Saturations of Subalgebras, SAGBI Bases, and U-invariants

Anna Maria Bigatti

Dip. di Matematica, Università degli Studi di Genova, Via Dodecaneso 35, I-16146 Genova, Italy

Lorenzo Robbiano

Dip. di Matematica, Università degli Studi di Genova, Via Dodecaneso 35, I-16146 Genova, Italy

Abstract

Given a polynomial ring P over a field K, an element $g \in P$, and a K-subalgebra S of P, we deal with the problem of saturating S with respect to g, i.e. computing $\mathrm{Sat}_g(S) = S[g, g^{-1}] \cap P$. In the general case we describe a procedure/algorithm to compute a set of generators for $\mathrm{Sat}_g(S)$ which terminates if and only if it is finitely generated. Then we consider the more interesting case when S is graded. In particular, if S is graded by a positive matrix W and g is an indeterminate, we show that if we choose a term ordering σ of g-`DegRev` type compatible with W, then the two operations of computing a σ-SAGBI basis of S and saturating S with respect to g commute. This fact opens the doors to nice algorithms for the computation of $\mathrm{Sat}_g(S)$. In particular, under special assumptions on the grading one can use the truncation of a σ-SAGBI basis and get the desired result. Notably, this technique can be applied to the problem of directly computing some U-invariants, classically called semi-invariants, even in the case that K is not the field of complex numbers.

Key words: Subalgebra saturation, SAGBI bases, CoCoA, U-invariants
1991 MSC: [2010] 13P10, 08A30, 13-04, 14R20, 68W30

1. Introduction

This paper has two main ancestors. Our attention to the problem discussed here was drawn by a nice discussion with Claudio Procesi about the paper [7] where the following claim is made: *If we want to understand U-invariants from these formulas it is necessary*

Email addresses: `bigatti@dima.unige.it` (Anna Maria Bigatti), `robbiano@dima.unige.it` (Lorenzo Robbiano).

[1] This research was partly supported by the "National Group for Algebraic and Geometric Structures, and their Applications" (GNSAGA-INdAM).

to compute the intersection $S_n = \mathbb{C}[c_2, \dots, c_n][a_0, a_0^{-1}] \cap \mathbb{C}[a_0, \dots, a_n]$. Here $\mathbb{C}$ denotes the field of complex numbers, $a_0, \dots, a_n$ are indeterminates, and the formulas are expressions of the c_i given, for $i = 1, \dots, 6$, as follows:

$$
\begin{aligned}
c_2 &= -a_1^{[2]} + a_0a_2 \\
c_3 &= 2a_1^{[3]} - a_0a_1a_2 + a_0^2a_3 \\
c_4 &= -3a_1^{[4]} + a_0a_1^{[2]}a_2 - a_0^2a_1a_3 + a_0^3a_4 \\
c_5 &= 4a_1^{[5]} - a_0a_1^{[3]}a_2 + a_0^2a_1^{[2]}a_3 - a_0^3a_1a_4 + a_0^4a_5 \\
c_6 &= -5a_1^{[6]} + a_0a_1^{[4]}a_2 - a_0^2a_1^{[3]}a_3 + a_0^3a_1^{[2]}a_4 - a_0^4a_1a_5 + a_0^5a_6
\end{aligned}
$$

where $\alpha^{[i]}$ means $\frac{1}{i!}\alpha^i$. In version 1 of [7] the theoretical background for this claim was fully explained and in its Section 3.5 a sketch of an algorithm to compute S_n was illustrated. In version 3 of [7] the authors dropped the section about the algorithm and wrote: *A general algorithm for these types of problems has been in fact developed by Bigatti-Robbiano in a recent preprint*, referring to the first arXiv version of this paper.

Why are the elements of S_n called U-invariants? A detailed explanation can be found in [7]. For the sake of completeness, let us summarise it here.

Let $\mathbb{C}[x]_{\leq n}$ denote the vector space of polynomials in $\mathbb{C}[x]$ of degree $\leq n$. The algebra S_n of U-invariants of polynomials of degree n, is the subalgebra of the algebra of polynomial functions on $\mathbb{C}[x]_{\leq n}$ which are invariant under the action of $(\mathbb{C}, +)$ defined by $p(x) \to p(x + \lambda)$ for $\lambda \in \mathbb{C}$. Now let $\mathbb{HC}[x, y]_n$ denote the vector space of homogeneous polynomials in $\mathbb{C}[x, y]$ of degree n, and let $U = \{\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)\}$, the unipotent subgroup of $\mathrm{SL}(2, \mathbb{C})$. We can identify $\mathbb{C}[x]_{\leq n}$ with $\mathbb{HC}[x, y]_n$, and then the action of $(\mathbb{C}, +)$ can be identified with the action of U on the algebra of polynomial functions on $\mathbb{HC}[x, y]_n$.

For example, let $f(x) = a_0\frac{x^2}{2} + a_1x + a_2 \in \mathbb{C}[x]_{\leq 2}$ and compute $f(x + \lambda)$.

$$
f(x+\lambda) \;=\; a_0\tfrac{(x+\lambda)^2}{2} + a_1(x+\lambda) + a_2 \;=\; a_0\tfrac{x^2}{2} + (a_0\lambda + a_1)x + (a_0\tfrac{\lambda^2}{2} + a_1\lambda + a_0)\,.
$$

Then consider $c_2 = -a_1^{[2]} + a_0a_2 = -\frac{a_1^2}{2} + a_0a_2$ (as above), and compute the new c_2 relative to the coefficients of $f(x + \lambda)$. We get $-\frac{(a_0\lambda+a_1)^2}{2} + a_0(a_0\frac{\lambda^2}{2} + a_1\lambda + a_2)$ which is equal to c_2 for every $\lambda \in \mathbb{C}$, proving that c_2 is a U-invariant.

The first motivation for our investigation is that the problem of computing a set of generators of $S_n = \mathbb{C}[c_2, \dots, c_n][a_0, a_0^{-1}] \cap \mathbb{C}[a_0, \dots, a_n]$ can be viewed as a special case of the following task.

Problem 1.1. *Given a field K, a polynomial ring $P = K[a_0, a_1, \dots, a_n]$, and polynomials $g_1, \dots, g_r \in P$, let S denote the subalgebra $K[g_1, \dots, g_r]$ of P, and let $g \in P \backslash \{0\}$. The problem is to compute generators of the K-algebra $S[g, g^{-1}] \cap P$.*

The second motivation for taking on this challenge is the evidence of the analogy with the standard problem in computer algebra of computing the saturation of an ideal. The analogy is clearly explained by recalling that the saturation of an ideal $I \subseteq P$ with respect to g is the ideal $IP[g^{-1}] \cap P$. How to compute the saturation of an ideal with respect to an element in P and also with respect to another ideal is well-understood and its solutions are described in the literature (see for instance [8, Section 3.5.B] and [9, Sections 4.3 and 4.4]) and implemented in most computer algebra systems.

On the other hand, the main problem formulated above has not received the same attention. In this paper we describe a solution if the algebra $\mathrm{Sat}_g(S) = S[g, g^{-1}] \cap P$ is finitely generated. As suggested by Gregor Kemper, a similar description is contained in [4, Semi-algorithm 4.10.16].

Then we present algorithms removing redundant generators of $\mathrm{Sat}_g(S)$. A strategy is to use elimination techniques, another strategy is to make a good use of SAGBI bases. The acronym SAGBI stands for "Subalgebra Analog to Gröbner Bases for Ideals". The theory of SAGBI bases was introduced by Robbiano and Sweedler in [11] and independently by Kapur and Madlener in [6]. Since then many improvements and applications were discovered (see for instance [3]). A more modern approach is contained in [9, Section 6.6], and [14, Chapter 11], and a nice survey is described in [2]. In [13] there are results somehow related to this paper.

In the case $\mathrm{Sat}_g(S)$ is not finitely generated, the algorithms turns out to be merely procedures providing a sequence of algebras ever closer to $\mathrm{Sat}_g(S)$. We show that this phenomenon can happen (see Examples 3.14 and 5.3), which is not a surprise, since there are even examples of finitely generated subalgebras of a polynomial ring whose intersection is not finitely generated (see for instance [10]).

We observe that our solutions do not require any assumption about the base field K, and do not need that the polynomials $g_1, \dots g_r$ are homogeneous. However, if they are homogeneous we have better results in Sections 5, 6, 7, which make a clever use of SAGBI bases and are the core of our paper.

Now we give a more precise description of the content of the paper. The general setting is as follows. We are given a field K, a polynomial ring P over K, a K-subalgebra S of P, and an element $g \in P \backslash \{0\}$.

In Section 2 we introduce the notion of the saturation $\mathrm{Sat}_g(S)$ of S with respect to g. The main point is that if $g \in S$, then $\mathrm{Sat}_g(S) = S : g^\infty$ (see Definition 2.1), as shown in Proposition 2.4. Using this fact we can rephrase the main problem addressed in this paper (see Problem 1.1).

Section 3 provides a first solution. After recalling standard results in computer algebra (see Propositions 3.2 and 3.3) we prove Theorem 3.4 which shows how to add new elements to S in order to get closer to $\mathrm{Sat}_g(S)$. With the help of this result we prove Theorem 3.10 and Corollary 3.11. They provide the building blocks for Algorithm 3.12 which solves the problem if $\mathrm{Sat}_g(S)$ is finitely generated. If not, the algorithm does not terminate producing an infinite sequence of subalgebras ever closer to $\mathrm{Sat}_g(S)$. A case of $\mathrm{Sat}_g(S)$ not being a finitely generated K-algebra is shown in Example 3.14.

Algorithm 3.12 is largely inspired by the suggestion contained in [7] and similar to [4, Semi-algorithm 4.10.16].

At this point we describe methods for rewriting the computed generators of $\mathrm{Sat}_g(S)$. The first part of Section 4 recalls different procedures to reduce elements in a subalgebra and the second part generalises these techniques to combine reduction and saturation.

As anticipated, our problem shows different features when the subalgebra S is graded. Section 5 marks the beginning of the most original part of the paper by showing some good aspects of this setting. Nevertheless, even in the graded case there are examples of subalgebras whose saturation is not finitely generated (see Example 5.3).

After the first glimpse provided in the previous section into the theory of SAGBI bases, its full strength comes alive in the case of a graded subalgebra.

The first benefit from the assumption that our subalgebra S is positively graded is described in Section 6 where we show how to make a good use of a truncated SAGBI basis for minimalizing the generators of S (see Algorithm 6.2).

Then we come to the main novelties contained in Section 7. Given a grading defined by a positive matrix W and an indeterminate, say a_0, there are special term orderings called of a_0-`DegRev` type compatible with W (see Definition 7.1). If σ is one of these, its full power is shown in Theorem 7.2 which essentially says that the two operations of computing a σ-SAGBI basis of S and saturating S commute. Using this fact, if the subalgebra S has a finite σ-SAGBI basis, then the problem of saturating S with respect to a_0 is *essentially* solved, and not only we get a set of generators of $\mathrm{Sat}_{a_0}(S)$ but also its σ-SAGBI basis. Procedure 7.5 captures this idea, and some examples show its good behaviour (see for instance Examples 7.9 and 7.10). However, the reason why we said *essentially* is that currently we can only conjecture that the procedure is indeed an algorithm, *i.e.* terminates, whenever $\mathrm{Sat}_{a_0}(S)$ is finitely generated.

Finally, in Section 8 we come back to the beginning of the story and use our methods to compute U-invariants via the computation of the algebras S_n. The ideas developed in Section 7 frequently collide with the fact that computing a SAGBI basis can be very expensive. In many cases it is even not clear if it is finite or not. So, what about computing a truncated SAGBI basis, as described in Section 6? The problem is that the saturation of a polynomial with respect to a_0 lowers its degree unless $\deg(a_0) = 0$, and unfortunately this condition cannot be paired with a term ordering of a_0-`DegRev` type. However, if the subalgebra S is graded also with respect to another grading with $\deg(a_0) > 0$, we are in business. And this is the case of U-invariants. Given a multi-grading of this special type and a term ordering of a_0-`DegRev` type compatible with it we have the nice Algorithm 8.4. The algebras S_3 and S_4 can be easily computed, and indeed we compute even a SAGBI basis of them together with a minimal set of generators. But when we come to S_5 and S_6 we need a bit of extra information which comes from the classical work, namely that the maximum weighted degree is 45 for both. The weighted degree is such that $\deg(a_0) = 0$, so it suffices to use Algorithm 8.4, truncating the computation in weighted degree 45. Once the truncated SAGBI basis is computed, we can use Algorithm 6.2 to get a minimal set of generators. To see some information about the computation of S_5 and S_6 see Examples 8.8 and 8.9.

All the examples described in the paper were computed on a MacBook Pro 2.9GHz Intel Core i7, using our implementation in CoCoA 5. Unless explicitly stated otherwise, we use the definitions and notation given in [8] and [9].

Acknowledgements

Thanks are due to Claudio Procesi who drew our attention to the problem. Moreover, the algorithm suggested in [7] was a source of inspiration for our work. Thanks are due to Hanspeter Kraft who took the job of checking that our results concerning U_5 (see Example 8.8) are in agreement with the classical knowledge. Special thanks are also due to Kraft and Procesi for modifying their paper by citing the preprint of this paper, as mentioned above. We are grateful to Gregor Kemper for pointing out the result contained in [4, Semi-algorithm 4.10.16]. Finally, we thank the referees for their careful reading and useful suggestions.

2. Basic Results

In this section we recall some basic definitions and results. In particular, we define the weak saturation and the saturation of a subalgebra of P with respect to an element, which allows us to rewrite the main problem described in the introduction (see Problem 1.1).

In the following we let K be a field, let $a_0, a_1, \dots, a_n$ be indeterminates, and let $P = K[a_0, a_1, \dots, a_n]$. The word *term* is a synonym of *power product* while the word *monomial* indicates a *power product multiplied by a coefficient*. Consequently, if σ is a term ordering and f is a polynomial, the symbols $\mathrm{LT}_\sigma(f)$, $\mathrm{LM}_\sigma(f)$, $\mathrm{LC}_\sigma(f)$ denote the leading term, the leading monomial, and the leading coefficient of f, so that we have $\mathrm{LM}_\sigma(f) = \mathrm{LC}_\sigma(f) \cdot \mathrm{LT}_\sigma(f)$. For the ideal generated by elements $g_1, \dots, g_r$ we use the notation $\langle g_1, \dots, g_r \rangle$.

For a polynomial $f \in P$ we write $\boldsymbol{f : g^\infty}$ to denote the **saturation of $\boldsymbol{f}$ with respect to $\boldsymbol{g}$**, i.e. the polynomial f/g^i, where g^i is the highest power of g which divides f. Given a subset $T \subseteq P$, the K-subalgebra of P generated by T is denoted by $\boldsymbol{K[T]}$.

We recall some definitions and properties from the context of ideals. Let I be an ideal in P, and $g \neq 0$ in P. We first recall the **colon ideal**, defined as $I : g = \{f \in P \mid g\, f \in I\}$. Notice that we naturally have that $I : g$ is an ideal, and $I \subseteq I : g$.

Then, we recall the **saturation of $\boldsymbol{I}$ with respect to the element $\boldsymbol{g}$**, defined as $I : g^\infty = \bigcup_{i \in \mathbb{N}} I : g^i$, and we also have $I : g^\infty = IP_g \cap P = IP[g^{-1}] \cap P$.

