SAGBI AND SAGBI-GRÖBNER BASES OVER PRINCIPAL IDEAL DOMAINS

WILLIAM W. ADAMS, SERKAN HOŞTEN, PHILIPPE LOUSTAUNAU, J. LYN MILLER

1. Introduction

In this paper we will discuss computational and structural properties of subalgebras of polynomial rings when the base ring is a principal ideal domain (PID). The objects we study are the so-called SAGBI (subalgebra analogues of Gröbner bases for ideals) bases for the subalgebras themselves and SAGBI-Gröbner bases for the ideals in the subalgebras (SG bases). We will discuss how to compute these objects, and our goal is to avoid computations over the PID as much as possible. Further we will show the existence of strong SAGBI bases for these subalgebras and give an algorithm to compute them. For the general theory of SAGBI and SAGBI-Gröbner bases over any commutative Noetherian ring we refer the reader to Miller [6].

In [6] algorithms are given for the computation of SAGBI and SG bases over an arbitrary Noetherian commutative ring R. In addition to the usual Buchberger-style algorithms the algorithms presented there relied on elimination order computations of Gröbner bases over R. When R is a field, these extra Gröbner basis computations were replaced by computing the minimal Hilbert basis for the set of solutions of certain linear diophantine equations. These in turn can be constructed by Gröbner basis techniques, but over a field. In this paper first we show that in the construction of SAGBI bases over R, a PID, we can avoid these extra Gröbner basis computations over R. Next we go on to consider the same question for SG bases. Here we show that the elimination order computations over R can be replaced by a degree reverse lexicographic (degrevlex) computation over the same ring R. In the last section we will show that strong SAGBI bases, the analogue of strong Gröbner bases for ideals in polynomial rings, always exist, and we will give an algorithm for their construction. This last problem leads to some interesting results in integer programming and its connection to Gröbner bases. Again, given a finite SAGBI basis, all the relevant computations are carried out over a field.

We consider the polynomial ring $R[x_1, \ldots, x_n]$ where R is a PID. For a fixed term order on $R[x_1, \ldots, x_n]$ and for $f \in R[x_1, \ldots, x_n]$ we denote as usual $\mathrm{lp}(f)$ = the leading power product of f, $\mathrm{lc}(f)$ = the leading coefficient of f, and $\mathrm{lt}(f) = \mathrm{lc}(f)\mathrm{lp}(f)$ = the leading term of f. Moreover for a subset F of $R[x_1, \ldots, x_n]$ we denote $\mathrm{Lt}F = \{\mathrm{lt}(f) : f \in F\}$.

We will now recall the definitions of the basic notions. Let F be a subset of $R[x_1, \ldots, x_n]$ and consider the R-subalgebra of $R[x_1, \ldots, x_n]$ generated by F which we denote by $A = R[F]$. By a *SAGBI basis* for A with respect to a given term order we mean a subset S of A such that $R[\mathrm{Lt}S] = R[\mathrm{Lt}A]$. Also if $I \subseteq A$ is an ideal of the algebra A we call a subset G of I a *SAGBI-Gröbner basis (SG-basis)* of I provided that $\mathrm{Lt}G$ generates the ideal $\langle \mathrm{Lt}I \rangle$ in the algebra $R[\mathrm{Lt}A]$. For a finite subset $G = \{g_1, \ldots, g_t\} \subseteq A$ and a vector $\boldsymbol{\psi} = (\psi_1, \ldots, \psi_t)$ in $\mathbb{N}^t$ (where $\mathbb{N}$ denotes the natural numbers) set $G^{\boldsymbol{\psi}} = g_1^{\psi_1} \cdots g_t^{\psi_t}$. We say that G is a *strong SAGBI basis* provided that each $f \in A$, there is an $r \in R$ and a $\boldsymbol{\psi} \in \mathbb{N}^t$ such that $\mathrm{lt}(f) = r\mathrm{lt}(G^{\boldsymbol{\psi}})$. It is not clear whether such an object should exist, but we prove in the last section that they always do exist, and we give

Date: March 19, 1998.

an algorithm for computing them from a SAGBI basis. The necessary tools for the algorithm are prime factorization in R and Gröbner bases computations over a field.

2. Construction of a Toric Ideal over a PID

Let R be a PID and consider the polynomial ring $R[x_1, \dots, x_n]$. Let $c_1 x^{\boldsymbol{a}_1}, c_2 x^{\boldsymbol{a}_2}, \dots, c_t x^{\boldsymbol{a}_t}$ be terms with $c_i \in R$ and $\boldsymbol{a}_i \in \mathbb{N}^n$, where here we adopt the notation that for a vector $\boldsymbol{a} = (a_1, \dots, a_n) \in \mathbb{N}^n$, $x^{\boldsymbol{a}} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$. We introduce t new variables $y_1, \dots, y_t$, and we wish to compute a generating set for the kernel of the map

$$\begin{array}{rrcl} \varphi: & R[y_1, \dots, y_t] & \longrightarrow & R[x_1, \dots, x_n] \\ & y_i & \longmapsto & c_i x^{\boldsymbol{a}_i}. \end{array} \tag{1}$$

It is well-known (see, for example, [1], Theorem 4.3.13) that this kernel is equal to the ideal $I \cap R[y_1, \dots, y_t]$, where I is the ideal $\langle y_i - c_i x^{\boldsymbol{a}_i} : i = 1, \dots, t\rangle$ in $R[x_1, \dots, x_n, y_1, \dots, y_t]$. To compute this intersection, one computes a Gröbner basis G for I with respect to an elimination order with the x-variables larger than the y-variables and one uses the fact that $I \cap R[y_1, \dots, y_t] = \langle G \cap R[y_1, \dots, y_t]\rangle$. Here we give explicit formulas for generators of $\ker(\varphi)$ without having to compute a Gröbner basis over the ring R. We note however that one way to compute these generators is to compute a Gröbner basis, but over a field (see Algorithm 7.2 in [8]).

For $\boldsymbol{\psi} = (\psi_1, \dots, \psi_t) \in \mathbb{N}^t$, we define similar to the above $y^{\boldsymbol{\psi}} = y_1^{\psi_1} \dots y_t^{\psi_t}$ and $c^{\boldsymbol{\psi}} = c_1^{\psi_1} \dots c_t^{\psi_t}$. Define

$$\pi : \mathbb{N}^t \longrightarrow \mathbb{N}^n \text{ by } \pi((u_1, \dots, u_t)) = u_1 \boldsymbol{a}_1 + \cdots + u_t \boldsymbol{a}_t,$$

and let $\mathfrak{L}$ be the submonoid of $\mathbb{N}^{2t}$ defined by

$$\mathfrak{L} = \left\{ (\boldsymbol{\psi}, \boldsymbol{\eta}) | \boldsymbol{\psi}, \boldsymbol{\eta} \in \mathbb{N}^t \text{ and } \pi(\boldsymbol{\psi}) = \pi(\boldsymbol{\eta}) \right\}. \tag{2}$$

It is well known that this monoid is finitely generated and has a unique minimal generating set called its Hilbert basis (see Section 16.4 in [7]). Let $\left\{ (\boldsymbol{\psi}^{(1)}, \boldsymbol{\eta}^{(1)}), \dots, (\boldsymbol{\psi}^{(s)}, \boldsymbol{\eta}^{(s)}) \right\}$ be any generating set for $\mathfrak{L}$. For $i = 1, \dots, s$, we define $c^{(i)} \in R$ to be a gcd of $c^{\boldsymbol{\psi}^{(i)}}$ and $c^{\boldsymbol{\eta}^{(i)}}$. Then it is easy to see that, for each $i = 1, \dots, s$,

$$g_i = \frac{c^{\boldsymbol{\eta}^{(i)}}}{c^{(i)}} y^{\boldsymbol{\psi}^{(i)}} - \frac{c^{\boldsymbol{\psi}^{(i)}}}{c^{(i)}} y^{\boldsymbol{\eta}^{(i)}} \in \ker(\varphi). \tag{3}$$

Theorem 2.1. *The polynomials $g_1, \dots, g_s$ in equation (3) generate $\ker(\varphi)$ for the φ given in equation (1).*

Proof. We first note that $\ker(\varphi)$ is generated by binomials. This is well known in the field case and we can prove it over a PID as follows. Let $f \in \ker(\varphi)$, say $f = \sum_{\nu=1}^{m} r_\nu y^{\boldsymbol{\psi}_\nu}$, with $r_\nu \in R$ and $\boldsymbol{\psi}_\nu \in \mathbb{N}^t$. Then $0 = f(c_1 x^{\boldsymbol{a}_1}, c_2 x^{\boldsymbol{a}_2}, \dots, c_t x^{\boldsymbol{a}_t}) = \sum_{\nu=1}^{m} r_\nu c^{\boldsymbol{\psi}_\nu} x^{\pi(\boldsymbol{\psi}_\nu)}$, so we may assume that all the terms in f have corresponding x power products equal, say $x^{\boldsymbol{a}}$. Hence we have that

$$0 = \sum_{\nu=1}^{m} r_\nu c^{\boldsymbol{\psi}_\nu} x^{\pi(\boldsymbol{\psi}_\nu)} = \left(\sum_{\nu=1}^{m} r_\nu c^{\boldsymbol{\psi}_\nu} \right) x^{\boldsymbol{a}},$$

and so

$$\sum_{\nu=1}^{m} r_\nu c^{\boldsymbol{\psi}_\nu} = 0$$

and we have that the r_ν's are syzygies of the $c^{\boldsymbol{\psi}_\nu}$'s. Since R is a PID, the syzygy module of $(c^{\boldsymbol{\psi}_1}, \dots, c^{\boldsymbol{\psi}_m})$ is generated by vectors with only two non-zero coordinates (see, for example, [1, Proposition 4.5.3]). Therefore f can be written as the sum of polynomials in $\ker(\varphi)$ of the form $ay^{\boldsymbol{\psi}} - by^{\boldsymbol{\eta}}$, where $a, b \in R$, $ac^{\boldsymbol{\psi}} - bc^{\boldsymbol{\eta}} = 0$, and $\pi(\boldsymbol{\psi}) = \pi(\boldsymbol{\eta})$. That is, $\ker(\varphi)$ is generated by binomials. In order to complete the proof, we need the following identity.

Lemma 2.2. *Let $f_1 = a_1 y^{\boldsymbol{\psi}_1} - b_1 y^{\boldsymbol{\eta}_1}$ and $f_2 = a_2 y^{\boldsymbol{\psi}_2} - b_2 y^{\boldsymbol{\eta}_2}$ be non-zero polynomials in ker(φ), with $\gcd(a_1, b_1) = \gcd(a_2, b_2) = 1$. Also, let $f_3 = a_3 y^{\boldsymbol{\psi}_1 + \boldsymbol{\psi}_2} - b_3 y^{\boldsymbol{\eta}_1 + \boldsymbol{\eta}_2}$ be a non-zero polynomial in ker(φ), with $\gcd(a_3, b_3) = 1$. Then there exist $\alpha_1, \alpha_2, \beta_1, \beta_2 \in R$ such that*

$$f_3 = \left(\alpha_2 y^{\boldsymbol{\psi}_2} - \beta_2 y^{\boldsymbol{\eta}_2}\right) f_1 - \left(\alpha_1 y^{\boldsymbol{\psi}_1} - \beta_1 y^{\boldsymbol{\eta}_1}\right) f_2.$$

Proof. First note that $a_1 c^{\boldsymbol{\psi}_1} = b_1 c^{\boldsymbol{\eta}_1}$, $a_2 c^{\boldsymbol{\psi}_2} = b_2 c^{\boldsymbol{\eta}_2}$, and $a_3 c^{\boldsymbol{\psi}_1 + \boldsymbol{\psi}_2} = b_3 c^{\boldsymbol{\eta}_1 + \boldsymbol{\eta}_2}$. Then, since $\gcd(a_i, b_i) = 1$, we have that a_i divides $c^{\boldsymbol{\eta}_i}$, for $i = 1, 2$. Write $c^{\boldsymbol{\eta}_1} = a_1 v$ and $c^{\boldsymbol{\eta}_2} = a_2 w$, for some $v, w \in R$, and so we also have $c^{\boldsymbol{\psi}_1} = b_1 v$ and $c^{\boldsymbol{\psi}_2} = b_2 w$. Therefore $a_3 b_1 b_2 = b_3 a_1 a_2$.

