Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Symbolic Computation 40 (2005) 1087–1105
Journal of Symbolic Computation
www.elsevier.com/locate/jsc

Using resultants for SAGBI basis verification in the univariate polynomial ring

Anna Torstensson, Victor Ufnarovski, Hans Öfverbeck*

Centre for Mathematical Sciences, Lund University, Box 118, SE-221 00 Lund, Sweden

Received 19 November 2003; accepted 21 June 2004
Available online 4 June 2005

Abstract

A resultant-type identity for univariate polynomials is proved and used to characterise SAGBI bases of subalgebras generated by two polynomials. A new equivalent condition, expressed in terms of the degree of a field extension, for a pair of univariate polynomials to form a SAGBI basis is derived.

MSC: 12Y05; 68W30; 13P99

Keywords: SAGBI basis; Resultant; Reduction; Subalgebra; Univariate polynomial ring

1. Introduction

Let

$$f(x) = x^3 + a_2x^2 + a_1x + a_0, \qquad g(x) = x^2 + b_1x + b_0.$$

Is it possible to find a polynomial of degree 1 in the subalgebra generated by $f(x)$ and $g(x)$? It seems to be easy to find such a polynomial. Consider

$$h_1(x) = f^2(x) - g^3(x) = c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$$

* Corresponding author. Tel.: +46 46 222 3408; fax: +46 46 222 4213.
E-mail addresses: anna.to@home.se (A. Torstensson), ufn@maths.lth.se (V. Ufnarovski), hans@maths.lth.se (H. Öfverbeck).

0747-7171/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2004.06.002

and reduce it to degree four:

$$h_2(x) = h_1(x) - c_5 f(x)g(x) = d_4x^4 + d_3x^3 + d_2x_2 + d_1x + d_0.$$

Continuing the reduction in the same manner we get a polynomial

$$h(x) = h_2(x) - d_4g^2(x) - \alpha f(x) - \beta g(x),$$

which has degree at most 1 and we can expect that for some choice of the coefficients a_i, b_j it should have degree exactly 1.

Nevertheless the famous epimorphism theorem by Abhyankar and Moh (1973a,b, 1975) shows that this is not the case in characteristic zero. We will see later that the same is true in any characteristic and from Torstensson (2002) we know that the reason is that $f(x)$ and $g(x)$ form a SAGBI basis if their degrees are relatively prime. But what is the reason for this? There should be some kind of identity that explains why $h(x)$ becomes a constant. The aim of this article is to find an identity which explains why $f(x)$ and $g(x)$ form a SAGBI basis if their degrees are relatively prime. As we will see this identity is closely related to the resultant. The essential advantage of this approach is that the identity gives some information on the structure of the subalgebra generated by two polynomials even in the case when their degrees have a common factor.

Besides that, we discuss how a general SAGBI theory looks in the univariate polynomial ring and describe two different necessary and sufficient conditions for polynomials $f(x)$ and $g(x)$ to form a SAGBI basis.

The present article is an extended version of Torstensson et al. (2003). Only minor differences exist in Sections 2–4. In Section 5 there is a major difference: in Torstensson et al. (2003) Theorem 24 is stated without proof; in the present article a full proof including Lemmas 22 and 23 is added. This is the only major difference in Section 5. Sections 6 and 7 do not appear in the shorter version.

2. Basic definitions and notation

Let $K[x]$ denote the polynomial ring in one variable with coefficients in the field K. If $f = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, where $a_n \neq 0$, is a polynomial of degree $n = \deg(f)$, then the *leading term* of f is a_nx^n. Let R be a subset of $K[x]$ then $\deg(R) = \{\deg(r) \mid r \in R \setminus \{0\}\}$. If A is a subalgebra, then $\deg(A)$ is an additive subsemigroup of $\mathbb{N}$. Note that we assume that $0 \in \mathbb{N}$.

Our goal is to study subalgebras of $K[x]$ generated by a subset R of $K[x]$. Denote this subalgebra as $K[R]$. This notation is natural since $K[R]$ consists precisely of the "polynomials" in the "variables" R. In line with this analogy we will call a finite product of elements from R an *R-monomial*; the identity of $K[x]$ is by convention an empty product and thus always an R-monomial.