Next, we generalize the definitions above to the context of subalgebras, and we point out some properties which do not extend to this setting.

Definition 2.1. Let S be a K-subalgebra of the polynomial ring P, and let $g \neq 0$ in P.

(a) The subalgebra $\boldsymbol{S[g^{-1}] \cap P}$ is called the **weak saturation of $\boldsymbol{S}$ with respect to $\boldsymbol{g}$** and denoted by $\mathbf{wSat}_{\boldsymbol{g}}\boldsymbol{(S)}$.

(b) The subalgebra $\boldsymbol{S[g, g^{-1}] \cap P}$ is called the **saturation of $\boldsymbol{S}$ with respect to $\boldsymbol{g}$** and denoted by $\mathbf{Sat}_{\boldsymbol{g}}\boldsymbol{(S)}$.

(c) We denote the set $\{f \in P \mid g^i\, f \in S\}$ by $\boldsymbol{S : g^i}$ and the set $\bigcup_{i \in \mathbb{N}} S : g^i$ by $\boldsymbol{S : g^\infty}$.

Remark 2.2. Notice that $S \subseteq S : g$ if and only if $g \in S$. Thus, only in this case $S : g^i$ is an ascending chain of sets for increasing $j \in \mathbb{N}$. We also observe that $S = S : g^0 \subseteq S : g^\infty$.

The following example shows that in general $S : g$ and $S : g^\infty$ are not subalgebras.

Example 2.3. Let $P = \mathbb{Q}[a_0, a_1]$ and $S = \mathbb{Q}[a_0 a_1] \subseteq P$. Trivially, a_1 is in $S : a_0$, but its square a_1^2 is not in $S : a_0$ because $a_0 a_1^2 \notin S$.

Now consider $S = \mathbb{Q}[a_0^2 a_1] \subseteq P$. Then $a_0 a_1 \in S : a_0$, and $a_1 \in S : a_0^2$, thus they are in $S : a_0^\infty$, but their sum $a_0 a_1 + a_1$ is not in $S : a_0^\infty$ because $a_0^d(a_0 a_1 + a_1) \notin S$ for any $d \in \mathbb{N}$.

Next, we prove that if $g \in S$ then $S : g^\infty$ is a K-subalgebra of P, and $S : g^\infty$ is indeed the saturation of S with respect to g.

Proposition 2.4. *Let S be a K-subalgebra of P, and $g \neq 0$ in P.*

(a) We have $S : g^\infty \subseteq \mathrm{wSat}_g(S)$.

(b) We have $\mathrm{wSat}_g(\mathrm{wSat}_g(S)) = \mathrm{wSat}_g(S)$.

(c) If A is a K-subalgebra of P with $S \subseteq A \subseteq \mathrm{wSat}_g(S)$, then $\mathrm{wSat}_g(A) = \mathrm{wSat}_g(S)$.

(d) If $g \in S$ we have $S : g^\infty = \mathrm{wSat}_g(S) = \mathrm{Sat}_g(S)$.

Proof. To prove claim (a) we observe that for $f \in S : g^\infty$ there exists r such that $g^r f \in S$ hence $f = g^r f (g^{-1})^r \in S[g^{-1}] \cap P$.

To prove claim (b) it is clearly enough to show $\mathrm{wSat}_g(\mathrm{wSat}_g(S)) \subseteq \mathrm{wSat}_g(S)$. Let $f = \sum_{i=0}^d f_i g^{-i}$ with $f \in P$ and $f_i \in \mathrm{wSat}_g(S)$ for $i = 0, \ldots, d$. Then we have the equalities $f_i = \sum_{j_i=0}^{\delta_i} s_{j_i} g^{-j_i}$ with $f_i \in P$ for $i = 0, \ldots, \delta_i$ and $s_{j_i} \in S$ for $i = 0, \ldots, d$, $j_i = 0, \ldots, \delta_i$. Hence we have $f = \sum_{\substack{i=0,\ldots,d \\ j_i=0,\ldots,\delta_i}} s_{j_i} g^{-i-j_i}$, which shows that $f \in \mathrm{wSat}_g(S)$.

Let us prove claim (c). From the assumption $S \subseteq A \subseteq \mathrm{wSat}_g(S)$ we get the chain of inclusions $\mathrm{wSat}_g(S) \subseteq \mathrm{wSat}_g(A) \subseteq \mathrm{wSat}_g(\mathrm{wSat}_g(S))$, and the conclusion follows from claim (b).

Finally, we prove claim (d). The second equality is obvious, and from (a) we get the inclusion $S : g^\infty \subseteq \mathrm{wSat}_g(S)$. To conclude the proof, we need to show the inclusion $\mathrm{Sat}_g(S) \subseteq S : g^\infty$. An element $f \in S[g^{-1}] \cap P$ can be viewed as polynomial in g^{-1} with coefficients $s_i \in S$, hence it can be written as $f = \sum_{i=0}^d s_i g^{-i} = (\sum_{i=0}^d s_i g^{d-i})/g^d$. The assumption $g \in S$ implies that $f g^d = \sum_{i=0}^d s_i g^{d-i} \in S$, hence $f \in S : g^\infty$. $\square$

Example 2.3 shows that without the assumption $g \in S$, the set $S : g^\infty$ need not be a K-algebra, hence the inclusion in item (a) may be strict.

Under the light of these definitions and properties, we rephrase the problem stated in the introduction (see Problem 1.1) with the extra assumption that $g \in S \setminus \{0\}$.

Problem 2.5. *Given a field K, a polynomial ring $P = K[a_0, a_1, \ldots, a_n]$, and polynomials $g_1, \ldots, g_r \in P$, let S denote the subalgebra $K[g_1, \ldots, g_r]$ of P, and let $g \in S \setminus \{0\}$. The problem is to compute a set of generators of $S : g^\infty$.*

The assumption that g is an element of S can be weakened as shown by the following proposition.

Proposition 2.6. *Let S be a K-subalgebra of P, let $g \in P \backslash \{0\}$, and let $f(z) \in K[z] \backslash K$. If $f(g) \in S$ then* $\mathrm{wSat}_g(S) = \mathrm{Sat}_g(S[g]) = S[g] : g^\infty$.

Proof. The second equality trivially follows from Proposition 2.4.(d) because $g \in S[g]$. Let us prove $\mathrm{wSat}_g(S) = \mathrm{Sat}_g(S[g])$ using induction on $\deg(f(z))$. If $\deg(f(z)) = 1$, *i.e.* $f(z) = c_1 z + c_0$, clearly $g = (c_1)^{-1} \cdot (f(g) - c_0) \in S$, hence the claim follows from Proposition 2.4.(d). Then assume that if a K-subalgebra A of P contains $f(g)$ with $\deg(f(z)) < d$ then $\mathrm{wSat}_g(A) = \mathrm{Sat}_g(A[g])$.

Now, we let $f(g) \in S$ with $\deg(f(z)) = d$, *i.e.* $f(z) = \sum_{i=0}^d c_i z^i$ with $c_d \neq 0$, and we let $\tilde{f}(z) = \sum_{i=1}^d c_i z^{i-1}$, thus $g \cdot \tilde{f}(g) = f(g) - c_0 \in S$, in other words, $\tilde{f}(g) \in S : g^\infty$. Then, by Proposition 2.4.(a) it follows that $\tilde{f}(g) \in \mathrm{wSat}_g(S)$, therefore we define $A = S[\tilde{f}(g)]$ and we have $S \subseteq A \subseteq \mathrm{wSat}_g(S)$. Consequently, by Proposition 2.4.(c),

$$\mathrm{wSat}_g(A) = \mathrm{wSat}_g(S) \qquad (*)$$

On the other hand, from $\deg(\tilde{f}(z)) = d - 1$ and the inductive assumption we get the equalities $\mathrm{wSat}_g(A) = \mathrm{Sat}_g(A[g])$. From the obvious equality $A[g] = S[\tilde{f}(g)][g] = S[g]$ we get $\mathrm{wSat}_g(A) = \mathrm{Sat}_g(S[g])$ which, combined with $(*)$, concludes the proof. $\square$

3. The General Case

In this section we tackle Problem 2.5. We start with the following theorem which shows how to add new generators to a subalgebra of P in order to get closer to its saturation. The theorem uses generators of $\mathrm{Rel}_{\mathbf{g}}(g_1, \ldots, g_r)$ (see Definition 3.1) which can be effectively computed according to Proposition 3.2.

3.1. Ideal of Relations and Subalgebra Membership

The following K-algebra homomorphisms will be used systematically throughout the paper. Let $S = K[g_1, \ldots, g_r] \subseteq P = K[a_0, \ldots, a_n]$ and let $g \in P$. We will use the homomorphism **ev**: $K[x_1, \ldots, x_r] \longrightarrow P$, defined by $\mathrm{ev}(x_i) = g_i$, and the canonical homomorphism $\boldsymbol{\pi_g}$: $P \longrightarrow P/\langle g\rangle$. The fundamental notion of an ideal of relations is recalled.

Definition 3.1. The kernel of the composition $\pi_g \circ \mathrm{ev}$ is called the **ideal of relations of $\boldsymbol{g_1, \ldots, g_r}$ modulo $\boldsymbol{g}$** and is denoted by $\mathbf{Rel_g(\boldsymbol{g_1, \ldots, g_r})}$.

In the following proposition we show how to compute $\mathrm{Rel}_g(g_1, \ldots, g_r)$ using an elimination ideal. We recall the following propositions using new indeterminates $y_1, \ldots, y_m$ to emphasize that they are quite general.

Proposition 3.2 (Computing $\mathbf{Rel_g}$).
Let g, $g_1, \ldots, g_r \in K[y_1, \ldots, y_m]$. Then let $Q = K[x_1, \ldots, x_r, y_1, \ldots, y_m]$, and define the ideal $J = \langle g,\, x_1 - g_1, \ldots, x_r - g_r\rangle \subseteq Q$.

(a) We have the equality $\mathrm{Rel}_g(g_1, \ldots, g_r) = J \cap K[x_1, \ldots, x_r]$.

(b) Let G be the reduced σ-Gröbner basis of J where σ is an elimination ordering for $\{y_1, \ldots, y_m\}$. Then we have $\mathrm{Rel}_g(g_1, \ldots, g_r) = \langle G \cap K[x_1, \ldots, x_r]\rangle$.

Proof. See [8, Proposition 3.6.2]. □

We will also need to test subalgebra membership. A method for checking it is recalled here.

Proposition 3.3 (Subalgebra Membership Test).
Let $g_1, \ldots, g_r \in K[y_1, \ldots, y_m]$. Then let $Q = K[x_1, \ldots, x_r, y_1, \ldots, y_m]$, and define the ideal $J = \langle x_1 - g_1, \ldots, x_r - g_r\rangle \subseteq Q$. Finally, let $S = K[g_1, \ldots, g_r] \subseteq K[y_1, \ldots, y_m]$.

Then a polynomial $f \in K[y_1, \ldots, y_m]$ is such that $f \in S$ if and only if we have $\mathrm{NF}_{\sigma,J}(f) \in K[x_1, \ldots, x_r]$ where σ is an elimination ordering for $\{y_1, \ldots, y_m\}$. In this case, if we let $h = \mathrm{NF}_{\sigma,J}(f)$, then $f = h(g_1, \ldots, g_r)$ is an explicit representation of f as an element of S.

Proof. See [8, Corollary 3.6.7]. □

We are ready to prove the first theorem of this paper.

Theorem 3.4. *Let $g_1, \ldots, g_r \in P = K[a_0, a_1, \ldots, a_n]$, let $S = K[g_1, \ldots, g_r]$, and let $\mathbf{g} \in S\backslash\{0\}$. Then let $\{H_1, \ldots, H_t\}$ be a set of generators of the ideal $\mathrm{Rel}_{\mathbf{g}}(g_1, \ldots, g_r)$, and finally let $\tilde{h}_i = H_i(g_1, \ldots, g_r)/\mathbf{g}$ and $h_i = H_i(g_1, \ldots, g_r) : \mathbf{g}^\infty$ for $i = 1, \ldots, t$. We have*

$$S \subseteq K[S : \mathbf{g}] = K[g_1, \ldots, g_r, \tilde{h}_1, \ldots, \tilde{h}_t] \subseteq K[g_1, \ldots, g_r, h_1, \ldots, h_t] \subseteq S : \mathbf{g}^\infty$$

Proof. The first inclusion follows from Remark 2.2.

Now we prove the inclusion $K[S:\mathbf{g}] \subseteq K[g_1,\dots,g_r,\tilde{h}_1,\dots,\tilde{h}_t]$. If $f \in S:\mathbf{g}$ we deduce that $\mathbf{g}f \in K[g_1,\dots,g_r]$, hence there is a polynomial $F \in K[x_1,\dots,x_r]$ such that we have $\mathbf{g}f = F(g_1,\dots,g_r)$. This means that $F(x_1,\dots,x_r) \in \mathrm{Rel}_{\mathbf{g}}(g_1,\dots,g_r)$, thus F may be written as $\sum_{j=1}^{t} B_j H_j$ which implies $F(g_1,\dots,g_r) = \sum_{j=1}^{t} B_j(g_1,\dots,g_r)H_j(g_1,\dots,g_r) = \sum_{j=1}^{t} B_j(g_1,\dots,g_r)\mathbf{g}\tilde{h}_j$, and hence we have $\mathbf{g}f = F(g_1,\dots,g_r) = \sum_{j=1}^{t} B_j(g_1,\dots,g_r)\mathbf{g}\tilde{h}_j$. From this relation we deduce the equality $f = \sum_{j=1}^{t} B_j(g_1,\dots,g_r)\tilde{h}_j$.

Next we prove that $K[g_1,\dots,g_r,\tilde{h}_1,\dots,\tilde{h}_t] \subseteq K[S:\mathbf{g}]$. Firstly, $\mathbf{g}\,g_i \in S$ for every $i = 1,\dots,r$ since $\mathbf{g} \in S$. Moreover, we have $\mathbf{g}\tilde{h}_i = H_i(g_1,\dots,g_r) \in S$, hence also $\tilde{h}_i \in S:\mathbf{g}$ for $i = 1,\dots t$. Thus the inclusion is proved which concludes the proof of the equality $K[S:\mathbf{g}] = K[g_1,\dots,g_r,\tilde{h}_1,\dots,\tilde{h}_t]$.

The inclusion $K[g_1,\dots,g_r,\tilde{h}_1,\dots,\tilde{h}_t] \subseteq K[g_1,\dots,g_r,h_1,\dots,h_t]$ follows again from the assumption that $\mathbf{g} \in S$, and the last inclusion of the claim is clear since $S:\mathbf{g}^\infty$ is a K-algebra by Proposition 2.4.(b). $\square$

The following example shows that if $\mathbf{g} \notin S$ then $S \subseteq K[S:\mathbf{g}]$ may not hold, and $K[S:\mathbf{g}]$ may not be a finitely generated K-algebra.

Example 3.5. Let $P = K[a_0,a_1]$, and let $\mathbf{g} = a_0$.

(a) Let $S = K[a_1]$. Then $S:a_0 = \{0\}$, hence $K[S:a_0] = K$.

(b) Let $S = K[a_0a_1]$. Then $K[S:a_0] = K[a_1, a_0a_1^2, a_0^2a_1^3,\dots,a_0^ia_1^{i+1},\dots] \subsetneq K[a_1,a_0a_1]$, and $S \not\subseteq K[S:a_0]$ since $a_0a_1 \notin K[S:a_0]$.

