Matemática Contemporânea, Vol. 21, 1–25
http://doi.org/10.21711/231766362001/rmc211

TORIC IDEALS

Anna Bigatti **Lorenzo Robbiano** *

Introduction

Toric ideals are binomial ideals which represent the algebraic relations of finite sets of power-products. Their importance comes from on the fact that they show up in many problems arising from different branches of science, for instance Integer Programming and Combinatorics.

Largely inspired by the fundamental book [St], we have recently addressed the problem of computing toric ideals in the paper [BLR], and even more recently we became aware of a new use of toric ideals in Statistics (see for instance [Din] and [PRW]) after the pioneering work [DiSt].

The broadening scope of use of this beautiful piece of theory suggested the need for the present paper, which is mainly expository, although it contains some important remarks which we were unable to find in the literature (see for instance Theorem 2.18).

Some essential background for reading this paper can be found for instance in the book [KrRo]. The paper is subdivided into three sections. The first one introduces toric ideals associated both to power products and to Laurent power products. The first fundamental properties of toric ideals are proved (see Theorems 1.6 and 1.13).

In the second section we introduce a different point of view, which turns out to be of fundamental importance. Namely we think of toric ideals as related to Diophantine matrices, which enable us to develop a nice piece of theory. Of great importance, for instance in computation, is Theorem 2.10, which relates

*This work was partially supported by CNR.

the toric ideal associated to a matrix $\mathcal{A}$ to the set of solutions of the Diophantine system $\mathcal{A}z = 0$. Then we show how to exploit suitable gradings associated to $\mathcal{A}$ (see Definition 2.11), and prove the already mentioned Theorem 2.18.

The third and final section deals with the problem of navigating inside the set of the solutions of a Diophantine system $\mathcal{A}z = b$. We show how to use Gröbner bases to compute solutions (see Proposition 3.2 and Corollary 3.3). As an example of "navigating" we discuss integer programming briefly.

1 Definitions and first Properties

In this section we give the basic definitions, and state the first properties of toric ideals.

1.1 Toric Ideals and Power Products

Definition 1.1 Let K be a field, let $y_1, \ldots, y_m$ be indeterminates, and let $\tau_1, \tau_2, \ldots, \tau_n$ be power products in $y_1, \ldots, y_m$. Then let $x_1, \ldots, x_n$ be other indeterminates and $P = K[x_1, \ldots, x_n]$. The **toric ideal** associated to the tuple $(\tau_1, \tau_2, \ldots, \tau_n)$ is the ideal of all polynomials $g \in P$ which vanish at $\tau_1, \tau_2, \ldots, \tau_n$, i.e. such that $g(\tau_1, \tau_2, \ldots, \tau_n) = 0$ in $K[y_1, \ldots, y_m]$. It is denoted by $\mathcal{I}(\tau_1, \tau_2, \ldots, \tau_n)$, or simply by $\mathcal{I}$.

In other words, if we let $\varphi : P \to K[y_1, \ldots, y_m]$ be the K-algebra homomorphism given by $\varphi(x_1) = \tau_1, \ldots, \varphi(x_n) = \tau_n$, then $\mathcal{I} = \mathrm{Ker}(\varphi)$.

Example 1.2 For instance $(y_1y_2)^2 - (y_1^2)(y_2^2) = 0$, hence $x_2^2 - x_1x_3 = 0$ is an algebraic relation among $y_1^2,\ y_1y_2,\ y_2^2$. We may consider $x_2^2 - x_1x_3$ as a polynomial in x_2 with coefficients in $K[x_1, x_3]$, and then express every polynomial $f(x_1, x_2, x_3) \in K[x_1, x_2, x_3]$ as

$$f(x_1, x_2, x_3) = a(x_1, x_3) \cdot (x_2^2 - x_1x_3) + b(x_1, x_3) \cdot x_2 + c(x_1, x_3)$$

The relation $f(y_1^2, y_1y_2, y_2^2) = 0$ implies $b(y_1^2, y_2^2) \cdot y_1y_2 + c(y_1^2, y_2^2) = 0$, hence $b(y_1^2, y_2^2) = c(y_1^2, y_2^2) = 0$, hence $b(x_1, x_3) = c(x_1, x_3) = 0$. We conclude that $\mathcal{I}(y_1^2,\ y_1y_2,\ y_2^2) = (x_1x_3 - x_2^2) \subset K[x_1, x_2, x_3]$.

Unlike in the above example, it is generally difficult to compute $\mathcal{I}$. More tools are needed.

Proposition 1.3 *Let R be a ring, let $R[x_1, \ldots, x_n]$ be a polynomial ring over R, let $f_1, \ldots, f_n \in R$, and let $\psi : R[x_1, \ldots, x_n] \longrightarrow R$ be the R-homomorphism of substitution defined by $\psi(x_i) = f_i$ for $i = 1, \ldots, n$*

a) The kernel of ψ is the ideal $(x_1 - f_1, \ldots, x_n - f_n)$ in $R[x_1, \ldots, x_n]$.

b) For every $g \in R[x_1, \ldots, x_n]$, there exist $h_1, \ldots, h_n \in R[x_1, \ldots, x_n]$ such that

$$g = \sum_{i=1}^{n} h_i \cdot (x_i - f_i) + g(f_1, \ldots, f_n)$$

Proof. For a full proof see Proposition 3.6.1 in [KrRo].

Here we simply say that the formula $g = \sum_{i=1}^{n} h_i \cdot (x_i - f_i) + r$ with $r \in R$ works exactly like a division with remainder, and of course if we do have an equality $g = \sum_{i=1}^{n} h_i \cdot (x_i - f_i) + r$, then $r = g(f_1, \ldots, f_n)$, as one checks by using the substitution $x_i = f_i$ for $i = 1, \ldots, n$.

□

Proposition 1.4 *Let K be a field, let $\tau_1, \tau_2, \ldots, \tau_n$ be power products in the indeterminates $y_1, \ldots, y_m$, and let J be the ideal in $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ generated by $\{x_1 - \tau_1,\ x_2 - \tau_2, \ldots,\ x_n - \tau_n\}$.*

a) We have $\mathcal{I}(\tau_1, \ldots, \tau_n) = J \cap P$.

b) Let G be a Gröbner basis of J with respect to an elimination ordering for $\{y_1, \ldots, y_m\}$. Then $\mathcal{I}$ is generated by the elements in $G \cap P$.

Proof. To prove *a)* we consider the K-algebra homomorphism

$$K[x_1, \ldots, x_n, y_1, \ldots, y_m] \xrightarrow{\psi} K[y_1, \ldots, y_m]$$

which is defined by $\psi(y_i) = y_i$ for $i = 1, \ldots, m$, and $\psi(x_i) = \tau_i$ for $i = 1, \ldots, n$. We consider P as a subring of $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and observe that $\varphi = \psi_{|P}$. Proposition 1.3.a implies that $J = \mathrm{Ker}(\psi)$, hence $\mathcal{I} = \mathrm{Ker}(\varphi) = \mathrm{Ker}(\psi_{|P}) = J \cap P$.

Claim *b*) follows from Theorem 3.4.5 in [KrRo], where it is proved that $G \cap P$ is a Gröbner basis, hence a set of generators, of $J \cap P$.

□

Definition 1.5 We call **binomial** a polynomial of the type $t_1 - t_2$, where t_1, t_2 are power products. We say that a binomial $t_1 - t_2$ is **pure** if $\gcd(t_1, t_2) = 1$.

Theorem 1.6 *Let K be a field, let $\tau_1, \tau_2, \ldots, \tau_n$ be power products in the indeterminates $y_1, \ldots, y_m$. Let $x_1, \ldots, x_n$ be other indeterminates over K, and let $\mathcal{I}$ be the toric ideal in $P = K[x_1, \ldots, x_n]$ associated to $(\tau_1, \ldots, \tau_n)$. Consider any grading on the polynomial ring $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$, where the degrees of the y_i are arbitrary integers and $\deg(x_i) = \deg(\tau_i)$ for $i = 1, \ldots, n$. Then*

a) The ideal $\mathcal{I}$ is prime.

b) The ideal $\mathcal{I}$ is generated by pure binomials. Actually

$$\mathcal{I} = (\{t_1 - t_2 \mid \varphi(t_1) = \varphi(t_2),\ \gcd(t_1, t_2) = 1\})$$

c) The ideal $\mathcal{I}$ is homogeneous.

Proof. The ideal $\mathcal{I}$ is prime since it is the kernel of a homomorphism from P to the integral domain $K[y_1, \ldots, y_m]$. To prove *b*) we use the equality $\mathcal{I} = J \cap P$ (see Proposition 1.4.a). Since J is generated by binomials, Gröbner bases theory implies that all the elements in any reduced Gröbner basis of J are binomials. Using Proposition 1.4, we see that $\mathcal{I}$ is generated by binomials. Now, let $t_1 - t_2$ be a binomial in $\mathcal{I}$. By definition, $\varphi(t_1 - t_2) = 0$, hence $\varphi(t_1) = \varphi(t_2)$, which shows that $\mathcal{I} \subseteq (\{t_1 - t_2 \mid \varphi(t_1) = \varphi(t_2)\})$. On the other hand, we have just seen that $\mathcal{I}$ is prime, and clearly it does not contain any indeterminate, so that $t(t_1 - t_2) \in \mathcal{I}$ implies $t_1 - t_2 \in \mathcal{I}$. The other inclusion follows from the definition of $\mathcal{I}$.

