite.

In this paper we use the known relation between the k-vector space $V_1(m)$ and the reduced homology of the simplicial complex Δ_m (Remark 11). We describe a finite set $\mathcal{C}$ containing C_1. This set is computed by Algorithm 19. Hilbert bases for some linear diophantine systems in congruences are required. Thus, we obtain our main result which establishes that C_1 can be computed by means of some simplicial complexes (Theorem 20).

As an application, a new method computing minimal generating set of N_1 is obtained. Although there exists an alternative method using Gröbner bases (Schreiyer's Theorem, see for example [13]), our view point is interesting because it allows to obtain an explicit bound for the degree of the minimal first syzygies (Theorem 23).

The philosophy of this paper is like in [4]. It is not to give the most efficient algorithm to compute the first syzygies, but the combinatorial knowledge of these syzygies. In fact, the computation using Gröbner Basis Theory is more efficient, but this is only a computing method and does not explain how these syzygies are.

The technics we use in this paper are based in the structures and computations of the $\mathbf{N}-$solutions of diophantine equations. It is well-known these structures in diophantine equations non in congruence (see [23], [24], [25]), being the same ones in congruence case.

There are a lot of methods to compute the $\mathbf{N}-$solutions of diophantine equations non in congruence: [19], [11], [22], [25], [12], [17], etc. But if the system is in congruence, the references are few: [21], [28]. Clasically, to solve diophantine equations in congruence, one must add new indeterminates, making more complicated the calculate. The algorithm we submit in this paper is based in Gröbner Basis Theory and the Dickson's Lemma, and compute $\mathbf{N}-$solutions adding less variables than the standard method.

In section 1, we will make extensive the results appearing in [17], given an algorithm to compute the general $\mathbf{N}-$solution of a system of diophantine equations in congruence (non needfully homogeneous) adding less indeterminates than the standard method, Algorithm 10.

In section 2, we will find a finite set, $\mathcal{C}$, containing C_1. We explain how to obtain a minimal generating set of N_1 from the knowledge of $\mathcal{C}$. We use an isomorphism explicited in Remark 3.6 of [5].

In section 3, as an application, by using the bounds in [19] (see also [18]), we prove that the doubly-exponential degree in a minimal $1-$syzygy for binomial ideals (see [2]) can be improved for the subclass of toric ideals. A similar result for the minimal generators of I_S appears in [27].

Acknowledgement We would like to thank Antonio Quintero for a very helpful discussion for the statement of lemma 13.

1 On Diophantine Equations in Congruence

Let $\gg$ be the partial natural order in $\mathbf{N}^r$. We will call $\mathbf{N}-$solution of a system of diophantine equations to any one solution of the system whose entries are non negative integers. In the homogeneous case, the set of $\mathbf{N}-$solutions which are minimal for $\gg$, is called the Hilbert basis of the system. It is well-known the set of $\mathbf{N}-$solutions of a homogeneous systems is a finitely generated semigroup (see [24]). Moreover, the minimal generating set of the $\mathbf{N}-$solutions of a system of homogeneous diophantine equations is its Hilbert basis.

In the following notations and remarks we recollect these facts and others we will need in this paper.

Given $L \subset \mathbf{N}^r$,

- if $L \neq \{0\}$, $\mathcal{H}L = \{x \in L - \{\mathbf{0}\} \ \mid \ x \text{ is minimal for } \ \gg\}$,
- if $L = \{0\}$, $\mathcal{H}L := \{0\}$.

Dickson's lemma guarantees that $\mathcal{H}L$ is finite, for any $L \subset \mathbf{N}^r$.

Let $Gx = 0$ be a homogeneous system of diophantine equations with $G \in \mathcal{M}_{m\times r}(\mathbf{Z})$.

Remark 1. *Let $\mathcal{G} = \{x \in \mathbf{N}^r \,|\, Gx = 0\}$, then $\mathcal{H}\mathcal{G}$ is a generating set of $\mathcal{G}$. (See [14])*

If the system is non homogeneous, $Gx = b$ with $b \in \mathbf{Z}^m$, the set of the $\mathbf{N}-$solutions can be written as a finite union of subsets. Any subset is the sum of a $\gg -$minimal $\mathbf{N}-$solution and the semigroup of the $\mathbf{N}-$solutions of the associated homogeneous system.

Remark 2. *Let $\mathcal{G}'$ be the set $\{x \in \mathbf{N}^r \,|\, Gx = b\}$, and $\mathcal{G} = \{x \in \mathbf{N}^r \,|\, Gx = 0\}$, then*

$$\mathcal{G}' = \cup_{x\in\mathcal{H}\mathcal{G}'}(x + \mathcal{G}).$$

(See [11])

There are a lot of methods to compute the general $\mathbf{N}-$solution of a system diophantine equations (see [25]). Actually, methods using Gröbner Bases are improving the classical methods in Integer Programming (see [17]). The following remark shows how the problem is reduced to computing Hilbert bases of homogeneous systems. Its verification is an easy exercise.

Remark 3.

- *$\mathcal{H}\mathcal{G}' = \mathcal{H}\{x \in \mathbf{N}^r \,|\, (G| - b)(x, 1) = 0\}$.*
- *If $\mathcal{G}'' := \{x \in \mathbf{N}^{r+1} \,|\, (G| - b)x = 0\}$, then*

$$\mathcal{H}\mathcal{G}' = \{x \in \mathbf{N}^r \,|\, (x, 1) \in \mathcal{H}\mathcal{G}''\}.$$

Working out $\mathbf{N}-$solutions is a $\mathcal{NP}-$complete problem, and adding a new indeterminate increases the complexity of the calculate. For this reason, methods computing directly $\mathcal{H}\mathcal{G}'$ are interesting.

On the other hand, fix $e \in \mathbf{N}^r$. Let

$$\mathcal{G}_e := \{x \in \mathbf{N}^r \,|\, Gx = 0, \, x \gg e\}.$$

How can we compute $\mathcal{H}\mathcal{G}_e$? It is easy to verify the following remark.

Remark 4. *Let*

$$\mathcal{G}'_e := \{x \in \mathbf{N}^r \,|\, G(x + e) = 0\}.$$

Then $\mathcal{G}_e = \mathcal{G}'_e + e$, and $\mathcal{H}\mathcal{G}_e = \mathcal{H}\mathcal{G}'_e + e$.

Notice that by Remarks 3 and 4, the set $\mathcal{H}\mathcal{G}_e$ can be computed by means of the Hilbert basis of a homogeneous system.