The main tool for investigating and representing subalgebras is called *SAGBI bases*, where SAGBI is an acronym for Subalgebra Analogue to Gröbner Bases for Ideals. The theory of SAGBI bases was originally developed for multivariate polynomial rings by Robbiano and Sweedler (1990) and independently by Kapur and Madlener (1989);

another source for material on SAGBI bases is Sturmfels (1996). The definition can in our one-variable setting be somewhat simplified:

Definition 1 (*SAGBI Basis*). Let A be a subalgebra of $K[x]$ and $R \subseteq A$. R is a *SAGBI basis* for A if $\deg(R)$ generates $\deg(A)$ as an additive semigroup, that is if every element in $\deg(A)$ can be written as a finite (or empty) sum of elements in $\deg(R)$.

Remark 2. Note that the defining property of a SAGBI basis R depends only on the degrees of the polynomials, thus multiplication of the elements in R by non-zero elements of K is always permitted. This allows us to assume that all polynomials in R are monic. Whenever convenient we will use this fact without further comment.

Remark 3. Perhaps the biggest difference between SAGBI bases in the one-variable setting and the multi-variable setting is that all subalgebras in the former have a finite SAGBI basis while this does not hold in the latter. This was noted by Robbiano and Sweedler (1990) and follows from the fact that any semigroup consisting of natural numbers is finitely generated.

If R is a SAGBI basis for A then it is known (Robbiano and Sweedler, 1990) that A is the subalgebra generated by R. Therefore we say that R is a *SAGBI basis* (without reference to a subalgebra) if R is a SAGBI basis for the subalgebra it generates.

One of the cornerstones of SAGBI theory is the concept of subduction; *sub*algebra re*duction*.

Definition 4 (*Subduction*). Let R be a subset of $K[x]$ and f a polynomial. If there exist R-monomials $p_1, \ldots, p_k$ and constants $a_1, \ldots, a_k$ such that $a_i p_i$ has the same leading term as $f - \sum_{j=1}^{i-1} a_j p_j$, for $i = 1, \ldots, k$, then we say that f *subduces* to $r = f - \sum_{j=1}^{k} a_j p_j$ over R. We call r a *remainder* of f if it cannot be subduced further.

Remark 5. Note that we do *not* require R to be a SAGBI basis for subduction over R to be defined and that remainders are not unique in general.

In our definition of subduction we allow subtraction of constants; this differs from Robbiano and Sweedler's definition, cf. Remark 1.8 of Robbiano and Sweedler (1990). This difference is only minor and we can easily translate results; in particular, Proposition 2.3 (a–b) of Robbiano and Sweedler (1990) becomes:

Theorem 6. *Let R be a subset of $K[x]$, then the following conditions are equivalent:*

(i) *R is a SAGBI basis.*
(ii) *All elements of $K[R]$ subduce to zero over R.*

2.1. Construction and verification of SAGBI bases

The results in this article will give some alternative ways of checking if a set consisting of two, and in certain cases three, polynomials is a SAGBI basis. Before we go into this we will give a brief exposition of the standard SAGBI testing and construction algorithms.

Let $R = \{f_1, \ldots, f_l\}$ be a finite subset of $K[x]$.

The key to the SAGBI test lies in the definition of a SAGBI basis. Since the elements in $K[R]$ are sums over K of R-monomials, and each R-monomial clearly has a degree which is the sum of degrees of elements in R, one might think that the condition in the definition should always be satisfied. This is however wrong since the terms of the highest degree might cancel and then the degree of the sum need not be the degree of any of the R-monomials in the sum. The simplest form of cancellation is when we take the difference of two polynomials with the same leading term.

Definition 7. A difference

$$f_1^{a_1} \cdots f_l^{a_l} - f_1^{b_1} \cdots f_l^{b_l} \tag{1}$$

of two polynomials such that $f_1^{a_1} \cdots f_l^{a_l}$ and $f_1^{b_1} \cdots f_l^{b_l}$ have the same leading term is called a *T-polynomial*.