A straightforward consequence of Theorem 3.4 is an interesting independence of the set of generators of the ideal $\mathrm{Rel}_{\mathbf{g}}(g_1,\dots,g_r)$.

Corollary 3.6. *With the same assumptions of the theorem, let* $\{H_1',\dots,H_u'\}$ *be another set of generators of* $\mathrm{Rel}_{\mathbf{g}}(g_1,\dots,g_r)$, *and let* $\widetilde{h'}_i = H_i'(g_1,\dots g_r)/a_0$ *for* $i = 1,\dots,u$. *Then we have* $K[g_1,\dots,g_r,\tilde{h}_1,\dots,\tilde{h}_t] = K[g_1,\dots,g_r,\widetilde{h'}_1,\dots,\widetilde{h'}_u]$.

Proof. The claim follows immediately from the theorem since both algebras are equal to the K-algebra $K[S:\mathbf{g}]$. $\square$

This independence does not hold if we substitute $\tilde{h}_i$ with h_i for $i = 1,\dots,t$, and likewise $\widetilde{h'}_i$ with h_i' for $i = 1,\dots,u$, as the following example shows. Please note that in all examples using $\mathbf{g} = a_0$ we identify $K[a_0,a_1,\dots,a_n]/\langle a_0\rangle$ with $K[a_1,\dots,a_n]$.

Example 3.7. Let $P = \mathbb{Q}[a_0,a_1,a_2]$, let $g_1 = a_1^2 - a_0^2a_2$, $g_2 = a_1a_2 - a_0$, $g_3 = a_2^2$, $g_4 = a_1a_2^2$, $\mathbf{g} = a_0$, and $S = \mathbb{Q}[g_1,g_2,g_3,g_4,\mathbf{g}]$. Then we have $\pi_{\mathbf{g}}(g_1) = a_1^2$, $\pi_{\mathbf{g}}(g_2) = a_1a_2$, $\pi_{\mathbf{g}}(g_3) = a_2^2$, $\pi_{\mathbf{g}}(g_4) = a_1a_2^2$.

If we let $I = \mathrm{Rel}_{\mathbf{g}}(g_1,\dots,g_4,\mathbf{g}) \subseteq \mathbb{Q}[x_1,x_2,x_3,x_4,x_5]$ we get $I = \langle H_1,H_2,H_3\rangle$ where $H_1 = x_2^2 - x_1x_3$, $H_2 = x_1x_3^2 - x_4^2$, $H_3 = x_5$. Then it is also true that $I = \langle H_1,H_2',H_3\rangle$ where $H_2' = H_2 + x_3H_1 = x_2^2x_3 - x_4^2$.

Let $\tilde{h}_i = H_i(g_1, g_2, g_3, g_4, \mathbf{g})/\mathbf{g}$ and let $h_i = H_i(g_1, g_2, g_3, g_4, \mathbf{g}) : \mathbf{g}^\infty$ for $i = 1, 2, 3$. Similarly, let $\widetilde{h'}_2 = H'_2(g_1, g_2, g_3, g_4, \mathbf{g})/\mathbf{g}$, and $h'_2 = H'_2(g_1, g_2, g_3, g_4, \mathbf{g}) : \mathbf{g}^\infty$. We have

$$\begin{array}{ll}
\tilde{h}_1 = H_1(g_1, g_2, g_3, g_4, \mathbf{g})/\mathbf{g} = -2a_1a_2 + a_0(a_2^3 + 1) & h_1 = H_1(g_1, g_2, g_3, g_4, \mathbf{g}) : \mathbf{g}^\infty = \tilde{h}_1 \\
\tilde{h}_2 = H_2(g_1, g_2, g_3, g_4, \mathbf{g})/\mathbf{g} = -a_0a_2^5 & h_2 = H_2(g_1, g_2, g_3, g_4, \mathbf{g}) : \mathbf{g}^\infty = -a_2^5 \\
\widetilde{h'}_2 = H'_2(g_1, g_2, g_3, g_4, \mathbf{g})/\mathbf{g} = -2a_1a_2^3 + a_0a_2^2 & h'_2 = H'_2(g_1, g_2, g_3, g_4, \mathbf{g}) : \mathbf{g}^\infty = \widetilde{h'}_2 \\
\tilde{h}_3 = H_3(g_1, g_2, g_3, g_4, \mathbf{g})/\mathbf{g} = \mathbf{g}/\mathbf{g} = 1 & h_3 = H_3(g_1, g_2, g_3, g_4, \mathbf{g}) : \mathbf{g}^\infty = 1
\end{array}$$

According to Corollary 3.6 and these equalities we have

$$\mathbb{Q}[g_1, g_2, g_3, g_4, \mathbf{g}, h_1, h'_2] = \mathbb{Q}[g_1, g_2, g_3, g_4, \mathbf{g}, h_1, \tilde{h}_2] \tag{$*$}$$

Let us check it using Proposition 3.3. On the polynomial ring $\mathbb{Q}[x_1, \ldots, x_7, a_0, a_1, a_2]$ we introduce a term ordering σ of elimination for $\{a_0, a_1, a_2\}$, and we let

$$J_1 = \langle \mathbf{g},\ x_1 - g_1,\ x_2 - g_2,\ x_3 - g_3,\ x_4 - g_4,\ x_5 - \mathbf{g},\ x_6 - h_1,\ x_7 - h'_2 \rangle$$
$$J_2 = \langle \mathbf{g},\ x_1 - g_1,\ x_2 - g_2,\ x_3 - g_3,\ x_4 - g_4,\ x_5 - \mathbf{g},\ x_6 - h_1,\ x_7 - \tilde{h}_2 \rangle$$

We get $\mathrm{NF}_{\sigma,J_1}(\tilde{h}_2) = -x_3x_6 + x_7$ which means that $\tilde{h}_2 = -g_3h_1 + h'_2$ and hence we deduce that $\tilde{h}_2 \in \mathbb{Q}[g_1, g_2, g_3, g_4, \mathbf{g}, h_1, h'_2]$. We get $\mathrm{NF}_{\sigma,J_2}(h'_2) = x_3x_6 + x_7$ which means that $h'_2 = g_3h_1 + \tilde{h}_2$ and hence we deduce that $h'_2 \in \mathbb{Q}[a_0, g_1, g_2, g_3, g_4, h_1, \tilde{h}_2]$.

Finally, we claim that

$$\mathbb{Q}[g_1, g_2, g_3, g_4, \mathbf{g}, h_1, h'_2] \subsetneq \mathbb{Q}[g_1, g_2, g_3, g_4, \mathbf{g}, h_1, h_2]$$

The inclusion $\mathbb{Q}[g_1, g_2, g_3, g_4, \mathbf{g}, h_1, h'_2] \subseteq \mathbb{Q}[g_1, g_2, g_3, g_4, \mathbf{g}, h_1, h_2]$ follows from $(*)$ since clearly $\mathbb{Q}[g_1, g_2, g_3, g_4, \mathbf{g}, h_1, \tilde{h}_2] \subseteq \mathbb{Q}[g_1, g_2, g_3, g_4, \mathbf{g}, h_1, h_2]$. Finally, to check the claim we show that $h_2 \notin \mathbb{Q}[g_1, g_2, g_3, g_4, \mathbf{g}, h_1, h'_2]$. To do this we compute $\mathrm{NF}_{\sigma,J_1}(h_2) = -x_3^2a_2$, and the conclusion follows from Proposition 3.3.

3.2. *The general Algorithm*

Theorem 3.4 motivates the following definition.

Definition 3.8. Given a subalgebra $S = K[g_1, \ldots, g_r]$ of P, and $\mathbf{g} \in S \setminus \{0\}$, we denote by $\boldsymbol{E_{\mathbf{g}}(S)}$ the algebra $K[g_1, \ldots, g_r, h_1, \ldots, h_t]$ as described in Theorem 3.4. Then we let $\boldsymbol{E^0_{\mathbf{g}}(S)} = S$, and recursively $\boldsymbol{E^i_g(S)} = \boldsymbol{E_{\mathbf{g}}(E^{i-1}_{\mathbf{g}}(S))}$ for $i > 0$.

Remark 3.9. We observe that there is an abuse of notation since $E_{\mathbf{g}}(S)$ depends on the set of generators of S, as shown in Example 3.7. Moreover, we notice that the last inclusion of Theorem 3.4 can be read as $E_{\mathbf{g}}(S) \subseteq S : \mathbf{g}^\infty$.

We are ready to prove some fundamental results for our algorithm.

Theorem 3.10. *Let $P = K[a_0, a_1, \ldots, a_n]$, let $g_1, \ldots, g_r \in P$, let $S = K[g_1, \ldots, g_r]$, and $\mathbf{g} \in S \setminus \{0\}$. Then let A be a finitely generated K-subalgebra of P such that $S \subseteq A \subseteq S : \mathbf{g}^\infty$.*

(a) We have $K[S : \mathbf{g}^i] \subseteq E^i_{\mathbf{g}}(S) \subseteq S : \mathbf{g}^\infty$ for every $i \geq 0$.

(b) We have $S = E^0_{\mathbf{g}}(S) \subseteq E^1_{\mathbf{g}}(S) \subseteq \cdots \subseteq E^i_{\mathbf{g}}(S) \subseteq S : \mathbf{g}^\infty$ for every $i \geq 0$.

(c) We have $A:\mathbf{g}^\infty = S:\mathbf{g}^\infty$.
(d) If $A = E_\mathbf{g}(A)$ *then* $A = S:\mathbf{g}^\infty$.

Proof. For claim (a) we have to prove two inclusions. For the first inclusion it suffices to show $S:\mathbf{g}^i \subseteq E^i_\mathbf{g}(S)$ for $i > 0$. From Theorem 3.4 and Remark 3.9 we get $S:\mathbf{g} \subseteq E^1_\mathbf{g}(S)$. By induction we may assume that $S:\mathbf{g}^{i-1} \subseteq E^{i-1}_\mathbf{g}(S)$ and let $f \in P$ be such that $\mathbf{g}^i f \in S$. Then $\mathbf{g}f \in S:\mathbf{g}^{i-1} \subseteq E^{i-1}_\mathbf{g}(S)$ by induction, and hence $f \in E^{i-1}_\mathbf{g}(S):\mathbf{g} \subseteq E^i_\mathbf{g}(S)$ by Theorem 3.4 applied to the subalgebra $E^{i-1}_\mathbf{g}(S)$.

The second inclusion of claim (a) is true for $i = 0$. By induction we may assume that $E^{i-1}_\mathbf{g}(S) \subseteq S:\mathbf{g}^\infty$. Let $f \in E^i_\mathbf{g}(S)$. Since $E^i_\mathbf{g}(S) = E_\mathbf{g}(E^{i-1}_\mathbf{g}(S))$ there exists s such that $\mathbf{g}^s f \in E^{i-1}_\mathbf{g}(S) \subseteq S:\mathbf{g}^\infty$. Consequently, there exists t such that $\mathbf{g}^{s+t} f \in S$, and hence we get $f \in S:\mathbf{g}^\infty$.

Claim (b) follows from the definition of $E^i_\mathbf{g}(S)$ and claim (a).

Claim (c) follows from Proposition 2.4.(c),(d).

To prove claim (d) it suffices to show the inclusion $S:\mathbf{g}^\infty \subseteq A$. So let $f \in S:\mathbf{g}^\infty$ which means that there exists $i \in \mathbb{N}$ such that $\mathbf{g}^i f \in S$. If $i = 0$ we have $f \in S \subseteq A$. Using induction on i we may assume that $\mathbf{g}^{i-1} f \in S$ implies $f \in A$. From $\mathbf{g}^i f \in S$ we deduce $\mathbf{g}^{i-1}(\mathbf{g}f) \in S$, hence by induction we get $\mathbf{g}f \in A$. Consequently, we get $f \in A:\mathbf{g} \subseteq E_\mathbf{g}(A)$ by Theorem 3.4. By assumption we have $E_\mathbf{g}(A) = A$ hence $f \in A$ and the proof is complete. $\square$

From this theorem we deduce the following result.

Corollary 3.11. *Let* K *be a field, let* $P = K[a_0, a_1, \ldots, a_n]$*, let* $S{=}K[g_1, \ldots, g_r] \subseteq P$*, and let* $\mathbf{g} \in S\backslash\{0\}$*. The following conditions are equivalent.*
(a) The algebra $S:\mathbf{g}^\infty$ *is finitely generated.*
(b) There exists i such that $E^i_\mathbf{g}(S) = E^{i+1}_\mathbf{g}(S)$.
Moreover, if the two equivalent conditions are satisfied, then $S:\mathbf{g}^\infty = E^i_\mathbf{g}(S)$.

Proof. To show the implication $(a) \Rightarrow (b)$ we assume that $S:\mathbf{g}^\infty = K[h_1, \ldots, h_s]$ and let $m = \max_{i=1}^s \{i \mid \mathbf{g}^i h_j \in S \text{ for } j = 1, \ldots, s\}$. We deduce that $K[h_1, \ldots, h_s] \subseteq K[S:\mathbf{g}^m]$. By Theorem 3.10.(a) we have $K[S:\mathbf{g}^m] \subseteq E^m_\mathbf{g}(S)$, hence

$$S:\mathbf{g}^\infty = K[h_1, \ldots, h_s] \subseteq K[S:\mathbf{g}^m] \subseteq E^m_\mathbf{g}(S) \subseteq E^{m+1}_\mathbf{g}(S) \subseteq S:\mathbf{g}^\infty$$

which implies the equality $E^m_\mathbf{g}(S) = E^{m+1}_\mathbf{g}(S)$.

To show that $(b) \Rightarrow (a)$ it suffices to prove that $S:\mathbf{g}^\infty = E^i_\mathbf{g}(S)$ since $E^i_\mathbf{g}(S)$ is finitely generated by definition. We have the equality $E^i_\mathbf{g}(S) = E_\mathbf{g}(E^i_\mathbf{g}(S))$ by assumption, and hence $E^i_\mathbf{g}(S) = S:\mathbf{g}^\infty$ by Theorem 3.10.(d). $\square$

We are ready to describe an algorithm to compute a set of generators for $S:\mathbf{g}^\infty$, if it is finitely generated. If it is not, this procedure does not terminate, producing an infinite sequence of subalgebras ever closer to $S:\mathbf{g}^\infty$. Instances of $S:\mathbf{g}^\infty$ being not finitely generated are Example 3.14 and Example 5.3. A similar algorithm/procedure is contained in [4, Semi-algorithm 4.10.16]. In our case we can claim that it is an algorithm since we assume that $S:\mathbf{g}$ is finitely generated.

Algorithm 3.12. SUBALGEBRASATURATION

notation: $P = K[a_0, \dots, a_n]$ is a polynomial ring.
Input $S = K[g_1, \dots, g_r] \subseteq P$, and $\mathbf{g} \in S\backslash\{0\}$ such that $S : \mathbf{g}^\infty$ is finitely generated.
1 Let $S' = S$
2 *Main Loop:*
- **2.1** call $g'_1, \dots, g'_s$ the non-constant generators of S'
- **2.2** compute $\{H_1, \dots, H_t\}$, a set of generators of the ideal $\mathrm{Rel}_{\mathbf{g}}(g'_1, \dots, g'_s)$
- **2.3** for $j = 1, \dots, t$, let $h_j = H_j(g'_1, \dots, g'_s) : \mathbf{g}^\infty$
- **2.4** if $h_1, \dots, h_t \in S'$, i.e. if $E_{\mathbf{g}}(S') = S'$, then **return** $\boldsymbol{S'}$
- **2.5** redefine S' as $K[g'_1, \dots, g'_s, h_1, \dots, h_t]$

Output $S : \mathbf{g}^\infty$

Proof. Since $S : \mathbf{g}^\infty$ is finitely generated, correctness and termination follow immediately from Corollary 3.11. □

Remark 3.13. When $\mathbf{g}$ is indeed in the list G of the generators of the subalgebra S, say in position i, then x_i is in $\mathrm{Rel}_{\mathbf{g}}(G)$. Then $h_i = 1$ which trivially belongs to S. In the following examples we will use this fact sistematically.