The equation

$$f_3 = \left(\alpha_2 y^{\boldsymbol{\psi}_2} - \beta_2 y^{\boldsymbol{\eta}_2}\right) f_1 - \left(\alpha_1 y^{\boldsymbol{\psi}_1} - \beta_1 y^{\boldsymbol{\eta}_1}\right) f_2$$

is equivalent to

$$\alpha_2 a_1 - \alpha_1 a_2 = a_3, \quad \beta_1 b_2 - \beta_2 b_1 = b_3, \quad \beta_1 a_2 - \alpha_2 b_1 = 0, \quad \alpha_1 b_2 - \beta_2 a_1 = 0. \tag{4}$$

Let $h = \gcd(a_2, b_1)$, and $k = \gcd(b_2, a_1)$. Note that $\gcd(h, k) = 1$, since $\gcd(a_1, b_1) = \gcd(a_2, b_2) = 1$. The last two equations in (4) are valid for $\alpha_2 = \frac{a_2}{h} t, \beta_1 = \frac{b_1}{h} t$, and $\beta_2 = \frac{b_2}{k} u, \alpha_1 = \frac{a_1}{k} u$, for any $t, u \in R$. Using these formulas in the first two equations in (4), we obtain

$$(a_1 a_2 k)t - (a_1 a_2 h)u = hka_3, \quad (b_1 b_2 k)t - (b_1 b_2 h)u = hkb_3. \tag{5}$$

We note that these two equations have the same solutions. Indeed, if we multiply the first equation by b_3 we obtain $(b_3 a_1 a_2 k)t - (b_3 a_1 a_2 h)u = hka_3 b_3$, and, using the fact that $b_3 a_1 a_2 = a_3 b_1 b_2$, we obtain $(a_3 b_1 b_2 k)t - (a_3 b_1 b_2 h)u = hka_3 b_3$; after cancelling a_3 we obtain the second equation in (5). Now the first equation in (5) has a solution t, u if and only if $\gcd(a_1 a_2 k, a_1 a_2 h) = a_1 a_2$ divides hka_3. From the equation $a_3 b_1 b_2 = b_3 a_1 a_2$, we obtain $a_3 \frac{b_1}{h} \frac{b_2}{k} = b_3 \frac{a_1}{k} \frac{a_2}{h}$, and hence $\frac{a_1}{k} \frac{a_2}{h}$ divides a_3, so that $a_1 a_2$ divides hka_3 and the lemma is proved. □

We now continue the proof of the theorem. We need to show that any $f = ay^{\boldsymbol{\psi}} - by^{\boldsymbol{\eta}} \in \ker(\varphi)$ lies in $\langle g_1, \ldots, g_s \rangle$. We may assume that $\gcd(a, b) = 1$. Note that

$$a \frac{c^{\boldsymbol{\psi}}}{d} = b \frac{c^{\boldsymbol{\eta}}}{d},$$

where $d = \gcd(c^{\boldsymbol{\eta}}, c^{\boldsymbol{\psi}})$. Thus

$$a = \frac{c^{\boldsymbol{\eta}}}{d} v \text{ and } b = \frac{c^{\boldsymbol{\psi}}}{d} v,$$

where v is in R.

Since $f \in \ker(\varphi)$, we have $(\boldsymbol{\psi}, \boldsymbol{\eta}) \in \mathfrak{L}$ and so $(\boldsymbol{\psi}, \boldsymbol{\eta}) = \sum_{i=1}^{s} u_i (\boldsymbol{\psi}^{(i)}, \boldsymbol{\eta}^{(i)})$, for some $u_i \in \mathbb{N}$. We first see that

$$\frac{c^{u_i \boldsymbol{\eta}^{(i)}}}{d_i} y^{u_i \boldsymbol{\psi}^{(i)}} - \frac{c^{u_i \boldsymbol{\psi}^{(i)}}}{d_i} y^{u_i \boldsymbol{\eta}^{(i)}} \in \langle g_1, \ldots, g_s \rangle,$$

where d_i is the gcd of $c^{u_i \boldsymbol{\eta}^{(i)}}$ and $c^{u_i \boldsymbol{\psi}^{(i)}}$, since $d_i = c^{(i) u_i}$ and so this binomial is divisible by g_i. Then, we see that

$$f \in \langle \frac{c^{u_i \boldsymbol{\eta}^{(i)}}}{d_i} y^{u_i \boldsymbol{\psi}^{(i)}} - \frac{c^{u_i \boldsymbol{\psi}^{(i)}}}{d_i} y^{u_i \boldsymbol{\eta}^{(i)}}, i = 1, \ldots, s \rangle,$$

using induction on s and Lemma 2.2. Therefore $f \in \langle g_1, \ldots, g_s \rangle$ and the theorem is proved. □

We will now relate what we have done to the case where $R = k$ is a field. In this case $\ker(\varphi)$ is a *toric ideal*; see [8]. As noted above, it is easy to see that $\ker(\varphi)$ is generated by binomials. A binomial $y^{\boldsymbol{\psi}} - by^{\boldsymbol{\eta}} \in \ker(\varphi)$ is said to be *primitive* provided there is no other binomial $y^{\boldsymbol{\psi}'} - b'y^{\boldsymbol{\eta}'} \in /rmker(\varphi)$ such that $y^{\boldsymbol{\psi}'}|y^{\boldsymbol{\psi}}$ and $y^{\boldsymbol{\eta}'}|y^{\boldsymbol{\eta}}$. The set of all such primitive binomials is called the *Graver basis* for $\ker(\varphi)$. An algorithm for computing a Graver basis for $\ker(\varphi)$ is given in [8]. Moreover it is proved there that this Graver basis contains a universal Gröbner basis for $\ker(\varphi)$.

Now consider the monoid $\mathfrak{L}$ given in (2) and a generating set, $\left\{(\boldsymbol{\psi}^{(1)}, \boldsymbol{\eta}^{(1)}), \ldots, (\boldsymbol{\psi}^{(s)}, \boldsymbol{\eta}^{(s)})\right\}$ for $\mathfrak{L}$. Also consider the corresponding polynomials $f_i = y^{\boldsymbol{\psi}^{(i)}} - b_i y^{\boldsymbol{\eta}^{(i)}} \in \ker(\varphi)$ $(1 \leq i \leq s)$. We observe that $\left\{(\boldsymbol{\psi}^{(1)}, \boldsymbol{\eta}^{(1)}), \ldots, (\boldsymbol{\psi}^{(s)}, \boldsymbol{\eta}^{(s)})\right\}$ is a Hilbert basis for $\mathfrak{L}$ if and only if $\{f_1, \ldots, f_s\}$ is a Graver basis of $\ker(\varphi)$. To see this, we first assume that $\left\{(\boldsymbol{\psi}^{(1)}, \boldsymbol{\eta}^{(1)}), \ldots, (\boldsymbol{\psi}^{(s)}, \boldsymbol{\eta}^{(s)})\right\}$ is a Hilbert basis of $\mathfrak{L}$. We note then that each f_i is primitive since if $f = y^{\boldsymbol{\psi}'} - b'y^{\boldsymbol{\eta}'} \in \ker(\varphi)$ is non-zero and different from f_i and $y^{\boldsymbol{\psi}'}|y^{\boldsymbol{\psi}^{(i)}}$ and $y^{\boldsymbol{\eta}'}|y^{\boldsymbol{\eta}^{(i)}}$ we would get $(\boldsymbol{\psi}', \boldsymbol{\eta}') \in \mathfrak{L}$ and $(\boldsymbol{\psi}^{(i)}, \boldsymbol{\eta}^{(i)}) - (\boldsymbol{\psi}', \boldsymbol{\eta}') \in \mathfrak{L}$; they are both strictly smaller than $(\boldsymbol{\psi}^{(i)}, \boldsymbol{\eta}^{(i)})$ and so in writing them as a non-negative linear combination of the $(\boldsymbol{\psi}^{(j)}, \boldsymbol{\eta}^{(j)})$ we must have that the coefficient of $(\boldsymbol{\psi}^{(i)}, \boldsymbol{\eta}^{(i)})$ is zero and this would allow us to eliminate $(\boldsymbol{\psi}^{(i)}, \boldsymbol{\eta}^{(i)})$ from the Hilbert basis violating, the definition of Hilbert basis as a minimal generating set. Moreover if $f = y^{\boldsymbol{\psi}} - b'y^{\boldsymbol{\eta}} \in \ker(\varphi)$ is primitive, then $(\boldsymbol{\psi}, \boldsymbol{\eta}) \in \mathfrak{L}$ implies that $(\boldsymbol{\psi}, \boldsymbol{\eta})$ is a non-negative sum of the $(\boldsymbol{\psi}^{(j)}, \boldsymbol{\eta}^{(j)})$'s, and then the primitivity would imply that $(\boldsymbol{\psi}, \boldsymbol{\eta})$ is one of the $(\boldsymbol{\psi}^{(j)}, \boldsymbol{\eta}^{(j)})$. Conversely, suppose that the f_i form a Graver basis for $\ker(\varphi)$. Choose $(\boldsymbol{\psi}, \boldsymbol{\eta}) \in \mathfrak{L}$. Then either $(\boldsymbol{\psi}, \boldsymbol{\eta})$ is primitive and we are done, or there is a primitive f_i such that $y^{\boldsymbol{\psi}^{(i)}}|y^{\boldsymbol{\psi}}$ and $y^{\boldsymbol{\eta}(i)}|y^{\boldsymbol{\eta}}$ and so $(\boldsymbol{\psi}, \boldsymbol{\eta}) - (\boldsymbol{\psi}^{(i)}, \boldsymbol{\eta}^{(i)}) \in \mathfrak{L}$ and we see that the $(\boldsymbol{\psi}^{(i)}, \boldsymbol{\eta}^{(i)})$ generate $\mathfrak{L}$; also the set is easily seen to be a minimal generating set.

We now go back to considerations over the PID R. We showed in Theorem 2.1 that if we consider the polynomials $\{g_1, \ldots, g_s\}$ in (3) corresponding to the Graver basis $\{f_1, \ldots, f_s\}$ in the preceding paragraph, we automatically get a generating set for $\ker(\varphi)$. In particular, the algorithm given in [8] provides an algorithm for computing this generating set and uses no computations over the PID except for computing greatest common divisors. It is interesting to note that the polynomials in (3) do not necessarily form a universal Gröbner basis for $\ker(\varphi)$. We do note, however, that in most of the examples we computed, the set of polynomials in (3) is a Gröbner basis.