The T-polynomial (1) has a *low representation* over R if it can be written as a K-linear combination of R-monomials of degree strictly less than $\deg(f_1^{a_1} \cdots f_l^{a_l}) = \deg(f_1^{b_1} \cdots f_l^{b_l})$.

Note that if a T-polynomial subduces to zero over R, then it has a low representation over R. The "T" in "T-polynomial" is chosen since a pair of R-monomials $(f_1^{a_1} \cdots f_l^{a_l}, f_1^{b_1} \cdots f_l^{b_l})$ as in the definition is called a "*t*ête-a-tête" by Robbiano and Sweedler (1990).

Now let us see in more detail what the T-polynomials look like. Let $R = \{f_1, \ldots, f_l\}$ be a finite subset of $K[x]$, where $\deg(f_i) = n_i$, and assume for simplicity that all elements of R are monic. Two R-monomials, $\prod_{i=1}^{l} f_i^{a_i}$ and $\prod_{i=1}^{l} f_i^{b_i}$, have the same leading term if and only if

$$[(a_1, \ldots, a_l), (b_1, \ldots, b_l)] \in \mathbb{N}^l \times \mathbb{N}^l$$

is a solution of the linear Diophantine equation:

$$\sum_{i=1}^{l} a_i n_i - \sum_{i=1}^{l} b_i n_i = 0. \tag{2}$$

The T-polynomial corresponding to this solution is then:

$$T((a_1, \ldots, a_l), (b_1, \ldots, b_l)) = \prod_{i=1}^{l} f_i^{a_i} - \prod_{i=1}^{l} f_i^{b_i}.$$

If $a = (a_1, \ldots, a_l) \in \mathbb{N}^l$, then for convenience we define f^a to be the product $\prod_{i=1}^{l} f_i^{a_i}$. Of course Eq. (2) has an infinite number of solutions, so it is not possible to check *all* T-polynomials. We also note that the set of all solutions of (2), denoted by $M = M(\deg(R))$, is a semigroup under componentwise addition. The following proposition is the key to reducing the number of T-polynomials we need to check:

Proposition 8. *Suppose that a solution $[a, b] \in \mathbb{N}^l \times \mathbb{N}^l$ of the linear Diophantine Eq. (2) can be written as a sum of two non-zero solutions $[a', b']$ and $[a'', b'']$ of (2). Then the*

T-polynomial $T(a, b)$ has a low representation over R if the T-polynomials $T(a', b')$ and $T(a'', b'')$ both have low representations over R.

Proof. Rewrite the T-polynomial:

$$\begin{aligned} T(a,b) &= f^a - f^b = f^{a'+a''} - f^{b'+b''} = f^{a'+a''} - f^{a'+b''} \\ &\quad + f^{a'+b''} - f^{b'+b''} = f^{a'}(f^{a''} - f^{b''}) + f^{b''}(f^{a'} - f^{b'}) \\ &= f^{a'}T(a'', b'') + f^{b''}T(a', b'). \quad \square \end{aligned}$$

The consequence of the proposition above is that we need only check the T-polynomials corresponding to elements of M which cannot be written as non-trivial sums of other elements. Such an element is called *minimal*; the set of minimal elements of M is finite.

An element of the kind $[e_i, e_i]$, where e_i is the vector in $\mathbb{N}^l$ with 1 on the i-th place and zeroes elsewhere, is clearly minimal, but corresponds to a trivial T-polynomial: $T(e_i, e_i) = 0$, for $i = 1, \ldots, l$. Thus, using Proposition 8 we see that it suffices to check the minimal elements of the form $[(a_1, \ldots, a_l), (b_1, \ldots, b_l)]$ where, for each $i \in \{1, \ldots, l\}$, at least one of a_i and b_i is zero; such an element is called a *critical pair*. The set of all critical pairs corresponding to a given l-tuple $(n_1, n_2, \ldots, n_l)$ of positive integer coefficients for (2) is denoted by $C(n_1, n_2, \ldots, n_l)$. If R is a subset of $K[x] \setminus K$ then we define (by abuse of notation) $C(R) = C(\deg(R))$.