But, *what's happening if the system is in congruence?* For example, let $(Sist)$ be the system

$$(Sist) \equiv \left\{ \begin{array}{cccccc} n_{11}x_1 + n_{12}x_2 + & \cdots & +n_{1r}x_r & = & b_1 & \\ n_{21}x_1 + n_{22}x_2 + & \cdots & +n_{2r}x_r & = & b_2 & \\ \vdots & \vdots & \vdots & & & \\ n_{h1}x_1 + n_{h2}x_2 + & \cdots & +n_{hr}x_r & = & b_h & \\ n_{(h+1)1}x_1 + n_{(h+1)2}x_2 + & \cdots & +n_{(h+1)r}x_r & = & b_{h+1} & mod\, a_1 \\ \vdots & \vdots & \vdots & & \vdots & \\ n_{(h+s)1}x_1 + n_{(h+s)2}x_2 + & \cdots & +n_{(h+s)r}x_r & = & b_{h+s} & mod\, a_s \end{array} \right.$$

We consider the system above as $Gx = b\ mod\ a$, with $G \in \mathcal{M}_{(h+s)\times r}(\mathbf{Z})$, $b \in \mathbf{Z}^{h+s}$ and $a \in \mathbf{Z}^s$. One can easily extend the results above to it.

Remark 5. *The recollected properties in 1, 2, 3, and 4, are true if the system of diophantine equations is in congruence.*

To work theoretically with systems in congruence arises no difficulty. The main problem is computing the $\mathbf{N}-$solutions of $(Sist)$. The natural way, (see [21]), is to add new indeterminates (two by equation in congruence) and to solve the system:

$$(Sist') \equiv \left\{ \begin{array}{cccccccc} n_{11}x_1 + n_{12}x_2 + & \cdots & +n_{1r}x_r & & & = & b_1 \\ n_{21}x_1 + n_{22}x_2 + & \cdots & +n_{2r}x_r & & & = & b_2 \\ \vdots & \vdots & \vdots & & & & \\ n_{h1}x_1 + n_{h2}x_2 + & \cdots & +n_{hr}x_r & & & = & b_h \\ n_{(h+1)1}x_1 + n_{(h+1)2}x_2 + & \cdots & +n_{(h+1)r}x_r & +t_{11}a_1 & -t_{12}a_1 & = & b_{h+1} \\ \vdots & \vdots & \vdots & & \vdots & & \\ n_{(h+s)1}x_1 + n_{(h+s)2}x_2 + & \cdots & +n_{(h+s)r}x_r & +t_{s1}a_s & -t_{s2}a_s & = & b_{h+s} \end{array} \right.$$

Precisely, if we consider the matrix

$$T := \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ a_1 & -a_1 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & a_2 & -a_2 & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & & a_s & -a_s \end{pmatrix} \in \mathcal{M}(\mathbf{Z})_{(h+s)\times 2s},$$

and we call

$$L := \{x \in \mathbf{N}^r \,|\, Gx = b \bmod a\},$$

and

$$L' := \{x' \in \mathbf{N}^{r+2s} |\, (G|T)x' = b\},$$

the following properties are satisfied.

Remark 6.

$$L = \pi(L'),\ \textit{and}\ \mathcal{H}L \subset \pi(\mathcal{H}L'),$$

where $\pi : \mathbf{N}^{r+s} \longrightarrow \mathbf{N}^r$ *is the projection over the first coordinates.*

But we cannot forget that adding new indeterminates may drastically increase the complexity of the calculate ($\mathcal{NP}-$complete problem). For this reason, we propose employing the generalization of an algorithm using Gröbner basis which appears in [17]. We need to generalize the method to the case in congruence. See now how we do this.

We consider

$$L(i,\alpha) := \{\beta = (\beta_1,\dots,\beta_r) \in L | \beta_i = \alpha\},$$

where $1 \le i \le r$, and $\alpha \in \mathbf{N}$.

Remark 7. *Let $s = (s_1,\dots,s_r) \in L$, $s \neq 0$, and let*

$$F = \{s\} \cup \bigcup_{i=1}^{r} \bigcup_{\alpha=0}^{s_i-1} \mathcal{H}(L(i,\alpha)).$$

Then, $\mathcal{H}L = \mathcal{H}F$. (See [17])

By recursively using 7, the problem of computing $\mathcal{H}L$ is reduced to the computation of a particular $\mathbf{N}-$solution of the given system, and particular solutions of a finite number of new systems where some variables have been fixed. Since all of these systems is in congruence, one can think that again it is necessary to add $2s$ new indeterminates to find each particular solution of these systems. However, one can employ the following algorithm ([28, Alg. 19]) computing a particular $\mathbf{N}-$solution.

Algorithm 8. *Particular $\mathbf{N}$-solution by means of Semigroup Ideals*
Input: A system $Gx = b \bmod a$, where G is a $(h+s)\times r$ $\mathbf{Z}$-matrix, $b \in \mathbf{Z}^{h+s}$ and $a \in \mathbf{Z}^s$.
Output: $\emptyset$ if there is no $\mathbf{N}-$solution, or a vector $u \in \mathbf{N}^r$ such that $Gu = b \bmod a$, $u \neq 0$ if it exists.
1. If $b = 0$

- *Take Γ the subsemigroup of*

$$\mathbf{Z}^h \oplus \mathbf{Z}/a_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/a_s\mathbf{Z}.$$

generated by the column vectors of G, $\{n_1,\dots,n_r\}$.

- *Compute a generating set of I_Γ, $\mathcal{G}n$.*
- *If there is a binomial $\pm(1-\mathbf{X}^\alpha) \in \mathcal{G}n$, output $u = \alpha$ and STOP.*
- *Otherwise, output $u = 0$ and STOP.*

2. If $b \neq 0$

- *Take Γ the subsemigroup of*

$$\mathbf{Z}^h \oplus \mathbf{Z}/a_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/a_s\mathbf{Z}.$$

generated by the column vectors of G and b, $\{n_1,\dots,n_r,b\}$.