To prove *c*) we observe that the ideal J is homogeneous, since it is generated by homogeneous polynomials, and recall again that $\mathcal{I} = J \cap P$. Now, let f be a polynomial in $J \cap P$. All its homogeneous components are in J, since

J is homogeneous, and are clearly in P. Consequently, all its homogeneous components are in $\mathcal{I}$, which shows that $\mathcal{I}$ is homogeneous (see Proposition 1.7.10 in [KrRo]).

□

Example 1.7 We shall now compute an explicit example, namely a set of generators of the toric ideal $\mathcal{I}(y_1y_2,\ y_1^3y_2^2,\ y_1y_2^3,\ y_1^5y_2^2)$. According to what we have seen, we have to compute the kernel of the K-algebra homomorphism $\varphi : K[x_1,x_2,x_3,x_4] \longrightarrow K[y_1,y_2]$, which is given by the following rules $\varphi(x_1) = y_1y_2$, $\varphi(x_2) = y_1^3y_2^2$, $\varphi(x_3) = y_1y_2^3$, $\varphi(x_4) = y_1^5y_2^2$. We consider the ideal J in $K[x_1,x_2,x_3,x_4,y_1,y_2]$ which is generated by the set $\{x_1 - y_1y_2,\ x_2 - y_1^3y_2^2,\ x_3 - y_1y_2^3,\ x_4 - y_1^5y_2^2\}$. The solution of our problem is $\mathcal{I} = J \cap K[x_1,x_2,x_3,x_4]$. It can be computed with CoCoA by performing `Elim(y,J)`. The reduced Gröbner basis from which we compute `Elim(y,J)` is $\{x_2^4 - x_1x_3x_4^2,\ x_1^3x_2 - x_3x_4,\ x_1^4x_4 - x_2^3,\ x_1^7 - x_2^2x_3,\ y_2x_2 - x_1^3,\ y_2x_3x_4 - x_1^6,\ y_1x_3x_4 - x_1x_2^2,\ y_2x_1x_4 - x_2^2,\ y_1x_2x_3 - x_1^5,\ y_1x_2^2 - x_1^2x_4,\ y_1x_1x_2 - y_2x_4,\ y_2x_1^2 - y_1x_3,\ y_1x_1^2 - x_2,\ y_1y_2 - x_1,\ y_2^2x_4 - x_1^2x_2,\ y_1^2x_3 - x_1^3,\ y_1^2x_2 - x_4,\ y_2^2x_1 - x_3\}$.

Therefore the solution is $\mathcal{I} = (x_2^4 - x_1x_3x_4^2,\ x_1^3x_2 - x_3x_4,\ x_1^4x_4 - x_2^3,\ x_1^7 - x_2^2x_3)$. We have a relation $x_2^4 - x_1x_3x_4^2 = x_1x_4(x_1^3x_2 - x_3x_4) - x_2(x_1^4x_4 - x_2^3)$, so that $x_2^4 - x_1x_3x_4^2$ is redundant, and it is possible to check that a minimal set of generators of the ideal $\mathcal{I}$ is $\{x_1^3x_2 - x_3x_4,\ x_1^4x_4 - x_2^3,\ x_1^7 - x_2^2x_3\}$. We observe that the computed Gröbner basis has 18 elements.

1.2 Toric Ideals and Laurent Power Products

Now we are going to examine the case of power products $\tau_1,\dots,\tau_n$ with both *positive* and *negative* exponents.

Definition 1.8 Let K be a field. An expression $\sum_{(i_1,\dots,i_m)\in\mathbb{Z}^m} c_{(i_1,\dots,i_m)}\, y_1^{i_1}\cdots y_m^{i_m}$, where only finitely many elements $c_{(i_1,\dots,i_m)} \in K$ are different from zero, is called a **Laurent polynomial** in the indeterminates $y_1,\dots,y_m$. Consequently, en expression $y_1^{a_1}y_2^{a_2}\cdots y_m^{a_m}$, where $a_i \in \mathbb{Z}$ for $i = 1,\dots,m$, is called a **Laurent term** or a **Laurent power product**.

Laurent polynomials are polynomial expressions in $y_1, \ldots, y_m, y_1^{-1}, \ldots, y_m^{-1}$. Therefore the set of all Laurent polynomials is a finitely generated K-subalgebra of the field $K(y_1, \ldots, y_m)$, and is denoted by $L = K[y_1, \ldots, y_m, y_1^{-1}, \ldots, y_m^{-1}]$.

Henceforth, we denote by f the power product $\prod_{i=1}^{m} y_i$. It is a standard fact in commutative algebra that L is isomorphic to the localization $K[y_1, \ldots, y_m]_f$.

In the next definition we extend the notion of a toric ideal to the case of Laurent power products.

Definition 1.9 Let $\tau_1, \ldots, \tau_n$ be Laurent power products in the indeterminates $y_1, \ldots, y_m$, and let $\varphi : P \longrightarrow K[y_1, \ldots, y_m]_f$ be the K-algebra homomorphism defined by $\varphi(x_1) = \tau_1, \ldots, \varphi(x_n) = \tau_n$. The toric ideal associated to the tuple $(\tau_1, \tau_2, \ldots, \tau_n)$ is the ideal $\mathcal{I}(\tau_1, \ldots, \tau_n) = \mathrm{Ker}(\varphi)$.

Definition 1.10 Let τ be a Laurent power product. Then there exists a minimum natural number $p(\tau)$ and a power product called τ' such that $\tau = \frac{\tau'}{f^{p(\tau)}}$.

Proposition 1.11 *Let K be a field, let $y_1, \ldots, y_m$ be indeterminates, and let $\tau_1, \tau_2, \ldots, \tau_n$ be Laurent power products in $y_1, \ldots, y_m$. Then let $f = \prod_{i=1}^{m} y_i$ and consider the ideal J in $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ generated by the following set $\{f^{p(\tau_1)}x_1 - \tau_1',\ f^{p(\tau_2)}x_2 - \tau_2', \ldots, f^{p(\tau_n)}x_n - \tau_n'\}$.*

a) We have $\mathcal{I}(\tau_1, \ldots, \tau_n) = (J : f^\infty) \cap P$.

b) Let u be a new indeterminate and let G be a Gröbner basis of the ideal $J + (fu - 1)$ with respect to an elimination ordering for $\{u, y_1, \ldots, y_m\}$. Then $\mathcal{I}(\tau_1, \ldots, \tau_n)$ is generated by the elements in $G \cap P$.

Proof. To prove *a)* we look at the following commutative diagram of K-algebra homomorphisms

$$\begin{array}{ccc} P = K[x_1, \ldots, x_n] & \xrightarrow{\varphi} & K[y_1, \ldots, y_m]_f \\ \downarrow \alpha & & \uparrow \psi \\ K[x_1, \ldots, x_n, y_1, \ldots, y_m] & \xrightarrow{\beta} & K[x_1, \ldots, x_n, y_1, \ldots, y_m]_f \end{array}$$

where α and β are the canonical injective homomorphisms, and the K-algebra homomorphism $\psi : K[x_1, \ldots, x_n, y_1, \ldots, y_m]_f \longrightarrow K[y_1, \ldots, y_m]_f$ is defined by

$\psi(y_i) = y_i$ for $i = 1, \ldots, m$, and $\psi(x_i) = \tau_i$ for $i = 1, \ldots, n$. Consequently $\mathcal{I}(\tau_1, \ldots, \tau_n) = \mathrm{Ker}(\varphi) = \alpha^{-1}(\beta^{-1}(\mathrm{Ker}(\psi)))$. To get the conclusion we need to prove that $J : f^\infty = \beta^{-1}(\mathrm{Ker}(\psi))$. We consider the ideal $\widehat{J}$ generated by $\{x_1 - \tau_1,\ x_2 - \tau_2, \ldots, x_n - \tau_n\}$ in $K[x_1, \ldots, x_n, y_1, \ldots, y_m]_f$. Then $\widehat{J}$ is the extension of J to the ring $K[x_1, \ldots, x_n, y_1, \ldots, y_m]_f$ via the map β. This ring is isomorphic to $R[x_1, \ldots, x_n]$, where $R = K[y_1, \ldots, y_m]_f$, and we deduce from Proposition 1.3 that $\widehat{J} = \mathrm{Ker}\,(\psi)$. Therefore $\beta^{-1}(\mathrm{Ker}(\psi)) = \beta^{-1}(\widehat{J}) = \beta^{-1}(\beta(J))$, and the latter is $J : f^\infty$ (see Proposition 3.5.11.b. in [KrRo]).

To prove *b*) we consider the sequence of K-algebra homomorphisms

$$P = K[x_1, \ldots, x_n] \xrightarrow{\alpha} K[x_1, \ldots, x_n, y_1, \ldots, y_m] \xrightarrow{\gamma} K[x_1, \ldots, x_n, y_1, \ldots, y_m, u]$$

where α and γ are the canonical injective homomorphisms. Let us denote by L the ideal $J + (fu - 1)$. From Theorem 3.5.13.a in [KrRo] we deduce that $\gamma^{-1}(L) = J : f^\infty$. We may identify P with its image $\gamma(\alpha(P))$, and use *a*) to conclude that $\mathcal{I}(\tau_1, \ldots, \tau_n) = \alpha^{-1}(J : f^\infty) = \alpha^{-1}(\gamma^{-1}(L)) = L \cap P$. We conclude the proof by using the same argument invoked in the proof of Proposition 1.4.b.