Lemma 9. *Let*

$$\deg f(x) = n, \quad \deg g(x) = m, \quad d = \gcd(n, m), \quad n' = n/d, \quad m' = m/d.$$

Then

$$C(f, g) = \{[(m', 0), (0, n')], [(0, n'), (m', 0)]\}.$$

Proof. Suppose that

$$[(i, 0), (0, j)] \in C(f, g).$$

Then

$$in = jm \Rightarrow in' = jm' \Rightarrow i = km' \Rightarrow j = kn'.$$

So

$$[(i, 0), (0, j)] = k[(m', 0), (0, n')]$$

and $k = 1$ because we have assumed that $[(i, 0), (0, j)]$ is minimal. By a symmetric argument any element of $C(f, g)$ which has the form $[(0, j), (i, 0)]$ has to be $[(0, n'), (m', 0)]$. $\square$

Now we can state the main theorem about the SAGBI test:

Theorem 10. *Let R be a subset of $K[x]$, then the following are equivalent:*

(i) *R is a SAGBI basis*

(ii) *All T-polynomials corresponding to $C(R)$ have a low representation over R.*
(iii) *All T-polynomials corresponding to $C(R)$ subduce to zero over R.*

Proof. The interested reader may find the full proof in Robbiano and Sweedler (1990). □

Note that if $[a, b] \in C(R)$ then the *transpose* of $[a, b]$, $[b, a]$, also lies in $C(R)$. Since $T(a, b)$ is a scalar multiple of $T(b, a)$ it suffices to check *one* of these T-polynomials. Combining this fact with Lemma 9 and Theorem 10 we get the following corollary.

Corollary 11. *Let f and g as in Lemma 9, then $\{f, g\}$ is a SAGBI basis if $f^{m'} - g^{n'}$ has a low representation over $\{f, g\}$.*

Suppose we wish to find a SAGBI basis for the subalgebra generated by a set R, then we can start by using Theorem 10 and check if the T-polynomials subduce to zero over R. If they do we can conclude that R is a SAGBI basis. If they do not subduce to zero, then we have performed the first step of the SAGBI construction algorithm.

Algorithm 1. SAGBI basis construction algorithm
INPUT: $R = \{f_1, \ldots, f_l\} \subset K[x]$
OUTPUT: $S = \{s_1, \ldots, s_t\}$ a SAGBI basis for $K[R]$
INITIALISATION: $R_0 = \emptyset$, $R_1 = R$ and $i = 1$
WHILE $R_i \neq R_{i-1}$ **DO**
  Let $R_{i+1} = R_i$, compute the remainders over R_i of all T-polynomials corresponding to $C(R_i)$
  IF some remainders are non-zero **THEN**
    add all of them to R_{i+1}
  ELSE
    put $S = R_i$
  FI
  put $i = i + 1$
OD

Theorem 12. *Given finite input $R = \{f_1, \ldots, f_l\} \subset K[x]$ the SAGBI basis construction algorithm terminates and the output is a finite SAGBI basis for the subalgebra $K[R]$.*

Proof. Note that the degree of every element in $R_{i+1} \setminus R_i$ does not belong to the semigroup generated by $\deg(R_i)$. So if the algorithm would not terminate we would have an infinite increasing chain of subsemigroups in $\mathbb{N}$, but this is impossible. That is why the algorithm terminates and from Theorem 10 it follows that the output, S, is a SAGBI basis for $K[R]$. □

3. Two equivalent conditions for SAGBI

In this section we will give a completely new characterisation of a SAGBI basis consisting of two polynomials. The new characterisation is formulated in the language of field extensions $K \subset L \subset K(x)$, where $K(x)$ stands for the field of all rational functions in the free variable x. The simplest non-trivial case is when L has the form $K(h)$

for some non-constant polynomial h. Let us look at the degree of the extension $K(h) \subseteq K(x)$.