Example 2.3. *Generators for a toric ideal.*

We consider the monomials $2x_1^2, 6x_2^2, 2x_1x_2^3, 3x_1^4x_2$ in $\mathbb{Z}[x_1, x_2]$. So in this case

$$\pi((u_1, u_2, u_3, u_4)) = u_1 \begin{bmatrix} 2 \\ 0 \end{bmatrix} + u_2 \begin{bmatrix} 0 \\ 2 \end{bmatrix} + u_3 \begin{bmatrix} 1 \\ 3 \end{bmatrix} + u_4 \begin{bmatrix} 4 \\ 1 \end{bmatrix}.$$

Then, eliminating the trivial solutions and the symmetric solutions to the given ones, we get that the Hilbert basis for $\mathfrak{L}$ in this case is

$$\{((1,3,0,0),(0,0,2,0)),((4,1,0,0),(0,0,0,2)),((3,0,2,0),(0,2,0,2)),((2,0,4,0),(0,5,0,2)),$$
$$((7,0,2,0),(0,1,0,4)),((1,0,6,0),(0,8,0,2)),((11,0,2,0),(0,0,0,6)),((0,0,8,0),(0,11,0,2))\}.$$

This computation was carried out using the subroutine Dragon of the software package Pegasus designed by Dachsel (see [4]). Then we have immediately from Theorem 2.1 that

$$g_1 = y_1y_2^3 - 108y_3^2,\ g_2 = 3y_1^4y_2 - 32y_4^2,\ g_3 = 81y_2^3y_3^2 - 8y_2^2y_4^2,\ g_4 = 3^7y_1^2y_3^4 - 2y_2^5y_4^2,$$
$$g_5 = 3^5y_1^7y_3^2 - 64y_2y_4^4,\ g_6 = 2 \cdot 3^{10}y_1y_3^6 - y_2^8y_4^2,\ g_7 = 3^6y_1^{11}y_3^2 - 2^{13}y_4^6,\ g_8 = 2^8 \cdot 3^{13}y_3^8 - y_2^{11}y_4^2.$$

We note that this ideal is homogeneous with respect to the natural weights $(2, 2, 4, 5)$ given by the degrees of $2x_1^2, 6x_2^2, 2x_1x_2^3, 3x_1^4x_2$. If we compute the reduced Gröbner basis for this ideal with respect to the degrevlex ordering with these weights and $y_3 > y_1 > y_2 > y_4$, we discover that this Gröbner basis contains the polynomial $y_1^5y_2^4 - 11y_1y_2^3y_4^2 + 36y_3^2y_4^2$ whose leading term $y_1^5y_2^4$ is not reducible with respect to the polynomials $g_1, \dots, g_8$ above. This shows that $\{g_1, \dots, g_8\}$ is not a Gröbner basis with respect to this order. This latter computation was carried out on Mathematica 3.0, using the CoefficientDomain option of Integers.

3. Construction of SAGBI Bases

As in Section 1 we let R be a PID and F be a finite subset of $R[x_1, \dots, x_n]$ with $A = R[F]$. We note that there is an obvious generalization of the notion of reduction with respect to a subset S of A in this situation (see [6]), which we denote by $\xrightarrow{S}$. It can be used to reduce elements of $R[x_1, \dots, x_n]$ and has the property that S is a SAGBI basis for A if and only if the following holds: if $f \in R[x_1, \dots, x_n]$ then $f \xrightarrow{S} 0$ if and only if $f \in A$.

We now recall the method presented in [6] for constructing a SAGBI basis for A. We assume that $F = \{f_1, \dots, f_t\}$ and set $\operatorname{lt} f_i = c_i x^{\boldsymbol{a}_i}$ for $i = 1, \dots, t$. We then have the R-algebra homomorphism in Section 2

$$\begin{array}{rrcl} \varphi: & R[y_1, \dots, y_t] & \longrightarrow & R[\operatorname{Lt} F] \subseteq R[x_1, \dots, x_n] \\ & y_i & \longmapsto & c_i x^{\boldsymbol{a}_i}. \end{array}$$

We see that $\ker(\varphi)$ is a homogeneous ideal with respect to the multigrading where the degree of y_i is the exponent vector $\boldsymbol{a}_i$. Then the degree of a monomial y^ψ is $\pi(\psi)$. The main result on constructing SAGBI bases in [6] states that if $P_1(y), \dots, P_m(y)$ is a homogeneous set of generators of $\ker(\varphi)$, then F is a SAGBI basis for A if and only if

$$P_j(F) \xrightarrow{F} 0$$

for each $j = 1, \dots, m$. Thus using the notation of the previous section and Theorem 2.1 we have the following.

Theorem 3.1. *F is a SAGBI basis for A if and only if*

$$\frac{\boldsymbol{c}^{\boldsymbol{\eta}^{(i)}}}{c^{(i)}} F^{\boldsymbol{\psi}^{(i)}} - \frac{\boldsymbol{c}^{\boldsymbol{\psi}^{(i)}}}{c^{(i)}} F^{\boldsymbol{\eta}^{(i)}} \xrightarrow{F} 0, \quad \textit{for } i = 1, \dots, s. \tag{6}$$

So the SAGBI analogue of Buchberger's algorithm is as follows: given the set F we find a basis of $\mathfrak{L}$ in equation (2) (for example, using Algorithm 7.2 in [8]), and then we check that all of the polynomials in equation (6) reduce to zero. If they do, then the algorithm ends, and if not, we add all of the final reducta to F and repeat the process. The procedure will eventually stop provided that there is a finite SAGBI basis with respect to the given order. Unfortunately this need not be so; see [6].

4. Construction of SAGBI-Gröbner Bases

We now turn to the construction of SAGBI-Gröbner bases (SG-bases). We assume throughout that A has a fixed finite SAGBI basis S. In particular it follows that each ideal in A has a finite SG-basis. There is a straight forward notion of reduction with respect to finite subsets, say, G in A which we again denote by $\xrightarrow{G}$ (note that this is not the same reduction as used in the last section for SAGBI bases). The actual reduction algorithm is more complicated, however, because of the necessity of staying inside the algebra A. The basic result we use is given in [6], Theorem 4.8:

Let $G = \{g_1, \dots, g_k\} \subseteq A$ and let I be the ideal generated by G in A. Let $\mathfrak{Q} \subset A^k$ with $\mathfrak{Q} = \{\boldsymbol{q}_1, \dots, \boldsymbol{q}_M\}$ and set $\boldsymbol{q}_i = (q_{i1}, \dots, q_{ik})$, $(1 \le i \le M)$. Assume that the vectors $(\mathrm{lt}(q_{i1}), \dots, \mathrm{lt}(q_{ik}))$ $(1 \le i \le M)$ are homogeneous generators with respect to the multigrading in Section 3 of the module of syzygies of $(\mathrm{lt}(g_1), \dots, \mathrm{lt}(g_k))$ inside $R[\mathrm{Lt}A]^k$ $(\mathrm{Syz}_{R[\mathrm{Lt}A]}(\mathrm{lt}(g_1), \dots, \mathrm{lt}(g_k)))$. Then G is a SG-basis for I if and only if we have $\sum_{j=1}^k q_{ij} g_j \xrightarrow{G} 0$ for $1 \le i \le M$. So it suffices to solve the following problem since we are assuming we have an explicit finite SAGBI basis for A:

Let $c_1 x^{\boldsymbol{a}_1}, \dots, c_t x^{\boldsymbol{a}_t}$ be in $R[x_1, \dots, x_n]$ where the $c_i \in R$ and the $x^{\boldsymbol{a}_j}$ are power products, as usual. Let $B = R[c_1 x_1^{\boldsymbol{a}}, \dots, c_t x^{\boldsymbol{a}_t}]$ and let $d_1 x^{\boldsymbol{b}_1}, \dots, d_k x^{\boldsymbol{b}_k} \in B$. We want to compute $\mathrm{Syz}_B(d_1 x^{\boldsymbol{b}_1}, \dots, d_k x^{\boldsymbol{b}_k})$, the module of syzygies of $(d_1 x^{\boldsymbol{b}_1}, \dots, d_k x^{\boldsymbol{b}_k})$ inside B^k.

In [6] this was done using an elimination order in a polynomial ring over R. Our purpose here is to eliminate this step in that we compute over R only using a degrevlex order and we solve diophantine equations as in Section 2.1.

The first step is to compute the kernel K of the evaluation map

$$\begin{array}{rcl} R[y_1, \dots, y_t, z_1, \dots, z_k] & \longrightarrow & R[c_1 x_1^{\boldsymbol{a}}, \dots, c_t x^{\boldsymbol{a}_t}, d_1 x^{\boldsymbol{b}_1}, \dots, d_k x^{\boldsymbol{b}_k}] \\ y_i & \longmapsto & c_i x^{\boldsymbol{a}_i} \\ z_i & \longmapsto & d_i x^{\boldsymbol{b}_i}. \end{array} \tag{7}$$

This is done in Theorem 2.1. The next step is to compute $K \cap \langle z_1, \dots, z_k \rangle$ in $R[y_1, \dots, y_t, z_1, \dots, z_k]$. For this we introduce the following term order on $R[y_1, \dots, y_t, z_1, \dots, z_k]$. Let $w_1, \dots, w_t, v_1, \dots, v_k$ denote a set of positive weights. Given two monomials in $R[y_1, \dots, y_t, z_1, \dots, z_k]$ we first compare them using the weights above and then break ties by using the reverse lexicographical ordering with $y_1 > \dots > y_t > z_1 > \dots > z_k$. With this we have the following basic fact: Let $J = \langle z_1, \dots, z_k \rangle$ and let $g \in R[y_1, \dots, y_t, z_1, \dots, z_k]$ be homogeneous with respect to the given weights. Assume there is an i, $1 \le i \le k$, such that $z_i | \mathrm{lp}(g)$. Then $g \in J$. We now have the following

Proposition 4.1. *Let I be any ideal in $R[y_1, \dots, y_t, z_1, \dots, z_k]$, homogeneous with respect to a set of positive weights on the variables. Let G be a homogeneous Gröbner basis for I with respect to the ordering described above with the given weights and such that $y_1 > \dots > y_t > z_1 > \dots > z_k$. Let $J = \langle z_1, \dots, z_k \rangle$. Then*

$$I \cap J = IJ + \langle G \cap J \rangle. \tag{8}$$

Proof. Since it is obvious that $IJ + \langle G \cap J \rangle \subseteq I \cap J$, it suffices to prove (see for example [1], Lemma 4.4.3) that

$$\mathrm{Lt}(I \cap J) \subseteq \mathrm{Lt}(IJ + \langle G \cap J \rangle).$$

Write $G = \{g_1, \dots, g_s\}$ and let $f \in I \cap J$. Then $f \in I$ and since G is assumed to be a Gröbner basis for I,

$$\mathrm{lt}(f) = \sum a_j y^{\boldsymbol{\beta}_j} z^{\boldsymbol{\gamma}_j} \mathrm{lt}(g_j)$$

where the $a_j \in R$, the $y^{\boldsymbol{\beta}_j}$ and $z^{\boldsymbol{\gamma}_j}$ are power products in the y and z variables respectively, and for each j such that $a_j \neq 0$ we have $y^{\boldsymbol{\beta}_j} z^{\boldsymbol{\gamma}_j} \mathrm{lp}(g_j) = \mathrm{lp}(f)$. Also $f \in J$ and so there is an i with $1 \le i \le k$ such that z_i divides $\mathrm{lp}(f)$. Fix a j such that $a_j \neq 0$. Then z_i divides $y^{\boldsymbol{\beta}_j} z^{\boldsymbol{\gamma}_j} \mathrm{lp}(g_j)$. If z_i divides $\mathrm{lp}(g_j)$ then by the basic property of the order we are using we have $g_j \in G \cap J$ and so

$$a_j y^{\boldsymbol{\beta}_j} z^{\boldsymbol{\gamma}_j} \mathrm{lt}(g_j) \in \mathrm{Lt}(IJ + \langle G \cap J \rangle). \tag{9}$$

On the other hand if z_i does not divide $\mathrm{lp}(g_j)$ then z_i divides z^{γ_j} and so $a_j y^{\boldsymbol{\beta}_j} z^{\gamma_j} g_j \in IJ$ and again (9) holds. Combining these two gives the result. $\square$

To apply this Proposition to K we first observe that K is indeed homogeneous with respect to certain weights. For example, the analogous ideal, $\ker(\varphi)$, described in Theorem 2.1 is homogeneous as described in Section 3. Then applying this to K, we see that K is also homogeneous with respect to the positive weights $w_j = a_{j1} + \cdots + a_{jn}$ for the y-variables, where $\boldsymbol{a}_j = (a_{j1}, \ldots, a_{jn})$, and $v_j = b_{j1} + \cdots + b_{jn}$ for the z-variables, where $\boldsymbol{b}_j = (b_{j1}, \ldots, b_{jn})$. That the weight is positive follows by the assumption that in each of the $c_i x^{\boldsymbol{a}_i}$, respectively the $d_i x^{\boldsymbol{b}_i}$, there are non-trivial terms. This, then completes the process for computing $K \cap \langle z_1, \ldots, z_k\rangle$ in $R[y_1, \ldots, y_t, z_1, \ldots, z_k]$. We note that this computation can probably be shortened by using the generating set described in Theorem 2.1.