□

Example 1.12 Let us compute the toric ideal $\mathcal{I}(y_1y_2^{-1},\ y_1^{-1}y_2^3,\ y_1y_2^3,\ y_1^3y_2^{-2})$. Let $f = y_1y_2$. We have $y_1y_2^{-1} = f^{-1}y_1^2$, $y_1^{-1}y_2^3 = f^{-1}y_2^4$, $y_1^3y_2^{-2} = f^{-2}y_1^5$. Therefore we consider the ideal J in $K[x_1, x_2, x_3, x_4, y_1, y_2]$ which is generated by the set $\{fx_1 - y_1^2, fx_2 - y_2^4, x_3 - y_1y_2^3, f^2x_4 - y_1^5\}$. Following the above proposition, we take in account the ideal $L = J + (fu - 1)$. Then we eliminate $[y_1, y_2, u]$, and get $\mathcal{I}(y_1y_2^{-1},\ y_1^{-1}y_2^3,\ y_1y_2^3,\ y_1^3y_2^{-2}) = (x_3 - x_1^3x_2^2,\ x_4^2 - x_1^7x_2)$.

Theorem 1.13 *Let K be a field, let $\tau_1, \tau_2, \ldots, \tau_n$ be Laurent power products in the indeterminates $y_1, \ldots, y_m$, let $x_1, \ldots, x_n$ be other indeterminates over K, and let $\mathcal{I}$ be the toric ideal in $P = K[x_1, \ldots, x_n]$ associated to $(\tau_1, \tau_2, \ldots, \tau_n)$. Consider any grading on $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ where the degrees of the y_i are arbitrary integers and $\deg(x_i) = \deg(\tau_i)$ for $i = 1, \ldots, n$. Then*

a) The ideal $\mathcal{I}$ is prime.

b) The ideal $\mathcal{I}$ is generated by pure binomials. Actually

$$\mathcal{I} = (\{t_1 - t_2 \mid \varphi(t_1) = \varphi(t_2),\ \gcd(t_1, t_2) = 1\})$$

c) The ideal $\mathcal{I}$ is homogeneous.

Proof. The proof is obtained as a variation on the proof of Theorem 1.6. □

Remark 1.14 Theorem 1.13 is an extension of Theorem 1.6. However there is an *important difference.* Namely, in the case of Theorem 1.6 if we choose positive degrees for the y_i, we obtain positive degrees for the x_i. Therefore the toric ideal $\mathcal{I}$ turns out to be homogeneous with respect to a positive grading (see Definition 2.11). This conclusion cannot be drawn in general in the case of Theorem 1.13. As a counterexample it suffices to take $\mathcal{I}(y_1,\ y_1^{-1})$. More on this will be discussed in Subsection 2.2.

2 Toric Ideals and Diophantine Matrices

In this section we switch our point of view and consider toric ideals as algebraic objects associated to Diophantine matrices.

Let $\tau_1, \ldots, \tau_n$ be Laurent power products in the indeterminates $y_1, \ldots, y_m$. We write $\tau_i = y_1^{a_{1i}} y_2^{a_{2i}} \cdots y_m^{a_{mi}}$ for $i = 1, \ldots, n$, and obtain the matrix $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ with m rows, n columns, and integer entries. Conversely, given such a matrix, we may consider the n-tuple $(\tau_1, \ldots, \tau_n)$, where $\tau_i = y_1^{a_{1i}} y_2^{a_{2i}} \cdots y_m^{a_{mi}}$, for $i = 1, \ldots, n$. In other words we see that tuples of Laurent power products can be encoded by matrices with integer entries. This remark suggests the following definition.

Definition 2.1 Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ and let $\tau_i = y_1^{a_{1i}} y_2^{a_{2i}} \cdots y_m^{a_{mi}}$ for $i = 1, \ldots, n$. We define the **toric ideal associated to $\mathcal{A}$** to be the toric ideal $\mathcal{I}(\tau_1, \ldots, \tau_n) \subset K[x_1, \ldots, x_n]$. It will be also denoted by $\mathcal{I}(\mathcal{A})$.

2.1 Toric Ideals and Kernels of Matrices

If we look at toric ideals in the way suggested by the above definition, we may be led to explore a possible connection between generators of toric ideals and $\mathbb{Z}$-module generators of kernels of integer matrices.

Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. We consider the homogeneous system of Diophantine equations associated to $\mathcal{A}$.

$$\begin{cases} a_{11}z_1 + a_{12}z_2 + \cdots + a_{1n}z_n &= 0 \\ a_{21}z_1 + a_{22}z_2 + \cdots + a_{2n}z_n &= 0 \\ \vdots & \vdots \ \ \vdots \\ a_{m1}z_1 + a_{m2}z_2 + \cdots + a_{mn}z_n &= 0 \end{cases}$$

whose set of integer solutions is a $\mathbb{Z}$-module (or integer lattice) called $\mathrm{Ker}(\mathcal{A})$.

We need some technical definitions.

Definition 2.2 Let $a \in \mathbb{Z}$. We define $a^+ = \max(a, 0)$, $a^- = \max(-a, 0)$. Let $u = (u_1, \ldots, u_n)$ be a vector in $\mathbb{Z}^n$. It can be written as $u = u^+ - u^-$, where $u^+ = ({u_1}^+, \ldots, {u_n}^+)$ and $u^- = ({u_1}^-, \ldots, {u_n}^-)$. For instance $(3, 2, -1) = (3, 2, 0) - (0, 0, 1)$. Given a vector $u \in \mathbb{Z}^n$, we denote by $\mathbf{x}^u$ the Laurent power product $x_1^{u_1} \cdots x_n^{u_n}$.

Definition 2.3 Let $S \subseteq P$. We denote by $\mathrm{Bin}(S)$ the set of binomials in S, and by $\mathrm{PBin}(S)$ the set of pure binomials in S.

Let $\varrho' : \mathbb{Z}^n \longrightarrow P$, and $\vartheta' : \mathrm{Bin}(P) \longrightarrow \mathbb{Z}^n$ be defined in the following way. For $u = (u_1, \ldots, u_n) \in \mathbb{Z}^n$, we let

$$\varrho'(u_1, \ldots, u_n) = \mathbf{x}^{u^+} - \mathbf{x}^{u^-} = x_1^{{u_1}^+} \cdots x_n^{{u_n}^+} - x_1^{{u_1}^-} \cdots x_n^{{u_n}^-}$$

For $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^n$, and $b = \mathbf{x}^\alpha - \mathbf{x}^\beta \in \mathrm{Bin}(P)$, we let

$$\vartheta'(b) = (\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n)$$

Proposition 2.4 *With the above definitions and assumptions, the following conditions hold true.*

a) $\varrho'(\mathrm{Ker}(\mathcal{A})) \subseteq \mathrm{PBin}(\mathcal{I}(\mathcal{A}))$, $\vartheta'(\mathrm{PBin}(\mathcal{I}(\mathcal{A}))) \subseteq \mathrm{Ker}(\mathcal{A})$, *hence there exist two maps* $\varrho : \mathrm{Ker}(\mathcal{A}) \longrightarrow \mathrm{PBin}(\mathcal{I}(\mathcal{A}))$, $\vartheta : \mathrm{PBin}(\mathcal{I}(\mathcal{A})) \longrightarrow \mathrm{Ker}(\mathcal{A})$, *which are induced by* ϱ' *and* ϑ'.

b) The maps ϱ *and* ϑ *are inverse to each other.*

Proof. First, we prove *a)*. For $u = (u_1, \ldots, u_n) \in \mathrm{Ker}(\mathcal{A})$ we get

$$\left\{\begin{array}{rcl} a_{11}u_1^+ + a_{12}u_2^+ + \cdots + a_{1n}u_n^+ & = & a_{11}u_1^- + a_{12}u_2^- + \cdots + a_{1n}u_n^- \\ a_{21}u_1^+ + a_{22}u_2^+ + \cdots + a_{2n}u_n^+ & = & a_{21}u_1^- + a_{22}u_2^- + \cdots + a_{2n}u_n^- \\ \vdots & \vdots & \vdots \\ a_{m1}u_1^+ + a_{m2}u_2^+ + \cdots + a_{mn}u_n^+ & = & a_{m1}u_1^- + a_{m2}u_2^- + \cdots + a_{mn}u_n^- \end{array}\right.$$

We get $\tau_1^{u_1^+} \cdots \tau_n^{u_n^+} = \tau_1^{u_1^-} \cdots \tau_n^{u_n^-}$, hence $x_1^{u_1^+} \cdots x_n^{u_n^+} - x_1^{u_1^-} \cdots x_n^{u_n^-} \in \mathcal{I}(\mathcal{A})$, and it is clearly pure.