The following example shows that the procedure may not terminate, and $S : a_0^\infty$ needs not be a finitely generated K-algebra.

Example 3.14. Let $P = \mathbb{Q}[a_0, a_1, a_2]$, let $\mathbf{g} = a_0$, $g_2 = a_1 - a_0 a_1^2$, $g_3 = a_2$, $g_4 = a_1 a_2$, and let $S = \mathbb{Q}[\mathbf{g}, g_2, g_3, g_4]$. Notice that $P/\langle \mathbf{g} \rangle \simeq \mathbb{Q}[a_1, a_2]$. Then we have $\pi_{\mathbf{g}}(g_2) = a_1$, $\pi_{\mathbf{g}}(g_3) = a_2$, $\pi_{\mathbf{g}}(g_4) = a_1 a_2$, hence $\mathrm{Rel}_{\mathbf{g}}(\mathbf{g}, g_2, g_3, g_4) = \langle x_1,\, x_4 - x_2 x_3 \rangle$. First, from $H_1 = x_1$ we have $h_1 = 1 \in S$ (as shown in Remark 3.13). Then, from $H_2 = x_4 - x_2 x_3$ we have $g_4 - g_2 g_3 = a_0(a_1^2 a_2)$ hence $h_2 = a_1^2 a_2$. Therefore, after the first loop, $E_{\mathbf{g}}(S) = \mathbb{Q}[a_0,\, a_1 - a_0 a_1^2,\, a_2,\, a_1 a_2,\, a_1^2 a_2]$. Inductively, we may assume that

$$E^i_{\mathbf{g}}(S) = \mathbb{Q}[a_0,\, a_1 - a_0 a_1^2,\, a_2,\, a_1 a_2,\, a_1^2 a_2, \dots, a_1^{i+1} a_2]$$

The only new relation in $\mathrm{Rel}_{\mathbf{g}}(\mathbf{g}, g_2, g_3, g_4, a_1^2 a_2, \dots, a_1^i a_2, a_1^{i+1} a_2)$ is $x_2 x_{i+3} - x_{i+4}$ and after the loop we get $a_1^{i+2} a_2$. The procedure does not stop, nevertheless we can conclude that

$$S : a_0^\infty = \mathbb{Q}[a_0,\, a_1 - a_0 a_1^2,\, a_2,\, a_1 a_2,\, a_1^2 a_2, \dots, a_1^{i+1} a_2, \dots]$$

hence it is not finitely generated.

Let us see an example where the procedure stops, hence it computes $S : a_0^\infty$.

Example 3.15. Let $P = \mathbb{Q}[a_0, a_1, a_2, a_3]$, let $\mathbf{g} = a_0$, $g_2 = a_1^2 - a_0 a_2$, $g_3 = a_1^3 - a_0 a_3$, and let $S = \mathbb{Q}[\mathbf{g}, g_2, g_3]$. We have $\pi_{\mathbf{g}}(g_2) = a_1^2$ and $\pi_{\mathbf{g}}(g_3) = a_1^3$, hence $\mathrm{Rel}_{\mathbf{g}}(\mathbf{g}, g_2, g_3) = \langle x_1,\, x_3^2 - x_2^3 \rangle$. We get $g_3^2 - g_2^3 = 3a_0 a_1^4 a_2 - 2a_0 a_1^3 a_3 - 3a_0^2 a_1^2 a_2^2 + a_0^2 a_3^2 + a_0^3 a_2^3$, hence $g_4 = a_1^4 a_2 - \frac{2}{3} a_1^3 a_3 - a_0 a_1^2 a_2^2 + \frac{1}{3} a_0 a_3^2 + \frac{1}{3} a_0^2 a_2^3$, and hence we deduce $E_{\mathbf{g}}(S) = K[\mathbf{g}, g_2, g_3, g_4]$, and indeed we can check that $g_4 \notin S$. Moreover, we have $\pi_{\mathbf{g}}(g_4) = a_1^4 a_2 - \frac{2}{3} a_1^3 a_3$ and

$\mathrm{Rel}_{\mathbf{g}}(\mathbf{g}, g_2, g_3, g_4) = \langle x_2^2 - x_1^3 \rangle$, so no new generator is created in Step 2.2 and the procedure stops in Step 2.3. The conclusion is that $S : a_0^\infty = K[\mathbf{g}, g_2, g_3, g_4]$.

Moreover, from the computation we deduce the equality $a_0 g_4 = \frac{1}{3}(g_3^2 - g_2^3)$ which gives an explicit proof of the fact that $g_4 \in S : a_0^\infty$.

Algorithm 3.12 comes as a direct application of the theory developed in Section 3, in particular Corollary 3.11. It is useful to improve it by using suitable rewriting procedures which we are going to describe in the next section.

4. Subalgebra Reduction, Interreduction, and Sat-Interreduction

We recall some definitions and facts from the theory of SAGBI bases. For a general introduction to this topic see [9, Section 6.6]; here, we reshape its Definition 6.6.16 and adapt it for our purposes.

Definition 4.1. Let $P = K[a_0, \ldots, a_n]$ with term-ordering σ. Let $G = \{g_1, \ldots, g_r\}$, where all g_i's are monic polynomials in P, and let h be a non-zero polynomial in P. If $\mathrm{LT}_\sigma(h) \in K[\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_r)]$, and we have $\mathrm{LT}_\sigma(h) = \mathrm{LT}_\sigma(g_1)^{\alpha_1} \cdots \mathrm{LT}_\sigma(g_r)^{\alpha_r}$, then we let $h' = h - \mathrm{LC}_\sigma(h) \cdot g_1^{\alpha_1} \cdots g_r^{\alpha_r}$ and we say that the passage from h to h' is an $\boldsymbol{\mathcal{S}_{\mathrm{LT}}}$**-reduction step** for h.

The following is a running example for this section.

Example 4.2. Let $P = \mathbb{Q}[a_0, a_1, a_2]$, with $\mathbb{T}(a_0, a_1, a_2)$ ordered by σ, the term-ordering defined by the matrix $\begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$. Then, let $h = a_1 a_2^6 - 4a_0^5 a_1 a_2 + 4a_0^5 a_1^2 + a_0^6 a_2 + a_0^7$, and

$$g_1 = a_0, \quad g_2 = a_1 a_2 - a_1^2, \quad g_3 = a_2^2, \quad g_4 = a_1 a_2^2$$

We observe that all polynomials are monic and we have

$$\mathrm{LT}_\sigma(g_1) = a_0, \quad \mathrm{LT}_\sigma(g_2) = a_1 a_2, \quad \mathrm{LT}_\sigma(g_3) = a_2^2, \quad \mathrm{LT}_\sigma(g_4) = a_1 a_2^2, \quad \mathrm{LT}_\sigma(h) = a_1 a_2^6,$$

We observe that $\mathrm{LT}_\sigma(h) = \mathrm{LT}_\sigma(g_3)^2 \, \mathrm{LT}_\sigma(g_4)$. Hence we have an $\mathcal{S}_{\mathrm{LT}}$-reduction step $h' = h - g_3^2 g_4 = -4a_0^5 a_1 a_2 + 4a_0^5 a_1^2 + a_0^6 a_2 + a_0^7$.

Note that an $\mathcal{S}_{\mathrm{LT}}$-reduction step replaces $\mathrm{LT}_\sigma(h)$ with σ-smaller terms. Therefore, being σ a term ordering, a chain of LT-reduction steps must end in a finite number of steps. This motivates the following definitions.

Definition 4.3. Let $P = K[y_1, \ldots, y_m]$, and let σ be a term ordering on $\mathbb{T}(y_1, \ldots, y_m)$. Then let $G = \{g_1, \ldots, g_r\}$, where all g_i's are monic polynomials in P and let $0 \neq h \in P$.

(a) We say that h' is an $\boldsymbol{\mathcal{S}_{\mathrm{LT}}}$**-remainder** for h and denote it by $\mathcal{SR}_{\mathrm{LT}}(h, G)$, if there is a chain of $\mathcal{S}_{\mathrm{LT}}$-reduction steps from h to h', and $\mathrm{LT}_\sigma(h') \notin K[\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_r)]$.

(b) Let $h' = \mathcal{SR}_{\mathrm{LT}}(h, G)$. We may compute $\mathrm{LM}_\sigma(h') - \mathcal{SR}_{\mathrm{LT}}(h' - \mathrm{LM}_\sigma(h'), G)$, and repeat this process until we obtain a polynomial h'' such that no power-product in its support is in $K[\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_r)]$. We say that h'' is an $\boldsymbol{\mathcal{S}}$**-remainder** for h and denote it by $\mathcal{SR}(h, G)$.

Remark 4.4. Notice that, according to Definition 4.1, we may get different $\mathcal{SR}_{\mathrm{LT}}(h, G)$ and $\mathcal{SR}(h, G)$, depending on the way of representing $\mathrm{LT}_\sigma(h) = \mathrm{LT}_\sigma(g_1)^{\alpha_1} \cdots \mathrm{LT}_\sigma(g_r)^{\alpha_r}$.

This definition is a natural generalization of the remainder of the division algorithm in the context of polynomial ideal, but the difficult step here is to find the α_i giving the equality $\mathrm{LT}_\sigma(h) = \mathrm{LT}_\sigma(g_1)^{\alpha_1} \cdots \mathrm{LT}_\sigma(g_r)^{\alpha_r}$.

There are two strategies for doing this: elimination and toric ideals.

Remark 4.5. As described in Proposition 3.3 we may determine an explicit representation of $\mathrm{LT}_\sigma(h)$ as an element of $K[\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_r)]$ by defining the ideal $J = \langle x_1 - \mathrm{LT}_\sigma(g_1), \ldots, x_r - \mathrm{LT}_\sigma(g_r)\rangle$ in $K[x_1, \ldots, x_r, a_0, \ldots, a_n]$ and then computing $\tau = \mathrm{NF}_{\sigma,J}(\mathrm{LT}(h))$. It is easy to show that τ is a power-product, and, if $\tau = x_1^{\alpha_1} \cdots x_r^{\alpha_r}$ we have the desired exponents. Otherwise, if some a_i occurs in τ, we may conclude that $\mathrm{LT}_\sigma(h) \notin K[\mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_r)]$, *i.e.* there is no $\mathcal{S}_{\mathrm{LT}}$-reduction step for h.

The other strategy is by looking for a binomial $x_0 - \tau$ in the kernel of the map $\varphi : K[x_0, x_1, \ldots, x_r] \longrightarrow P$, defined by $\varphi(x_0) = \mathrm{LT}_\sigma(h)$ and $\varphi(x_i) = \mathrm{LT}_\sigma(g_i)$.

Again this may be computed by mimicking Proposition 3.2, but much more efficiently by computing the toric ideal $\mathrm{Rel}(\mathrm{LT}_\sigma(h), \mathrm{LT}_\sigma(g_1), \ldots, \mathrm{LT}_\sigma(g_r))$ as described for instance in [1], and using the following proposition.

Proposition 4.6. *Let $t_0, t_1, \ldots, t_r$ be power-products in P and $\varphi : K[x_0, x_1, \ldots, x_r] \longrightarrow P$ be the K-algebra homomorphism defined by $\varphi(x_i) = t_i$ for $i = 0, \ldots, r$. Then the following conditions are equivalent.*

(a) We have $t_0 \in K[t_1, \ldots, t_r]$.
(b) There exists a binomial $b \in \ker(\varphi)$ such that $x_0 \in \mathrm{Supp}(b)$.
(c) Given a finite set B of binomial generators of $\ker(\varphi)$, there exists a binomial $b \in B$ such that $x_0 \in \mathrm{Supp}(b)$. In this case, if $b = \pm(x_0 - \tau)$, then $t_0 = \tau(t_1, \ldots, t_r)$.

Proof. The implications $(c) \Rightarrow (b)$ and $(b) \Rightarrow (a)$ are clear.

Let us prove $(a) \Rightarrow (c)$. The multi-homogeneity of $K[t_1, \ldots, t_r]$ implies that the only way to have $t_0 \in K[t_1, \ldots, t_r]$ is to have an equality of type $t_0 = \prod_{i=1}^r t_i^{\alpha_i}$. This implies (b), *i.e.* $x_0 - \prod_{i=1}^r x_i^{\alpha_i} \in \ker(\varphi)$. Given $B = \{b_1, \ldots, b_t\}$, we get $x_0 - \prod_{i=1}^r x_i^{\alpha_i} = \sum_{i=1}^t f_i b_i$ with $f_i \in K[x_0, \ldots, x_r]$. By putting $x_1 = \cdots = x_r = 0$ in this relation we see that one of the b_i has to be either of type $\pm(x_0 - \prod_{i=1}^r x_i^{\beta_i})$, or of type $\pm(1 - \prod_{i=1}^r x_i^{\beta_i})$. The latter is excluded by the homogeneity of the generators of $\ker(\varphi)$, therefore the proof is complete. $\square$

Remark 4.7. There is an obvious but practically effective improvement of Proposition 4.6. Asking whether $t_0 \in K[t_1, \ldots, t_r]$ is equivalent to asking whether $t_0 \in K[T]$ where $T = \{t_i \mid t_i \text{ divides } t_0\}$.

Example 4.8. (Example 4.2, continued)
Let $P = \mathbb{Q}[a_0, a_1, a_2]$, σ, g_i and h as in Example 4.2. After the first $\mathcal{S}_{\mathrm{LT}}$-reduction step we got $h' = h - g_3^2 g_4 = -4a_0^5 a_1 a_2 + 4a_0^5 a_1^2 + a_0^6 a_2 + a_0^7$.

Now, $\mathrm{LT}_\sigma(h') = a_0^5 a_1 a_2 = \mathrm{LT}_\sigma(g_1)^5\, \mathrm{LT}_\sigma(g_2)$ gives us a following $\mathcal{S}_{\mathrm{LT}}$-reduction step: $h'' = h' + 4g_1^5 g_2 = a_0^6 a_2 + a_0^7$, whose leading term cannot be further reduced. Therefore $\mathcal{SR}_{\mathrm{LT}}(h, G) = h'' = a_0^6 a_2 + a_0^7$.

Setting apart its leading monomial, we can now consider $\tilde{h} = h'' - \mathrm{LM}_\sigma(h'')$, and we see that $\tilde{h} = \mathrm{LT}_\sigma(g_1)^7 = g_1^7$, therefore $\mathcal{SR}_{\mathrm{LT}}(\tilde{h}, G) = 0$. In conclusion, $\mathcal{SR}(h, G) = a_0^6 a_2$.