Lemma 13. *If $h \in K[x]$ has degree $d \geq 1$ then $[K(x) : K(h)] = d$.*

Proof. Consider the polynomial

$$p(t) = h(t) - h \ \in K(h)[t],$$

where $h(t)$ denotes the polynomial obtained by replacing all occurrences of x in h by t. The idea of the proof is to show that this polynomial is, up to a constant factor, the minimal polynomial of x over $K(h)$. Then the lemma will follow from a well known result in the theory of field extensions. It is obvious from our definition of p that it has x as a zero, so x is algebraic over $K(h)$ and its minimal polynomial has degree less than or equal to d. Since $\deg(h) \neq 0$, $K[h] \cong K[x]$, thus $K[h]$ is a UFD and $K(h)$ is its field of quotients. Hence, by Gauss' lemma, it suffices to prove that p is irreducible over $K[h]$ to deduce that it is irreducible over $K(h)$.

Suppose for contradiction that there exists a non-zero polynomial, $q \in K[h, t]$ of degree $k < d$ having x as a zero. Then q has the form:

$$q = q_k t^k + q_{k-1} t^{k-1} + \cdots + q_0,$$

where each q_i belongs to $K[h]$. Our assumption can be written:

$$0 = q(x) = q_k x^k + q_{k-1} x^{k-1} + \cdots + q_0. \tag{3}$$

For this equality to hold, all terms containing the same power of x must cancel, but if we consider the degree of each term above modulo d, then we get:

$$\begin{aligned} \deg(q_k x^k) &\equiv k \mod d, \\ \deg(q_{k-1} x^{k-1}) &\equiv k-1 \mod d, \\ &\vdots \\ \deg(q_0) &\equiv 0 \mod d. \end{aligned}$$

The reason for this is that $q_i \in K[h]$ so $\deg(q_i) \equiv 0 \mod d$, since d is the degree of h. Since $k < d$ all these residue classes are different. Hence the highest terms in Eq. (3) cannot cancel, contradiction. Thus a constant multiple of p is the minimal polynomial of x in $K(h)$. □

To proceed we will have to use the following extension of Lüroth's theorem:

Theorem 14. *An intermediate field $K \subset F \subset K(x)$ containing non-constant elements of $K[x]$ has the form $F = K(y)$ for some $y \in K[x]$.*

Proof. This extension is stated as exercise 12 (a) (with a hint making it trivial) in Bourbaki (1990, p. 148–149). □

The result above allows us to prove the main theorem of this section independently of characteristic.

Theorem 15. *Let f and g be polynomials of degree n and m respectively, let $d = \gcd(n, m)$ and let K be any field. Then the following conditions are equivalent:*

(i) *f, g is a SAGBI basis.*
(ii) *There exists a polynomial h of degree d and polynomials F and G such that $f = F \circ h$ and $g = G \circ h$.*
(iii) $[K(x) : K(f, g)] = d$.

Proof. The equivalence (i) $\Leftrightarrow$ (ii) was already proved by Torstensson (2002) for characteristic zero. To make this proof work in any characteristic it is sufficient to replace the reference to the zero-characteristic version of Theorem 14 in Lausch and Nöbauer (1973) by Theorem 14. It remains to prove that (iii) $\Leftrightarrow$ (ii).

- (ii) $\Rightarrow$ (iii) Since f and g are polynomials in h we have $K(f, g) \subseteq K(h)$; hence we have $[K(x) : K(f, g)] \geq [K(x) : K(h)] = d$, where the equality follows from Lemma 13. On the other hand we can combine the tower law and Lemma 13:

$$n = [K(x) : K(f)] = [K(x) : K(f, g)][K(f, g) : K(f)],$$
$$m = [K(x) : K(g)] = [K(x) : K(f, g)][K(f, g) : K(g)].$$