Now we observe that $b = x_1^{\alpha_1} \cdots x_n^{\alpha_n} - x_1^{\beta_1} \cdots x_n^{\beta_n} \in \mathrm{PBin}(\mathcal{I}(\mathcal{A}))$ implies $\tau_1^{\alpha_1} \cdots \tau_n^{\alpha_n} = \tau_1^{\beta_1} \cdots \tau_n^{\beta_n}$, hence

$$\left\{\begin{array}{rcl} a_{11}\alpha_1 + a_{12}\alpha_2 + \cdots + a_{1n}\alpha_n & = & a_{11}\beta_1 + a_{12}\beta_2 + \cdots + a_{1n}\beta_n \\ a_{21}\alpha_1 + a_{22}\alpha_2 + \cdots + a_{2n}\alpha_n & = & a_{21}\beta_1 + a_{22}\beta_2 + \cdots + a_{2n}\beta_n \\ \vdots & \vdots & \vdots \\ a_{m1}\alpha_1 + a_{m2}\alpha_2 + \cdots + a_{mn}\alpha_n & = & a_{m1}\beta_1 + a_{m2}\beta_2 + \cdots + a_{mn}\beta_n \end{array}\right.$$

We conclude that $(\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n) \in \mathrm{Ker}(\mathcal{A})$.

Finally we prove *b)*. By definition $\vartheta \circ \varrho = \mathrm{id}_{\mathrm{Ker}(\mathcal{A})}$. On the other hand, let $b = x_1^{\alpha_1} \cdots x_n^{\alpha_n} - x_1^{\beta_1} \cdots x_n^{\beta_n} \in \mathrm{PBin}(\mathcal{I}(\mathcal{A}))$. Then $\vartheta(b) = (\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n)$, and the fact that b is a pure binomial implies that $((\alpha_1 - \beta_1)^+, \ldots, (\alpha_n - \beta_n)^+) - ((\alpha_1 - \beta_1)^-, \ldots, (\alpha_n - \beta_n)^-) = (\alpha_1, \ldots, \alpha_n) - (\beta_1, \ldots, \beta_n)$.

It follows that $\varrho \circ \vartheta = \mathrm{id}_{\mathrm{PBin}(\mathcal{I}(\mathcal{A}))}$.

□

Definition 2.5 Let $B = \{v_1, \ldots, v_r\}$ be a subset of $\mathbb{Z}^n$ and denote the ideal $(\varrho'(v_1), \ldots, \varrho'(v_r))$ by $I(B)$. If B generates $\mathrm{Ker}(\mathcal{A})$ as a $\mathbb{Z}$-module, the ideal $I(B)$ is called a **lattice ideal** associated to $\mathrm{Ker}(\mathcal{A})$.

Lemma 2.6 *Let* $v \in \mathbb{Z}^n$, $B = \{v_1, \ldots, v_r\} \subset \mathbb{Z}^n$. *If* $\mathbf{x}^{v^+} - \mathbf{x}^{v^-} \in I(B)$, *there exist* $n_1, \ldots, n_r \in \mathbb{Z}$ *such that* $v = \sum_{i=1}^r n_i v_i$.

Proof. If we use Gröbner basis theory to compute a representation of b as a combination of the elements $\mathbf{x}^{v_{i_j}^+} - \mathbf{x}^{v_{i_j}^-}$, we see that at every step of the computation only operations involving integer coefficients are used. Therefore, if $B' = B \cup \{-v_1, \ldots, -v_r\}$, and we allow possible repetitions of summands, we get a representation

$$\mathbf{x}^{v^+} - \mathbf{x}^{v^-} \quad = \quad \sum_{j=1}^{N} \mathbf{x}^{w_j} \cdot (\mathbf{x}^{v_{i_j}^+} - \mathbf{x}^{v_{i_j}^-}) \tag{1}$$

where each v_{i_j} is a vector in B'. Now it suffices to show that $v = \sum_{j=1}^{N} v_{i_j}$, and we shall proceed by induction on N. If $N = 1$ then (1) implies $v = v_{i_1}$. In general the power product $\mathbf{x}^{v^+}$ is equal to one of the terms $\mathbf{x}^{w_j}\mathbf{x}^{v_{i_j}^+}$ or $\mathbf{x}^{w_j}\mathbf{x}^{v_{i_j}^-}$ appearing in the expansion of the right hand side of (1). By possibly changing the position in the sum, we may assume that $\mathbf{x}^{v^+} = \mathbf{x}^{w_1}\mathbf{x}^{v_{i_1}^+}$, therefore $v^+ = w_1 + v_{i_1}^+$. It follows that $v - v_{i_1} = v^+ - v^- - v_{i_1}^+ + v_{i_1}^- = w_1 + v_{i_1}^+ - v^- - v_{i_1}^+ + v_{i_1}^- = w_1 + v_{i_1}^- - v^-$. Now, deleting the first summand in the right hand side of (1), we get an expression for $\mathbf{x}^{w_1 + v_{i_1}{}^-} - \mathbf{x}^{v^-}$ which has length $N - 1$. By induction, $v - v_{i_1} = w_1 + v_{i_1}{}^- - v^- = \sum_{j=2}^{N} v_{i_j}$. Therefore we conclude that $v = \sum_{j=1}^{N} v_{i_j}$. □

Remark 2.7 Suppose we have the equality $\frac{\mathbf{x}^a}{\mathbf{x}^b} = \frac{\mathbf{x}^c}{\mathbf{x}^d} \cdot \frac{\mathbf{x}^e}{\mathbf{x}^f}$ of Laurent power products. Then $\frac{\mathbf{x}^a}{\mathbf{x}^b} - 1 = (\frac{\mathbf{x}^c}{\mathbf{x}^d} - 1) \cdot \frac{\mathbf{x}^e}{\mathbf{x}^f} + (\frac{\mathbf{x}^e}{\mathbf{x}^f} - 1)$ in P_π, where $\pi = \prod_{i=1}^{n} x_i$. Thus we have the equality $\mathbf{x}^d\mathbf{x}^f(\mathbf{x}^a - \mathbf{x}^b) = \mathbf{x}^b\mathbf{x}^e(\mathbf{x}^c - \mathbf{x}^d) + \mathbf{x}^b\mathbf{x}^d(\mathbf{x}^e - \mathbf{x}^f)$ in P.

Remark 2.8 Given a vector $v \in \mathbb{Z}^n$ and $s \in \mathbb{N}_{>0}$, the binomial $\varrho(sv)$ is a multiple of $\varrho(v)$. Namely $\mathbf{x}^{sv^+} - \mathbf{x}^{sv^-} = (\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) \sum_{j=1}^{s} (\mathbf{x}^{(j-1)v^+}\mathbf{x}^{(s-j)v^-})$.

Lemma 2.9 *Let $B = \{v_1, \ldots, v_r\}$ be a subset of $\mathbb{Z}^n$, and let $v = \sum_{i=1}^{r} n_i v_i$. Then there exists a power product t and polynomials $f_i \in P$ for $i = 1, \ldots, r$ such that*

$$t\,(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) = \sum_{i=1}^{r} f_i\,(\mathbf{x}^{v_i^+} - \mathbf{x}^{v_i^-})$$

Moreover $f_i = \sum_{j=1}^{n_i} t_{ij}$ if $n_i > 0$ and $f_i = -\sum_{j=1}^{-n_i} t_{ij}$ if $n_i < 0$, and the t_{ij} are distinct power products.

Proof. First we prove by induction on s that if $v = \sum_{i=1}^{s} w_i$, then there exist power products $t, t_1, \ldots, t_s \in P$ such that $t\,(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) = \sum_{i=1}^{s} t_i\,(\mathbf{x}^{w_i^+} - \mathbf{x}^{w_i^-})$: If $v = w_1 + w_2$, then $\frac{\mathbf{x}^{v^+}}{\mathbf{x}^{v^-}} = \frac{\mathbf{x}^{w_1^+}}{\mathbf{x}^{w_1^-}} \cdot \frac{\mathbf{x}^{w_2^+}}{\mathbf{x}^{w_2^-}}$ in P_π. Thus, from Remark 2.7, we have in P the equality

$$\mathbf{x}^{w_1^-}\mathbf{x}^{w_2^-}(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) \;=\; \mathbf{x}^{v^-}\mathbf{x}^{w_2^+}(\mathbf{x}^{w_1^+} - \mathbf{x}^{w_1^-}) \;+\; \mathbf{x}^{v^-}\mathbf{x}^{w_1^-}(\mathbf{x}^{w_2^+} - \mathbf{x}^{w_2^-})$$

Let $v = \sum_{i=1}^{s} w_i$. If $s \geq 2$ we write $v = w_1 + w$ where $w = \sum_{i=2}^{s} w_i$. By induction we have that there exist $\tilde{t}, \tilde{t}_1, \tilde{t}_2$ and $t', t'_2, \ldots, t'_s$ power products in P such that $\tilde{t}\,(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) = \tilde{t}_1\,(\mathbf{x}^{w_1^+} - \mathbf{x}^{w_1^-}) + \tilde{t}_2\,(\mathbf{x}^{w^+} - \mathbf{x}^{w^-})$ and $t'\,(\mathbf{x}^{w^+} - \mathbf{x}^{w^-}) = \sum_{i=2}^{s} t'_i\,(\mathbf{x}^{w_i^+} - \mathbf{x}^{w_i^-})$.