We recall from Definition 3.8 that $E_{\mathbf{g}}(A)$ is obtained by adding new generators to those of the algebra A. Now we investigate on how, using $\mathcal{S}$-remainders, we can find a new set of generators for $E_{\mathbf{g}}(A)$ or, even better, a set of polynomials generating an algebra B such that $E_{\mathbf{g}}(A) \subseteq B \subseteq A : a_0^\infty$

Proposition 4.9. *Let $P = K[a_0, a_1, \ldots, a_n]$, with term ordering σ on $\mathbb{T}^{n+1}$, and let $S = K[g_1, \ldots, g_r]$, with $g_i \in P$, and $\mathbf{g} \in S \setminus \{0\}$. Let $g_i' = \mathcal{SR}(g_i, \{g_1, \ldots, \hat{g}_i, \ldots, g_r\})$, then*

$$S \ \subseteq \ K[g_1, \ldots, g_i' : \mathbf{g}^\infty, \ldots g_r] \ \subseteq \ S : \mathbf{g}^\infty$$

Proof. From the definition of $\mathcal{S}$-remainder it is clear that $S = K[g_1, \ldots, g_i', \ldots g_r]$, Then the assumption $\mathbf{g} \in S$ implies the inclusion $K[g_1, \ldots, g_i', \ldots g_r] \subseteq K[g_1, \ldots, g_i' : \mathbf{g}^\infty, \ldots g_r]$, and the conclusion follows. $\square$

Definition 4.10. Let $P = K[a_0, a_1, \ldots, a_n]$, with term ordering σ, and $S = K[g_1, \ldots, g_r]$, where all g_i's are monic polynomials in P. Repeating the substitution described in Proposition 4.9 until no more $\mathcal{S}$-reductions and saturations are possible, we obtain a set of sat-$\mathcal{S}$-interreduced generators of a K-algebra A such that $S \subseteq A \subseteq S : a_0^\infty$.

We denote such A by $\mathbf{Sat}\boldsymbol{\mathcal{SI}(S)}$, and again, as in Definition 3.8, there is an abuse of notation since $\mathrm{Sat}\mathcal{SI}(S)$ depends on the set of generators of S and also on the steps of reduction.

The following easy example illustrates this definition.

Example 4.11. Let $P = K[a_0, a_1, a_2]$ with `DegRevLex`. Let $S = K[a_0,\ a_1,\ a_0 a_2^2 - a_1]$, then $\mathrm{Sat}\mathcal{SI}(S) = K[a_0,\ a_1,\ a_2^2] = S : a_0^\infty$.

In general, the set of interreduced generators is obtained after more than one iteration through the generators.

Example 4.12. (Examples 4.2 and 4.8 continued)
As in Example 4.2. we let $P = \mathbb{Q}[a_0, a_1, a_2]$, with $\mathbb{T}(a_0, a_1, a_2)$ ordered by σ, the term-ordering defined by the matrix $\left(\begin{smallmatrix} 1 & 1 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{smallmatrix}\right)$. Let $g_1 = a_0,\ g_2 = a_1 a_2 - a_1^2,\ g_3 = a_2^2$, $g_4 = a_1 a_2^2$, let $g_5 = h = a_1 a_2^6 - 4a_0^5 a_1 a_2 + 4a_0^5 a_1^2 + a_0^6 a_2 + a_0^7$, and let $A = K[g_1, g_2, g_3, g_4, g_5]$.

Notice that $\mathrm{LT}(g_1) < \mathrm{LT}(g_2) < \mathrm{LT}(g_3) < \mathrm{LT}(g_4) < \mathrm{LT}(g_5)$, thus g_i may be reduced only by the g_j's with $j < i$. The only one which may be reduced is g_5, and we computed $\mathcal{SR}(h, G) = a_0^6 a_2$ (see Example 4.8), whose saturation is a_2.

Then, we re-sort and re-number the g_i's:

$$g_1 = a_0, \quad g_2 = a_2, \quad g_3 = a_1 a_2 - a_1^2, \quad g_4 = a_2^2, \quad g_5 = a_1 a_2^2\ .$$

Now, we see that g_4 can be $\mathcal{S}$-reduced to 0 using g_2, and g_5 can be $\mathcal{S}$-reduced to $a_1^2 a_2$ using $g_2 g_3$. Re-sorting and re-numbering again, we have

$$g_1 = a_0, \quad g_2 = a_2, \quad g_3 = a_1 a_2 - a_1^2, \quad g_4 = a_1^2 a_2\ .$$

In conclusion we have $\mathrm{Sat}\mathcal{SI}(A) = k[a_0,\ a_2,\ a_1 a_2 - a_1^2,\ a_1^2 a_2]$. Moreover, it is easy to see that $\mathrm{Sat}\mathcal{SI}(A) = A : a_0^\infty$.

As said, the process of sat-interreducing the generators of a subalgebra of P can improve the subsequent steps of the computation of $\mathrm{Rel}_{\mathbf{g}}$. But we cannot hope that it substitutes such computation, as the following example shows.

Example 4.13. Let $P = \mathbb{Q}[a_0, a_1, a_2]$, with $\mathbb{T}(a_0, a_1, a_2)$ ordered by σ, the term-ordering defined by the matrix $\left(\begin{smallmatrix} 1 & 1 & 1 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{smallmatrix}\right)$. Let $G = \{\mathbf{g}, g_2, g_3, g_4\}$ where $\mathbf{g} = a_0,\ g_2 = a_1a_2 - a_0a_1 + a_0a_2,\ g_3 = a_1^2 - a_2^2 + a_0a_1,\ g_4 = a_1^3 - a_0a_2^2$, and $S = K[G]$.

Then $\mathrm{Rel}_{\mathbf{g}}(G) = \langle x_1,\ x_2^6 + 3x_2^2x_3x_4^2 + x_3^3x_4^2 - x_4^4\rangle$

The second relation, evaluated in G, and a_0-saturated gives h, and $\mathcal{SR}(h, G) : a_0^\infty = \mathcal{SR}(h, G) = a_1^5a_2^6 - 6a_1^4a_2^7 - a_1^3a_2^8 + 40a_0a_1^4a_2^6 - 2a_0a_1^3a_2^7 - 45a_0a_1^2a_2^8 - 40a_0a_1a_2^9 - 10a_0a_2^{10} + 107a_0^2a_1^5a_2^4 + 484a_0^2a_1^4a_2^5 + 441a_0^2a_1^3a_2^6 + 38a_0^2a_1^2a_2^7 - 101a_0^2a_1a_2^8 - 40a_0^2a_2^9 - 808a_0^3a_1^3a_2^5 + 615a_0^3a_1^2a_2^6 + 116a_0^3a_1a_2^7 - 39a_0^3a_2^8 - 3798a_0^4a_1^4a_2^3 + 4935a_0^4a_1^3a_2^4 - 3846a_0^4a_1^2a_2^5 + 304a_0^4a_1a_2^6 + 82a_0^4a_2^7 + 23372a_0^5a_1^2a_2^4 - 2720a_0^5a_1a_2^5 + 90a_0^5a_2^6 - 50860a_0^6a_1^3a_2^2 + 5256a_0^6a_1^2a_2^3 + 30105a_0^6a_1a_2^4 - 166a_0^6a_2^5 + 78690a_0^7a_1a_2^3 + 8438a_0^7a_2^4 - 228828a_0^8a_1^2a_2 + 63304a_0^8a_1a_2^2 + 77232a_0^8a_2^3 + 258692a_0^9a_2^2 - 369708a_0^{10}a_1 + 228828a_0^{10}a_2$.

But $\mathcal{SR}(h, G)$ is indeed in S, being $\mathcal{SR}(h, G) = 228828\mathbf{g}^9g_2 + 85356\mathbf{g}^7g_2^2 + 14530\mathbf{g}^5g_2^3 + 1492\mathbf{g}^3g_2^4 - 72\mathbf{g}g_2^5 - 140880\mathbf{g}^9g_3 - 58116\mathbf{g}^7g_2g_3 - 8051\mathbf{g}^5g_2^2g_3 + 38\mathbf{g}^3g_2^3g_3 + 151\mathbf{g}g_2^4g_3 - 2592\mathbf{g}^7g_3^2 - 1576\mathbf{g}^5g_2g_3^2 + 1009\mathbf{g}^3g_2^2g_3^2 - 180\mathbf{g}g_2^3g_3^2 + 529\mathbf{g}^5g_3^3 - 492\mathbf{g}^3g_2g_3^3 + 99\mathbf{g}g_2^2g_3^3 + 114\mathbf{g}^3g_3^4 - 46\mathbf{g}g_2g_3^4 + 11\mathbf{g}g_3^5 - 32456\mathbf{g}^8g_4 - 4586\mathbf{g}^6g_2g_4 - 3263\mathbf{g}^4g_2^2g_4 + 740\mathbf{g}^2g_2^3g_4 - 1751\mathbf{g}^6g_3g_4 + 2196\mathbf{g}^4g_2g_3g_4 - 654\mathbf{g}^2g_2^2g_3g_4 + 18g_2^3g_3g_4 - 424\mathbf{g}^4g_3^2g_4 + 232\mathbf{g}^2g_2g_3^2g_4 - 3g_2^2g_3^2g_4 - 50\mathbf{g}^2g_3^3g_4 + 6g_2g_3^3g_4 - g_3^4g_4 - 25\mathbf{g}^5g_4^2 + 64\mathbf{g}^3g_2g_4^2 - 22\mathbf{g}g_2^2g_4^2 - 27\mathbf{g}^3g_3g_4^2 + 22\mathbf{g}g_2g_3g_4^2 - 8\mathbf{g}g_3^2g_4^2 + 14\mathbf{g}^2g_4^3 - 6g_2g_4^3 + g_3g_4^3$.

5. The Graded Case: Introduction

As mentioned in the introduction, the problem of computing the saturation of a subalgebra S of P can benefit from the fact that S is graded. In this section we prepare the ground for new results related to our problem.

We introduce here the language of (multi or single) positive gradings. All our results in this and the following section are valid for every positive grading and, in particular, for every (single) grading defined by a row-matrix of positive weights.

We recall that a grading on P defined by a weight matrix W is called **positive** if no column of W is zero and the first (from the top) non-zero element in each column is positive. In this case, we shall also say that W is a positive matrix. For more on positive gradings see [9, Chapter 4]. In this section we assume that P has a positive grading such that our algebra S is generated by homogeneous elements.

From now on we consider $P = K[a_0, a_1, \ldots, a_n]$ with a positive (multi)grading defined by W, and $S = K[g_1, \ldots, g_r]$ a W-graded K-subalgebra of P, generated by W-homogeneous g_i's. It is easy to prove that there exist positive row-matrices W', so that every W-homogeneous polynomial is also W'-homogeneous. Therefore, alongside W we can consider a (single)grading defined by such a W' which gives positive integer degree to every non-constant polynomial in P. The following easy example illustrates this claim.

Example 5.1. Let $P = \mathbb{Q}[a_0, a_1]$ be graded by $W = \left(\begin{smallmatrix} 1 & 0 \\ -7 & 2 \end{smallmatrix}\right)$, and let $W' = (1\ 2)$. Notice that $W' = 8(1\ 0) + (-7\ 2)$, thus every W-homogeneous element in P is also W'-homogeneous.

Suppose that we have a positive grading on P and that S is a K-subalgebra of P generated by homogeneous elements. Are there advantages depending on this assumption?

Remark 5.2. Let $S = K[g_1, \dots, g_r]$ subalgebra of P, with g_i, non constant and homogeneous of degree d_i. Consider on the ring $R = K[x_1, \dots, x_r]$ the grading defined by the matrix $W = (d_1 \ \dots \ d_r)$. Then, for every term ordering σ on P, the toric ideal $\mathrm{Rel}(\mathrm{LT}_\sigma(g_1), \dots, \mathrm{LT}_\sigma(g_s)) \subseteq R$ is homogeneous, and any homogeneous relation of degree d in R evaluated in $(g_1, \dots, g_r)$, gives a homogeneous polynomial of degree d in P.

In Example 3.14 the polynomial $g_1 = a_1 - a_0 a_1^2$ is not homogeneous with respect to any positive grading, and no term ordering σ is such that $\mathrm{LT}_\sigma(\pi_{\mathbf{g}}(g_1)) = a_1$. Example 3.14 was used to show that $S : a_0^\infty$ needs not to be finitely generated. However, the following example shows that $S : a_0^\infty$ needs not be a finitely generated K-algebra even when S has a positive grading. It is inspired by the similar Example 6.6.7 contained in [9, Section 6].

Example 5.3. Let $P = \mathbb{Q}[a_0, a_1, a_2]$ be graded by $W = \left(\begin{smallmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{smallmatrix}\right)$.

Let $G = \{\mathbf{g}, g_2, g_3, g_4\} \subseteq P$ and $S = \mathbb{Q}[G]$ where

$$\mathbf{g} = a_0, \quad g_2 = a_1 + a_0 a_2, \quad g_3 = a_1 a_2, \quad g_4 = a_1 a_2^2$$

From $\pi_{\mathbf{g}}(g_2) = a_1$, $\pi_{\mathbf{g}}(g_3) = g_3$, $\pi_{\mathbf{g}}(g_4) = g_4$, it follows that $E^0_{\mathbf{g}}(S) = S$ and $\mathrm{Rel}_{\mathbf{g}}(G) = \mathrm{Rel}(\mathbf{g},\ a_1,\ a_1 a_2,\ a_1 a_2^2) = \langle x_1,\ x_2 x_4 - x_3^2 \rangle$. The first generator gives $\mathbf{g}$, and the second gives $g_2 g_4 - g_3^2 = a_0 a_1 a_2^3$ whose saturation is $a_1 a_2^3$. No sat-reduction is possible hence we obtain $G_1 = G \cup \{a_1 a_2^3\}$, and $E^1_{\mathbf{g}}(S) = \mathbb{Q}[G_1]$.

By induction on i we assume that $G_i = \{a_0, a_1, a_1 a_2, \dots, a_1 a_2^{i+2}\}$, and $E^i_{\mathbf{g}}(S) = \mathbb{Q}[G_i]$. We prove that $E^{i+1}_{\mathbf{g}}(S) = \mathbb{Q}[a_0, a_1, a_1 a_2, \dots, a_1 a_2^{i+3}]$.

Induced by W, we have a grading on $\mathbb{Q}[x_1, x_2, \dots, x_{i+4}]$ given by $V = \left(\begin{smallmatrix} 0 & 1 & 2 & \cdots & i+3 \\ 1 & 1 & 1 & \cdots & 1 \end{smallmatrix}\right)$ so that $\mathrm{Rel}_{\mathbf{g}}(G_i)$ is V-homogenous, and we consider the term ordering σ defined by a matrix whose first two lines are the lines of V, and the third line is $(-1 \ \ 0 \ \ \cdots \ \ 0)$. Then σ is $\deg_V$-compatible.

It is well-known that toric ideals are generated by pure binomials (see [14]). We claim that the binomials in the reduced σ-Gröbner basis $\mathcal{G}_\sigma$ of the ideal $\mathrm{Rel}_{\mathbf{g}}(G_i)$ are quadratic, i.e. of type $x_\alpha x_\beta - x_\gamma x_\delta$.