- *Compute a generating set of I_Γ, $\mathcal{G}n$.*
- *If there is a binomial $\pm(X_{r+1}-\mathbf{X}^\beta) \in \mathcal{G}n$, where $\mathbf{X}$ does not contain the variable X_{r+1}, output $u = \beta$ and STOP. Otherwise, continue.*
- *If there is no binomial $\pm(1-\mathbf{X}^\alpha) \in \mathcal{G}n$, output $\emptyset$ and STOP. Otherwise, fix a monomial order giving priority to the last variable, and take a Gröbner basis for I_Γ, $\mathcal{G}b$.*
- *If there is a binomial $\pm(X_{r+1}-\mathbf{X}^\beta) \in \mathcal{G}b$, where $\mathbf{X}$ does not contain the variable X_{r+1}, output $u = \beta$ and STOP.*

- *Otherwise, output $\emptyset$ and STOP.*

In order to prove that this algorithm does not add $2s$ new indeterminates, we must show how a generating set of I_Γ is computed, where Γ is a finitely generated subsemigroup of

$$\mathbf{Z}^h \oplus \mathbf{Z}/a_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/a_s\mathbf{Z}.$$

For this, we use a set of generators of the lattice $ker(\Gamma)$. There exist two methods ([3] and [15]) computing the ideal I_Γ using the lattice $ker(\Gamma)$. Both are based in the computation of Gröbner Bases in a polynomial ring with the same number of variables than generators for Γ. Both require a set of generators for the lattice $ker(\Gamma)$ as input. The following remark explains how to get it.

Remark 9. *We associate to the semigroup $S = \langle n_1, \ldots, n_r\rangle$ subsemigroup of*

$$\mathbf{Z}^h \oplus \mathbf{Z}/a_1 \oplus \cdots \oplus \mathbf{Z}/a_s,$$

the semigroup $S' \subset \mathbf{Z}^{h+s}$, $S' := \langle n'_1, \ldots, n'_{r+s}\rangle$, where $n'_i := n_i$, for any i, $1 \le i \le r$, and

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

for any i, $r+1 \le i \le r+s$. Then, if C' is a set of generators for $ker(S') \subset \mathbf{Z}^{r+s}$, then $\pi(C')$ is a set of generators for $ker(S)$, where $\pi : \mathbf{Z}^{r+s} \longrightarrow \mathbf{Z}^r$ is the projection over the first coordinates.

Therefore, Algorithm 8 only need to add s variables, and to solve systems over $\mathbf{Z}$ but not over $\mathbf{N}$.

Finally, the following algorithm to compute $\mathcal{H}L$.

Algorithm 10. *Computing $\mathcal{H}L$*
Input: A system $Gx = b \bmod a$, where G is a $(h+s) \times r$ $\mathbf{Z}-$matrix, $b \in \mathbf{Z}^{h+s}$ and $a \in \mathbf{Z}^s$.
Output: $\mathcal{H}L$ for $L = \{s \in \mathbf{N}^r | Gs = b \bmod a\}$.
1. If $r = 1$, one has only one indeterminate, so solve it is trivial and $\mathcal{H}L$ is unique, STOP.
2. If $r \ge 2$, determine whether or not $L = \emptyset$ or $\{0\}$ using Algorithm 8.
3. If $L = \emptyset$ or $\{0\}$, output $\mathcal{H}L = L$ and STOP.
4. Otherwise, take $s = (s_1, \ldots, s_r) \in L \setminus \{0\}$.
5. For $i = 1, \ldots, r$, and $\alpha = 0, \ldots, s_i - 1$, compute $\mathcal{H}(L(i, \alpha))$ by recursively calling Algorithm 10.
6. Compute $\mathcal{H}F$ for

$$F = \{s\} \cup \bigcup_{i=1}^{r} \bigcup_{\alpha=0}^{s_i-1} \mathcal{H}(L(i, \alpha)).$$

7. Output $\mathcal{H}L = \mathcal{H}F$.

At this moment, there is no research likening the computational behavior of this algorithm with the natural method.

2 Finite Check Set

We are going to introduce and recall different notations and definitions we will need in the following sections.

Let $S \subset \mathbf{Z}^h \oplus \mathbf{Z}/a_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/a_s\mathbf{Z}$ be a finitely generated semigroup with zero element, such that $S \cap (-S) = \{0\}$, and $a = (a_1, \ldots, a_s) \in \mathbf{Z}^s$. Let $\{n_1, \ldots, n_r\} \subset S$ be a set of generators for S. We consider the $((h+s) \times r)-$matrix

$$\mathcal{A} := (n_1 | n_2 | \cdots | n_r) \in \mathcal{M}_{(h+s)\times r}(\mathbf{Z}),$$

considering $n_1, \dots, n_r \in \mathbf{Z}^{h+s}$.

Let k be a field, let $k[S]$ be the semigroup $k-$algebra associated to S, and let $R = k[X_1, \dots, X_r]$ be the polynomial ring in r indeterminates. We write $\mathbf{m} = \oplus_{m \in S-\{0\}} R_m$ for the irrelevant maximal ideal in R. Let I_S be the ideal of R corresponding to $\{n_1, \dots, n_r\}$, and let N_1 be the first syzygy module associated to a chosen minimal generating set of I_S.

We want to find a finite set $\mathcal{C}$ to check possible elements in S corresponding to the degrees of the minimal first syzygies. This means that

$$C_1 := \{m \in S \;\mid\; V_1(m) \neq 0\},$$

is contained in $\mathcal{C}$, where

$$V_1(m) := \frac{(N_1)_m}{(\mathbf{m}N_1)_m}.$$

By recurrence, for $i \geq 2$ fixing a minimal generating set of N_{i-1} we consider N_i the i-syzygy module, and the associated space

$$V_i(m) := \frac{(N_i)_m}{(\mathbf{m}N_i)_m}.$$

On the other hand, set $\Lambda := \{1, \dots, r\}$ and $n_F := \sum_{i \in F} n_i$ $(n_\emptyset = 0)$, for each $F \subset \Lambda$. One has an abstract simplicial complex given by

$$\Delta_m := \{F \subset \Lambda \,|\, m - n_F \in S\},$$

for each $m \in S$.

Fixing a concrete choice for the orientation of the simplices, we consider the augmented chain complex

$$0 \to \tilde{C}_r(k, \Delta_m) \cong k \xrightarrow{\partial_r} \cdots \xrightarrow{\partial_2} \tilde{C}_1(k, \Delta_m) \xrightarrow{\partial_1} \tilde{C}_0(k, \Delta_m) \xrightarrow{\partial_0} \tilde{C}_{-1}(k, \Delta_m) \cong k \to 0$$

where $\tilde{C}_i(k, \Delta_m)$ is the $k-$vector space generated by the faces F of Δ_m of dimension i, i.e. $\sharp F = i+1$. Let $Z_i(\Delta_m)$ be the kernel of ∂_i, and let $B_i(\Delta_m)$ be the image of ∂_{i+1}. We denote by $\tilde{H}_i(\Delta_m) = Z_i(\Delta_m)/B_i(\Delta_m)$ the $k-$vector spaces of the reduced homology.

