Some Facts About Canonical Subalgebra Bases

ANA BRAVO

ABSTRACT. This is a brief exposition of canonical subalgebra bases, their uses and their computation.

CONTENTS

1. Introduction

Let k be a field, let $R \subset k[x_1, \ldots, x_n]$ be a finitely generated subalgebra, and let $>$ be a term ordering in $k[x_1, \ldots, x_n]$. A subset B of R is said to be a *canonical subalgebra basis*, or *SAGBI basis*, of R, if

$$\mathrm{in}_> B := \{\mathrm{in}_> f : f \in B\}$$

generates the subalgebra $\mathrm{in}_> R := \{\mathrm{in}_> g : g \in R\}$ of $k[x_1, \ldots, x_n]$. If B is a SAGBI basis for R, it generates R as a k-algebra.

The abbreviation SAGBI stands for "subalgebra analog to Gröbner basis for ideals"; as we will see in Section 2 there are several similarities between canonical subalgebra bases and Gröbner bases.

The simplest example occurs when $R \subset k[x_1, \ldots, x_n]$ is generated by a single element, in which case this same generator is also a canonical subalgebra basis.

The notion was introduced by Kapur and Madlener [1989] and independently by Robbiano and Sweedler [1990]. SAGBI bases are used to test subalgebra

membership. Algorithms for computing canonical subalgebra bases are presented in both [Kapur and Madlener 1989] and [Robbiano and Sweedler 1990].

From the algebraic point of view, canonical bases are very interesting. For instance, if $\mathrm{in}_> R$ is finitely generated, the study of $\mathrm{in}_> R$ is simpler than that of R, and in many cases both algebras share the same properties. As an example, in [Conca et al. 1996] it is shown that if $\mathrm{in}_> R$ is normal, Cohen–Macaulay, and has rational singularities, R has the same properties.

From the geometric perspective, SAGBI bases also offer interesting possibilities. When $\mathrm{in}_> R$ is finitely generated, it can be regarded as the associated graded ring of a suitable degree filtration of R. As a consequence $\mathrm{in}_> R$ can be interpreted as the special fiber of a one-parameter family with R as a general fiber. In this case the general fiber and the special fiber of the family share geometric properties. See [Conca et al. 1996; Sturmfels 1996] and also Section 6 below for discussion.

This philosophy appears, in the analytic case, in [Teissier 1975] and [Goldin and Teissier 2000], as an approach to resolution of singularities of plane curves: Given a suitable parametrization of a plane curve, construct a flat family of curves in such a way that the general fiber is isomorphic to the original curve, and the special fiber is a monomial curve. Then a toric resolution of singularities of the special fiber induces a resolution of the generic fiber [Goldin and Teissier 2000, § 6].

Canonical subalgebra bases have also been studied for algebras over arbitrary rings in [Miller 1996] and [Stillman and Tsai 1999]. For other applications and examples, see [Göbel 2002; 2001; 2000; 1999c; 1999b; 1999a; 1998; Göbel and Maier 2000; Miller 1998; Nordbeck 2002].

2. SABGI Bases Versus Gröbner Bases

As pointed out in the introduction, canonical subalgebra bases and Gröbner bases play similar roles in two different contexts: The first are used to test subalgebra membership while the second do the same work for ideals.

This similarity can be carried out one step further in two different directions: The computational point of view and the geometric interpretation.

The Subduction Algorithm described in [Sturmfels 1996, Chapter 11] corresponds to the subalgebra analog of the Division Algorithm for ideals (which produces, for any element f in an ideal I, an expression of f as a linear combination of a Gröbner basis of I):

ALGORITHM 2.1 (SUBDUCTION ALGORITHM FOR A CANONICAL BASIS $\mathscr{C}$). Given a canonical basis $\mathscr{C}$ for a subalgebra $R \subset k[x_1, \ldots, x_n]$ and given $f \in k[x_1, \ldots, x_n]$, the algorithm computes an expression for f as a polynomial in the elements of $\mathscr{C}$, provided that $f \in R$.

Step 1. Find $f_1, \ldots, f_r \in \mathscr{C}$ and exponents $i_1, \ldots, i_r \in \mathbb{N}$ and $c \in k \setminus \{0\}$ such that

$$\mathrm{in}_> f = c \cdot \mathrm{in}_> f_1^{i_1} \cdots \mathrm{in}_> f_r^{i_r}. \qquad (2\text{--}1)$$

Step 2. If it is not possible to find an expression as in (2–1) then $f \notin R$, and the algorithm stops.