Now we multiply the first equality by t' and substitute $t'\tilde{t}_2(\mathbf{x}^{w^+} - \mathbf{x}^{w^-})$ using the second. Then $t = \tilde{t}\,t'$, $t_1 = \tilde{t}_1\,t'$ and $t_i = \tilde{t}_2\,t'_i$ for $i = 2, \ldots, s$ and we get

$$t(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) = \sum_{i=1}^{s} t_i\,(\mathbf{x}^{w_i^+} - \mathbf{x}^{w_i^-})$$

So we have that a sum of s vectors w_i corresponds to a sum of the s associated binomials $\varrho(w_i)$ multiplied by a power product. But we may be more precise. If $v = \sum_{i=1}^{s} n_i v_i$, we have just proved that then there exist power products $t, t_1, \ldots, t_s$ and $t_i \in P$ such that $t(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) = \sum_{i=1}^{s} t_i\,(\mathbf{x}^{n_i v_i^+} - \mathbf{x}^{n_i v_i^-})$, and by Remark 2.8 it follows that $t(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) = \sum_{i=1}^{s} t_i f_i\,(\mathbf{x}^{v_i^+} - \mathbf{x}^{v_i^-})$ where $f_i = \sum_{j=1}^{n_i}(\mathbf{x}^{(j-1)v_i^+}\mathbf{x}^{(n_i-j)v_i^-})$ if $n_i > 0$ and $f_i = -\sum_{j=1}^{-n_i}(\mathbf{x}^{(j-1)v_i^+}\mathbf{x}^{(-n_i-j)v_i^-})$ if $n_i < 0$. In particular each $t_i f_i$ has $|n_i|$ distinct monomials, all with coefficient 1 or all with coefficient -1.

□

The next result (see Lemma 12.2 in [St]) plays a fundamental role, since it states the desired link between generators of toric ideals and $\mathbb{Z}$-module generators of kernels of integer matrices. The link is obtained with the aid of lattice ideals.

Theorem 2.10 *Let* $B = \{v_1, \ldots, v_r\} \subseteq \mathrm{Ker}(\mathcal{A})$ *and let* $\pi = \prod_{i=1}^{n} x_i$. *The following conditions are equivalent*

a) $I(B) : \pi^\infty = \mathcal{I}(\mathcal{A})$.

b) $I(B)\, P_\pi = \mathcal{I}(\mathcal{A})\, P_\pi$.

c) B *is a set of generators of* $\mathrm{Ker}(\mathcal{A})$, *i.e.* $I(B)$ *is a lattice ideal.*

Proof. The implication $a) \Rightarrow b)$ follows from $I(B)\, P_\pi = (I(B) : \pi^\infty)\, P_\pi$, and to prove this equality it suffices to show that $(I(B) : \pi^\infty)\, P_\pi \subseteq I(B)\, P_\pi$. Let $\frac{a}{\pi^r} \in (I(B) : \pi^\infty)\, P_\pi$. Then there exists $s \in \mathbb{N}$ and an element $b \in I(B)$, such that $\frac{a}{\pi^r} = \frac{b}{\pi^{r+s}}$, and the claim follows.

To prove $b) \Rightarrow a)$ we recall the fact that $I(B) : \pi^\infty = I(B)\, P_\pi \cap P$ (see Proposition 3.5.11.b in [KrRo]). Moreover, we know from Theorem 1.6.b that $\mathcal{I}(\mathcal{A})$ is a prime ideal and $\pi \notin \mathcal{I}(\mathcal{A})$, hence $\mathcal{I}(\mathcal{A}) : \pi^\infty = \mathcal{I}(\mathcal{A})$, which implies that $\mathcal{I}(\mathcal{A}) = \mathcal{I}(\mathcal{A})\, P_\pi \cap P$. From the two equalities we get the desired implication.

We show that $a) \Rightarrow c)$. Let $v \in \mathrm{Ker}(\mathcal{A})$. Then $\varrho(v) = \mathbf{x}^{v^+} - \mathbf{x}^{v^-} \in \mathcal{I}(\mathcal{A})$, which is equal to $I(B) : \pi^\infty$ by assumption. It follows that there exists r such that $\pi^r(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) \in I(B)$. We use Lemma 2.6 to see that $\vartheta'(\pi^r \cdot (\mathbf{x}^{v^+} - \mathbf{x}^{v^-})) = \vartheta(\mathbf{x}^{v^+} - \mathbf{x}^{v^-}) = v$ is in the submodule of $\mathrm{Ker}(\mathcal{A})$ generated by B.

Finally we prove that $c) \Rightarrow a)$. We know from Theorem 1.13 that $\mathcal{I}(\mathcal{A})$ is generated by pure binomials. So let b be a pure binomial in $\mathcal{I}(\mathcal{A})$ and let $v = \vartheta(b)$. Then $v \in \mathrm{Ker}(\mathcal{A})$, hence it is a linear combination of the vectors in B with integral coefficients. It suffices to use Lemma 2.9 to get a relation which implies $b \in I(B) : \pi^\infty$. The proof is now complete.

□

The last theorem has a noteworthy consequence in the computation. Namely, a toric ideal $\mathcal{I}(\mathcal{A})$ can be computed by the two steps

a) computing a lattice basis B of $\mathrm{Ker}(\mathcal{A})$, hence a lattice ideal $I(B)$;

b) computing the saturation of $I(B)$ with respect to $\pi = \prod_{i=1}^{n} x_i$.

A detailed discussion on this issue can be found in [BLR]. Here we content ourselves to show the improvement in the computation of Example 1.7, where we dealt with $\mathcal{I}(y_1y_2,\ y_1^3y_2^2,\ y_1y_2^3,\ y_1^5y_2^2)$.

Example 1.7 (continued) Using the point of view discussed in the previous subsection, we can say that the problem is to compute $\mathcal{I}(\mathcal{A})$, where

$$\mathcal{A} = \begin{pmatrix} 1 & 3 & 1 & 5 \\ 1 & 2 & 3 & 2 \end{pmatrix}$$

It is easily seen that a basis of $\mathrm{Ker}(\mathcal{A})$ is $B = \{(-7, 2, 1, 0), (4, -3, 0, 1)\}$. Therefore we may consider $I(B) = (x_1^7 - x_2^2 x_3,\ x_1^4 x_4 - x_2^3)$ and compute its saturation with respect to $\pi = x_1 x_2 x_3 x_4$ by eliminating u from the ideal $J = I(B) + (u\pi - 1)$. We get the same result as in Example 1.7. However, the number of elements in the reduced Gröbner basis of J is 7. This is in contrast with the number of elements in the Gröbner basis computed in Example 1.7, which is 18. We remark that in general this method produces Gröbner bases which are much smaller than the Gröbner bases computed with the method explained in Proposition 1.4.

2.2 Gradings on Toric Ideals

In the last subsection we saw how Theorem 2.10 can be used to improve the computation of toric ideals. Now we are going to discuss another improvement which depends on the fact that toric ideals are homogeneous. We saw in Theorem 1.6 that we may give arbitrary integral degrees to the indeterminates $y_1, \ldots, y_m$ and deduce that the toric ideal is homogeneous with respect to the grading given by $\deg(x_i) = \deg(\tau_i)$ for $i = 1, \ldots, n$.

Definition 2.11 Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. If an n-tuple of integers is obtained as a $\mathbb{Q}$-linear combination of the rows of $\mathcal{A}$ and is taken as the tuple of degrees of the indeterminates, we obtain a grading on P which is called a **grading associated to** $\mathcal{A}$. If all the elements in the tuple are positive we say that the grading is a **positive grading**.

Example 2.12 Let us consider the matrix $\mathcal{A}$ already introduced in Example 1.7 (continued). A non-positive grading associated to $\mathcal{A}$ is obtained by the tuple $3(1, 3, 1, 5) - (1, 2, 3, 2) = (2, 7, 0, 13)$. We observe that the toric ideal

$\mathcal{I} = (x_1^3x_2 - x_3x_4,\ x_1^4x_4 - x_2^3,\ x_1^7 - x_2^2x_3)$ is homogeneous with respect to the grading defined by $\deg(x_1) = 2,\ \deg(x_2) = 7,\ \deg(x_3) = 0,\ \deg(x_4) = 13$.

The following result yields a better insight into this aspect of the theory.

Proposition 2.13 *Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ and let $\mathcal{I}(\mathcal{A})$ be the toric ideal in $K[x_1, \ldots, x_n]$ associated to $\mathcal{A}$. Then $\mathcal{I}(\mathcal{A})$ is homogeneous with respect to every grading associated to $\mathcal{A}$.*

Proof. Following the proof of Theorem 1.6, we may consider the grading given by putting $\deg(y_i) = 0$ for $i \neq k$ and $\deg(y_i) = 1$ for $i = k$. Then the degrees of $x_1, \ldots, x_n$ are given by the k^{th} row of $\mathcal{A}$. Therefore $\mathcal{I}(\mathcal{A})$ is homogeneous with respect to the tuples of degrees given by the rows of $\mathcal{A}$, hence it is homogeneous with respect to every grading associated to $\mathcal{A}$.

□

In the theory of Gröbner bases there is a lot of emphasis on improvements in computation speed which can be achieved whenever one deals with ideals or modules which are homogeneous with respect to a tuple of positive integers. Unfortunately, given $\mathcal{A}$, it is not always true that such a linear combination exists, as we have already seen in Example 1.14. The case treated there corresponds to the matrix $\mathcal{A} = (1, -1)$. But there is a nice way around this problem.