Remark 11. *In our reasoning it is basic that there exists an isomorphism between the spaces $V_i(m)$ and $\tilde{H}_i(\Delta_m)$. Indeed, we use an such isomorphism explicited in Remark 3.6 of [5]. For our purpose it is enough to take $i = 1$.*

Then, we have that

$$C_1 = \{m \in S \;\mid\; \tilde{H}_1(\Delta_m) \neq 0\}.$$

Definition 12. *Let $m \in S$ and $F := \{i_1, \dots, i_t\} \subset \Lambda$ such that $\sharp F \geq 3$, and let σ be a polygon (non needfully plane) whose vertex set is F. We say σ is an $F-$cavity of Δ_m if the following conditions are satisfied:*

1. *$F_j \in \Delta_m$, $\forall j = 1, \dots, t$ where*

$$F_j := \{i_j, i_{j+1}\}, \forall j = 1, \dots, t-1, \text{ and } F_t := \{i_t, i_1\},$$

are the faces of σ.

2. *If $F_j \neq F' \subset F$, $\sharp F' \geq 2$, then $F' \notin \Delta_m$.*

Viewing the graph associated to Δ_m, one can imagine the meaning of σ is an $F-$cavity of Δ_m (see figure 1).

Notice that given a set of vertices F with $\sharp F = t$, the quantity of different polygons over F is $(t-1)!/2$.

We prove the following result.

Figure 1: $\sigma = (2\,3\,4)$ $F = \{2,3,4\}-$cavity of Δ_m

Lemma 13. *Let $m \in S$ such that $\tilde{H}_1(\Delta_m) \neq 0$. Then, there is σ an $F-$cavity of Δ_m with faces F_i satisfying*

$$c = \sum_{j=1}^{t} \epsilon_j F_j \in Z_1(\Delta_m) \setminus B_1(\Delta_m),$$

for some $\epsilon_j = \pm 1$, $\forall j = 1, \dots, t$.

Proof. By $\tilde{H}_1(\Delta_m) \neq 0$, there exists

$$d = \sum_{j=1}^{t} \lambda_j F_j \in Z_1(\Delta_m) \setminus B_1(\Delta_m).$$

We can assume that d is such that t is minimal. In this situation, $\lambda_j \neq 0$, for any j.

Suppose $F_1 = \{i_1, i_2\}$. Then, for some $\epsilon_1 = \pm 1$

$$\partial_1 d = \lambda_1 \epsilon_1 (\{i_2\} - \{i_1\}) + \cdots = 0.$$

Therefore, there is F_j with $j \neq 1$, and $i_2 \in F_j$. Suppose $j = 2$, and $F_2 = \{i_2, i_3\}$. Notice that $i_1 \neq i_3$ because $F_1 \neq F_2$.

In a similar way, one finds a set $F_3 = \{i_3, i_4\}$ (then $t \geq 3$) where $i_3 \neq i_4$ and $i_4 \neq i_2$.

- If $i_4 = i_1$, we have

  $$F_1 = \{i_1, i_2\},\ F_2 = \{i_2, i_3\},\ F_3 = \{i_3, i_1\}.$$

  We can get the elements

  $$d_1 = \lambda_1 F_1 + \epsilon_2 \lambda_1 F_2 + \epsilon_3 \lambda_1 F_3,$$

  $$d_2 = (\lambda_2 - \epsilon_2 \lambda_1) F_2 + (\lambda_3 - \epsilon_3 \lambda_1) F_3 + \sum_{j=4}^{t} \lambda_j F_j,$$

  with $\epsilon_i = \pm 1$, such that $\partial_1 d_1 = 0$, and then $d_2 = d - d_1 \in Z_1(\Delta_m)$. If $d_2 \neq 0$, $d_2 \in B_1(\Delta_m)$ because t is minimal. Then $d_1 \notin B_1(\Delta_m)$, and $d_2 = 0$. Take $c = 1/\lambda_1 d_1$.

- If $i_4 \neq i_1$, we know that $i_4 \neq i_2$, $i_4 \neq i_3$. Therefore $t \geq 4$.

  As before, we obtain that there is $F_j = \{i_4, i_5\}$, $i_5 \neq i_4, i_3$. Suppose $j = 4$.

  If $i_5 = i_1$ a reasoning as the step above yields an element $c = \sum_{j=1}^{4} \epsilon_j F_j \in Z_1(\Delta_m) \setminus B_1(\Delta_m)$.

  If $i_5 = i_2$ a reasoning as the step above yields an element $c = \sum_{j=2}^{4} \epsilon_j F_j \in Z_1(\Delta_m) \setminus B_1(\Delta_m)$. But it is a contradiction with $t \geq 4$.

  Otherwise, we get $F_5 = \{i_5, i_6\}$ and we continue with this process.

The process must finish because there is a finite number of possible i_j. Therefore, we conclude that there exists

$$c = \sum_{j=1}^{t} \epsilon_j F_j \in Z_1(\Delta_m) \setminus B_1(\Delta_m),$$

with

$$F_1 = \{i_1, i_2\},\ F_2 = \{i_2, i_3\},\ F_3 = \{i_3, i_4\},\ \ldots,\ F_t = \{i_t, i_1\},$$

for some $\epsilon_j = \pm 1\ \forall j = 1, \ldots, t$. Now we must prove that the polygon σ defined by $F_1, \ldots, F_t$ is an $F-$cavity of Δ_m, where $F = \bigcup_{j=1}^{t} F_j$. For this, we only need to prove the second condition of the definition of $F-$cavity.