Step 3. Otherwise, set $g := c \cdot f_1^{i_1} \cdots f_r^{i_r}$, and replace f by $f - g$. Repeat the previous steps until the algorithm stops or f is a constant in k.

In Section 5 we will also see how this algorithm can be used to produce an algorithm to compute SAGBI bases which is similar to Buchberger's algorithm for computing Gröbner bases.

As for the geometric interpretation, let $I \subset k[x_1, \ldots, x_n]$ be the ideal defining a variety X, and $>$ a term ordering in $k[x_1, \ldots, x_n]$. The question is:

How close are X and $\mathrm{Spec}\,(k[x_1, \ldots, x_n]/\mathrm{in}_> I)$*?*

The general theory of Gröbner basis says that one can construct a flat family of varieties over a one-dimensional scheme $\mathrm{Spec}\,(k[t])$, whose general fiber is isomorphic to X, and whose special fiber at $t = 0$ is $\mathrm{Spec}\,(k[x_1, \ldots, x_n]/\mathrm{in}_> I)$. In this sense we say that the original variety X deforms into $\mathrm{Spec}\,(k[x_1, \ldots, x_n]/\mathrm{in}_> I)$.

Now let Y be a variety parametrized by equations $f_1, \ldots, f_s \in k[t_1, \ldots, t_m]$, and let $>$ be a term ordering in $k[t_1, \ldots, t_m]$. If $\{g_1, \ldots, g_r\}$ is a canonical subalgebra basis of $k[f_1, \ldots, f_s]$, we will see in Section 6 that one can construct a one-parameter flat family of varieties, whose general fiber is isomorphic to Y, and whose special fiber is a toric variety; the generators of the algebras degenerate into monomials and the relations between them into binomials.

Perhaps the main difference between Gröbner bases and canonical subalgebra bases is that while the first are always finite, the second may fail to be so. This point is discussed in the next section.

3. When Are SAGBI Bases Finite?

Canonical subalgebra bases are not always finite; finiteness may even depend on the term ordering $>$ chosen on $k[x_1, \ldots, x_n]$. We examine some examples.

If $R \subset k[x, y]$ is generated by $\{x + y, xy, xy^2\}$, then R does not have a finitely generated canonical subalgebra basis, no matter what term ordering we fix in $k[x, y]$: If $x > y$, it can be shown that a SAGBI basis of R must contain the infinite set $S = \{x + y, \; xy^n : n > 0\}$. If $y > x$, note that R is also generated by $\{x + y, xy, x^2 y\}$. It can be shown that

$$S = \{x + y, \; yx^n : n > 0\}$$

should be contained in a SAGBI basis for R [Robbiano and Sweedler 1990, Example 1.20].

On the opposite extreme, the symmetric algebra $R \subset k[x_1, \ldots, x_n]$ always has a finitely generated canonical subalgebra basis B which does not depend on the order previously chosen: In this case, B is the set of elementary symmetric polynomials [Robbiano and Sweedler 1990, Theorem 1.14].

There are also examples of subalgebras that, depending on the order fixed, may or may not have a finite canonical subalgebra basis: Let $R \subset k[x, y]$ be the subalgebra generated by $\{x, \, xy - y^2, \, xy^2\}$. If we fix a term ordering on $k[x, y]$ such that $y > x$, then $B = \{x, \, xy - y^2, \, xy^2\}$ is indeed a canonical subalgebra basis for R, while if we fix a term ordering such that $x > y$ then it can be shown that $k[x, xy, xy^2, \ldots] \subset \text{in}_> R$, and therefore it cannot have a finite SAGBI basis [Robbiano and Sweedler 1990, Example 4.11]. For these and other examples, we refer the reader to [Göbel 2000; Göbel 1999b; Robbiano and Sweedler 1990].

In general, it is a hard problem to decide whether a given subalgebra does have a finite canonical subalgebra basis. Some conditions are as follows:

PROPOSITION 3.1 [Robbiano and Sweedler 1990, Proposition 4.7]. *Suppose that R is a subalgebra of $k[x_1, \ldots, x_n]$ and that C is a finitely generated subalgebra of $k[x_1, \ldots, x_n]$ containing $\text{in}_> R$. If C is integral over $\text{in}_> R$, then R has a finite SAGBI basis. In particular if $k[x_1, \ldots, x_n]$ is integral over $\text{in}_> R$, then R has a finite SAGBI basis.*