Definition 2.14 Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ be a non-zero matrix. We put $s_j = \sum_{k=1}^{m} a_{kj}$ for $j = 1, \ldots, n$, and $d = d(\mathcal{A}) = \max_i\{s_i\}$. When $d > 0$ we define the **homogenization of** $\mathcal{A}$ to be the matrix

$$\overline{\mathcal{A}} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} & 0 \\ a_{21} & a_{22} & \ldots & a_{2n} & 0 \\ \ldots & \ldots & \ldots & \ldots & 0 \\ a_{m1} & a_{m2} & \ldots & a_{mn} & 0 \\ d - s_1 & d - s_2 & \ldots & d - s_n & d \end{pmatrix}$$

Otherwise we define $\overline{\mathcal{A}}$ to be $\overline{-\mathcal{A}}$.

With the aid of this definition we make an easy observation.

Lemma 2.15 *Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ be a non-zero matrix and consider the map $\varphi : \mathrm{Ker}(\mathcal{A}) \longrightarrow \mathrm{Ker}(\overline{\mathcal{A}})$ defined by the following rule $\varphi(\alpha_1, \ldots, \alpha_n) = (\alpha_1, \ldots, \alpha_n, -\sum_{i=1}^{n} \alpha_i)$.*

a) The map φ is a $\mathbb{Z}$-linear isomorphism.

b) Assume that $B = \{v_1, \ldots, v_r\}$ is a $\mathbb{Z}$-basis of $\mathrm{Ker}(\mathcal{A})$. Then the set $\overline{B} = \{\varphi(v_1), \ldots, \varphi(v_r)\}$ is a $\mathbb{Z}$-basis of $\mathrm{Ker}(\overline{\mathcal{A}})$.

Proof. Since $\mathrm{Ker}(\mathcal{A}) = \mathrm{Ker}(-\mathcal{A})$, we may assume that $d > 0$. To prove claim *a)* let $(\alpha_1, \ldots, \alpha_n) \in \mathrm{Ker}(\mathcal{A})$ and let $\alpha_{n+1} = -\sum_{i=1}^{n} \alpha_i$. By definition $s_1\alpha_1 + s_2\alpha_2 + \cdots + s_n\alpha_n = 0$, hence

$$(d-s_1)\alpha_1+(d-s_2)\alpha_2+\cdots+(d-s_n)\alpha_n+d\alpha_{n+1} = d\alpha_1+d\alpha_2+\cdots+d\alpha_n+d\alpha_{n+1} = 0$$

We deduce that $\varphi(\mathrm{Ker}(\mathcal{A})) \subseteq \mathrm{Ker}(\overline{\mathcal{A}})$. It is also clear that φ is an injective homomorphism. On the other way, if $(\alpha_1, \ldots, \alpha_n, \alpha_{n+1}) \in \mathrm{Ker}(\overline{\mathcal{A}})$, then $(\alpha_1, \ldots, \alpha_n) \in \mathrm{Ker}(\mathcal{A})$, and $(d-s_1)\alpha_1+(d-s_2)\alpha_2+\cdots+(d-s_n)\alpha_n+d\alpha_{n+1} = 0$, hence $d\alpha_1 + d\alpha_2 + \cdots + d\alpha_n + d\alpha_{n+1} = 0$, hence $\alpha_{n+1} = -\sum_{i=1}^{n} \alpha_i$.

Claim *b)* is a direct consequence of *a)*.

□

Now we should look for a relationship between $\mathcal{I}(\mathcal{A})$ and $\mathcal{I}(\overline{\mathcal{A}})$. In the following we are going to use some facts from the theory of homogenization of ideals. A full account of that will be presented in [KrRo2]. The notation $\mathrm{Homog}(f, x_{n+1})$, and $\mathrm{Homog}(I, x_{n+1})$ will be used to indicate the homogenization of the polynomial f and the ideal I with respect to x_{n+1}. Given $\mathcal{A}$, we may assume that $d(\mathcal{A}) > 0$, because if this is not the case, we interchange $\mathcal{A}$ with $-\mathcal{A}$. As we have already observed, this operation does not change $\mathrm{Ker}(\mathcal{A})$.

After Proposition 2.4 we may say that if $v \in \mathrm{Ker}(\mathcal{A})$ is a non-zero vector then $\varrho(v) = \mathbf{x}^{v^+} - \mathbf{x}^{v^-}$. Likewise, if $w \in \mathrm{Ker}(\overline{\mathcal{A}})$ is a non-zero vector we denote by $\overline{\varrho}(w)$ the vector $\mathbf{x}^{w^+} - \mathbf{x}^{w^-}$.

Lemma 2.16 *The following diagram*

$$\begin{array}{ccc} \mathrm{Ker}(\mathcal{A}) & \xrightarrow{\varrho} & \mathrm{PBin}(\mathcal{I}(\mathcal{A})) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \mathrm{Homog}} \\ \mathrm{Ker}(\overline{\mathcal{A}}) & \xrightarrow{\overline{\varrho}} & \mathrm{PBin}(\mathcal{I}(\overline{\mathcal{A}})) \end{array}$$

is commutative.

Proof. Let $v \in \mathrm{Ker}(\mathcal{A})$ be a non-zero vector. We need to show that $\overline{\varrho}(\varphi(v)) = \mathrm{Homog}(\varrho(v), x_{n+1})$. Since $\overline{\varrho}(\varphi(v))$ and $\varrho(v)$ are pure binomials, which differ only for the presence of x_{n+1} in $\overline{\varrho}(\varphi(v))$, it suffices to show that the sum of the components of $\varphi(v)$ is 0, which is clearly true by the definition of φ.

□

Lemma 2.17 *Let $f, f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ and $I = (f_1, \ldots, f_r)$. The following equalities of ideals in $K[x_1, \ldots, x_n, x_{n+1}]$ hold true*

a) $\mathrm{Homog}(I, x_{n+1}) = (\mathrm{Homog}(f_1, x_{n+1}), \ldots, \mathrm{Homog}(f_r, x_{n+1})) : x_{n+1}^{\infty}$.

b) $\mathrm{Homog}(I, x_{n+1}) : f^{\infty} = \mathrm{Homog}(I : f^{\infty}, x_{n+1})$.

Proof. See [KrRo2].

□

Theorem 2.18 *With the notation introduced above, consider the two ideals $\mathcal{I}(\mathcal{A}) \subset K[x_1, \ldots, x_n]$, $\mathcal{I}(\overline{\mathcal{A}}) \subset K[x_1, \ldots, x_n, x_{n+1}]$.*

a) The ideal $\mathcal{I}(\overline{\mathcal{A}})$ is homogeneous with respect to the standard grading, i.e. the grading given by $(1, 1, \ldots, 1)$.

b) The ideal $\mathcal{I}(\overline{\mathcal{A}})$ is the homogenization of $\mathcal{I}(\mathcal{A})$ with respect to x_{n+1}.

Proof. By Proposition 2.4 the ideal $\mathcal{I}(\overline{\mathcal{A}})$ is generated by the pure binomials associated to $\mathrm{Ker}(\overline{\mathcal{A}})$, and they are homogeneous by Lemma 2.16. This proves *a)*. To prove *b)* we let $B = \{v_1, \ldots, v_r\}$ be a $\mathbb{Z}$-basis of $\mathrm{Ker}(\mathcal{A})$. Lemma 2.15 implies that $\varphi(B) = \{\varphi(v_1), \ldots, \varphi(v_r)\}$ is a $\mathbb{Z}$-basis of $\mathrm{Ker}(\overline{\mathcal{A}})$. Theorem 2.10 implies that $\mathcal{I}(\overline{\mathcal{A}}) = I(\varphi(B)) : (\pi \cdot x_{n+1})^{\infty}$. It is a standard fact and easy

to check that the latter is equal to $(I(\varphi(B)) : x_{n+1}^{\infty}) : \pi^{\infty}$, which is equal to $\mathrm{Homog}(I(B), x_{n+1}) : \pi^{\infty}$ by Lemma 2.17.a. Now we use Lemma 2.17.b to see that $\mathrm{Homog}(I(B), x_{n+1}) : \pi^{\infty} = \mathrm{Homog}(I(B) : \pi^{\infty}, x_{n+1})$, and we use Theorem 2.10 again to conclude the proof.

□

Remark 2.19 The above theorem can be used to improve computations in the following way. If we have to compute $\mathcal{I}(\mathcal{A})$, we compute a basis B of $\mathrm{Ker}(\mathcal{A})$, hence a basis $\varphi(B)$ of $\mathrm{Ker}(\overline{\mathcal{A}})$. Then we compute a system of generators G of the saturation of $I(\varphi(B))$ with respect to $x_1 x_2 \cdots x_n x_{n+1}$, taking advantage of the fact that $I(\varphi(B))$ is homogeneous. Finally, we compute a system of generators of $\mathcal{I}(\mathcal{A})$ by simply dehomogenizing G.

3 Toric Ideals and Diophantine Linear Systems

In this section we see how toric ideals are related to the solutions of Diophantine linear systems, even in the case where they are not homogeneous with respect to a positive grading.