Suppose that $F' \subset F$, $F' \neq F_j$, $\sharp F' \geq 2$ and $F' \in \Delta_m$. In that case, there exist $i_p, i_q \in F'$ such that $q \neq p+1$, $p \neq q+1$ and $\{p, q\} \neq \{1, t\}$. Suppose $p = 1$ and consider $F'' = \{i_1, i_q\}$. Then

$$\begin{array}{rcl} c & = & \sum_{j=1}^{t} \epsilon_j F_j + \epsilon_{t+1} F'' - \epsilon_{t+1} F'' \\ & = & \underbrace{\epsilon_1 F_1 + \epsilon_2 F_2 + \cdots + \epsilon_{q-1} F_{q-1} - \epsilon_{t+1} F''}_{c_1} \underbrace{+ \epsilon_{t+1} F'' + \epsilon_q F_q + \cdots + \epsilon_t F_t}_{c_2}\ . \end{array}$$

We determine $\epsilon_{t+1} = \pm 1$, such that $c_1, c_2 \in Z_1(\Delta_m)$. It is satisfied that $c_1 \notin B_1(\Delta_m)$ or $c_2 \notin B_1(\Delta_m)$ because $c \notin B_1(\Delta_m)$. But this is not possible because t is minimal. $\square$

Remark 14. *The numbers $\epsilon_i = \pm 1$ in the previous lemma depend of the considered orientation on Δ_m.*

Using the lemma 13, the problem of computing $\mathcal{C}$ is *to find $m \in S$ such that there exists σ an $F-$cavity of Δ_m*. We are going to make it employing some $\mathbf{N}-$solutions of diophantine equations.

Definition 15. *Let $>_S$ be the partial order in S such that $m \geq_S m'$ if $m - m' \in S$.*
Let H be a subset of S, $m \in H$ is $S-$minimal in H if

$$m \not>_S m',\ \forall m' \in H.$$

Given $\emptyset \neq H \subset S$, there is an element $m \in H$ $S-$minimal in H because S satisfies the condition $S \cap (-S) = \{0\}$, and let us have a finite number of shapes to write m in function of $\{n_1, \ldots, n_r\}$ (see [4, Proposition 1.2]).

If σ is an $F-$cavity of Δ_m, there is $\beta^{(i)} = (\beta_1^{(i)}, \ldots, \beta_{r-t+2}^{(i)}) \in \mathbf{N}^{(r-t+2)t}$ satisfying

$$\left\{ \begin{array}{lcll} m - n_{F_1} & = & \sum_{j \in (\Lambda \setminus F) \cup F_1} \beta_j^{(1)} n_j & mod\ a \\ m - n_{F_2} & = & \sum_{j \in (\Lambda \setminus F) \cup F_2} \beta_j^{(2)} n_j & mod\ a \\ & \vdots & & \\ m - n_{F_{t-1}} & = & \sum_{j \in (\Lambda \setminus F) \cup F_{t-1}} \beta_j^{(t-1)} n_j & mod\ a \\ m - n_{F_t} & = & \sum_{j \in (\Lambda \setminus F) \cup F_t} \beta_j^{(t)} n_j & mod\ a \end{array} \right. \Rightarrow \left\{ \begin{array}{lcll} m & = & n_{F_1} + \mathcal{A}_{F_1} \beta^{(1)} & mod\ a \\ m & = & n_{F_2} + \mathcal{A}_{F_2} \beta^{(2)} & mod\ a \\ & \vdots & & \\ m & = & n_{F_{t-1}} + \mathcal{A}_{F_{t-1}} \beta^{(t-1)} & mod\ a \\ m & = & n_{F_t} + \mathcal{A}_{F_t} \beta^{(t)} & mod\ a \end{array} \right.$$

where $\mathcal{A}_{F_i} \in \mathcal{M}_{(h+s)\times(r-t+2)}(\mathbf{Z})$ is the matrix which columns are the columns of $\mathcal{A}$ corresponding to $(\Lambda \setminus F) \cup F_i$.

Then, if $e_1, \ldots, e_r$ are the canonical basis in $\mathbf{N}^r$, set

$$e_{F_i} := \pi_i(\sum_{j \in F_i} e_j),$$

where $\pi_i : \mathbf{N}^r \to \mathbf{N}^{r+t-2}$ is the projection which omits the coordinates corresponding to $F \setminus F_i$, $1 \le i \le t$.

So we have that there exists $\alpha = (\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(t)}) \in \mathbf{N}^{(r-t+2)t}$ such that

$$m = \mathcal{A}_{F_1}\alpha^{(1)} = \mathcal{A}_{F_2}\alpha^{(2)} = \cdots = \mathcal{A}_{F_t}\alpha^{(t)} \ mod\ a,$$

and $\alpha \gg e_\sigma$ with $e_\sigma := (e_{F_1}, e_{F_2}, \ldots, e_{F_{t-1}}, e_{F_t}) \in \mathbf{N}^{(r-t+2)t}$.

Then, the way to get $m \in S$ such that σ is an $F-$cavity of Δ_m, is computing some $\mathbf{N}-$solutions, $\alpha \in \mathbf{N}^{(r-t+2)t}$, of the system of equations

$$\begin{pmatrix} \mathcal{A}_{F_1} & -\mathcal{A}_{F_2} & 0 & 0 & 0 & & 0 & 0 \\ 0 & \mathcal{A}_{F_2} & -\mathcal{A}_{F_3} & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \mathcal{A}_{F_3} & -\mathcal{A}_{F_4} & 0 & & 0 & 0 \\ & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & 0 & 0 & 0 & & \mathcal{A}_{F_{t-1}} & -\mathcal{A}_{F_t} \end{pmatrix} \begin{pmatrix} \alpha^{(1)} \\ \alpha^{(2)} \\ \vdots \\ \alpha^{(t-1)} \\ \alpha^{(t)} \end{pmatrix} = 0,$$

where each $(h+s)-$file of this system is in congruence $mod\ a$. We consider the above system as

$$\mathcal{A}_\sigma \alpha = 0 \ \ mod\ \tilde{a},$$

where

$$\mathcal{A}_\sigma := \begin{pmatrix} \mathcal{A}_{F_1} & -\mathcal{A}_{F_2} & 0 & 0 & 0 & & 0 & 0 \\ 0 & \mathcal{A}_{F_2} & -\mathcal{A}_{F_3} & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \mathcal{A}_{F_3} & -\mathcal{A}_{F_4} & 0 & & 0 & 0 \\ & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & 0 & 0 & 0 & & \mathcal{A}_{F_{t-1}} & -\mathcal{A}_{F_t} \end{pmatrix} \in \mathcal{M}_{(t-1)(h+s)\times(r-t+2)t}(\mathbf{Z}).$$

Let R_σ be the set of $\mathbf{N}-$solutions

$$R_\sigma := \{\alpha = (\alpha^{(1)}, \ldots, \alpha^{(t)}) \in \mathbf{N}^{(r-t+2)t} |\, \mathcal{A}_\sigma \alpha = 0 \ \ mod\ \tilde{a}, \alpha \gg e_\sigma\}.$$