We may now write down a generating set for $\mathrm{Syz}_B(d_i x^{\boldsymbol{b}_1}, \ldots, d_k x^{\boldsymbol{b}_k})$ as follows.

Theorem 4.2. *Let G be the Gröbner basis constructed in Proposition 4.1 with $K = I$. Write each element of $G \cap \langle z_1, \ldots, z_k\rangle$ in the form*

$$f_1^{(i)}(y_1, \ldots, y_t, z_1, \ldots, z_k)z_1 + \cdots + f_k^{(i)}(y_1, \ldots, , y_t, z_1, \ldots, z_k)z_k, \quad 1 \le i \le \ell. \tag{10}$$

Then the vectors

$$\sum_{j=1}^{k} f_j^{(i)}(c_1 x^{\boldsymbol{a}_1}, \ldots, c_t x^{\boldsymbol{a}_1}, d_1 x^{\boldsymbol{b}_1}, \ldots, d_k x^{\boldsymbol{b}_k})\boldsymbol{e}_j, \qquad 1 \le i \le \ell \tag{11}$$

together with the trivial syzygies $d_j x^{\boldsymbol{b}_j}\boldsymbol{e}_i - d_i x^{\boldsymbol{b}_i}\boldsymbol{e}_j$ for $1 \le i < j \le k$ generate the syzygy module $Syz_B(d_1 x^{\boldsymbol{b}_1}, \ldots, d_k x^{\boldsymbol{b}_k})$ where $\boldsymbol{e}_j$ for $1 \le j \le k$ are the standard unit vectors in k-space.

Proof. The proof that when we write the generators of $K \cap \langle z_1, \ldots, z_k\rangle$ in the form (10) and and then use the corresponding syzygies in (11) together with the trivial syzygies we get a generating set for $\mathrm{Syz}_B(d_1 x^{\boldsymbol{b}_1}, \ldots, d_k x^{\boldsymbol{b}_k})$ is straight forward. Here we are making use of the easily proved fact that $\mathrm{Syz}_{R[y_1,\ldots,z_k]}(z_1, \ldots, z_k)$ is generated by the vectors $z_j\boldsymbol{e}_i - z_i\boldsymbol{e}_j$ for $1 \le i < j \le k$. Then using Proposition 4.1 we see that the generators for $K \cap \langle z_1, \ldots, z_k\rangle$ are of two types. One of these gives rise to the syzygies in (11) of the theorem, and the other, coming from KJ, give rise to zero syzygies when expressed in the form (11). $\square$

Example 4.3. *Generators for a syzygy module.*

Consider the subalgebra $B = \mathbb{Z}[2x_1^2, 2x_2^2, 3x_1x_2]$ of $\mathbb{Z}[x_1, x_2]$. We consider $4x_1^2x_2^2, 18x_1^2x_2^4 \in B$. Then using the method of Theorem 2.1 (see Example 2.3) we get a generating set for K consisting of the 9 polynomials $y_1y_2 - z_1, 9z_1 - 4y_3^2, 4z_2 - 9y_2z_1, 4y_3^2 - 9y_1y_2, z_2 - y_2y_3^2, 4z_2 - 9y_1y_2^2, 4y_1z_2 - 9z_1^2, y_3^2z_1 - y_1z_2, 4y_3^4 - 9y_1z_2$. Computing the degrevlex Gröbner basis of Proposition 4.1 with the weights $(2, 2, 2, 4, 6)$ on $(y_1, y_2, y_3, z_1, z_2)$ and the order given there, we get the 6 polynomials $G = \{y_1y_2 - z_1, 9z_1 - 4y_3^2, 4z_2 - 9y_2z_1, z_2 - y_2y_3^2, 4y_1z_2 - 9z_1^2, y_3^2z_1 - y_1z_2\}$ (a subset of the first set of polynomials). Then $G \cap \langle z_1, z_2\rangle = \{4z_2 - 9y_2z_1, 4y_1z_2 - 9z_1^2, y_3^2z_1 - y_1z_2\}$. These give rise to the syzygies $18x_2^2\boldsymbol{e}_1 - 4\boldsymbol{e}_2, 36x_1^2x_2^2\boldsymbol{e}_1 - 8x_1^2\boldsymbol{e}_2, 9x_1^2x_2^2\boldsymbol{e}_1 - 2x_1^2\boldsymbol{e}_2$ together with the trivial syzygy $18x_1^2x_2^4\boldsymbol{e}_1 - 4x_1^2x_2^2\boldsymbol{e}_2$. The second and fourth are multiples of the third and so we get finally that $\mathrm{Syz}_B(4x_1^2x_2^2, 18x_1^2x_2^4) = \{18x_2^2\boldsymbol{e}_1 - 4\boldsymbol{e}_2, 9x_1^2x_2^2\boldsymbol{e}_1 - 2x_1^2\boldsymbol{e}_2\}$.

We note that if R is a field then the polynomials in (3) are a universal Gröbner basis and the extra degrevlex computation in Proposition 4.1 is unnecessary. Even though, as we pointed out in Section 2, there do exist orders in which the set G of polynomials in (3) is not a Gröbner basis, the identity $I \cap J = IJ + \langle G \cap J\rangle$ still holds for this G in all the examples we have checked. For example, in Example 2.3 we have checked the identity for all possible term orders and it always is valid (and, of course, in Example 4.3 this is also the case.) It would be interesting to resolve this question.

The algorithm presented in this section suffers from the defect that we must add extra variables in order to do the computation. One way to get around this might be as follows. Consider again the map

$$\varphi : R[y_1, \dots , y_t] \longrightarrow R[c_1x^{\boldsymbol{a}_1}, \dots , c_tx^{\boldsymbol{a}_t}]. \tag{12}$$

We lift $d_1x^{\boldsymbol{b}_1}, \dots , d_kx^{\boldsymbol{b}_k}$ to $h_1, \dots , h_k$ in $R[y_1, \dots , y_t]$. As in the last section and as explained in [6], the main point is to compute $\ker(\varphi) \cap \langle h_1, \dots , h_k\rangle$. This should be much easier if we can take the $h_1, \dots , h_k$ to be monomials. This is clearly equivalent to the statement that each of the monomials $d_ix^{\boldsymbol{b}_i}$ can be expressed as a monomial in the $c_1x^{\boldsymbol{a}_1}, \dots , c_tx^{\boldsymbol{a}_t}$. This property in general means that the $c_1x^{\boldsymbol{a}_1}, \dots , c_tx^{\boldsymbol{a}_t}$ form a strong SAGBI basis. Although we have not been able to get a good formula for the intersection in this case, we do show in the next section that strong SAGBI bases exist and we show how to compute them.

5. Strong SAGBI bases

In this section we first show the existence of strong SAGBI bases of subalgebras in a polynomial ring over a PID and then give an algorithm to compute them. For a simple family of subalgebras we will also give a bound on the number of elements in a strong SAGBI basis. We will also mention a few implications in the theory of integer programming. First of all we see that it suffices to show the existence of strong SAGBI bases for monomial subalgebras only.

Proposition 5.1. *Let $S' = \{f'_1, \dots , f'_s\}$ be a SAGBI basis and let $P = \{c_1x^{\boldsymbol{a}_1}, \dots , c_tx^{\boldsymbol{a}_t}\}$ be a strong SAGBI basis for $R[\mathrm{Lt}(S')]$. Suppose $c_ix^{\boldsymbol{a}_i} = p_i(\mathrm{lt}(f'_1), \dots , \mathrm{lt}(f'_s))$ where p_i is a polynomial in $R[y_1, \dots , y_s]$. Then $S = \{f_1, \dots , f_t\}$ where $f_i = p_i(f'_1, \dots , f'_s)$ is a strong SAGBI basis.*

Proof. If f is a subalgebra element in $R[S']$, then $\mathrm{lt}(f) = rP^{\boldsymbol{\psi}}$ for some $r \in R$ and $\boldsymbol{\psi} \in \mathbb{N}^t$. By our construction $P^{\boldsymbol{\psi}} = (\mathrm{Lt}S)^{\boldsymbol{\psi}}$. □

Now let $F = \{c_1x^{\boldsymbol{a}_1}, \dots , c_tx^{\boldsymbol{a}_t}\}$ and let $A = R[F]$ be the monomial subalgebra in $R[x_1, \dots , x_n]$. We let $\mathcal{A} = [\boldsymbol{a}_1, \dots , \boldsymbol{a}_t] \in \mathbb{N}^{n\times t}$ be the matrix whose columns are the exponent vectors of the elements in F. As in Section 2 we consider the map $\pi(\boldsymbol{u}) = \mathcal{A}\boldsymbol{u}$ for $\boldsymbol{u} \in \mathbb{N}^t$. Since each c_i is an element of R, it will be a product of primes. In particular, we let $c_i = \prod_{j=1}^{k} p_j^{\omega_{ij}}$ with p_j, $j = 1, \dots , k$ primes and $\omega_{ij} \in \mathbb{N}$. The following lemma connects the coefficients of monomials in the algebra A to certain integer programs. We denote by $\mathbb{N}(\mathcal{A})$ the monoid of non-negative integral linear combinations of the columns of $\mathcal{A}$.

Lemma 5.2. *For $\boldsymbol{b} \in \mathbb{N}(\mathcal{A})$, let $k_{\boldsymbol{b}} = gcd(c^{\boldsymbol{u}} : \boldsymbol{u} \in \pi^{-1}(\boldsymbol{b}))$. Then $k_{\boldsymbol{b}}x^{\boldsymbol{b}}$ is in A and if we write $k_{\boldsymbol{b}} = \prod_{j=1}^{k} p_j^{\omega_j}$, we have for each j, $1 \le j \le k$, that ω_j is the optimal solution value for the integer program*

$$IP^j_{\mathcal{A}}(\boldsymbol{b}) : \quad \textit{minimize} \ \sum_{i=1}^{t} \omega_{ij}u_i \ \ \textit{subject to} \ \boldsymbol{u} \in \pi^{-1}(\boldsymbol{b}).$$

Proof. Let $k_{\boldsymbol{b}} = \sum_{\boldsymbol{u}\in\pi^{-1}(\boldsymbol{b})} r_{\boldsymbol{u}}c^{\boldsymbol{u}}$ where $r_{\boldsymbol{u}} \in R$. Then $\sum_{\boldsymbol{u}\in\pi^{-1}(\boldsymbol{b})} r_{\boldsymbol{u}}F^{\boldsymbol{u}} = (\sum_{\boldsymbol{u}\in\pi^{-1}(\boldsymbol{b})} r_{\boldsymbol{u}}c^{\boldsymbol{u}})x^{\boldsymbol{b}} = k_{\boldsymbol{b}}x^{\boldsymbol{b}}$, therefore $k_{\boldsymbol{b}}x^{\boldsymbol{b}}$ is in A. The power of p_j in $k_{\boldsymbol{b}}$ must be the minimum of the powers of p_j over all $c^{\boldsymbol{u}}$ with $\boldsymbol{u} \in \pi^{-1}(\boldsymbol{b})$. But this is precisely the optimal solution value for the above integer program. □

In order to show the existence of strong SAGBI bases, we need to define and work with the *standard pairs* of a monomial ideal M in $K[y_1, \dots, y_t]$, where K is an arbitrary field now. Recall that a monomial $y^{\boldsymbol{\alpha}} \notin M$ is called a *standard monomial.* For a monomial $y^{\boldsymbol{\alpha}}$ and a subset Z of $\{1, \dots, t\}$ such that $\mathrm{supp}(\boldsymbol{\alpha}) \cap Z = \emptyset$, the pair $(y^{\boldsymbol{\alpha}}, Z)$ is called *admissible* if all the monomials in $y^{\boldsymbol{\alpha}} \cdot K[y_i : i \in Z]$ are standard. The admissible pairs of M are partially ordered by

$$(y^{\boldsymbol{\alpha}}, Z_1) \prec (y^{\boldsymbol{\beta}}, Z_2) \iff \boldsymbol{\beta} \leq \boldsymbol{\alpha} \text{ and } \mathrm{supp}(\boldsymbol{\alpha} - \boldsymbol{\beta}) \cup Z_1 \subseteq Z_2,$$

where $\boldsymbol{\beta} \leq \boldsymbol{\alpha}$ means that $\boldsymbol{\beta}_i \leq \boldsymbol{\alpha}_i$ for $i = 1, \dots, t$. The pairs corresponding to the maximal elements of this partial order are called *standard pairs.* Observe that every standard monomial of M is "covered" by a standard pair. For more details about the standard pairs and for the following theorem, we refer to [10].