3.1 Solving Systems with Elimination Orderings

Let $\mathcal{A} = (a_{ij}) \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ be a matrix with m rows, n columns, and integer entries. Furthermore, let $(b_1, \ldots, b_m) \in \mathbb{Z}^m$ be a vector and let $z_1, \ldots, z_n$ be indeterminates. We want to find the non-negative integer solutions $(\alpha_1, \ldots, \alpha_n)$ of the system $\mathcal{S}$:

$$\begin{cases} a_{11}z_1 + a_{12}z_2 + \cdots + a_{1n}z_n &= b_1 \\ a_{21}z_1 + a_{22}z_2 + \cdots + a_{2n}z_n &= b_2 \\ \vdots & \vdots \quad \vdots \\ a_{m1}z_1 + a_{m2}z_2 + \cdots + a_{mn}z_n &= b_m \end{cases}$$

The next proposition tells us that all the power products associated to solutions have the same degree.

Proposition 3.1 *Let $\mathcal{S}$ be a Diophantine system as above, let K be any field and let P be graded with a grading associated to $\mathcal{A}$, in particular let $\lambda_i \in \mathbb{Q}$*

for $i = 1, \ldots, m$ *be such that* $(\deg(x_1), \ldots, \deg(x_n)) = \sum_{i=1}^{m} \lambda_i (a_{i1}, \ldots, a_{in})$. *If* $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ *is a solution of* $\mathcal{S}$, *then* $\deg(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = \sum_{i=1}^{m} \lambda_i b_i$.

Proof. We check that $\deg(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = \sum_{j=1}^{n} \alpha_j \deg(x_j)$ which is equal to $\sum_{j=1}^{n} \alpha_j (\sum_{i=1}^{m} \lambda_i a_{ij}) = \sum_{i=1}^{m} \lambda_i (\sum_{j=1}^{n} a_{ij} \alpha_j) = \sum_{i=1}^{m} \lambda_i b_i$.

□

And now let us look for solutions using algebraic methods.

Proposition 3.2 *Let* $\mathcal{S}$ *be as above, and assume that the elements* b_i *as well as the entries of* $\mathcal{A}$ *are non-negative integers. Let* K *be any field, let* $y_1, \ldots, y_m$ *be indeterminates, let* $\tau_i = y_1^{a_{1i}} y_2^{a_{2i}} \cdots y_m^{a_{mi}}$ *for* $i = 1, \ldots, n$, $\tau = y_1^{b_1} \cdots y_m^{b_m}$, *and let* $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. *Let* $f = \prod_{i=1}^{m} y_i$ *and let* J *in* $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ *be the ideal generated by the set* $\{x_1 - \tau_1,\ x_2 - \tau_2, \ldots, x_n - \tau_n\}$. *The following conditions are equivalent.*

a) The tuple $(\alpha_1, \ldots, \alpha_n)$ *is a solution of* $\mathcal{S}$.

b) There is an equality of power products $\tau_1^{\alpha_1} \cdots \tau_n^{\alpha_n} = y_1^{b_1} \cdots y_m^{b_m}$.

c) The binomial $y_1^{b_1} \cdots y_m^{b_m} - x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ *is in* J.

Proof. A tuple $(\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ is a solution of $\mathcal{S}$ if and only if

$$\begin{cases} y_1^{a_{11}\alpha_1 + a_{12}\alpha_2 + \cdots + a_{1n}\alpha_n} &= y_1^{b_1} \\ y_2^{a_{21}\alpha_1 + a_{22}\alpha_2 + \cdots + a_{2n}\alpha_n} &= y_2^{b_2} \\ \qquad\qquad \vdots & \vdots \quad \vdots \\ y_m^{a_{m1}\alpha_1 + a_{m2}\alpha_2 + \cdots + a_{mn}\alpha_n} &= y_m^{b_m} \end{cases}$$

hence if and only if $y_1^{a_{11}\alpha_1 + a_{12}\alpha_2 + \cdots + a_{1n}\alpha_n} \cdots y_m^{a_{m1}\alpha_1 + a_{m2}\alpha_2 + \cdots + a_{mn}\alpha_n} = y_1^{b_1} \cdots y_m^{b_m}$. By reordering the exponents we get the desired equivalence between *a)* and *b)*.

We use Proposition 1.3.b to show that $y_1^{b_1} \cdots y_m^{b_m} - x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in J$ if and only if $y_1^{b_1} \cdots y_m^{b_m} - x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ vanishes under the following substitution $\varphi(x_1) = \tau_1$, $\varphi(x_2) = \tau_2, \ldots, \varphi(x_n) = \tau_n$, hence if and only if $y_1^{b_1} \cdots y_m^{b_m} - \tau_1^{\alpha_1} \cdots \tau_n^{\alpha_n} = 0$. This is exactly condition c), and the proof is now complete.

□

We are ready to explain a criterion to check whether $\mathcal{S}$ has solutions in $\mathbb{N}^n$.

Corollary 3.3 *With the same assumptions as in the proposition, let σ be an elimination ordering for $\{y_1, \ldots, y_m\}$.*

a) $\mathcal{S}$ has non-negative solutions if and only if $\mathrm{NF}_{\sigma,J}(y_1^{b_1} \cdots y_m^{b_m}) \in P$.

b) If $\mathrm{NF}_{\sigma,J}(y_1^{b_1} \cdots y_m^{b_m}) = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, then $(\alpha_1, \ldots, \alpha_n)$ is a solution of $\mathcal{S}$.

Proof. First, we prove *a*). Suppose that $(\alpha_1, \ldots, \alpha_n)$ is a non-negative solution of $\mathcal{S}$. From Proposition 3.2.c we obtain $y_1^{b_1} \cdots y_m^{b_m} - x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in J$. This implies (see Proposition 2.4.10.a in [KrRo]) that $\mathrm{NF}_{\sigma,J}(y_1^{b_1} \cdots y_m^{b_m}) = \mathrm{NF}_{\sigma,J}(x_1^{\alpha_1} \cdots x_n^{\alpha_n})$. But σ is an elimination ordering for $\{y_1, \ldots, y_m\}$, from which it follows that $\mathrm{NF}_{\sigma,J}(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) \in P$.

Conversely suppose that $\mathrm{NF}_{\sigma,J}(y_1^{b_1} \cdots y_m^{b_m}) \in P$. We have already recalled that a reduced Gröbner basis of J is a set of binomials. This fact implies that the normal form of a power product is a power product. So there exists a tuple of non-negative integers $(\alpha_1, \ldots, \alpha_n)$ such that $\mathrm{NF}_{\sigma,J}(y_1^{b_1} \cdots y_m^{b_m}) = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. This implies that $y_1^{b_1} \cdots y_m^{b_m} - x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in J$, and $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ is a solution of $\mathcal{S}$ by Proposition 3.2. This argument proves *b*) as well.

□

Remark 3.4 Of course it is possible to deduce an algorithm from the above corollary, but such an algorithm turns out to be rather inefficient. On the other hand, in many cases it is more important to *navigate* inside the set of solutions, and this is possible with the aid of toric ideals, once a solution is known.

The next subsection describes an important case of that kind of navigation.

3.2 Integer Programming

In some cases finding some solution of a Diophantine system is easy, but interest really lies in finding a "special" solution. In this section we see how the theory of Gröbner bases and toric ideals provides a method to deal with Integer Programming, that is, given any "cost vector" $c \in \mathbb{Q}^n$, find a solution α for $\mathcal{S}$ which minimizes the value of the linear functional $u \mapsto c \cdot u$.

Definition 3.5 Let $\mathcal{A}$ be a matrix with non-negative entries. Let K be any field and let $P = K[x_1, \ldots, x_n]$ be graded with a positive grading associated to $\mathcal{A}$. Given a cost vector $c \in \mathbb{Q}^n$, a **cost compatible ordering** σ_c is a term ordering with the property that $t_1 \geq_{\sigma_c} t_2$ implies $c \cdot \log(t_1) \geq c \cdot \log(t_2)$.

Remark 3.6 If there is a positive grading associated to $\mathcal{A}$, then a cost compatible term ordering is obtained by a non-singular matrix whose first row is a positive linear combination of the rows of $\mathcal{A}$ and second row equal to c. This follows from the fact that, by Proposition 3.1, two power product associated to solutions of $\mathcal{S}$ have the same degree. If there is no positive grading associated to $\mathcal{A}$, but each component of the cost vector is positive, then a cost compatible term ordering is obtained by a matrix whose first row is c (see [KrRo] 1.4 for orderings represented by matrices).

Lemma 3.7 *Let $\alpha \in \mathbb{N}^n$ be a solution of the system $\mathcal{S}$ and let t be a power product in P. Then for any cost compatible ordering σ_c, the normal form $\mathrm{NF}_{\sigma_c}(t, \mathcal{I}(\mathcal{A}))$ is associated to a solution of minimum cost.*

Proof. Let $t = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $t' = \mathrm{NF}_{\sigma_c}(t, \mathcal{I}(\mathcal{A}))$ with $t' = x_1^{\alpha'_1} \cdots x_n^{\alpha'_n}$. The binomial $t - t'$ is in the toric ideal $\mathcal{I}(\mathcal{A})$ so, by Proposition 2.4, the vector $(\alpha_1 - \alpha'_1, \ldots, \alpha_n - \alpha'_n)$ is in $\mathrm{Ker}(\mathcal{A})$. Therefore $\alpha' = \alpha - (\alpha - \alpha')$ is a solution of $\mathcal{S}$. If α'' is another solution and t'' is the associated power product, we have that $t - t'' \in \mathcal{I}(\mathcal{A})$ and therefore, by a property of the normal forms, $\mathrm{NF}_{\sigma_c}(t'', \mathcal{I}(\mathcal{A})) = \mathrm{NF}_{\sigma_c}(t, \mathcal{I}(\mathcal{A})) = t'$ from which $t'' >_{\sigma_c} t'$. By definition of cost compatibility, this implies that $c \cdot \log(t'') \geq c \cdot \log(t')$, and the proof is complete. □

Theorem 3.8 *Let $\mathcal{A}$ be an $m \times n$-matrix, let $b \in \mathbb{N}^m$ be a right hand side vector, let $c \in \mathbb{Q}^n$ be a cost vector, and let σ_c be a cost compatible term ordering. Consider the following set of instructions.*

TS1 *Compute the toric ideal $\mathcal{I}$ associated to $\mathcal{A}$.*

TS2 *Compute the Gröbner basis $\mathcal{G}_{\sigma_c}$ for $\mathcal{I}$ with respect to σ_c (sometimes $\mathcal{G}_{\sigma_c}$ is called* **Test Set***).*

TS3 *Find a solution* α' *of the system* $\mathcal{A}z = b$.