Let $\mathcal{H}R_\sigma$ be the set of $\gg -$minimal elements of R_σ, and let ΣR_σ be the subset of S,

$$\Sigma R_\sigma := \{p \in S |\, p = \mathcal{A}_{F_1}\alpha^{(1)} = \mathcal{A}_{F_2}\alpha^{(2)} = \cdots = \mathcal{A}_{F_t}\alpha^{(t)},\ (\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(t)}) \in R_\sigma\}.$$

Set

$$\mathcal{C}_\sigma := \{p \in S |\, p \text{ is } S-\text{minimal in } \Sigma R_\sigma\}.$$

We are in conditions to prove the following proposition,

Proposition 16. *If $\tilde{H}_1(\Delta_m) \neq 0$, then there is σ an $F-$cavity of Δ_m such that $m \in \mathcal{C}_\sigma$.*

Proof. By lemma 13, there is σ an $F-$cavity of Δ_m with faces F_i satisfying

$$c = \sum_{j=1}^{t} \epsilon_j F_j \in Z_1(\Delta_m) \setminus B_1(\Delta_m),$$

for some $\epsilon_j = \pm 1$, $\forall j = 1, \ldots, t$. It is clear that $m \in \Sigma R_\sigma$.

Assume $m \in \Sigma R_\sigma \setminus \mathcal{C}_\sigma$. In that case, there are $m' \in \mathcal{C}_\sigma$ and $m'' \in S$, such that $m = m' + m''$.

If $m'' = 0$, then $m \in \mathcal{C}_\sigma$, and we have finished.

Suppose $m'' \neq 0$, $m'' = \sum_{i=1}^{r} d_i n_i$.

We have two possibilities:

- $i \in F$. Take l such that $i \notin F_l$.

$$\left.\begin{array}{lcl} d_i \neq 0 & \Rightarrow & m'' - n_i \in S \\ m' \in \mathcal{C}_\sigma & \Rightarrow & m' - n_{F_l} \in S,\ i \notin F_l \end{array}\right\} \Rightarrow m - n_{F_l} - n_i \in S \Rightarrow F_l \cup \{i\} \in \Delta_m.$$

  But it is not possible because σ is an $F-$cavity of Δ_m.

- $i \notin F$.

$$\left.\begin{array}{lcl} d_i \neq 0 & \Rightarrow & m'' - n_i \in S \\ m' \in \mathcal{C}_\sigma & \Rightarrow & m' - n_{F_j} \in S,\ i \notin F \end{array}\right\} \Rightarrow m - n_{F_j} - n_i \in S,\ \forall j = 1, \dots, t.$$

  Then, $F'_j = F_j \cup \{i\} \in \Delta_m$, $\forall j = 1, \dots, t$. It is easy to see that

$$c = \partial_2 (\sum_{j=1}^{t} \epsilon_j F'_j).$$

  But this is a contradiction because $c \notin B_1(\Delta_m)$. Graphically, this can be see in figure 2.

Figure 2: Non $S-$minimal

We have proved $m \in \mathcal{C}_\sigma$. □

Another problem is *to compute the set $\mathcal{C}_\sigma$ and to prove that it is a finite set.* To do it, we consider

$$\Sigma \mathcal{H} R_\sigma := \{ p \in S | \, p = \mathcal{A}_{F_1} \alpha^{(1)} = \cdots = \mathcal{A}_{F_t} \alpha^{(t)},\ \alpha = (\alpha^{(1)}, \dots, \alpha^{(t)}) \in \mathcal{H} R_\sigma \}.$$

By Dickson's lemma $\mathcal{H} R_\sigma$ is finite, hence $\Sigma \mathcal{H} R_\sigma$ is finite.

Lemma 17. *It is satisfied that $\mathcal{C}_\sigma \subset \Sigma \mathcal{H} R_\sigma$. In particular, $\mathcal{C}_\sigma$ is a finite set.*

Proof. Assume $m \in \mathcal{C}_\sigma \setminus \Sigma \mathcal{H} R_\sigma$.
$m \in \mathcal{C}_\sigma \Rightarrow \exists \alpha = (\alpha^{(1)}, \dots, \alpha^{(t)}) \in R_\sigma \,|\, m = \mathcal{A}_{F_1} \alpha^{(1)} = \cdots = \mathcal{A}_{F_t} \alpha^{(t)}$.

By $m \notin \Sigma \mathcal{H} R_\sigma$, α is not $\gg -$minimal in R_σ. In that case, $\exists \alpha' \in \mathcal{H} R_\sigma$ and $\exists \alpha''$ $\mathbf{N}-$solution of $\mathcal{A}_\sigma \alpha'' = 0$ such that $\alpha = \alpha' + \alpha''$. If we consider $m' = \mathcal{A}_{F_1} \alpha'^{(1)} \in \Sigma \mathcal{H} R_\sigma$, we have $m - m' \in S$. Then, m is not $S-$minimal in ΣR_σ, because $m \neq m'$. This is a contradiction with $m \in \mathcal{C}_\sigma$.

$\mathcal{C}_\sigma$ is a finite set because $\Sigma \mathcal{H} R_\sigma$ is a finite set. □

Remark 18. *Notice that lemma 17 connects the $S-$minimal elements in ΣR_σ with the $\gg -$minimal elements of R_σ, $\mathcal{H}R_\sigma$. This is the key to bound the degree of the minimal first syzygies of $k[S]$ (section 3).*

Applying lemma 17, we obtain an algorithm computing a finite set $\mathcal{C} \subset S$ to check whether $\tilde{H}_1(\Delta_m) \neq 0$.

Algorithm 19. Check Algorithm
Input: Set of generators $\{n_1, \ldots, n_r\}$ of S.
Output: $\mathcal{C}$ set to check whether $\tilde{H}_1(\Delta_m) \neq 0$.

$G := \emptyset$
$\mathcal{F} := \{F \subset \mathcal{P}(\Lambda) |\, \sharp F \geq 3\}$
While $\mathcal{F} \neq \emptyset$ do
For $F \in \mathcal{F}$ and $\forall \sigma$ polygon whose vertex set is F, do
Compute the subset of $\mathbf{N}-$solutions, $\mathcal{H}R_\sigma$ [1].
Compute the set $\mathcal{C}_\sigma$ from $\mathcal{H}R_\sigma$ [2].
$G = G \cup \{(m, \sigma, F) |\, m \in \mathcal{C}_\sigma\}$
$\mathcal{F} = \mathcal{F} \setminus F$.
$\mathcal{C} := \{m \in S |\, \sigma \ F - \text{cavity of } \Delta_m \ (m, \sigma, F) \in G\}$

Algorithm 19 allow us to enunciate the following theorem.