Theorem 5.3. *Let M be a monomial ideal in $K[y_1, \dots, y_t]$.*

1. *The prime ideal $P_Z = \langle y_i : i \notin Z \rangle$ is an associated prime of M if and only if there exists a standard pair $(y^{\boldsymbol{\alpha}}, Z)$ of M. Furthermore, P_Z is a minimal prime if and only if $(1, Z)$ is a standard pair.*
2. *The multiplicity of P_Z in a minimal primary decomposition of M is the number of standard pairs of the form $(y^{\boldsymbol{\alpha}}, Z)$. Hence the* **arithmetic degree** *(see [3], [10]) of M is the total number of the standard pairs of M.*

Example 5.4. *Standard pairs of a monomial ideal.*

Let M be the monomial ideal in $K[y_1, y_2, y_3]$ with minimal generators $\{y_3^{11}, y_1y_3, y_1^4y_2^7, y_1^5y_2^5, y_1^6y_2^3, y_1^7y_2, y_1^8\}$. There is a total of 14 standard pairs associated to $Z = \{2\}$: $\{(y_3^{10}, \{2\}), \dots, (y_3, \{2\}), (1, \{2\}), (y_1, \{2\}), \dots, (y_1^3, \{2\})\}$ and there are 16 standard pairs of the form $(y_1^iy_2^j, \emptyset)$ where $i = 4, \dots, 7$ and $j = 0, \dots, (14 - 2i)$. As Theorem 5.3 predicts, M has $\langle y_1, y_3 \rangle$ as its minimal prime with multiplicity 14, and $\langle y_1, y_2, y_3 \rangle$ as its embedded prime with multiplicity 16. So the arithmetic degree of M is 30. These can be checked from the following minimal primary decomposition of $M = \langle y_1y_3, y_1^4, y_3^{11} \rangle \cap \langle y_1^8, y_1^7y_2, y_1^6y_2^3, y_1^5y_2^5, y_2^7, y_3 \rangle$.

Suppose $I_{\mathcal{A}}$ is the toric ideal in $K[y_1, \dots, y_t]$ associated with $\mathcal{A} = [\boldsymbol{a}_1, \dots, \boldsymbol{a}_t] \in \mathbb{N}^{n \times t}$. Given a nonnegative integral vector $\boldsymbol{w} = (w_1, \dots, w_t)$, let $\prec_{\boldsymbol{w}}$ be a degree term order in which $\deg(y_i) = w_i$. The following connects the standard monomials of the initial ideal $\mathrm{Lt}_{\prec_{\boldsymbol{w}}}(I_{\mathcal{A}})$ to integer programming.

Proposition 5.5. *(cf. [11]) A monomial $y^{\boldsymbol{\alpha}}$ is a standard monomial of $\mathrm{Lt}_{\prec_{\boldsymbol{w}}}(I_{\mathcal{A}})$ if and only if $\boldsymbol{\alpha}$ is the optimal solution vector for the integer program:*

$$\text{minimize} \sum_{i=1}^{t} w_i u_i \quad \text{subject to } \pi(\boldsymbol{u}) = \pi(\boldsymbol{\alpha}) \text{ and } \boldsymbol{u} \in \mathbb{N}^t.$$

Given $\boldsymbol{b} = \pi(\boldsymbol{u})$ for some $\boldsymbol{u} \in \mathbb{N}^t$, each integer program $\mathrm{IP}^j_{\mathcal{A}}(\boldsymbol{b})$ has an optimal solution $\boldsymbol{\beta}_j$, $j = 1, \dots, k$, corresponding to the standard monomial $y^{\boldsymbol{\beta}_j}$ of $\mathrm{Lt}_{\prec_{\boldsymbol{\omega}_j}}(I_{\mathcal{A}})$ where $\boldsymbol{\omega}_j = (\omega_{1j}, \omega_{2j}, \dots, \omega_{tj})$. The standard monomial $y^{\boldsymbol{\beta}_j}$ will be covered by a standard pair $S_j = (y^{\boldsymbol{\alpha}_j}, Z_j)$.

Lemma 5.6. *Let $C_{S_1,\dots,S_k}$ be the set of all $\boldsymbol{b} \in \mathbb{N}(\mathcal{A})$ such that the optimal solution for $IP^j_{\mathcal{A}}(\boldsymbol{b})$ is covered by the standard pair S_j of $\mathrm{Lt}_{\prec_{\boldsymbol{\omega}_j}}(I_{\mathcal{A}})$ for $j = 1, \dots, k$. So $C_{S_1,\dots,S_k} = \bigcap_{j=1}^k (\pi(\boldsymbol{\alpha}_j) + \mathbb{N}(\mathcal{A}_{Z_j}))$, where $\mathcal{A}_{Z_j} = [\boldsymbol{a}_i : i \in Z_j]$. Moreover, $C_{S_1,\dots,S_k}$ is the finite union of translates of a certain integral* *monoid, i.e.,*

$$C_{S_1,\dots,S_k} = \bigcup_{p=1}^{s} (\boldsymbol{b}_p + \mathbb{N}(\mathcal{D})) \text{ for some } \boldsymbol{b}_p \in C_{S_1,\dots,S_k}, \tag{13}$$

where each column $\boldsymbol{d}_i$ of $\mathcal{D}$ is in $\mathbb{N}(\mathcal{A}_{Z_j})$ for all $j = 1, \dots, k$.

If we prove the above lemma then the existence of strong SAGBI bases follows:

Theorem 5.7. *Let St_j be the set of all standard pairs of $IP^j_{\mathcal{A}}(\boldsymbol{b})$ for $j = 1, \dots, k$. For each $(S_1, \dots, S_k) \in St_1 \times \cdots \times St_k$, let $B_{S_1,\dots,S_k}$ be the collection of $\boldsymbol{b}_p$'s in (13) belonging to $C_{S_1,\dots,S_k}$ together with the columns in $\mathcal{D}$ whenever the corresponding $\boldsymbol{b}_p$ is zero. Then $F = \{k_{\boldsymbol{b}} x^{\boldsymbol{b}} : \boldsymbol{b} \in \bigcup_{(S_1,\dots,S_k)} B_{S_1,\dots,S_k}\}$ is a strong SAGBI basis for the monomial subalgebra $A = R[c_1 x^{\boldsymbol{a}_1}, \dots, c_t x^{\boldsymbol{a}_t}]$.*

Proof. Suppose $rx^{\boldsymbol{b}}$ is a monomial in A where $r \in R$. Then clearly $\boldsymbol{b} \in \mathbb{N}(\mathcal{A})$, hence $rx^{\boldsymbol{b}} = r'(k_{\boldsymbol{b}} x^{\boldsymbol{b}})$. So we just have to consider monomials of the form $k_{\boldsymbol{b}} x^{\boldsymbol{b}}$. Now $\boldsymbol{b}$ is in one of $C_{S_1,\dots,S_k} = \bigcap_{j=1}^{k} (\pi(\boldsymbol{\alpha}_j) + \mathbb{N}(\mathcal{A}_{Z_j}))$, and by the above lemma it is in some $\boldsymbol{b}_p + \mathbb{N}(\mathcal{D})$. Therefore $\boldsymbol{b} - \boldsymbol{b}_p \in \mathbb{N}(\mathcal{D}) \subseteq \mathbb{N}(\mathcal{A}_{Z_j})$ for $j = 1, \dots, k$. If $\boldsymbol{b}_p = 0$, then $\boldsymbol{b} \in \mathbb{N}(\mathcal{D}_p)$ and we can assume that $\boldsymbol{b}_p$ is one of the vectors in $\mathcal{D}$ which is used to express $\boldsymbol{b}$. Since both $\boldsymbol{b}$ and $\boldsymbol{b}_p$ are in $\pi(\boldsymbol{\alpha}_j) + \mathbb{N}(\mathcal{A}_{Z_j})$ for all $j = 1, \dots, k$, we have $\boldsymbol{b} = \pi(\boldsymbol{\alpha}_j) + \pi(\boldsymbol{\beta}_j^1)$ and $\boldsymbol{b}_p = \pi(\boldsymbol{\alpha}_j) + \pi(\boldsymbol{\beta}_j^2)$ for $\boldsymbol{\beta}_j^1, \boldsymbol{\beta}_j^2 \in \mathbb{N}^t$ with $\mathrm{supp}(\boldsymbol{\beta}_j^1)$ and $\mathrm{supp}(\boldsymbol{\beta}_j^2)$ in Z_j. Here $\boldsymbol{\alpha}_j + \boldsymbol{\beta}_j^1$ and $\boldsymbol{\alpha}_j + \boldsymbol{\beta}_j^2$ are the optimal solutions for $\mathrm{IP}^j_{\mathcal{A}}(\boldsymbol{b})$ and $\mathrm{IP}^j_{\mathcal{A}}(\boldsymbol{b}_p)$ respectively. Hence $\boldsymbol{b} - \boldsymbol{b}_p = \pi(\boldsymbol{\beta}_j^1 - \boldsymbol{\beta}_j^2) \in \mathbb{N}(\mathcal{A}_{Z_j})$, and since by Lemma 12.14 in [8] the vectors in $\mathcal{A}_{Z_j}$ are linearly independent, we have $\boldsymbol{\beta}_j^1 - \boldsymbol{\beta}_j^2 \geq 0$. This means that $\boldsymbol{\beta}_j^1 - \boldsymbol{\beta}_j^2$ is a feasible solution of the integer program $\mathrm{IP}^j_{\mathcal{A}}(\boldsymbol{b} - \boldsymbol{b}_p)$ for $j = 1, \dots, k$. We need to show that it is actually an optimal solution. By Theorem 5.3 there exists $Z'_j \supseteq Z_j$ corresponding to a minimal prime of $\mathrm{Lt}_{\prec_{\boldsymbol{\omega}_j}}(I_{\mathcal{A}})$ for each Z_j. This says that $\pi(\boldsymbol{\beta}_j^1 - \boldsymbol{\beta}_j^2) \in \mathbb{N}(\mathcal{A}_{Z'_j})$, and hence the monomial $y^{\boldsymbol{\beta}_j^1 - \boldsymbol{\beta}_j^2}$ is covered by the standard pair $(1, Z'_j)$ for $j = 1, \dots, k$. Now Proposition 5.5 implies that $\boldsymbol{\beta}_j^1 - \boldsymbol{\beta}_j^2$ is the optimal solution for $\mathrm{IP}^j_{\mathcal{A}}(\boldsymbol{b} - \boldsymbol{b}_p)$ for each j. In fact we have shown that the optimal solution for $\mathrm{IP}^j_{\mathcal{A}}(\boldsymbol{b})$ is the sum of the optimal solution for $\mathrm{IP}^j_{\mathcal{A}}(\boldsymbol{b}_p)$ and the optimal solution for $\mathrm{IP}^j_{\mathcal{A}}(\boldsymbol{b} - \boldsymbol{b}_p)$ for $j = 1, \dots, k$. This implies that $k_{\boldsymbol{b}} x^{\boldsymbol{b}} = (k_{\boldsymbol{b}_p} x^{\boldsymbol{b}_p})(k_{\boldsymbol{b}-\boldsymbol{b}_p} x^{(\boldsymbol{b}-\boldsymbol{b}_p)})$. Now we can repeat this process for $k_{\boldsymbol{b}-\boldsymbol{b}_p} x^{(\boldsymbol{b}-\boldsymbol{b}_p)}$ and eventually have $k_{\boldsymbol{b}} x^{\boldsymbol{b}} = \prod k_{\boldsymbol{b}_p} x^{\boldsymbol{b}_p}$ where $k_{\boldsymbol{b}_p} x^{\boldsymbol{b}_p} \in F$. ☐