A corollary of the previous proposition is that when $n = 1$, things become less chaotic: Any subalgebra R of $k[x]$ has a finite subalgebra basis [Robbiano and Sweedler 1990, Corollay 4.8]. And when the number of generators is low, there are even easy criteria to decide if a given set of generators of a subalgebra of $k[x]$ is a canonical basis:

THEOREM 3.2 [Torstensson 2002, Theorems 10, 12]. *Let $f, g \in k[x]$ and consider the subalgebra $R \subset k[x]$ generated by them. Then:*

(i) *If f and g have relatively prime degrees, they form a canonical subalgebra basis for R.*
(ii) *If $\deg f$ divides $\deg g$, f and g form a canonical subalgebra basis for R if and only if g is a polynomial in f.*

For more along these lines see Propositions 6, 7, and Theorems 12 and 14 in [Torstensson 2002].

4. Finite SAGBI Bases

Let $R \subset k[x_1, \ldots, x_n]$ be a subalgebra generated by $B = \{f_1, \ldots, f_s\}$, let $>$ be a monomial ordering in $k[x_1, \ldots, x_n]$, and assume that R has a finite canonical subalgebra basis. The purpose of this section is to describe a criterion to decide whether B is a canonical basis for R. In Section 5 and 6 some consequences of this result will be discussed. The setup that follows can be found in [Sturmfels 1996, Chapter 11].

Consider the exact sequences

$$0 \longrightarrow I \longrightarrow k[t_1, \ldots, t_s] \longrightarrow k[f_1, \ldots, f_s] \longrightarrow 0$$
$$t_i \longmapsto f_i$$

(4–1)

$$0 \longrightarrow I_A \longrightarrow k[t_1, \ldots, t_s] \longrightarrow k[\operatorname{in}_> f_1, \ldots, \operatorname{in}_> f_s] \longrightarrow 0$$
$$t_i \longmapsto \operatorname{in}_> f_i$$

Since the kernel of the second map represents relations between monomials, the ideal I_A is generated by binomials—it is a toric ideal.

Let $\omega = (\omega_1, \ldots, \omega_n) \in \mathbb{R}^n$ be a weight vector which represents the term ordering $>$ for the polynomials $\{f_1, \ldots, f_s\}$.

Assume that $\operatorname{in}_> f_i = x_1^{a_{i1}} \cdots x_n^{a_{in}}$, for $i = 1, \ldots, s$. Then

$$A = \begin{pmatrix} a_{11} & \cdots & a_{s1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{sn} \end{pmatrix}$$

is an $n \times s$ matrix, and

$$A^T \omega = \begin{pmatrix} a_{11}\omega_1 + \ldots + a_{1n}\omega_n \\ \vdots \\ a_{s1}\omega_1 + \ldots + a_{sn}\omega_n \end{pmatrix}$$

is a vector in $\mathbb{R}^s$, which can be thought of as a weight vector defining an order in $k[t_1, \ldots, t_s]$. Therefore it can be used to form an initial ideal $\operatorname{in}_{A^T \omega} I$ of I. In general this will not be a monomial ideal since $A^T \omega$ may not be a generic vector, even if ω is (see Example 4.2 below).

The key point is that the comparison between I_A and $\operatorname{in}_{A^T \omega} I$ gives a criterion for deciding whether or not $\{f_1, \ldots, f_s\}$ is a canonical basis for the subalgebra that they generate.

In general $\operatorname{in}_{A^T \omega} I \subset I_A$ [Sturmfels 1996, Lemma 11.3], but if equality holds, then $\{f_1, \ldots, f_s\}$ is a canonical basis. More precisely:

THEOREM 4.1 [Sturmfels 1996, Theorem 11.4]. *The set $\{f_1, \ldots, f_s\}$ is a canonical basis if and only if $\operatorname{in}_{A^T \omega} I = I_A$.*

EXAMPLE 4.2. Let $R = k[x^2 + x^3, x + x^2] \subset k[x]$, and let us temporarily forget that we already know that $\{x^2 + x^3, x + x^2\}$ is a canonical subalgebra basis (since the degrees of the generators are coprime). With the notation above, we have $I = \langle t_2^3 - t_1^2 - t_1 t_2 \rangle$, and that $I_A = \langle t_2^3 - t_1^2 \rangle$. Let $A = (3, 2)$. Then $A^T \omega = \binom{3}{2}$ and $\operatorname{in}_{A^T \omega} I = \langle t_2^3 - t_1^2 \rangle = I_A$. Hence, by Theorem 4.1, $\{x^2 + x^3, x + x^2\}$ is a SAGBI basis for R.