Theorem 20. *The set C_1 of S-degrees for the minimal first syzygies of $k[S]$ can be computed by means of some simplicial complexes Δ_m, $m \in S$.*

Moreover, using Remark 11 we obtain a new method computing a minimal generating set of N_1: For every $m \in C_1$, take the images of the basis elements for the homology spaces $\tilde{H}_1(\Delta_m)$ by the isomorphism $\tilde{H}_1(\Delta_m) \cong V_1(m)$.

Corollary 21. *Minimal generating set for the first syzygy module of a toric variety can be determined using Algorithm 19.*

3 Application to the bounds of the degree

As we have seen, our finite check set is subseted in a set of minimal $\mathbf{N}-$solutions of diophantine equations. There are a lot of bounds for the minimal $\mathbf{N}-$solutions of systems of diophantine equations (see [25]). We are going to use one of them in order to bound the degree of the minimal first syzygies for $k[S]$. Our bound only depends from the generators of the semigroup.

In [19], we can find some bounds to the minimal $\mathbf{N}-$solution of diophantine equations. The author, Pottier, considers the system of diophantine equations $Ax = 0$, where $rank(A) = s$, and he denotes M the Hilbert basis of the $\mathbf{N}-$solutions of the system. The following notations are used $||A||_{1,\infty} := sup_i\{\sum_j |A(i,j)|\}$, $||x||_1 := \sum_i |x_i|$, and $||M||_1 := sup_{x \in M} ||x||_1$. Pottier proves in [19] the following result.

Theorem 22.
$$||M||_1 \leq (1 + ||A||_{1,\infty})^s.$$

[1] Using the remarks 3, 4 and 5, one can obtain this set computing the $\gg -$minimal $\mathbf{N}-$solutions of the systems
$$\mathcal{A}_\sigma \alpha = -\mathcal{A}_\sigma e_\sigma.$$

[2] Using lemma 17.

Proof. See [19]. ☐

In our particular case, let $m \in S$ be a degree such that $\tilde{H}_1(\Delta_m) \neq 0$, and let σ be an $F-$cavity of Δ_m (there exists σ by Proposition 16).

As the semigroup has torsion, we will need to *remove* the congruences of some systems of type

$$\mathcal{A}_\sigma \alpha = b \ \ mod \ \ \tilde{a}$$

to use the Pottier's theorem. In

$$\mathcal{M}_{(t-1)(h+s)\times((r-t+2)t+2s(t-1))}(\mathbf{Z}),$$

we consider the following matrix

$$\tilde{\mathcal{A}}_\sigma := \begin{pmatrix} \mathcal{A}_{F_1} & -\mathcal{A}_{F_2} & 0 & 0 & 0 & & 0 & 0 & T & 0 & 0 & & 0 \\ 0 & \mathcal{A}_{F_2} & -\mathcal{A}_{F_3} & 0 & 0 & \cdots & 0 & 0 & 0 & T & 0 & \cdots & 0 \\ 0 & 0 & \mathcal{A}_{F_3} & -\mathcal{A}_{F_4} & 0 & & 0 & 0 & 0 & 0 & T & & 0 \\ & & \ddots & \ddots & \ddots & & & & & \ddots & \ddots & & \\ 0 & 0 & 0 & 0 & 0 & & \mathcal{A}_{F_{t-1}} & -\mathcal{A}_{F_t} & 0 & 0 & 0 & & T \end{pmatrix}$$

with

$$T := \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ a_1 & -a_1 & 0 & 0 & 0 & 0 & 0 & & 0 & 0 \\ 0 & 0 & a_2 & -a_2 & 0 & 0 & 0 & \cdots & 0 & 0 \\ & & & & \ddots & \ddots & \ddots & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & & a_s & -a_s \end{pmatrix} \in \mathcal{M}(\mathbf{Z})_{(h+s)\times 2s}.$$

Set

$$D := max_{\eta \text{ polygon over } F, F\subset\Lambda}\{D_\eta\}$$

with

$$D_\eta := sup_i\{\sum_j |(\mathcal{A}_\eta \mid \mathcal{A}_\eta \cdot e_\eta)(i,j)|\} \in \mathbf{N}.$$

Theorem 23. *Let $m \in S$ be a* degree *of an element of a minimal system of homogeneous generators for the first syzygy module of $k[S]$. Then $\exists \beta^{(1)} \in \mathbf{N}^r$ such that $m = \mathcal{A}\beta^{(1)}$ and $||\beta^{(1)}||_1$ is at most*

$$(1 + 2max_{i=1,\dots,s}\{|a_i|\} + D)^{(h+s)(r-1)} + 2r - 1.$$

Therefore, this degree is singly-exponential in the number of variables.

Proof. We have proved in Proposition 16 and Lemma 17 that if $\tilde{H}_1(\Delta_m) \neq 0$, $m \in \mathcal{C}_\sigma$ for a polygon, σ, F-cavity for $F \subset \Lambda$, $\sharp F = t \geq 3$.

$$\begin{array}{lcl} m \in \mathcal{C}_\sigma & \overset{\text{lemma } 17}{\Rightarrow} & \exists \alpha \in \mathcal{H}R_\sigma |\, m = \mathcal{A}_{F_1}\alpha^{(1)} \\ & \overset{\text{remarks } 4,5}{\Rightarrow} & \alpha - e_\sigma \in \mathcal{H}\{\beta \in \mathbf{N}^{(r-t+2)t} |\, \mathcal{A}_\sigma\beta = -\mathcal{A}_\sigma e_\sigma \ \ mod \ \ \tilde{a}\} \\ & \overset{\text{remark } 6}{\Rightarrow} & \exists \lambda \in \mathbf{N}^{2s(t-1)} |\, (\alpha - e_\sigma, \lambda) \in \mathcal{H}\{\beta' \in \mathbf{N}^{(r-t+2)t+2s(t-1)} |\, \tilde{\mathcal{A}}_\sigma\beta' = -\mathcal{A}_\sigma e_\sigma\} \\ & \overset{\text{remark } 3}{\Rightarrow} & (\alpha - e_\sigma, \lambda, 1) \in \mathcal{H}\{\beta'' \in \mathbf{N}^{(r-t+2)t+2s(t-1)+1} |\, (\tilde{\mathcal{A}}_\sigma | \mathcal{A}_\sigma e_\sigma)\beta'' = 0\} \\ & \overset{\text{theorem } 22}{\Rightarrow} & ||(\alpha - e_\sigma, \lambda, 1)||_1 \leq (1 + 2max_{i=1,\dots,s}\{|a_i|\} + D_\sigma)^{(h+s)(t-1)} \leq \\ & & \leq (1 + 2max_{i=1,\dots,s}\{|a_i|\} + D)^{(h+s)(r-1)} \end{array}$$