Proof of Lemma 5.6: Since for each $j = 1, \dots, k$ the standard monomial corresponding to the optimal solution of $\mathrm{IP}^j_{\mathcal{A}}(\boldsymbol{b})$ is covered by $S_j = (y^{\boldsymbol{\alpha}_j}, Z_j)$, $\boldsymbol{b}$ is in $\pi(\boldsymbol{\alpha}_j) + \mathbb{N}(\mathcal{A}_{Z_j})$ for all $j = 1, \dots, k$. This shows $C_{S_1,\dots,S_k} = \bigcap_{j=1}^{k} (\pi(\boldsymbol{\alpha}_j) + \mathbb{N}(\mathcal{A}_{Z_j}))$. Now $C_{S_1,\dots,S_k}$ is the collection of $\boldsymbol{b} \in \mathbb{N}(\mathcal{A})$ where $\boldsymbol{b} = \pi(\boldsymbol{\alpha}_j) + \pi(\boldsymbol{\beta}_j)$ for all $j = 1, \dots, k$ for some $\boldsymbol{\beta}_j \in \mathbb{N}^t$ with $\mathrm{supp}(\boldsymbol{\beta}_j) \subseteq Z_j$. In other words, $\boldsymbol{b} = \pi(\boldsymbol{\alpha}_j) + \pi(\boldsymbol{\beta}_j)$ for $j = 1, \dots, k$ is in $C_{S_1,\dots,S_k}$ if and only if $(\boldsymbol{\beta}_1, \dots, \boldsymbol{\beta}_k)$ is an integral vector in the rational polyhedron $P = \{(\boldsymbol{u}_1, \dots, \boldsymbol{u}_k)^T \in \mathbb{R}_+^{tk} : \pi(\boldsymbol{\alpha}_r) - \pi(\boldsymbol{\alpha}_i) = \mathcal{A}(\boldsymbol{u}_i) - \mathcal{A}(\boldsymbol{u}_r),\ 1 \leq i < r \leq k \text{ and } \mathrm{supp}(\boldsymbol{u}_j) \subseteq Z_j,\ j = 1, \dots, k\}$. By Theorem 16.4 and the discussion after it in [7] we see that $P \cap \mathbb{Z}^{kt}$ is the union of translates of a certain integral monoid, i.e. there exists integer vectors $(\boldsymbol{w}_p^1, \dots, \boldsymbol{w}_p^k)^T \in \mathbb{N}^{kt}$ for $p = 1, \dots, s$ and matrices $\mathcal{B}^1, \dots, \mathcal{B}^k$ such that $P \cap \mathbb{Z}^{kt} = \bigcup_{p=1}^{s} ((\boldsymbol{w}_p^1, \dots, \boldsymbol{w}_p^k)^T + \mathbb{N}((\mathcal{B}^1, \dots, \mathcal{B}^k)^T))$. Now we can take $\boldsymbol{b}_p = \pi(\boldsymbol{\alpha}_j) + \pi(\boldsymbol{w}_p^j)$ and $\mathcal{D} = \pi(\mathcal{B}^j)$ for *any* $j = 1, \dots, k$. Therefore $C_{S_1,\dots,S_t} = \bigcup_{p=1}^{s} (\boldsymbol{b}_p + \mathbb{N}(\mathcal{D}))$. Since the support of the rows of $\mathcal{B}^j$ is in Z_j we also see that the columns of the matrix $\mathcal{D} = \pi(\mathcal{B}^j)$ are in $\mathbb{N}(\mathcal{A}_{Z_j})$. This completes the proof of Lemma 5.6.

Theorem 5.7 and Lemma 5.6 give an algorithm to compute strong SAGBI bases for monomial subalgebras over a PID.

Algorithm 5.8. *How to compute strong SAGBI bases.*

INPUT: A monomial subalgebra $A = R[c_1 x^{\boldsymbol{a}_1}, \dots, c_t x^{\boldsymbol{a}_t}]$ in $R[x_1, \dots, x_n]$.
OUTPUT: A strong SAGBI basis F for A.

1. Let $p_1, \dots, p_k$ be the distinct primes appearing in the coefficients c_i's, and write $c_i = \prod_{j=1}^{k} p_j^{\omega_{ij}}$. Let $\boldsymbol{\omega}_j = (\omega_{1j}, \dots, \omega_{tj})$.
2. For each $j = 1, \dots, k$, compute the initial ideal $\mathrm{Lt}_{\prec_{\boldsymbol{\omega}_j}}(I_{\mathcal{A}})$ of the toric ideal $I_{\mathcal{A}} \subset K[y_1, \dots, y_t]$ (where $\mathcal{A} = [\boldsymbol{a}_1, \dots, \boldsymbol{a}_n]$) with respect to a degree term order $\prec_{\boldsymbol{\omega}_j}$ with degree$(y_i) = \omega_{ij}$. This could be done by computing the reduced Gröbner basis of $I_{\mathcal{A}}$ with respect to $\prec_{\boldsymbol{\omega}_j}$. Let $M_1, \dots, M_k$ be the resulting initial ideals.
3. For each initial ideal M_j compute the standard pairs St_j of M_j (for an algorithm see [5]).
4. For every $(S_1, \dots, S_k) \in \mathrm{St}_1 \times \dots \times \mathrm{St}_k$ compute the generators $B_{S_1,\dots,S_k}$ of $C_{S_1,\dots,S_k}$ of Lemma 5.6, i.e., compute the $\boldsymbol{b}_p$'s and $\mathcal{D}$ in (13). This could be done by computing a generating set of the integral vectors in the polyhedron P of the proof of Lemma 5.6.
5. Let $F = \{k_{\boldsymbol{b}} x^{\boldsymbol{b}} \,:\, \boldsymbol{b} \in \cup_{(S_1,\dots,S_k)} B_{S_1,\dots,S_k}\}$ where $k_{\boldsymbol{b}} = \gcd(\prod_{i=1}^{t} c_i^{u_i} \,:\, \boldsymbol{u} \in \pi^{-1}(\boldsymbol{b}))$.

Example 5.9. *A strong SAGBI basis.*

Let $A = \mathbb{Z}[120x_1^3, 4x_1^2x_2, 3x_1x_2^2, 15x_2^3]$ in $\mathbb{Z}[x_1, x_2]$. Here

$$\mathcal{A} = [\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \boldsymbol{a}_4] = \begin{bmatrix} 3 & 2 & 1 & 0 \\ 0 & 1 & 2 & 3 \end{bmatrix},$$

and $120 = 2^3 \cdot 3 \cdot 5$, $4 = 2^2$, and $15 = 3 \cdot 5$. So we take $p_1 = 2$, $p_2 = 3$, and $p_3 = 5$; hence $\boldsymbol{\omega}_1 = (3, 2, 0, 0)$, $\boldsymbol{\omega}_2 = (1, 0, 1, 1)$, and $\boldsymbol{\omega}_3 = (1, 0, 0, 1)$. When we choose $\prec_{\boldsymbol{\omega}_j}$ to be the degree reverse lexicographic term order where $y_4 \prec_{\boldsymbol{\omega}_j} \cdots \prec_{\boldsymbol{\omega}_j} y_1$, we get three distict initial ideals of $I_{\mathcal{A}}$: $M_1 = \langle y_2y_4, y_2^2, y_1y_4 \rangle$, $M_2 = \langle y_1y_3, y_3^2, y_1y_4 \rangle$, and $M_3 = \langle y_2y_4, y_1y_3, y_1y_4 \rangle$. The corresponding standard pairs are $\mathrm{St}_1 = \{(1, \{1,3\}), (y_2, \{1,3\}), (1, \{3,4\})\}$, $\mathrm{St}_2 = \{(1, \{1,2\}), (1, \{2,4\}), (y_3, \{2,4\})\}$, and $\mathrm{St}_3 = \{(1, \{1,2\}), (1, \{2,3\}), (1, \{3,4\})\}$. There are 27 C_{S_1,S_2,S_3}'s to be computed in this case and the table on the next page lists the results of this computation. From the table, we see that the exponents of the strong SAGBI basis elements will be $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \boldsymbol{a}_4$, $2\boldsymbol{a}_2, 2\boldsymbol{a}_3$, and $(\boldsymbol{a}_2 + \boldsymbol{a}_3)$. In order to determine the coefficients of these elements we need to compute $\pi^{-1}(\boldsymbol{b})$ for each $\boldsymbol{b}$ in the above list. For instance $\pi^{-1}(2\boldsymbol{a}_2) = \{2\boldsymbol{a}_2, (\boldsymbol{a}_1 + \boldsymbol{a}_3)\}$, therefore the coefficient of $x_1^4x_2^2$ is the gcd of 4^2 and $120 \cdot 3$, which is 8. So we get as a strong SAGBI basis $F = \{120x_1^3, 4x_1^2x_2, 3x_1x_2^2, 15x_2^3, 8x_1^4x_2^2, 3x_1^2x_2^4, 12x_1^3x_2^3\}$.