5. An Algorithm to Compute SAGBI bases

Theorem 4.1 can be used to construct an algorithm for computing canonical subalgebra bases. With the same notation as in Section 4, first we state the following corollary to Theorem 4.1:

COROLLARY 5.1 [Sturmfels 1996, Corollary 11.5]. *Let $\{p_1, \ldots, p_t\}$ be generators for the toric ideal I_A. Then $\{f_1, \ldots, f_s\}$ is a canonical basis if and only if Algorithm 2.1 reduces $p_i(f_1, \ldots, f_s)$ to a constant for all $i = 1, \ldots, t$.*

Therefore, to apply the criterion of Theorem 4.1 there is no need to compute generators for I, since only the ones of I_A are used. Let us see how this works with an example:

EXAMPLE 5.2. Consider $R = [x^4 + x^3, \, x^2 + x] \subset k[x]$. By [Robbiano and Sweedler 1990, Corollay 4.8] there is a finite SAGBI basis for R. With the same notation as in Section 4 we have $A = (4, 2)$, $I = \langle t_1^2 - 2t_1 t_2^2 - t_1 t_2 + t_2^4 \rangle$, $A^T \omega = \binom{4}{2}$ and

$$\mathrm{in}_{A^T \omega} I = \langle t_1^2 - 2t_1 t_2^2 + t_2^4 \rangle \subsetneq I_A = \langle t_1 - t_2^2 \rangle.$$

Therefore, by Theorem 4.1, the set $\{x^4 + x^3, \, x^2 + x\}$ is not a SAGBI basis for R.

With the notation of Corollary 5.1, $p_1(t_1, t_2) = t_1 - t_2^2$ Algorithm 2.1 does not reduce $p_1(x^4 + x^3, \, x^2 + x)$ to a constant, since $p_1(x^4 + x^3, \, x^2 + x) = x^3 + x^2$. This is as expected. Hence we need to extend our generating set to

$$\{x^4 + x^3, \, x^2 + x, \, x^3 + x^2\}.$$

In this new setting, $I_A = \langle t_2^3 - t_3^2, \, t_1 - t_2^2 \rangle = \langle p_1(t_1, t_2, t_3), \, p_2(t_1, t_2, t_3) \rangle$, and it is easy to check that, in this case, Algorithm 2.1 reduces $p_i(t_1, t_2, t_3)$ to a constant for $i = 1, 2$, and therefore, $\{x^4 + x^3, \, x^2 + x, \, x^3 + x^2\}$ is a SAGBI basis for R.

REMARK 5.3. The algorithm that follows from Corollary 5.1 (used in Example 5.2) is similar to Buchberger's Algorithm to compute Gröbner bases of ideals, provided that we ahead of time know that there is a finite SAGBI basis.

6. Geometric Interpretation

As a final note we review the geometry behind the previous statements, specially diagram (4–1) and Theorem 4.1.

Assume that X is a variety parametrized by the equations $\{f_1, \ldots, f_s\}$. Using the same notation as in Section 4, if $\{f_1, \ldots, f_s\}$ is a canonical subalgebra bases then by Theorem 4.1, $I_A = \mathrm{in}_{A^T \omega} I$.

The following corollary to Theorem 4.1 relates any reduced Gröbner basis of I_A to a suitable reduced Gröbner basis of I:

COROLLARY 6.1 [Sturmfels 1996, Corollary 11.6]. *With the same notation as in Section 4, assume that $\{f_1, \ldots, f_s\}$ is a canonical subalgebra basis. Then every reduced Gröbner basis $\mathscr{G}$ of I_A lifts to a reduced Gröbner basis $\mathscr{H}$ of I, i.e. the elements of $\mathscr{G}$ are the initial forms with respect to $A^T\omega$ of the elements of $\mathscr{H}$.*

Now, the general theory of Gröbner bases tells us that we can construct a one-parameter flat family of varieties whose general fiber is isomorphic to X and whose special fiber is isomorphic to $\mathrm{Spec}\,(k[t_1, \ldots, t_s]/\mathrm{in}_{A^T\omega}I)$.

Therefore, Corollary 6.1, implies that we can construct a one-parameter flat family of varieties whose general fiber is isomorphic to X and whose special fiber is isomorphic to $\mathrm{Spec}\,(k[t_1, \ldots, t_s]/I_A)$: The parametric equations defining X degenerate into monomials and the relations among them into binomials. Therefore X degenerates to a toric variety.