Then

$$\begin{array}{rcl} ||\alpha^{(1)}||_1 & \leq & ||\alpha||_1 \\ & \leq & ||\alpha - e_\sigma + e_\sigma||_1 \\ & \leq & ||(\alpha - e_\sigma, \lambda)||_1 + ||e_\sigma||_1 \\ & = & ||(\alpha - e_\sigma, \lambda, 1)||_1 + ||e_\sigma||_1 - 1 \\ & \leq & (1 + 2max_{i=1,\dots,s}\{|a_i|\} + D)^{(h+s)(r-1)} + 2r - 1 \end{array}$$

To get $\beta^{(1)}$ in the theorem, one only must complete $\alpha^{(1)}$ with null elements. □

References

[1] A. ARAMOVA, J. HERZOG, Free resolution and Koszul homology. *J. of Pure and Applied Algebra,* **105** (1995), 1-16.

[2] D. BAYER, M. STILLMAN, On the Complexity of Computing syzygies. *J. Symbolic Computation* (1988) **6**, 135-147.

[3] F. DI BIASE, R. URBANKE, An Algorithm to Calculate the Kernel of Certain Polynomial Ring Homomorphisms, *Experimental Mathematics*, Vol.4, No. 3 (1995), 227-234.

[4] E. BRIALES, A. CAMPILLO, C. MARIJUÁN, P. PISÓN, Minimal Systems of Generators for Ideals of Semigroups, *J. of Pure and Applied Algebra,* **127** (1998), 7-30.

[5] E. BRIALES, A. CAMPILLO, C. MARIJUÁN, P. PISÓN, Combinatorics of syzygies for semigroup algebra. *Collect. Math.* **49** (1998), 239-256.

[6] W. BRUNS, J. HERZOG, Semigroup rings and simplicial complexes. *J. of Pure and Applied Algebra*, **122** (1997), 185-208.

[7] A. CAMPILLO, C. MARIJUÁN, Higher relations for a numerical semigroup. *Sém. Théor. Nombres Bordeaux* **3** (1991), 249-260.

[8] A. CAMPILLO, P. GIMÉNEZ, Syzygies of affine toric varieties. *Journal of Algebra* to appear.

[9] A. CAMPILLO, P. PISÓN, Generators of a monomial curve and graphs for the associated semigroup. *Bull. Soc. Math. Belg. Sér. A* **45**(1-2) (1993), 45-58.

[10] A. CAMPILLO, P. PISÓN, L'idéal d'un semi-grupe de type fini. *C. R. Acad. Sci. Paris, Série I*, **316** (1993), 1303-1306.

[11] E. COTEJEAN, H. DEVIE, An efficient Algorithm for solving systems of diophantine equations. *Information and Computation*, 113(1), (1994) 143-172.

[12] E. DOMENJOUD, *Outils pour la Déduction Automatique dans les Théories Associatives-Commutatives.* Thése de doctorat d'Université, Université de Nancy I (1991).

[13] D. EISENBUD, *Introduction to Commutative Algebra with a View Towards Algebraic Geometry.* Graduate Texts in Mathematics **150** (1995), Springer, New York.

[14] P. GORDAN, Uever die Aufföсung linearer Gleichungen mit reellen Coefficienten. *Mathematische Annalen* **6** (1873), 23-28.

[15] S. HOSTEN, B. STURMFELS, GRIN, An Implementation of Gröbner Bases for Integer Programming, In E. Balas and J. Clausen editors, *Integer Programming and Combinatorial Optimization*, LNCS **920**, Springer-Verlag (1995), 267-276.

[16] I. PEEVA, B. STURMFELS, Syzygies of codimension 2 lattice ideals, *Math. Z.* **229** (1998), 163-194.

[17] P. PISÓN-CASARES, A. VIGNERON-TENORIO, $\mathbf{N}-$solutions to linear systems over $\mathbf{Z}$. *Preprint of University of Sevilla* **43** (1998).

[18] L.POTTIER, Bornes et algorithmes de calcul des générateurs des solutions de systémes diphantiens linéaires *C. R. Acad. Sci. Paris, Série I*, **311** (1990), 813-816.

[19] L. POTTIER, Minimal solutions of linear diophantine systems: bounds and algorithms. *Proceedings of the Fourth International Conference on Rewriting Techniques and Applications,* Italy 1991, 162-173.

[20] J.C. ROSALES, *Semigrupos numéricos .* PhD Thesis, Universidad de Granada (1991).

[21] J. C. ROSALES, P. A. GARCÍA-SÁNCHEZ, Presentaciones de monoides cancelativos. *Proceedings of EACA'98,* Spain 1998, 130-141.

[22] A. SCHRIJVER, *Theory of Linear and Integer Programming.* Wiley-Interscience (1996).

[23] R. STANLEY, *Enumerative Combinatorics.* The Wadsworth & Brooks/Cole Mathematics Series, Vol.**I** (1986).

[24] R. STANLEY, *Combinatorics and commutative algebra 2nd ed.* Progress in Mathematics Vol.**41**, Boston Basel Berlin, Birkhäuser (1996).

[25] A. P. TOMÁS, *On Solving Linear Diophantine Constraints.* PhD Thesis, Facultade de Ciências da Universidade do Porto (1997).

[26] B. STURMFELS, *Gröbner Bases and Convex Polytopes*, AMS University Lectures Series, Vol. 8 (1995).

[27] B. STURMFELS, Gröbner bases of Toric Varieties. *Tôhoku Math. J.* **43** (1991), 249-261.

[28] A. VIGNERON-TENORIO, Semigroup Ideals and Linear Diophantine Equations. *Linear Algebra and its Applications,* **295** (1999), 133-144.