$S_1 \in \mathrm{St}_1$	$S_2 \in \mathrm{St}_2$	$S_3 \in \mathrm{St}_3$	C_{S_1,S_2,S_3}
$(1,\{1,3\})$	$(1,\{1,2\})$	$(1,\{1,2\})$	$\mathbb{N}(\boldsymbol{a}_1, 2\boldsymbol{a}_2)$
$(1,\{1,3\})$	$(1,\{1,2\})$	$(1,\{2,3\})$	$\mathbb{N}(2\boldsymbol{a}_2)$
$(1,\{1,3\})$	$(1,\{1,2\})$	$(1,\{3,4\})$	0
$(1,\{1,3\})$	$(1,\{2,4\})$	$(1,\{1,2\})$	$\mathbb{N}(2\boldsymbol{a}_2)$
$(1,\{1,3\})$	$(1,\{2,4\})$	$(1,\{2,3\})$	$\mathbb{N}(2\boldsymbol{a}_2, 2\boldsymbol{a}_3)$
$(1,\{1,3\})$	$(1,\{2,4\})$	$(1,\{3,4\})$	$\mathbb{N}(2\boldsymbol{a}_3)$
$(1,\{1,3\})$	$(y_3,\{2,4\})$	$(1,\{1,2\})$	$\emptyset$
$(1,\{1,3\})$	$(y_3,\{2,4\})$	$(1,\{2,3\})$	$\boldsymbol{a}_3 + \mathbb{N}(2\boldsymbol{a}_2, 2\boldsymbol{a}_3)$
$(1,\{1,3\})$	$(y_3,\{2,4\})$	$(1,\{3,4\})$	$\boldsymbol{a}_3 + \mathbb{N}(2\boldsymbol{a}_3)$
$(y_2,\{1,3\})$	$(1,\{1,2\})$	$(1,\{1,2\})$	$\boldsymbol{a}_2 + \mathbb{N}(\boldsymbol{a}_1, 2\boldsymbol{a}_2)$
$(y_2,\{1,3\})$	$(1,\{1,2\})$	$(1,\{2,3\})$	$\boldsymbol{a}_2 + \mathbb{N}(2\boldsymbol{a}_2)$
$(y_2,\{1,3\})$	$(1,\{1,2\})$	$(1,\{3,4\})$	$\emptyset$
$(y_2,\{1,3\})$	$(1,\{2,4\})$	$(1,\{1,2\})$	$\boldsymbol{a}_2 + \mathbb{N}(2\boldsymbol{a}_2)$
$(y_2,\{1,3\})$	$(1,\{2,4\})$	$(1,\{2,3\})$	$\boldsymbol{a}_2 + \mathbb{N}(2\boldsymbol{a}_2, 2\boldsymbol{a}_3)$
$(y_2,\{1,3\})$	$(1,\{2,4\})$	$(1,\{3,4\})$	$\emptyset$
$(y_2,\{1,3\})$	$(y_3,\{2,4\})$	$(1,\{1,2\})$	$\emptyset$
$(y_2,\{1,3\})$	$(y_3,\{2,4\})$	$(1,\{2,3\})$	$(\boldsymbol{a}_2 + \boldsymbol{a}_3) + \mathbb{N}(2\boldsymbol{a}_2, 2\boldsymbol{a}_3)$
$(y_2,\{1,3\})$	$(y_3,\{2,4\})$	$(1,\{3,4\})$	$\emptyset$
$(1,\{3,4\})$	$(1,\{1,2\})$	$(1,\{1,2\})$	$\emptyset$
$(1,\{3,4\})$	$(1,\{1,2\})$	$(1,\{2,3\})$	$\emptyset$
$(1,\{3,4\})$	$(1,\{1,2\})$	$(1,\{3,4\})$	$\emptyset$
$(1,\{3,4\})$	$(1,\{2,4\})$	$(1,\{1,2\})$	$\emptyset$
$(1,\{3,4\})$	$(1,\{2,4\})$	$(1,\{2,3\})$	$\mathbb{N}(2\boldsymbol{a}_3)$
$(1,\{3,4\})$	$(1,\{2,4\})$	$(1,\{3,4\})$	$\mathbb{N}(2\boldsymbol{a}_3, \boldsymbol{a}_4)$
$(1,\{3,4\})$	$(y_3,\{2,4\})$	$(1,\{1,2\})$	$\emptyset$
$(1,\{3,4\})$	$(y_3,\{2,4\})$	$(1,\{2,3\})$	$\boldsymbol{a}_3 + \mathbb{N}(2\boldsymbol{a}_3)$
$(1,\{3,4\})$	$(y_3,\{2,4\})$	$(1,\{3,4\})$	$\boldsymbol{a}_3 + \mathbb{N}(2\boldsymbol{a}_3, \boldsymbol{a}_4)$

In Algorithm 5.8, there will be $\prod_{j=1}^k \mathrm{arithdeg}(\mathrm{Lt}_{\prec_{\boldsymbol{\omega}_j}}(I_{\mathcal{A}}))$ different $C_{S_1,\dots,S_k}$'s to be considered, and each of these might have a lot of generators. Hence in general it is hard to estimate the number of elements in a strong SAGBI basis. But we can do this when $n = 1$, i.e., when there is only one variable.

Theorem 5.10. *Let $A = R[c_1x^{a_1}, \dots, c_tx^{a_t}]$ with $a_i \in \mathbb{N}$, and let $a = max\{a_1, \dots, a_t\}$. Suppose $I_{\mathcal{A}}$ where $\mathcal{A} = [a_1, \dots, a_t]$ has k distinct initial ideals. Then there is a strong SAGBI basis of A with at most a^{2k} elements.*

Proof. $\mathrm{Lt}_{\prec_{\boldsymbol{\omega}_j}}(I_{\mathcal{A}})$ is a one-dimensional ideal for $j = 1, \dots, k$, and therefore the standard pairs are either of the form $(y^{\boldsymbol{\alpha}_j}, \emptyset)$ or $(y^{\boldsymbol{\alpha}_j}, \{i\})$. If $(S_1, \dots, S_k) \in \mathrm{St}_1 \times \cdots \times \mathrm{St}_k$ contains a standard pair of the first kind, then $C_{S_1,\dots,S_k}$ consists of at most one point. If all S_j are of the second kind and $C_{S_1,\dots,S_k} \neq \emptyset$, then $C_{S_1,\dots,S_k} = b + \mathbb{N}(m)$ where b is the smallest nonnegative integer in $C_{S_1,\dots,S_k}$ and $m = \mathrm{lcm}\{a_i : S_j = (y^{\boldsymbol{\alpha}_j}, \{i\})\}$. So each $C_{S_1,\dots,S_k}$ contributes at most one element to the strong SAGBI basis. Since $\mathrm{arithdeg}(\mathrm{Lt}_{\prec_{\boldsymbol{\omega}_j}}(I_{\mathcal{A}}))$ is bounded above by a^2 (see [5]), there will be at most a^{2k} elements in the basis. $\square$

The number of initial ideals in the above theorem and in general the number of initial ideals one needs to compute in Algorithm 5.8 is bounded by the total number of initial ideals of $I_{\mathcal{A}}$. This is known to be equal to the number of vertices of the *state polytope* of $I_{\mathcal{A}}$ (cf. [2],[9]) and so, in particular, is independent of the number of primes used in the coefficients of subalgebra generators. This fact leads to a kind of *universal* strong SAGBI basis of a monomial subalgebra in the following sense: suppose a monomial subalgebra is generated by elements with exponent vectors $\mathcal{A} = [\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t] \in \mathbb{N}^{n\times t}$. In Algorithm 5.8, instead of computing the initial ideals dictated by the coefficients of the subalgebra generators, we can compute *all* initial ideals and find exponent vectors for strong SAGBI basis elements which will work for *any* choice of coefficients. Once these exponent vectors are computed, in order to give a strong SAGBI basis for a particular choice of monomial subalgebra, we need to compute the $k_{\boldsymbol{b}}$'s in step 5 of Algorithm 5.8. Note that this is the only step where the values of c_i's are needed.

Actually, in order to compute a universal strong SAGBI basis, we can use a more direct algorithm that does not use Algorithm 5.8. Given $\mathcal{A}$ with the associated map π, for each $\boldsymbol{b} \in \mathbb{N}(\mathcal{A})$ we define $P_{\boldsymbol{b}} = \mathrm{conv}(\boldsymbol{u} \in \pi^{-1}(\boldsymbol{b}))$ as the *$\boldsymbol{b}$-fiber* of π. Since $\mathcal{A} \in \mathbb{N}^n$, $P_{\boldsymbol{b}}$ is a polytope for all $\boldsymbol{b} \in \mathbb{N}(\mathcal{A})$.

Definition 5.11. *The $\boldsymbol{b}$-fiber $P_{\boldsymbol{b}}$ is called an* atomic *fiber of π if there do not exist two fibers $P_{\boldsymbol{b}_1}$ and $P_{\boldsymbol{b}_2}$ with $\boldsymbol{b} \neq \boldsymbol{b}_1, \boldsymbol{b}_2$ and $\boldsymbol{b}_1, \boldsymbol{b}_2 \leq \boldsymbol{b}$ such that $P_{\boldsymbol{b}} = P_{\boldsymbol{b}_1} + P_{\boldsymbol{b}_2}$. In other words, $P_{\boldsymbol{b}}$ cannot be written as a Minkowski sum of two fibers $P_{\boldsymbol{b}_1}$ and $P_{\boldsymbol{b}_2}$ where $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ are strictly smaller than $\boldsymbol{b}$.*

The following is a consequence of Algorithm 5.8 and has applications in integer programming.

Theorem 5.12. *Let $\mathcal{A} = [\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t] \in \mathbb{N}^{n\times t}$ and let π be the associated map. Then there are finitely many atomic fibers of π.*

Proof. Suppose that we compute all initial ideals of the toric ideal $I_{\mathcal{A}}$ and compute the generators of $C_{S_1,\ldots,S_k}$'s as in step 4 of Algorithm 5.8. With the notation of Theorem 5.7, these constitute the set $\cup_{(S_1,\ldots,S_k)} B_{S_1,\ldots,S_k}$. We will show that atomic fibers are contained in the finite set of fibers $\{P_{\boldsymbol{b}} : \boldsymbol{b} \in \cup_{(S_1,\ldots,S_k)} B_{S_1,\ldots,S_k}\}$. Suppose an atomic fiber $P_{\boldsymbol{b}}$ is not contained in this set. Then by the proof of Theorem 5.7, there is a $\boldsymbol{b}_p$ in $\cup_{(S_1,\ldots,S_k)} B_{S_1,\ldots,S_k}$ where $\boldsymbol{b} \neq \boldsymbol{b}_p$ and $\boldsymbol{b}_p \leq \boldsymbol{b}$ such that for *any* weight vector $\boldsymbol{w}$ the optimal solution to $\mathrm{IP}^{\boldsymbol{w}}_{\mathcal{A}}(\boldsymbol{b})$ is the sum of the optimal solutions of $\mathrm{IP}^{\boldsymbol{w}}_{\mathcal{A}}(\boldsymbol{b}_p)$ and $\mathrm{IP}^{\boldsymbol{w}}_{\mathcal{A}}(\boldsymbol{b} - \boldsymbol{b}_p)$. But this means $P_{\boldsymbol{b}} = P_{\boldsymbol{b}_p} + P_{(\boldsymbol{b}-\boldsymbol{b}_p)}$, contradicting the fact that $P_{\boldsymbol{b}}$ is an atomic fiber. □

As a corollary to Theorem 5.12 we obtain that there are *finitely* many facet directions which describe *all* $\boldsymbol{b}$-fibers $P_{\boldsymbol{b}}$ (see Theorem 17.4 in [7]). We state this corollary using *normal fans* of polytopes (for details see [12]). Recall that two polytopes P and Q are called *strongly isomorphic* if they have the same normal fans $\mathcal{N}(P)$ and $\mathcal{N}(Q)$. Strong isomorphism is obviously an equivalence relation.

Corollary 5.13. *Given $\mathcal{A} = [\boldsymbol{a}_1, \ldots, \boldsymbol{a}_t] \in \mathbb{N}^{n\times t}$ and the associated map π, the fibers of π are partitioned into finitely many strong isomorphism classes. The number of these classes is at most 2^p where p is the number of atomic fibers of π.*

Proof. By Theorem 5.12 any $\boldsymbol{b}$-fiber can be written as a Minkowski sum of finitely many atomic fibers:

$$P_{\boldsymbol{b}} = \sum_{P_{\boldsymbol{b}'} \text{ atomic}} n_{\boldsymbol{b}'} P_{\boldsymbol{b}'}, \quad n_{\boldsymbol{b}'} \in \mathbb{N},$$

where $n_{\boldsymbol{b}'} P_{\boldsymbol{b}'}$ is the polytope obtained by taking the Minkowski sum of $P_{\boldsymbol{b}'}$ with itself $n_{\boldsymbol{b}'}$ times. This means that the normal fan of $P_{\boldsymbol{b}}$ is $\bigcap_{n_{\boldsymbol{b}'} \neq 0} \mathcal{N}(P_{\boldsymbol{b}'})$. Therefore $\mathcal{N}(P_{\boldsymbol{b}})$ has to be one of the possible 2^p normal fans. □

Example 5.14. *Atomic fibers of the twisted cubic.*

Suppose $\mathcal{A}$ is the set of vectors in Example 5.9, i.e., $I_{\mathcal{A}}$ is the ideal of the twisted cubic in $\mathbf{P}^3$. There are 20 atomic fibers in this case and we list them together with the feasible points in each fiber.