  Hence $[K(x) : K(f, g)] \mid \gcd(m, n) = d$; combining this with the result above yields $[K(x) : K(f, g)] = d$.
- (iii) $\Rightarrow$ (ii) Assume that $[K(x) : K(f, g)] = d$. Since $K(f, g)$ contains non-constant elements of $K[x]$ we can deduce from Theorem 14 that $K(f, g) = K(h)$ for some $h \in K[x]$. Hence $\{f, g\} \subseteq K(h) \bigcap K[x] = K[h]$, where the last equality follows from Lemma 3 in Torstensson (2002); thus f and g are polynomials in h. From Lemma 13 it follows that $\deg(h) = d$. $\square$

Unfortunately Theorem 15 cannot be generalised to more than two polynomials. The implication (ii) $\Rightarrow$ (i) does not hold even for three polynomials, which was noted in Torstensson (2002), but can also be seen from the example in Remark 25 in Section 5. Since the proof of (ii) $\Leftrightarrow$ (iii) above can easily be extended to any finite number of polynomials it follows that the new characterisation of SAGBI bases (iii) only works for two polynomials. As was pointed out in Torstensson (2002), the implication (i) $\Rightarrow$ (ii) holds for any finite number of polynomials, so for three or more polynomials the analogue of Theorem 15 would be: (i) $\Rightarrow$ (ii) $\Leftrightarrow$ (iii).

4. Resultants

In this section we introduce a particular resultant which has some very interesting properties allowing us to prove theorems in Section 5. We begin by recalling the usual definition of the resultant:

Definition 16 (*Resultant*). Let $f(x) = a_n x^n + \ldots a_1 x + a_0$ and $g = b_m x^m + \ldots b_1 x + b_0$ be two polynomials, of degree n and m respectively, over a field L. The *resultant* of f and g, $\mathrm{Res}(f, g)$, is the determinant of the $(m + n) \times (m + n)$-matrix:

$$\begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 \\ b_m & b_{m-1} & b_{m-2} & \dots & b_1 & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_m & b_{m-1} & b_{m-2} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_m & b_{m-1} & b_{m-2} & \dots & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & b_m & b_{m-1} & b_{m-2} & \dots & b_1 & b_0 \end{pmatrix}.$$

The motivation for introducing the resultant can be found in the following standard theorem:

Theorem 17. *The resultant of two polynomials f and g is zero if and only if they have a common non-trivial factor.*

Proof. A proof can be found for example in Cox et al. (1997). □

Now consider the polynomials $F(t) = f(t) - f(x)$ and $G(t) = g(t) - g(x)$ in $K(x)[t]$; they have a common zero, x, in the field $K(x)$, thus by Theorem 17: $\mathrm{Res}(F, G) = 0$. In matrix terms this means that:

$$\det \begin{pmatrix} a_n & a_{n-1} & \dots & a_1 & a_0 - f(x) & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 - f(x) & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_n & a_{n-1} & \dots & a_1 & a_0 - f(x) \\ b_m & b_{m-1} & \dots & b_1 & b_0 - g(x) & 0 & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_1 & b_0 - g(x) & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & b_m & b_{m-1} & \dots & b_1 & b_0 - g(x) \end{pmatrix} = 0.$$

The identity above appears in Perron (1927, Section 43), together with parts of Lemma 19 below. We will be interested in the determinant above when f and g are treated as formal variables, thus we define:

Definition 18.

$$D(f, g) = \det \begin{pmatrix} a_n & a_{n-1} & \dots & a_1 & a_0 - f & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 - f & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_n & a_{n-1} & \dots & a_1 & a_0 - f \\ b_m & b_{m-1} & \dots & b_1 & b_0 - g & 0 & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_1 & b_0 - g & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & b_m & b_{m-1} & \dots & b_1 & b_0 - g \end{pmatrix}. \tag{4}$$

The expression $D(f,g)$ will allow us to study the equality $\mathrm{Res}(F,G) = 0$. To do this we start with a technical lemma.

Lemma 19. *$D(f,g)$ has the form:*

$$\sum_{(i,j)\in\Delta} \alpha_{(i,j)} f^i g^j, \tag{5}$$

where $\Delta = \{(i,j) \in \mathbb{N}\times\mathbb{N} \mid in + jm \leq mn\}$ and $\alpha_{(i,j)} \in K$ for all $(i,j) \in \Delta$. Furthermore, $\alpha_{(m,0)} = (-1)^{m(n+1)} b_m^n$ and $\alpha_{(0,n)} = (-1)^n a_n^m$.