To prove this claim we assume by contradiction that there is a pure binomial b in $\mathcal{G}_\sigma$ of type $b = x_{\alpha_1} x_{\alpha_2} \cdots x_{\alpha_r} - x_{\beta_1} x_{\beta_2} \cdots x_{\beta_s}$ with $\alpha_1 \le \alpha_2 \cdots \le \alpha_r$ and $\beta_1 \le \beta_2 \le \cdots \le \beta_s$ and $r > 2$. From the homogeneity with respect to the second line of V we deduce the equality $r = s$. As b is σ-monic, $\mathrm{LT}_\sigma(b) = x_{\alpha_1} x_{\alpha_2} \cdots x_{\alpha_r}$, hence $\alpha_1 < \beta_1$. Moreover, from the homogeneity with respect to the first row of V we deduce $\sum_{i=1}^r \alpha_i = \sum_{i=1}^r \beta_i$ hence we get the inequality $\alpha_r \ge \alpha_1 + 2$. Now, $H = x_{\alpha_1} x_{\alpha_r} - x_{\alpha_1+1} x_{\alpha_r - 1} \in \mathrm{Rel}_{\mathbf{g}}(G_i)$, and, since $\mathrm{LT}_\sigma(H) = x_{\alpha_1} x_{\alpha_r}$ divides $\mathrm{LT}_\sigma(b)$ properly, we have a contradiction with the assumption that $b \in \mathcal{G}_\sigma$. Therefore, all binomials in $\mathcal{G}_\sigma$ are quadratic.

The next claim is that only $a_1 a_2^{i+3}$ is added to $E^i_{\mathbf{g}}(S)$ via the binomials in $\mathrm{Rel}_{\mathbf{g}}(G_i)$. The only quadratic binomials which produce non-zero polynomials are those involving x_2, and those not in $\mathrm{Rel}_{\mathbf{g}}(G_{i-1})$ must involve x_{i+4}. Thus, using the same arguments as above, we deduce that they are of type $x_2 x_{i+4} - x_a x_b$ with $1 < a \le b < i + 4$. The corresponding evaluation gives $a_0 a_i a_2^{i+3}$ which sat-reduces to $a_1 a_2^{i+3}$, and hence we have $E^{i+1}_{\mathbf{g}}(S) = \mathbb{Q}[a_0, a_1 + a_0 a_2, a_1 a_2, \dots, a_1 a_2^{i+3}]$ as claimed.

In conclusion, $S : a_0^\infty = \mathbb{Q}[a_0,\ a_1 + a_0 a_2,\ a_1 a_2^2, \dots, a_1 a_2^i, \dots]$ is not finitely generated.

The following is a well-known fact which we recall here for the sake of completeness. It states that the degrees of a minimal system of homogeneous generators of a graded

K-subalgebra S of P is an invariant of S. For simplicity we state it here only in the special case where the grading is given by a positive row-matrix.

Proposition 5.4. *Let W be a positive row-matrix and let S be a W-graded finitely generated K-subalgebra of P. Then let $(g_1, \ldots, g_r)$ be a minimal system of homogeneous generators of S with $d_i = \deg_W(g_i)$ and $d_1 \leq \cdots \leq d_r$. If $(h_1, \ldots, h_s)$ is another minimal system of homogeneous generators of S with $\delta_i = \deg(h_i)$ and $\delta_1 \leq \cdots \leq \delta_s$, then $s = r$ and $d_i = \delta_i$ for $i = 1, \ldots, r$.*

Proof. It suffices to show that in each degree d the number of elements of degree d in any minimal system of generators of S is an invariant. Let $K[S_{<d}]$ be the algebra generated by the elements of S of degree less than d, and let $V = S_d \cap K[S_{<d}]$. It is a K-vector subspace of S_d and the number of minimal generators of degree d is $\dim_K(S_d/V)$. □

6. The Graded Case: Truncated SAGBI basis for Minimalization

Given homogeneous generators of a K-subalgebra S of P, the next question is how to find a minimal system of homogeneous generators of S. The best tool for tackling this problem is a truncated SAGBI basis of S. Let us see how. As mentioned, for a general introduction to this topic see [9, Section 6.6]. In particular, consider [9, Tutorial 96].

Remark 6.1. Recall Remark 5.2. Starting with homogeneous generators, the computation of a SAGBI basis may proceed by increasing degrees: after all relations and generators of degree $\leq d$ have been considered, the computation continues with relations and polynomials of higher degrees. Thus, the following generators and relations, have degree $> d$, and cannot affect, *i.e.* reduce, those, previously considered, of degree $\leq d$.

One application of this approach is that one can determine whether an element of degree d is in S by testing if it reduces to 0 or not with respect to a ***d*-truncated SAGBI basis** of S, *i.e.* a SAGBI basis computed up to degree d.

With these facts we are ready to describe the algorithm for computing the minimal generators. This algorithm is basically the same as the general algorithm for computing a SAGBI basis, except for the considerations on the degree.

Algorithm 6.2. SubalgebraMinGens

---

notation: $P = K[a_0, \ldots, a_n]$ is a polynomial ring graded by a positive row-matrix, and let σ on $\mathbb{T}^{n+1}$ be a degree-compatible term ordering.

Input $S = K[g_1, \ldots, g_r] \subseteq P$ with $g_1, \ldots, g_r$ homogeneous.

1 Initialise: Let $G = \{g_1, \ldots, g_r\}$, $D = \max\{\deg(g) \mid g \in G\}$, SB $= \emptyset$, and MinGens $= \emptyset$.

2 *Main Loop:* for d from $\min\{\deg(g) \mid g \in G\}$ to D

- **2.1** foreach $g \in G$ of degree d
  - **2.1.1** Compute $h = \mathcal{SR}(g,\ \text{SB})$
  - **2.1.2** if $h \neq 0$ then
    - redefine SB as SB $\cup\{h\}$
    - redefine MinGens as MinGens $\cup\{h\}$

2.2 if $d = D$ then **return MinGens**

2.3 compute $\{H_1, \dots, H_t\}$, the generators of degree $d+1$ of $\mathrm{Rel}(\mathrm{LT}_\sigma(g_1'), \dots, \mathrm{LT}_\sigma(g_s'))$, where $g_1', \dots, g_s'$ are the elements in SB

2.4 for $j = 1, \dots, t$, compute $h_j = \mathcal{SR}(H_j(g_1', \dots, g_s'),\ \mathrm{SB})$

2.5 redefine SB as SB $\cup\{h_1, \dots, h_t\}$

2.6 interreduce SB

Output MinGens, a minimal system of generators of S.

Proof. Each iteration of the main loop has a fixed d and computes SB, a truncated SAGBI basis of $K[G_{\le d}]$, where $G_{\le d} = \{g_i \in G \mid \deg(g_i) \le d\}$: in Step 2.1 it is truncated to degree d, and in Steps 2.3-2.6 it is truncated to degree d+1, because it involves the relations up to degree d+1. Having done that, in Step 2.1.1 of the next iteration, we use SB to determine whether each generator of degree d+1 is in $K[G_{\le d}]$, and also if there is a, necessarily linear, relation with the previously added generators of the same degree.

This procedure terminates because each iteration is finite, and there are at most D iterations. □

In the following example we see the algorithm at work.

Example 6.3. We reconsider Example 4.13. The algebra S is standard graded and its σ-SatSAGBI basis is $\{a_0,\, g_2,\, g_3,\, g_4,\, g_5\}$ where $g_5 = a_2^6 - 8a_0a_1^3a_2^2 - 6a_0a_1^2a_2^3 + 3a_0a_1a_2^4 + 6a_0^2a_1a_2^3 + 4a_0^2a_2^4 - 6a_0^3a_1^2a_2 - 12a_0^3a_1a_2^2 + 12a_0^3a_2^3 - a_0^4a_2^2 - 9a_0^5a_1 + 6a_0^5a_2$.

Using Algorithm 6.2 we get $S : a_0^\infty = K[a_0, g_2, g_3, g_4]$, and indeed we can check that

$$g_5 = 6a_0^4g_2 - 3a_0^4g_3 - 6a_0^2g_2g_3 - 3a_0^2g_3^2 + 4a_0^3g_4 - 3g_2^2g_3 - g_3^3 - 6a_0g_2g_4 + 3a_0g_3g_4 + g_4^2$$

7. The Graded Case: SAGBI basis for Saturation

We know that the main obstacle to the efficiency of Algorithm 3.12 is Step 2.2 which requires the computation of elimination ideals as explained in Proposition 3.2. The first observation is that if the input polynomials in Step 2.2 are homogeneous, then it is well-known that the efficiency of the computation of the elimination ideal can be improved.

The second observation is related to a good use of the reduction described in Section 4. In general, it is desirable to streamline $\pi_{\mathbf{g}}(f)$ as much as possible to simplify the elimination process. On the other end, if the leading term of a polynomial g is divisible by a_0, then an $\mathcal{S}$-remainder of a polynomial f divided by g in general does not "simplify" $\pi_{\mathbf{g}}(f)$

Consequently, to maximize the chance of getting $\mathcal{S}$-remainders divisible by a_0, our strategy is to use a term ordering σ with the property that $\mathrm{LT}_\sigma(g) = \mathrm{LT}_\sigma(\pi_{\mathbf{g}}(g))$ for every $g \in P\backslash\{0\}$. These considerations motivate the following definition.

Definition 7.1. Let $P = K[a_0, a_1, \dots, a_n]$, let $W \in \mathrm{Mat}_{m,n+1}(\mathbb{Z})$ be a positive matrix, Then let $\deg_W$ be the positive grading on P defined by W. A term ordering σ on $\mathbb{T}^{n+1}$ is said to be of ***a*$_0$-Deg$_W$Rev type** (or simply ***a*$_0$-DegRev type**) is σ is compatible with $\deg_W$ and if $t, t' \in \mathbb{T}^{n+1}$ are such that $\deg_W(t) = \deg_W(t')$ and $\log_{a_0}(t) < \log_{a_0}(t')$ then $t >_\sigma t'$.

We recall that a way to construct a term ordering σ of a_0-DegRev type is to add to the matrix W the row $(-1, 0, \dots, 0)$, and then completing it to a non-singular matrix. For further details about this notion see [9, Sections 4.2 and 4.4].

Now we come to the main point of this section. The most important feature of a positively graded finitely generated K-subalgebra S of P which contains an indeterminate, say a_0, is that the computation of $S : a_0^\infty$, and hence of $\mathrm{Sat}_{a_0}(S)$ by Proposition 2.4.(b), can be essentially done by computing a suitable SAGBI basis of S. Let us explain how.

Here is the main result of this section.

Theorem 7.2. *Let $\deg_W$ be the grading on P defined by a positive matrix W, and let σ on $\mathbb{T}^{n+1}$ be a term ordering of a_0-*DegRev *type. Then let S be a finitely generated W-graded K-subalgebra of P, let $a_0 \in S$, and let* SB *be a σ-SAGBI basis of S. Then the set $\{a_0\} \cup \{g : a_0^\infty \mid g \in \mathrm{SB}\}$ is a σ-SAGBI basis of* $\mathrm{Sat}_{a_0}(S)$.

Proof. It is enough to show that if $f \in \mathrm{Sat}_{a_0}(S)$ is not divisible by a_0, then $\mathrm{LT}_\sigma(f)$ is a power-product of elements in $\{\mathrm{LT}_\sigma(g : a_0^\infty) \mid g \in \mathrm{SB}\}$. From Proposition 2.4.(d) we have $\mathrm{Sat}_{a_0}(S) = S : a_0^\infty$, thus $a_0^d f \in S$ for some $d \in \mathbb{N}$. Therefore, there exist $\alpha_1, \dots, \alpha_t \in \mathbb{N}$ and $g_1, \dots, g_t \in \mathrm{SB}$ such that $\mathrm{LT}_\sigma(a_0^d f) = (\mathrm{LT}_\sigma(g_1))^{\alpha_1} \cdots (\mathrm{LT}_\sigma(g_t))^{\alpha_t}$. The assumptions on S and σ imply that $a_0 \nmid \mathrm{LT}_\sigma(f)$, and for $i = 1, \dots, t$, we have that $a_0 \nmid \mathrm{LT}_\sigma(g_i : a_0^\infty)$ and there exists $r_i \in \mathbb{N}$ such that $\mathrm{LT}_\sigma(g_i) = a_0^{r_i}\, \mathrm{LT}_\sigma(g_i : a_0^\infty)$. Thus, we have the equality

$$a_0^d\, \mathrm{LT}_\sigma(f) = a_0^{r_1\alpha_1} (\mathrm{LT}_\sigma(g_1 : a_0^\infty))^{\alpha_1}\ \cdots\ a_0^{r_t\alpha_t} (\mathrm{LT}_\sigma(g_t : a_0^\infty))^{\alpha_t}$$

By setting $a_0 = 1$ we get the desired conclusion. □

The following easy example shows that the assumption about the term ordering σ in the above theorem is essential.

Example 7.3. Let $P = \mathbb{Q}[a_0, a_1, a_2, a_3]$ and let $S = \mathbb{Q}[\mathbf{g}, g_2, g_3]$ where we have $\mathbf{g} = a_0$, $g_2 = a_0 a_2 - a_1^2$, $g_3 = a_0 a_3^2 - a_1^3$. If $\sigma =$ `DegLex`, which is not of a_0-DegRev type, then $\mathrm{LT}_\sigma(a_0) = a_0$, $\mathrm{LT}_\sigma(g_2) = a_0 a_2$, and $\mathrm{LT}_\sigma(g_3) = a_0 a_3^2$. The three power products are algebraically independent, hence $\mathrm{SB} = \{a_0, g_2, g_3\}$ is a σ-SAGBI basis of S by [9, Proposition 6.6.11]. Instead, if σ is the term ordering defined by the matrix $\begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$, then S is W-graded where $W = (1\ 1\ 1)$, and σ is a term ordering of a_0-DegRev type. Now we have $\mathrm{LT}_\sigma(a_0) = a_0$, $\mathrm{LT}_\sigma(g_2) = a_1^2$, and $\mathrm{LT}_\sigma(g_3) = a_1^3$. The σ-SAGBI basis of S is $\mathrm{SB} = \{a_0, g_2, g_3, g_4\}$ where $g_4 = a_0 a_1^4 a_2 - \frac{2}{3} a_0 a_1^3 a_3^2 - a_0^2 a_1^2 a_2^2 + \frac{1}{3} a_0^2 a_3^4 + \frac{1}{3} a_0^3 a_2^3$. By saturating g_4 we get $\tilde{g}_4 = g_4 : a_0^\infty = a_1^4 a_2 - \frac{2}{3} a_1^3 a_3^2 - a_0 a_1^2 a_2^2 + \frac{1}{3} a_0 a_3^4 + \frac{1}{3} a_0^2 a_2^3$. Moreover, by Algorithm 6.2 we check that $\mathrm{Sat}_{a_0}(S)$ is minimally generated by $(a_0, g_2, g_3, \tilde{g}_4)$.

The following example illustrates a subtlety of the theorem. It happens that while the SAGBI basis of S is infinite, the SAGBI basis of $\mathrm{Sat}_{a_0}(S)$ is finite.

Example 7.4. Let $P = \mathbb{Q}[a_0, a_1, a_2]$ be graded by the matrix $W = \begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 0 \end{pmatrix}$ and let $S = \mathbb{Q}[\mathbf{g}, g_2, g_3, g_4, g_5]$ where we have $\mathbf{g} = a_0$, $g_2 = a_0 a_1$, $g_3 = a_1 + a_2$, $g_4 = a_1 a_2$, $g_5 = a_1 a_2^2$. If σ is a term ordering compatible with W, the σ-SAGBI basis of S is not finite. It is

$$\{a_0,\ a_1 + a_2,\ a_0 a_2,\ a_1 a_2,\ a_0 a_2^2,\ a_1 a_2^2, \dots, a_0 a_2^i,\ a_1 a_2^i, \dots\}$$

while the σ-SAGBI basis of $\mathrm{Sat}_{a_0}(S)$ is finite. It is

$$\{a_0,\ a_1 + a_2,\ a_2\}.$$

The following procedure combines the saturation of the elements of a σ-SAGBI basis, as described in Theorem 7.2, within the iterations of the SAGBI basis computation. It is a procedure because termination is not guaranteed, but if it terminates the output is correct.