Degree 3 :	$(3,0)$:	$(1,0,0,0)$
	$(2,1)$:	$(0,1,0,0)$
	$(1,2)$:	$(0,0,1,0)$
	$(0,3)$:	$(0,0,0,1)$
Degree 6 :	$(4,2)$:	$(1,0,1,0),(0,2,0,0)$
	$(3,3)$:	$(1,0,0,1),(0,1,1,0)$
	$(2,4)$:	$(0,1,0,1),(0,0,2,0)$
Degree 9 :	$(6,3)$:	$(2,0,0,1),(1,1,1,0),(0,3,0,0)$
	$(5,4)$:	$(1,1,0,1),(1,0,2,0),(0,2,1,0)$
	$(4,5)$:	$(1,0,1,1),(0,2,0,1),(0,1,2,0)$
	$(3,6)$:	$(1,0,0,2),(0,1,1,1),(0,0,3,0)$
Degree 12 :	$(8,4)$:	$(2,1,0,1),(2,0,2,0),(1,2,1,0),(0,4,0,0)$
	$(6,6)$:	$(2,0,0,2),(1,1,1,1),(1,0,3,0),(0,3,0,1),(0,2,2,0)$
	$(4,8)$:	$(1,0,1,2),(0,2,0,2),(0,1,2,1),(0,0,4,0)$
Degree 15 :	$(9,6)$:	$(3,0,0,2),(2,1,1,1),(2,0,3,0),(1,3,0,1),(1,2,3,0),(0,4,1,0)$
	$(8,7)$:	$(2,1,0,2),(2,0,2,1),(1,1,3,0),(1,2,1,1),(0,4,0,1),(0,3,2,0)$
	$(7,8)$:	$(2,0,1,2),(1,2,0,2),(1,1,2,1),(1,0,4,0),(0,3,1,1),(0,2,3,0)$
	$(6,9)$:	$(2,0,0,3),(1,1,1,2),(1,0,3,1),(0,3,0,2),(0,2,2,1),(0,1,4,0)$
Degree 18 :	$(12,6)$:	$(4,0,0,2),(3,1,1,1),(3,0,3,0),(2,3,0,1),(2,2,2,0),(1,4,0,1),(0,6,0,0)$
	$(6,12)$:	$(2,0,0,4),(1,1,1,3),(1,0,4,1),(1,0,3,2),(0,3,0,3),(0,2,2,2),(0,0,6,0)$

The atomic fibers provide strong SAGBI bases for monomial subalgebras over PID's.

Theorem 5.15. *Let $A = R[c_1x^{\boldsymbol{a}_1},\dots,c_tx^{\boldsymbol{a}_t}] \subseteq R[x_1,\dots,x_n]$ be a monomial subalgebra over a PID R. Let $\mathcal{A} = [\boldsymbol{a}_1,\dots,\boldsymbol{a}_t] \in \mathbb{N}^{n\times t}$ and let π be the associated map. Then $F = \{k_{\boldsymbol{b}}x^{\boldsymbol{b}} : P_{\boldsymbol{b}}$ is an atomic fiber$\}$ with $k_{\boldsymbol{b}} = gcd(c^{\boldsymbol{u}} : \boldsymbol{u} \in \pi^{-1}(\boldsymbol{b}))$ is a strong SAGBI basis for A. Moreover, if R has sufficiently many primes, then F is a minimal strong SAGBI basis, i.e., there exists a choice of coefficients $c_1,\dots,c_k$ such that no element of F is redundant.*

Proof. Since we can write any $\boldsymbol{b}$-fiber as a Minkowski sum of atomic fibers, and by the proof of Theorem 5.7 we obtain that F is a strong SAGBI basis. For the second claim, suppose that $I_{\mathcal{A}}$ has k distinct initial ideals $M_1,\dots,M_k$ with $M_j = \mathrm{Lt}_{\prec_{\boldsymbol{\omega}_j}}(I_{\mathcal{A}})$ for $\boldsymbol{\omega}_j \in \mathbb{N}^t$. Let $p_1,\dots,p_k$ be k distinct primes of R and let $c_i = \prod_{j=1}^k p_j^{\omega_{ji}}$, $i = 1,\dots,t$. We claim that F is a minimal strong SAGBI basis for $A = R[c_1x^{\boldsymbol{a}_1},\dots,c_tx^{\boldsymbol{a}_t}]$. Suppose a strictly smaller subset F' of F is a strong SAGBI basis, and let $k_{\boldsymbol{b}}x^{\boldsymbol{b}} \in F\backslash F'$. Then there must be a $k_{\boldsymbol{b}'}x^{\boldsymbol{b}'} \in F'$ such that $k_{\boldsymbol{b}}x^{\boldsymbol{b}} = (k_{\boldsymbol{b}'}x^{\boldsymbol{b}'})(k_{\boldsymbol{b}-\boldsymbol{b}'}x^{\boldsymbol{b}-\boldsymbol{b}'})$. This means the optimal solution to $\mathrm{IP}^j_{\mathcal{A}}(\boldsymbol{b})$ is the sum of the optimal solutions of $\mathrm{IP}^j_{\mathcal{A}}(\boldsymbol{b}')$ and $\mathrm{IP}^j_{\mathcal{A}}(\boldsymbol{b}-\boldsymbol{b}')$ for $j = 1,\dots,k$. But since we are considering *all* initial ideals of $I_{\mathcal{A}}$, $\mathcal{N}(P_{\boldsymbol{b}}) = \mathcal{N}(P_{\boldsymbol{b}'}) \cap \mathcal{N}(P_{\boldsymbol{b}-\boldsymbol{b}'})$, i.e., $P_{\boldsymbol{b}} = P_{\boldsymbol{b}'} + P_{\boldsymbol{b}-\boldsymbol{b}'}$. This is a contradiction since $P_{\boldsymbol{b}}$ is an atomic fiber. $\square$

Example 5.16. *A minimal strong SAGBI basis for the twisted cubic.*

$I_{\mathcal{A}}$ in Example 5.9 has eight initial ideals. A set of eight vectors which induce these initial ideals is as follows:

$$\begin{aligned} \boldsymbol{\omega}_1 &= (1,0,0,1) \\ \boldsymbol{\omega}_2 &= (1,0,1,1) \\ \boldsymbol{\omega}_3 &= (0,0,2,1) \\ \boldsymbol{\omega}_4 &= (0,1,3,2) \\ \boldsymbol{\omega}_5 &= (2,3,3,2) \\ \boldsymbol{\omega}_6 &= (2,3,1,0) \\ \boldsymbol{\omega}_7 &= (0,2,1,2) \\ \boldsymbol{\omega}_8 &= (3,2,0,0) \end{aligned}$$

Let $p_1,\dots,p_8$ be distinct prime numbers and consider the subalgebra

$$\mathbb{Z}[(p_1p_2p_5^2p_6^2p_8^3)x_1^3,\ (p_4p_5^3p_6^3p_7^2p_8^2)x_1^2x_2,\ (p_2p_3^2p_4^3p_5^3p_6p_7)x_1x_2^2,\ (p_1p_2p_3p_4^2p_5^2p_7^2)x_2^3]$$

of $\mathbb{Z}[x_1,x_2]$. Using the atomic fibers and the feasible points in these fibers from the previous example we obtain the minimal strong SAGBI basis for this subalgebra:

$$\begin{aligned} F = \{&(p_1p_2p_5^2p_6^2p_8^3)x_1^3,\ (p_4p_5^3p_6^3p_7^2p_8^2)x_1^2x_2,\ (p_2p_3^2p_4^3p_5^3p_6p_7)x_1x_2^2,\ (p_1p_2p_3p_4^2p_5^2p_7^2)x_2^3, \\ &(p_4^2p_5^5p_6^3p_7p_8^3)x_1^4x_2^2,\ (p_2p_3p_4^2p_5^4p_6^2p_7^2p_8^2)x_1^3x_2^3,\ (p_2p_3p_4^3p_5^5p_6^2p_7^2)x_1^2x_2^4,\ (p_4^2p_5^6p_6^4p_7^2p_8^5)x_1^6x_2^3, \\ &(p_2p_3p_4^3p_5^7p_6^4p_7^2p_8^3)x_1^5x_2^4,\ (p_2p_3p_4^4p_5^7p_6^3p_7^3p_8^2)x_1^4x_2^5,\ (p_2^2p_3^2p_4^4p_5^6p_6^2p_7^3)x_1^3x_2^6,\ (p_4^3p_5^9p_6^6p_7^2p_8^6)x_1^8x_2^4, \\ &(p_2p_3p_4^4p_5^8p_6^4p_7^3p_8^3)x_1^6x_2^6,\ (p_2^2p_3^2p_4^6p_5^9p_6^3p_7^4)x_1^4x_2^8,\ (p_2p_3p_4^4p_5^{10}p_6^6p_7^3p_8^6)x_1^9x_2^6,\ (p_2p_3p_4^5p_5^{11}p_6^6p_7^4p_8^5)x_1^8x_2^7, \\ &(p_2^2p_3^2p_4^6p_5^{11}p_6^5p_7^4p_8^3)x_1^7x_2^8,\ (p_2^2p_3^2p_4^6p_5^{10}p_6^4p_7^5p_8^2)x_1^6x_2^9,\ (p_4^4p_5^{12}p_6^8p_7^3p_8^9)x_1^{12}x_2^6,\ (p_2^3p_3^3p_4^8p_5^{12}p_6^4p_7^6)x_1^6x_2^{12}\}. \end{aligned}$$

Acknowledgement: We thank Bernd Sturmfels and Rekha Thomas for helpful discussions.

References

[1] W.W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases,* American Mathematical Society 1994, Providence.

[2] D. Bayer and I. Morrison, Gröbner bases and geometric invariant theory I, *Journal of symbolic computation* **6** (1988) 209–217.

[3] D. Bayer and D. Mumford, What can be computed in algebraic geometry?, in *Computational algebraic geometry and commutative algebra* [Eisenbud, D. and Robbiano, L, eds.], pp. 1–48, Cambridge University Press, Cambridge, 1993.

[4] T. Dachsel, *Ein Vervollständigungsverfahren zur Berechnung Kanonischer Basen für unitäre Unterringe von Polynomringen,* Diplomarbeit. Universität Kaiserslautern, 1990.

[5] S. Hoşten and R.R. Thomas, Standard pairs and group relaxations in integer programming, (1998) 20 pages.

[6] J. L. Miller, Analogs of Gröbner Bases in Polynomial Rings over a Ring, *Journal of Symbolic Computation* **21** (1996) 139–153.

[7] A. Schrijver, *Theory of Linear and Integer Programming,* Series in Discrete Mathematics 1986, Wiley-Interscience, New York.

[8] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, AMS University Lecture Series **8** 1995, Providence.

[9] B. Sturmfels and R.R. Thomas, Variations of cost functions in integer programming, *Mathematical Programming* **77** (1997) 357–387.

[10] B. Sturmfels, N. Trung and W. Vogel, Bounds on projective schemes, *Math. Ann.* **302** (1995) 417–432.

[11] R.R. Thomas, A geometric Buchberger algorithm for integer programming, *Mathematics of Operations Research* **20** (1995) 864–884.

[12] G. Ziegler, *Lectures on Polytopes*, Graduate Text in Mathematics, Springer-Verlag 1995, New York.

University of Maryland, Department of Mathematics, College Park, MD 20740
E-mail address: `wwa@math.umd.edu`

George Mason University, Department of Mathematical Sciences, Fairfax, VA 22030
E-mail address: `shosten@gmu.edu`

Systems Planning and Analysis, Inc, Alexandria, VA 22311
E-mail address: `ploustau@spa.com`

Western Kentucky University, Department of Mathematics, Bowling Green, KY 42101
E-mail address: `lyn.miller@wku.edu`