TS4 *Compute the normal form* $\mathbf{x}^{\alpha}$ *of* $\mathbf{x}^{\alpha'}$ *with respect to* $\mathcal{G}_{\sigma_c}$. *Return* α.

This is an algorithm which returns a solution of the system $\mathcal{A}z = b$ *which minimizes the cost.*

Proof. It follows from Lemma 3.7.

□

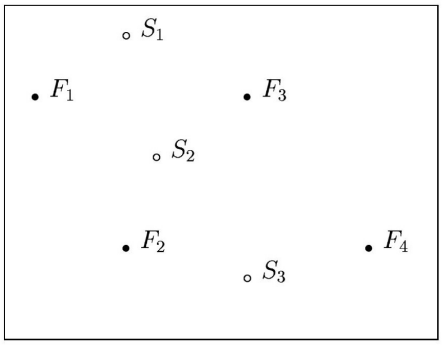
Remark 3.9 Step **TS2** can be very fast, since it takes advantage of all the properties of toric ideals that we have shown. So this method is computationally much more efficient than what we described in Section 3.1. Notice that it requires to find a solution (see Step **TS3**). In most cases this can be done efficiently too.

Now we see an example which illustrates how to compute a solution which has minimum cost.

Example 3.10 Consider $f = 4$ factories F_1, F_2, F_3, F_4 which produce a respective supply of $120, 204, 92, 55$ units of an indivisible good. Consider also $s = 3$ shops S_1, S_2, S_3 which have respective demands of $183, 190, 98$ units. There is a cost c_{ij} associated with transporting one unit from factory F_i to shop S_j. The possible transportation plans for shipping all 471 units from the factories to the shops are the elements α such that $\mathcal{A} \cdot \alpha = b$, where $b = (120, 204, 92, 55; 183, 190, 98)$ and $\mathcal{A} \in \mathrm{Mat}_{f+s,f\cdot s}(\mathbb{N})$. Here we see the associated system, where z_{ij} represents the units of goods to be shipped from factory F_i to shop S_j.

$$\begin{cases} z_{11} + z_{12} + z_{13} &= 120 \\ z_{21} + z_{22} + z_{23} &= 204 \\ z_{31} + z_{32} + z_{33} &= 92 \\ z_{41} + z_{42} + z_{43} &= 55 \\ z_{11} + z_{21} + z_{31} + z_{41} &= 183 \\ z_{12} + z_{22} + z_{32} + z_{42} &= 190 \\ z_{13} + z_{23} + z_{33} + z_{43} &= 98 \end{cases}$$

Here is an example of a cost function depending on the distance between factories and shops.



$$\begin{array}{c} \\ F_1 \\ F_2 \\ F_3 \\ F_4 \end{array} \begin{array}{c} \begin{array}{ccc} S_1 & S_2 & S_3 \end{array} \\ \begin{pmatrix} 1 & 1 & 3 \\ 2 & 1 & 1 \\ 1 & 1 & 2 \\ 3 & 2 & 1 \end{pmatrix} \end{array}$$

In this case it is particularly easy to find a solution of the above system. For example, if $(z_{11}, z_{12}, z_{13}, z_{21}, z_{22}, z_{23}, z_{31}, z_{32}, z_{33}, z_{41}, z_{42}, z_{43})$ is the vector of all the indeterminates, $\alpha' = (120, 0, 0,\ 14, 190, 0,\ 0, 0, 92,\ 49, 0, 6)$ is a solution, and the cost of α' is

$$c{\cdot}\alpha' = (1, 1, 3,\ 2, 1, 1,\ 1, 1, 2,\ 3, 2, 1){\cdot}(120, 0, 0,\ 14, 190, 0,\ 0, 0, 92,\ 49, 0, 6) = 675$$

But of course here we want a solution which minimizes the total cost. So we compute a Gröbner basis with respect to a cost compatible ordering σ_c. The vector $(1, 1, \ldots, 1) = \sum_{i=1}^{7} \frac{1}{2}(a_{i1}, \ldots, a_{in})$ describes a positive grading associated to $\mathcal{A}$ and $(1, 1, 3,\ 2, 1, 1,\ 1, 1, 2,\ 3, 2, 1)$ is the cost vector, so we may use any term ordering represented by a non-singular matrix like

$$\begin{pmatrix} 1\,1\,1 & 1\,1\,1 & 1\,1\,1 & 1\,1\,1 \\ 1\,1\,3 & 2\,1\,1 & 1\,1\,2 & 3\,2\,1 \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix}$$

We compute $\mathrm{NF}_{\sigma_c}(\mathbf{x}^{(120,0,0,\ 14,190,0,\ 0,0,92,\ 49,0,6)}, \mathcal{I}(\mathcal{A}))$ and get

$$\alpha = (120, 0, 0,\ 0, 161, 43,\ 63, 29, 0,\ 0, 0, 55)$$

which is a minimal solution and therefore the minimum cost is 471.

References

[Bu] Buchberger, B., *On finding a Vector Space Basis of the Residue Class Ring modulo a zero dimensional Polynomial Ideal (in German)*, PhD Thesis, Universität Innsbruck, Innsbruck (1965)

[BLR] Bigatti, A., La Scala, R., Robbiano, L., *Computing Toric Ideals,* J. Symb. Comput., 27 (1999), 351–365.

[CNR] Capani, A., Niesi, G., Robbiano, L., CoCoA*, a system for doing Computations in Commutative Algebra*, Version 4.0 is available via anonymous ftp from `cocoa.dima.unige.it`, (1999).

[CoTr] Conti, P., Traverso, C., *Buchberger algorithm and integer programming*, In Springer, editor, Proceedings AAECC-9 , volume 539 of *Lecture Notes in Comp.Sci.*, (1991), 130–139. Springer.

[Din] Dinwoodie, I.H., *The Diaconis-Sturmfels algorithm and rules of succession*, Bernoulli, 4, (1998), 401–410.

[DiBU] Di Biase, F., Urbanke, R., *An algorithm to calculate the kernel of certain polynomial ring homomorphisms*, Experimental Mathematics, 4, (1995).

[DiSt] Diaconis, P., Sturmfels, B., *Algebraic algorithms for sampling from conditional distributions*, Annals of Statistics, 26, (1998), 363–397.

[HoSt] Hosten, S., Sturmfels, B., *GRIN: An implementation of Gröbner bases for integer programming*, In E. Balas, J. C., editor, Integer Programming and Combinatorial Optimization, volume 920 of Lecture Notes in Comp.Sci., Springer Verlag, (1995), 267–276.

[HoTh] Hosten, S., Thomas, R., *Gröbner bases and Applications*, volume 251 of London Mathematical Society Lecture Notes Series, chapter Gröbner bases and integer programming. Cambridge University Press, (1998).

[KrRo] Kreuzer, M., Robbiano, L., *Computational Commutative Algebra 1*, Springer - Verlag, (2000).

[KrRo2] Kreuzer, M., Robbiano, L., *Computational Commutative Algebra 2*, In preparation.

[LGID] Li, Q., Guo, Y., Ida, T., Darligton, J., *The minimised geometric Buchberger Algorithm: An optimal algebraic algorithm for integer programming*, In Proceedings of ISSAC-97, ACM, (1997), 331–338.

[PRW] Pistone, G., Riccomagno, E., Wynn, H.P., *Computational Commutative Algebra In Discrete Statistics*, Preprint.

[Po] Pottier, L., *Gröbner bases of toric ideals*, Research report 2224, INRIA, Sophia Antipolis.

[Ro] Robbiano, L., *Gröbner Bases and Statistic*, In B. Buchberger, F. Winkler, editors, Gröbner Bases and Applications (Proc. of the Conf. 33 years of Gröbner Bases), volume 251 of London Mathematical Society Lecture Notes Series, Cambridge University Press, (1998), 179–204.

[St] Sturmfels, B., *Gröbner bases and convex polytopes*, volume 8 of University lecture series (Providence, R.I.). American Mathematical Society, (1996).

[Th] Thomas, R., *A geometric Buchberger algorithm for integer programming*, Mathematics of Operations Research, 77(1997), 357–387.

Anna Bigatti Lorenzo Robbiano
Dipartimento di Matematica
Università di Genova
Via Dodecaneso 35, 16146 Genova, Italy
e-mail: `bigatti,robbiano@dima.unige.it`
URL: `http://cocoa.dima.unige.it`