Procedure 7.5. SatSAGBI

---

notation: $P = K[a_0, \dots, a_n]$ is a polynomial ring graded by a positive matrix, and let σ on $\mathbb{T}^{n+1}$ be a term ordering of a_0-DegRev type.

Input $S = K[g_1, \dots, g_r] \subseteq P$, with $g_1, \dots, g_r$ homogeneous.

1 Let $G = \{g_1, \dots, g_r\}$

2 *Main Loop:*

  2.1 compute $G' = \{g'_1, \dots, g'_s\}$ the sat-interreduction of G.

  2.2 compute $\{H_1, \dots, H_t\}$, a set of generators of $\mathrm{Rel}(\mathrm{LT}_\sigma(g'_1), \dots, \mathrm{LT}_\sigma(g'_s))$

  2.3 for $j = 1, \dots, t$, let $h_j = \mathcal{SR}(H_j(g'_1, \dots, g'_s),\ G') : a_0^\infty$

  2.4 if $h_1 = \cdots = h_t = 0$ then **return** $\boldsymbol{\{a_0\} \cup G'}$

  2.5 redefine G as $G' \cup \{h_1, \dots, h_t\}$

Output $\{a_0\} \cup G'$, a σ-SAGBI basis of $S : a_0^\infty$

Proof. The definition of G' in Step 2.1, and redefinition of G in Step 2.5 correspond to the definition of new subalgebras $S' = K[G']$ and $S'' = K[G' \cup \{h_1, \dots, h_t\}]$ which satisfy $S \subseteq S' \subseteq S'' \subseteq S : a_0^\infty$, thus all algebras defined in this procedure have saturation $S : a_0^\infty$, by Theorem 3.10.(c).

Each iteration of Step 2.1 is equivalent to restarting the computation of a σ-SAGBI basis of $K[G']$, where all the elements in G' are a_0-saturated.

If the procedure stops in Step 2.4, then $\{a_0\} \cup G'$ is a σ-SAGBI basis of the algebra $A = K[\{a_0\} \cup G']$ and therefore, by Theorem 7.2, $A = A : a_0^\infty$.

In conclusion, if it terminates, the output is the σ-SAGBI basis of $S : a_0^\infty$. $\square$

Is this procedure the definitive solution of our problem? The answer is yes and no. The following example provides a negative answer by showing that for some input this procedure cannot terminate because there is no finite SAGBI basis.

Example 7.6. Let $P = \mathbb{Q}[a_0, a_1, a_2]$ and let $S = \mathbb{Q}[\mathbf{g}, g_2, g_3, g_4]$ where we have $\mathbf{g} = a_0$, $g_2 = a_1 + a_2$, $g_3 = a_1 a_2$, $g_4 = a_1 a_2^2$. Since g_2, g_3, g_4 do not involve a_0, it is clear that $S = S : a_0^\infty$. On the other hand, whatever term ordering we choose, the SAGBI basis and the SatSAGBI basis of S are infinite (see [9, Example 6.6.7]).

However, the computation of Example 7.4 immediately terminates when we add the generator $a_2 = a_0 a_2 : a_0^\infty$, and also terminates for many other examples we computed, leading us to formulate the following conjecture.

Conjecture 7.7. If there is a finite σ-SAGBI basis of $S : a_0^\infty$, Procedure 7.5 terminates in a finite number of iterations, hence it is an algorithm.

Remark 7.8. The delicate point in proving this conjecture is that Steps 2.1 and 2.5 might produce a sequence of algebras ever closer to $\mathrm{Sat}_g(S)$, but never getting to it.

The positive side is that the computation using SAGBI bases provides not only a set of generators of the saturation of S but also a SAGBI basis of it. Secondly the computation of a SAGBI basis needs to determine relations only among power-products, thus may use toric ideals whose computation is considerably faster than the computation via general elimination needed for determining $\mathrm{Rel}_{\mathbf{g}}$.

Let us show an example where the above procedure works very well.

Example 7.9. We let $P = \mathbb{Q}[a_0, a_1, a_2]$ graded by the matrix $W = (1, 1, 1)$ and use a term ordering of a_0-DegRev type. Then let $\mathbf{g} = a_0,\ g_2 = a_1^2 - a_2^2 + a_0a_2,\quad g_3 = a_1a_2 - a_2^2 + a_0a_1,\ g_4 = a_1^3,\ g_5 = a_2^4$. We want to saturate the algebra $S = \mathbb{Q}[\mathbf{g}, g_2, g_3, g_4, g_5]$ with respect to g. Using Algorithm 7.5, we get a SAGBI basis of $\mathrm{Sat}_{\mathbf{g}}(S)$ which consists of 12 polynomials. Using Algorithm 6.2 we get a minimal set of generators of $\mathrm{Sat}_{\mathbf{g}}(S)$. The result is $\mathrm{Sat}_{\mathbf{g}}(S) = \mathbb{Q}[\mathbf{g}, g_2, g_3, g_4, g_5, g_6, g_7, g_8]$ where

$$\begin{aligned}
g_6 \;=\;& a_1^3a_2^2 - \tfrac{23}{15}a_1^2a_2^3 - \tfrac{11}{45}a_1a_2^4 + \tfrac{44}{45}a_2^5 - \tfrac{5}{18}a_0a_1a_2^3 + \tfrac{6}{5}a_0^2a_1^2a_2 - \tfrac{23}{30}a_0^2a_1a_2^2 + \tfrac{5}{6}a_0^2a_2^3 - \tfrac{1}{5}a_0^3a_2^2 \\
& + \tfrac{11}{15}a_0^4a_1 - \tfrac{1}{2}a_0^4a_2 \\
g_7 \;=\;& a_2^7 - \tfrac{295}{2}a_0^2a_1^2a_2^3 - \tfrac{65}{6}a_0^2a_1a_2^4 + \tfrac{119}{6}a_0^2a_2^5 + \tfrac{1217}{12}a_0^3a_1a_2^3 - 30a_0^4a_1^2a_2 + \tfrac{319}{4}a_0^4a_1a_2^2 - \tfrac{275}{4}a_0^4a_2^3 \\
& -42a_0^5a_2^2 + \tfrac{65}{2}a_0^6a_1 + \tfrac{219}{4}a_0^6a_2 \\
g_8 \;=\;& a_1a_2^6 - \tfrac{576}{5}a_0^2a_1^2a_2^3 - \tfrac{179}{30}a_0^2a_1a_2^4 + \tfrac{193}{15}a_0^2a_2^5 + \tfrac{214}{3}a_0^3a_1a_2^3 - \tfrac{54}{5}a_0^4a_1^2a_2 + \tfrac{262}{5}a_0^4a_1a_2^2 \\
& -60a_0^4a_2^3 - \tfrac{126}{5}a_0^5a_2^2 + \tfrac{239}{10}a_0^6a_1 + 39a_0^6a_2
\end{aligned}$$

In this case the computation takes a few seconds. We could also use Algorithm 3.12 to compute $\mathrm{Sat}_g(S)$, but generally it gives neither a minimal set of generators, nor a SAGBI basis of it.

In the following example the performance of Procedure 7.5 is far superior.

Example 7.10. We let $P = \mathbb{Q}[a_0, a_1, a_2, a_3]$ graded by the matrix $W = (1, 1, 1, 1)$ and use a term ordering of a_0-DegRev type. Then let $g = a_0,\ g_2 = a_1^2 - a_0a_3,\quad g_3 = a_1a_2 + a_0a_1,\ g_4 = a_3^2,\ g_5 = a_2^2,\ g_6 = a_1^3 - a_2^3$. We want to saturate the algebra $S = \mathbb{Q}[\mathbf{g}, g_2, g_3, g_4, g_5, g_6]$ with respect to g. Using Procedure 7.5, we get a SAGBI basis of $\mathrm{Sat}_g(S)$ which consists of 21 polynomials. Using Algorithm 6.2 we get a minimal set of generators for $\mathrm{Sat}_{\mathbf{g}}(S)$.

The result is $\mathrm{Sat}_{\mathbf{g}}(S) = \mathbb{Q}[\mathbf{g}, g_2, g_3, g_4, g_5, g_6, g_7, \dots, g_{15}]$ where

$$
\begin{aligned}
g_7 &= a_1^2a_2 + \tfrac{1}{2}a_2^2a_3 + \tfrac{1}{2}a_0^2a_3\\
g_8 &= a_1^4a_3 - a_1a_2^3a_3 - a_0a_1a_2^2a_3 + \tfrac{2}{3}a_0^2a_2^3 - a_0^2a_1a_2a_3 - \tfrac{2}{3}a_0^2a_3^3 - a_0^3a_1a_3\\
g_9 &= a_2^3a_3^3 - a_0a_1a_2^3a_3 + \tfrac{1}{4}a_0a_2^2a_3^3 - a_0^2a_1a_2^2a_3 + \tfrac{1}{2}a_0^3a_2^3 - \tfrac{3}{4}a_0^3a_1a_2a_3 + \tfrac{3}{4}a_0^3a_3^3 - \tfrac{3}{4}a_0^4a_1a_3\\
g_{10} &= a_1a_2^4a_3 + a_0a_1a_2^3a_3\\
g_{11} &= a_1^4a_2a_3 + \tfrac{4}{3}a_0a_1a_2^3a_3 + \tfrac{2}{3}a_0a_2^2a_3^3 + \tfrac{4}{3}a_0^2a_1a_2^2a_3 - \tfrac{2}{3}a_0^3a_2^3 + a_0^3a_1a_2a_3 + a_0^4a_1a_3\\
g_{12} &= a_1^2a_2^2a_3^3 + \tfrac{1}{2}a_2^3a_3^4 - \tfrac{1}{4}a_0a_2^5a_3 + \tfrac{1}{4}a_0a_1^2a_2a_3^3 + \tfrac{9}{8}a_0^2a_1^3a_2a_3 - \tfrac{1}{8}a_0^2a_2^4a_3 - \tfrac{3}{4}a_0^2a_1^2a_3^3\\
&\quad + \tfrac{9}{8}a_0^3a_1^3a_3 + \tfrac{1}{2}a_0^3a_2^3a_3 + \tfrac{3}{8}a_0^4a_2^2a_3\\
g_{13} &= a_2^6a_3 + \tfrac{1}{8}a_2^3a_3^4 + \tfrac{39}{16}a_0a_2^5a_3 + \tfrac{9}{16}a_0a_1^2a_2a_3^3 - \tfrac{135}{32}a_0^2a_1^3a_2a_3 + \tfrac{15}{32}a_0^2a_2^4a_3 + \tfrac{9}{16}a_0^2a_1^2a_3^3\\
&\quad - \tfrac{135}{32}a_0^3a_1^3a_3 - \tfrac{19}{8}a_0^3a_2^3a_3 - \tfrac{45}{32}a_0^4a_2^2a_3\\
g_{14} &= a_1a_2^5a_3 - \tfrac{1}{4}a_2^4a_3^3 - a_0^2a_1a_2^3a_3 - \tfrac{1}{2}a_0^2a_2^2a_3^3 + \tfrac{3}{4}a_0^4a_3^3\\
g_{15} &= a_1^2a_2^4a_3 - \tfrac{1}{4}a_1a_2^3a_3^3 - \tfrac{1}{4}a_0a_1a_2^2a_3^3 - 2a_0^2a_1^2a_2^2a_3 - \tfrac{3}{4}a_0^2a_1a_2a_3^3 - a_0^3a_1^2a_2a_3 - \tfrac{3}{4}a_0^3a_1a_3^3
\end{aligned}
$$

The computation took about 75 seconds using Procedure 7.5 and Algorithm 6.2. We tried to do the computation using Algorithm 3.12 and we did not succeed.

8. A Special Multigraded Case: Truncated SAGBI basis for Saturation

In general, the computation of $S : a_0^\infty$ is very expensive. The performance of Algorithm 3.12 is poor even for examples of moderate size. The performance of Procedure 7.5 is usually much better, but the computation of a SAGBI basis may be prohibitive as well. However, there is a situation where it is possible to compute $(S : a_0^\infty)_{\le d}$, in other words a truncation of $S : a_0^\infty$ at degree d. Let us see how.

In Section 7 we have already seen that the main requirement to compute the saturation of S with respect to an indeterminate, is to compute an a_0-saturated SAGBI basis of S with respect to a term ordering of a_0-DegRev type. Our question is: if the computation of a saturating SAGBI basis is prohibitive, can we at least compute a truncation of a saturating SAGBI basis at a given degree? The main obstacle is that when we saturate a computed polynomial, we may lower its degree. If a_0 is the chosen indeterminate, the only possibility of keeping the degree fixed is when the input is homogeneous with respect to a grading where $\deg(a_0) = 0$. This condition is clearly incompatible with a term ordering of a_0-DegRev type, unless the input is homogeneous also with respect to another grading with $\deg(a_0) > 0$.

The following example shows that in many cases the computation of the saturation may be too hard even when working over a small prime field.

Example 8.1. We let $P = \mathbb{Z}/(101)[a_0, a_1, a_2, a_3, a_4]$ standard graded by the matrix $W = (1, 1, 1, 1, 1)$, and use a term ordering of a_0-DegRev type. Then we let $\mathbf{g} = a_0$, $g_2 = a_1^2 - a_2^2 + a_0a_3$, $g_3 = a_1^3 + a_2^3 + a_0^2a_4$, $g_4 = a_3^3 - a_0a_4^2$, $g_5 = a_4^3$, and want to saturate the algebra $S = \mathbb{Z}/(101)[\mathbf{g}, g_2, g_3, g_4, g_5]$ with respect to $\mathbf{g}$.

No matter which algorithm we use, there is no way. However, we observe that the given polynomials are also homogeneous with respect to the grading given by (0 1 1 2 3) and this observation suggests an interesting approach which we are going to explain. We continue this discussion in Example 8.5.

We start with the following easy lemma.

Lemma 8.2. *Let $P = K[a_0, a_1, \ldots, a_n]$, let $d_1, \ldots, d_n \in \mathbb{N}_+$, let P be (single) graded by $W = (0\ d_1 \cdots d_n)$, and let $S \subset P$ be a finitely generated monomial K-algebra. Then let $d \in \mathbb{N}_+$, and let $S_d = \{f \in P \mid f$ homogeneous of degree $d\}$.*

(a) The set S_d is a $K[a_0]$-module.

(b) The $K[a_0]$-module S_d is finitely generated, and there is a unique set of power products which minimally generate it.