Proof. The determinant of a $k \times k$ matrix $C = (c_{ij})$ can be calculated using the following formula:

$$\sum_{\sigma\in S_k} (-1)^\sigma \prod_{l=1}^{k} c_{l\sigma(l)}, \tag{6}$$

where S_k is the symmetric group. Equating formula (6) for the determinant (4) and collecting terms with the same $\{f,g\}$-monomials we get a formula with the same appearance as (5), where $\alpha_{(i,j)} \in K$. Since there are only m f's and n g's in (4) we can conclude that Δ is a subset of $\{0,\ldots,m\}\times\{0,\ldots,n\}$.

Let S be the subset of $\{1,\ldots,m+n\}\times\{1,\ldots,m+n\}$ containing all pairs $(l,\sigma(l))$ in one non-zero term of (6) and let i and j denote the number of $a_0 - f$ and $b_0 - g$ respectively in this product. Since the determinant is a sum of such products it suffices to prove that $in + jm \leq mn$ to conclude that Δ has the claimed form. With these notations we have:

$$\sum_{(l,r)\in S} l = \sum_{(l,r)\in S} r = 1 + 2 + \cdots + (m+n).$$

Hence

$$\sum_{(l,r)\in S} (l - r) = 0.$$

Thus we can group the terms:

$$\sum_{\substack{(l,r)\in S\\ l\leq m}} (r - l) = \sum_{\substack{(l,r)\in S\\ l>m}} (l - r) = s. \tag{7}$$

Since we are not interested in zero terms in the sum (6), the appearance of matrix (4) implies that we can assume:

- If $l \leq m$ then $0 \leq r - l \leq n$.
- If $l > m$ then $0 \leq l - r \leq m$.

Since any term in (6) such that any of the above inequalities is not satisfied will contain at least one zero as a factor. Thus all terms in the first sum in (7) are larger than or equal to zero, and precisely i of the terms are n, hence:

$$in \leq \sum_{\substack{(l,r)\in S\\ l\leq m}} (r - l) = s.$$

Considering the second sum in (7) we see that exactly $n - j$ terms are non-zero, and the value of these is at most m; hence:

$$s = \sum_{\substack{(l,r)\in S \\ l>m}} (l - r) \leq m(n - j).$$

Combining these inequalities yields:

$$in \leq s \leq m(n - j) \Rightarrow in + jm \leq mn.$$

To prove that $\alpha_{(m,0)} = (-1)^{m(n+1)} b_m^n$ we will use formula (7) again. To get an element of f-degree m we must have $\sigma(i) = n + i$ for $1 \leq i \leq m$. From here we get a factor $(-f)^m$ and $s = mn$ in the left-hand side of (7). Then the right-hand side of (7) and the inequality $l - r = l - \sigma(l) \leq m$ show that $\sigma(l) = l - m$ for $m + 1 \leq l \leq m + n$. Hence the corresponding term in (6) is:

$$(-1)^\sigma b_m^n (-f)^m = (-1)^\sigma (-1)^m b_m^n f^m.$$

To calculate $(-1)^\sigma$ we can permute the rows of the identity matrix of order $m + n$ as dictated by σ and call the obtained matrix A; then $(-1)^\sigma = \det(A)$. The determinant of A can easily be calculated for example by expansion over the first row, the result is: $\det(A) = (-1)^{m(n+2)} = (-1)^{mn}$. Thus $\alpha_{(m,0)} = (-1)^{mn}(-1)^m b_m^n = (-1)^{m(n+1)} b_m^n$.

The fact that $\alpha_{(0,n)} = (-1)^n a_n^m$ can be proved in a similar manner. □

5. Resultants as a tool for verifying SAGBI bases

The following result was originally published in Torstensson (2002) for characteristic zero (though, as we have noted above, that proof can be modified to work in arbitrary characteristic). The resultants introduced in the previous section in addition to giving us a new proof of the theorem below also give more insight in the form of an identity as claimed in the introduction.