Acknowledgments

References

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

[Göbel 1998] M. Göbel, "A constructive description of SAGBI bases for polynomial invariants of permutation groups", *J. Symbolic Comput.* **26**:3 (1998), 261–272.

[Göbel 1999a] M. Göbel, "The optimal lower bound for generators of invariant rings without finite SAGBI bases with respect to any admissible order", *Discrete Math. Theor. Comput. Sci.* **3**:2 (1999), 65–70.

[Göbel 1999b] M. Göbel, "The 'smallest' ring of polynomial invariants of a permutation group which has no finite SAGBI bases w.r.t. any admissible order", *Theoret. Comput. Sci.* **225**:1-2 (1999), 177–184.

[Göbel 1999c] M. Göbel, "Three remarks on SAGBI bases for polynomial invariants of permutation groups", pp. 190–201 in *Combinatorics, computation & logic '99* (Auckland, 1999), edited by C. S. Calude and M. J. Dinneen, Discrete Mathematics and Theoretical Computer Science **333**, Springer, Singapore, 1999.

[Göbel 2000] M. Göbel, "Rings of polynomial invariants of the alternating group have no finite SAGBI bases with respect to any admissible order", *Inform. Process. Lett.* **74**:1-2 (2000), 15–18.

[Göbel 2001] M. Göbel, "Visualizing properties of comprehensive SAGBI bases: two examples", *Appl. Algebra Engrg. Comm. Comput.* **12**:5 (2001), 429–435.

[Göbel 2002] M. Göbel, "Finite SAGBI bases for polynomial invariants of conjugates of alternating groups", *Math. Comp.* **71**:238 (2002), 761–765.

[Göbel and Maier 2000] M. Göbel and P. Maier, "Three remarks on comprehensive Gröbner and SAGBI bases", pp. 191–202 in *Computer algebra in scientific computing* (Samarkand, 2000), edited by V. G. Ganzha et al., Springer, Berlin, 2000.

[Goldin and Teissier 2000] R. Goldin and B. Teissier, "Resolving singularities of plane analytic branches with one toric morphism", pp. 315–340 in *Resolution of singularities* (Obergurgl, 1997), edited by H. Hauser et al., Progr. Math. **181**, Birkhäuser, Basel, 2000.

[Kapur and Madlener 1989] D. Kapur and K. Madlener, "A completion procedure for computing a canonical basis for a k-subalgebra", pp. 1–11 in *Computers and mathematics* (Cambridge, MA, 1989), edited by E. Kaltofen and S. M. Watt, Springer, New York, 1989.

[Miller 1996] J. L. Miller, "Analogs of Gröbner bases in polynomial rings over a ring", *J. Symbolic Comput.* **21**:2 (1996), 139–153.

[Miller 1998] J. L. Miller, "Effective algorithms for intrinsically computing SAGBI-Gröbner bases in a polynomial ring over a field", pp. 421–433 in *Gröbner bases and applications* (Linz, 1998), edited by B. Buchberger and F. Winkler, London Math. Soc. Lecture Note Ser. **251**, Cambridge Univ. Press, Cambridge, 1998.

[Nordbeck 2002] P. Nordbeck, "SAGBI bases under composition", *J. Symbolic Comput.* **33**:1 (2002), 67–76.

[Robbiano and Sweedler 1990] L. Robbiano and M. Sweedler, "Subalgebra bases", pp. 61–87 in *Commutative algebra* (Salvador, 1988), edited by W. Bruns and A. Simis, Lecture Notes in Math. **1430**, Springer, Berlin, 1990.

[Stillman and Tsai 1999] M. Stillman and H. Tsai, "Using SAGBI bases to compute invariants", *J. Pure Appl. Algebra* **139**:1-3 (1999), 285–302.

[Sturmfels 1996] B. Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series **8**, Amer. Math. Soc., Providence, 1996.

[Teissier 1975] B. Teissier, "Appendice", pp. 145–199 in *Le problème des modules pour les branches planes*, by O. Zariski, Centre de Mathématiques de l'École Polytechnique, Paris, 1975. Second edition, Hermann, 1986.

[Torstensson 2002] A. Torstensson, "Canonical bases for subalgebras on two generators in the univariate polynomial ring", *Beiträge Algebra Geom.* **43**:2 (2002), 565–577.

ANA BRAVO
DEPARTAMENTO DE MATEMÁTICAS
UNIVERSIDAD AUTÓNOMA DE MADRID
28049 MADRID
SPAIN
abravo@msri.org