Proof. Claim (a) follows from the fact that $\deg(a_0) = 0$. Let $S \subset P_d$ denote the set of power products of degree d in $\mathbb{T}(a_1, \ldots, a_n)$, and let $t_1, \ldots, t_r$ be the unique basis of power products of S_d as a K-vector space. For each t_i there is a minimum exponent e_i such that $\tau_i = a_0^{e_i} t_i \in S_d$. It follows that S_d is minimally generated by $\{\tau_1, \ldots, \tau_r\}$. □

Proposition 8.3. *Let $P = K[a_0, a_1, \ldots, a_n]$, let $d_1, \ldots, d_n \in \mathbb{N}_+$, $p_1, \ldots, p_n \in \mathbb{Z}$, let P be graded by W whose first two rows are $W_1 = (0\ d_1 \cdots d_n)$, $W_2 = (1\ p_1 \cdots p_n)$, and let σ be a term ordering on $\mathbb{T}^{n+1}$ compatible with W and of a_0-DegRev type. Then let S be a finitely generated W-graded K-subalgebra of P, let $a_0 \in S$, let SB be a σ-SAGBI basis of S, let $d \in \mathbb{N}_+$, and let $\mathrm{SB}_{\le d} = \{g \in \mathrm{SB} \mid g$ is W-homogeneous and $\deg_{W_1}(g) \le d\}$.*

Then $\{a_0\} \cup \{g : a_0^\infty \mid g \in \mathrm{SB}_{\le \mathrm{d}}\}$ is a d-truncated σ-SAGBI basis of S.

Proof. Our assumptions are compatible with those of Theorem 7.2. When we compute a σ-SAGBI basis of S we may proceed by increasing degrees as suggested by Remark 6.1. We proceed using the degree $\deg_{W_1}$. The merit is that the saturation of a polynomial does not change $\deg_{W_1}$. Then Lemma 8.2 shows that the computation of the σ-SAGBI basis jumps over d and clearly it does not come back anymore. The conclusion follows. □

Algorithm 8.4. TruncSatSAGBI

---

notation: $P = K[a_0, \ldots, a_n]$ is a polynomial ring graded by W whose first two rows are $W_1 = (0\ d_1 \cdots d_n)$, $W_2 = (1\ p_1 \cdots p_n)$, with $d_1, \ldots, d_n \in \mathbb{N}_+$, $p_1, \ldots, p_n \in \mathbb{Z}$.
Let σ be a term ordering on $\mathbb{T}^{n+1}$ compatible with W and of a_0-DegRev type.

Input $S = K[g_1, \ldots, g_r] \subseteq P$, with g_i W-homogeneous for $i = 1, \ldots, r$.

1 Let $G = \{g_1, \ldots, g_r\}$

2 *Main Loop:*

2.1 compute $G' = \{g'_1, \ldots, g'_s\}$ the sat-interreduction of G.

2.2 compute $\{H_1, \ldots, H_t\}$, the subset of elements of W_1-degree $\le d$ in a set of generators of $\mathrm{Rel}(\mathrm{LT}_\sigma(g'_1), \ldots, \mathrm{LT}_\sigma(g'_s))$

2.3 for $j = 1, \ldots, t$, let $h_j = \mathcal{SR}(H_j(g'_1, \ldots, g'_s),\ G') : a_0^\infty$

2.4 if $h_1 = \cdots = h_t = 0$ then **return G'**

2.5 redefine G as $G' \cup \{h_1, \ldots, h_t\}$

Output G', a σ-SAGBI basis of $S : a_0^\infty$ truncated at W_1-degree d.

Proof. Correctness and termination follow immediately from Proposition 8.3. □

Let us go back to Example 8.1.

Example 8.5. Using the data introduced in Example 8.1 we compute $(S : a_0^\infty)_{\le 30}$.

In less than a second we get $(S : a_0^\infty)_{\le 30} = (K[a_0, g_2, \dots, g_6, g_7])_{\le 30}$ where g_7 is a polynomial of bi-degree $(30, 29)$ with 767 terms and $\mathrm{LT}(g_7) = a_1^{20}a_2^8a_3$.

In about 23 seconds we compute $(S : a_0^\infty)_{\le 90} = (K[a_0, g_2, \dots, g_6, g_7, g_8])_{\le 90}$ where g_8 is a polynomial of bi-degree $(90, 86)$ with 19559 terms and $\mathrm{LT}(g_8) = a_1^59a_2^24a_3^2a_4$.

Then we try to compute $(S : a_0^\infty)_{\le 300}$ and after about 30 minutes we realise that the algorithm gets a new polynomial with 516775 terms and leading term $a_1^{176}a_2^{73}a_3^6a_4^3$. At this point we understand that the computation is not going to end in a reasonable amount of time.

In conclusion, we are able to compute $(S : a_0^\infty)_{\le 90}$, but we are not even able to know whether $S : a_0^\infty$ is finitely generated or not.

8.1. Computing U-invariants

Unlike Example 8.5, there are cases where a bit of extra knowledge allows us to fully compute the saturation of a subalgebra using the technique of truncation. And we go back to the introduction where we started our discussion about the computation the classical U-invariants, which gave us a first motivation of our work. Recall that the problem is to compute the $\mathbb{C}$-subalgebra $S_n = \mathbb{C}[c_2, \dots, c_n][a_0, a_0^{-1}] \cap \mathbb{C}[a_0, \dots, a_n]$ of $\mathbb{C}[a_0, \dots, a_n]$ where the polynomials c_i's are defined in the introduction.

First of all, it follows from Proposition 2.4.(d) that $S_n = \mathbb{C}[a_0, c_2, \dots, c_n] : a_0^\infty$. Then we observe that $a_0, c_2, \dots, c_n$ are elements of the polynomial ring $P = \mathbb{Q}[a_0, a_1, \dots, a_n]$, hence all the computation of the SatSAGBI basis involves polynomials in P, so the generators of S_n lie in P. To see more on this topic see [12].

The third remark is that $a_0, c_2, \dots, c_n$ are bi-homogeneous elements in P graded by the positive matrix $W_n = \left(\begin{smallmatrix} 0 & 1 & \cdots & n \\ 1 & 1 & \cdots & 1 \end{smallmatrix}\right)$.

Finally, classical results show that S_n is finitely generated and, for some n, compute the bi-degrees of a minimal set of generators. Consequently, according to Proposition 8.3 we can compute S_n by truncating the SatSAGBI basis at the maximum weighted degree given by the grading $(0\ \ 1\ \cdots\ n)$, the first row of W_n. And this is what we are able to do for the easy cases S_3 and S_4 and for the non-trivial cases S_5 and S_6. Our results agree with the classical ones (see [5]). Our main contribution is that we are able to directly compute the invariants.

Example 8.6. In a split second the computation of S_3 yields the following result. We have $S_3 = \mathbb{C}[a_0, 2g_2, 3g_3, g_4]$ where $g_4 = a_1^2a_2^2 - 2a_1^3a_3 - \frac{8}{3}a_0a_2^3 + 6a_0a_1a_2a_3 - 3a_0^2a_3^2$.

Example 8.7. In a split second the computation of S_4 yields the following result.

We have $S_4 = \mathbb{C}[a_0, 2g_2, 3g_3, g_4, g_5]$ where $g_4 = a_2^2 - 2a_1a_3 + 2a_0a_4$ and
$g_5 = a_2^3 - 3a_1a_2a_3 + 3a_1^2a_4 + \frac{9}{2}a_0a_3^2 - 6a_0a_2a_4$.

Here we come to the non-trivial cases.

Example 8.8. It is known that the highest weighted degree of a generator in a set of minimal generators of S_5 is 45. Therefore we compute a σ-SatSAGBI basis of $\mathbb{Q}[a_0, c_2, \dots, c_5]$ truncated in weighted degree 45, where σ is a term ordering a_0-DegRev type compatible with W.

We need about 7 minutes to compute a set of 57 generators of the truncated SatSAGBI basis and another 5 minutes to minimalize it. The conclusion is that we get 23 generators. Their leading terms are

$$a_0,\ a_1^2,\ a_1^3,\ a_2^2,\ a_1a_2^2,\ a_2^3,\ a_1a_2^3,\ a_1^2a_3^2,\ a_1^3a_3^2,\ a_2^2a_3^2,\ a_1a_2^2a_3^2,\ a_2^3a_3^2,\ a_1a_2^3a_3^2,\ a_1a_2^2a_3^3,\ a_1^3a_3^4,$$
$$a_2^4a_3^3a_2^5a_3^3,\ a_1^2a_2^2a_3^2a_4^2,\ a_1^2a_2^2a_3^5,\ a_1^2a_2^2a_3^7,\ a_1^2a_2^2a_3^8,\ a_1^2a_2^3a_3^8,\ a_1^2a_2^5a_3^{11}$$

Their bi-degrees are

$$(0,1),\ (2,2),\ (3,3), (4,2),\ (5,3),\ (6,3),\ (7,4), (8,4),\ (9,5),\ (10,4), (11,5),\ (12,5),\ (13,6),$$
$$(14,6),\ (15,7),\ (17,7),\ (19,8),\ (20,8),\ (21,9),\ (27,11),\ (30,12),\ (32,13),\ (45,18)$$

The sizes of the supports of the 23 polynomials are

(1, 2, 3, 3, 5, 5, 9, 9, 13, 12, 17, 20, 29, 30, 36, 49, 65, 59, 93, 183, 247, 319, 848)

For the interested reader the following link provides the code we wrote and the actual polynomials we computed
`http://www.dima.unige.it/~bigatti/data/ComputingSaturationsOfSubalgebras/`.

Example 8.9. It is known that the highest weighted degree of a generator in a set of minimal generators of S_6 is 45. Therefore we compute a σ-SatSAGBI basis of $\mathbb{Q}[a_0, c_2, \ldots, c_6]$ truncated in weighted degree 45, where σ is a term ordering a_0-DegRev type compatible with W.

We need about 2 hours and 15 minutes to compute a set of 83 generators of the truncated SatSAGBI basis and another 1 hour and 40 minutes to minimalize it. The conclusion is that we get 26 generators. Their leading terms are

$$a_0,\ a_1^2,\ a_1^3, a_2^2,\ a_1a_2^2,\ a_3^2,\ a_2^3,\ a_1a_2^3,\ a_2a_3^2,\ a_1a_2a_3^2,\ a_1a_3^3,\ a_1^2a_3^3,\ a_2^2a_4^2,\ a_2^2a_3^3,\ a_2^3a_4^2,\ a_1a_2^3a_4^2,$$
$$a_2^3a_3^3,\ a_2^3a_4^3,\ a_1a_2^2a_3^2a_4^2,\ a_2^4a_4^3,\ a_2^3a_3^3a_4^2,\ a_1a_2^3a_3^2a_4^3,\ a_2^4a_3^3a_4^3,\ a_1^2a_2^2a_3^2a_4^2a_5^2,\ a_1^2a_2^2a_3^3a_4^5,\ a_1^2a_2^2a_3^5a_4^6$$

Their bi-degrees are

$$(0,1),\ (2,2),\ (3,3),\ (4,2),\ (5,3),\ (6,2),\ (6,3),\ (7,4),\ (8,3),\ (9,4),\ (10,4),\ (11,5),$$
$$(12,4),\ (13,5),\ (14,5),\ (15,6),\ (15,6),\ (18,6),\ (19,7),\ (20,7),\ (23,8),\ (25,9),\ (29,10),$$
$$(30,10),\ (35,12),\ (45,15)$$

The sizes of the supports of the 26 polynomials are

1, 2, 3, 3, 5, 4, 6, 9, 8, 13, 12, 20, 16, 28, 29, 42, 47, 52, 77, 85, 135, 196, 312,

246, 586, 1370

As in Example 8.8, the following link provides the code and the polynomials
`http://www.dima.unige.it/~bigatti/data/ComputingSaturationsOfSubalgebras/`.

9. Conclusions

In this paper we deal with the problem of saturating S with respect to g, and we denote the resulting K-algebra by $\mathrm{Sat}_g(S)$. Here S is a finitely generated K-subalgebra of a polynomial ring $P = K[a_0, a_1, \dots, a_n]$ with K being any field. It turns out that $\mathrm{Sat}_g(S) = S : g^\infty$ if $g \in S$ which we always assume throughout this paper. After several preparatory results we get Algorithm 3.12 which solves the problem if $\mathrm{Sat}_g(S)$ is a finitely generated K-algebra. If not, the algorithm is simply a procedure which allows us to get closer and closer to the saturation. As said in the introduction, [4] contains a similar result (see [4, Semi-algorithm 4.10.16]).

Then we introduce techniques coming from the theory of SAGBI bases which show their power mainly in the case that S is graded. We describe an algorithm which allows to minimalize a given set of homogeneous generators of a K-subalgebra of P (see Algorithm 6.2). Then Theorem 7.2 illustrates a nice interplay between saturating S with respect to an indeterminate and computing a special SAGBI basis of S. The first output of this theorem is Procedure 7.5 whose power is illustrated by some interesting examples. We prove that Procedure 7.5 is correct and conjecture that it terminates whenever $\mathrm{Sat}_g(S)$ is a finitely generated K-algebra (see Conjecture 7.7).

The final part of the paper is dedicated to find a direct attack to the problem of computing the algebras S_n of U-invariants, a classical problem which goes back to the nineteenth century. We succeed up to degree 6, we do it without the assumption that $K = \mathbb{C}$, and we are able to compute not only a minimal set of U-invariants, but also a truncated SAGBI basis of the corresponding algebra.

If $g \notin S$ we denote $S[g^{-1}] \cap P$ by *weak saturation* of S with respect to g. It turns out that this algebra is very different from $S : g^\infty$ which, in general, is not even an algebra. The problem of computing $S[g^{-1}] \cap P$ if $g \notin S$ can be inspiration for future research.

References

[1] A.M. Bigatti, R. La Scala, and L. Robbiano. Computing Toric Ideals. *J. Symb. Comput.*, 27:351–365, 1999.

[2] A. Bravo. Some Facts About Canonical Subalgebra Bases. In *Trends in Commutative Algebra*, volume 51, pages 247–254. MSRI Publications, 2004.

[3] A. Conca, J. Herzog, and G. Valla. Sagbi bases with applications to blow-up algebras. *J. Reine Angew. Math.*, 474:113–138, 1996.

[4] H. Derksen and G. Kemper. *Computational Invariant Theory.* Number 130 in Encyclopaedia of Mathematical Sciences. Springer, Heidelberg, Heidelberg, New York, Dordrecht, London, 2 edition, 2015.

[5] M. Popoviciu Draisma. *Invariants of Binary Forms.* PhD thesis, Mathematics, Basel, 2013.

[6] D. Kapur and K. Madlener. A Completion Procedure for Computing a Canonical Basis for a k-Subalgebra. *Proc. of Computers and Mathematics '89, MIT, Cambridge*, pages 1–11, 1989.

[7] H. Kraft and C. Procesi. Perpetuants: A Lost Treasure. `ArXiv:1810.01131v1,v3`, 2018–2020.

[8] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 1.* Springer, Heidelberg, 2000, second edition 2008.

[9] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 2.* Springer, Heidelberg, 2005.

[10] P. Mondal. When is the intersection of two finitely generated subalgebras of a polynomial ring also finitely generated? *Arnold Mathematical Journal*, 3(3):333–350, 2017.

[11] L. Robbiano and M. Sweedler. Subalgebra Bases. In *Proceedings, Salvador 1988, Lect. Notes Math.*, volume 1430, pages 61–87, 1990.

[12] L. Robbiano and M. Sweedler. Ideal and Subalgebra Coefficients. *Proc. Amer. Math. Soc.*, 126:2213–2219, 1998.

[13] M. Stillman and H. Tsai. Using SAGBI bases to compute invariants. *J. Pure Appl. Algebra*, 139:285–302, 1999.

[14] B. Sturmfels. *Gröbner Bases and Convex Polytopes.* American Mathematical Society, Providence, RI, 1996.