Theorem 20. *Let f and g be polynomials of degree n and m respectively, then f, g is a SAGBI basis if* $\gcd(n, m) = 1$.

Proof. Assume for simplicity that f and g are monic. By Corollary 11 the only T-polynomial that we need to check is: $f^m - g^n$. Thus it suffices to prove that this polynomial has a low representation in terms of f and g. Now take a look at the form of $D(f, g)$ as presented in Lemma 19. Since m and n are relatively prime, the only possibility for equality in the inequality $in + jm \leq mn$ is $i = m$, $j = 0$ or $i = 0$, $j = n$. Thus the only $\{f, g\}$-monomials of the maximal degree, mn, are f^m and g^n; hence the corresponding terms must cancel, so $D(f, g)$ has the form:

$$\pm(f^m - g^n) + \sum_{(i,j)} \alpha_{(i,j)} f^i g^j,$$

where $\alpha_{(i,j)} \in K$ and $in + jm < mn$. Using the fact that $\mathrm{Res}(F, G) = 0$ we can deduce that $f^m - g^n$ can be written as a sum:

$$\mp \sum_{(i,j)} \alpha_{(i,j)} f^i g^j,$$

where $in + jm < mn$; this is the sought low representation. □

Remark 21. That the terms of degree mn cancel in the proof above can also be seen by studying the signs of $\alpha_{(m,0)} = (-1)^{m(n+1)}$ and $\alpha_{(0,n)} = (-1)^n$. If n is odd then $m(n+1)$ is even, so the signs are different. If n is even then m has to be odd since $\gcd(m, n) = 1$, so $m(n+1)$ is odd and the signs are different also in this case.

Fortunately this resultant method not only gives us this new proof of an old theorem, but it also yields some completely new results.

Suppose we want to determine a SAGBI basis for the algebra generated by f and g, when $n = \deg(f)$ and $m = \deg(g)$ are not relatively prime. Let

$$d = \gcd(m, n)$$

be their greatest common divisor and

$$n' = n/d, \qquad m' = m/d.$$

In this case we get no information from Theorem 20, so we would have to check whether the T-polynomial $f^{m'} - g^{n'}$ subduces to zero over $\{f, g\}$. If it does, then we may conclude that $\{f, g\}$ is SAGBI. If, on the other hand, it does not, we get a non-zero subduced remainder h after some subduction steps:

$$f^{m'} - g^{n'} = \sum_{(i,j)} \alpha_{(i,j)} f^i g^j + h,$$

where $\alpha_{(i,j)} \in K$ and $\deg(h) < in + jm < m'n'd$. Let l denote the degree of h. We will see that if d and l are relatively prime, then $\{f, g, h\}$ is a SAGBI basis. To verify this with the usual SAGBI algorithm we would need to calculate at least two new T-polynomials and check if they subduce to zero or not.

To prove the stated result we begin with two technical lemmata:

Lemma 22. *Let m, n be positive integers, $d = \gcd(m, n)$ and $m' = m/d$. Suppose that l is a positive integer and $\gcd(l, d) = 1$. Then the condition*

$$i_1 n + j_1 m + k_1 l = i_2 n + j_2 m + k_2 l$$
where $0 \le k_1 \le k_2 \le d$, $0 \le i_1 < m'$ and $0 \le i_2 < m'$

implies:

- *either $k_1 = k_2$, $i_1 = i_2$ and $j_1 = j_2$.*
- *or $k_2 = d$ and $k_1 = 0$.*

Proof. From our condition we have

$$(k_2 - k_1)l = (j_1 - j_2)m + (i_1 - i_2)n$$

so $d|(k_2 - k_1)$; hence either $k_2 = d$ and $k_1 = 0$, or $k_1 = k_2$. In the first case we are done; in the second case we can divide the equation above by d, to get

$$(j_1 - j_2)m' = (i_2 - i_1)n'.$$

This implies that $m'|(i_1 - i_2)$ so we can deduce that $i_1 = i_2$ and hence also $j_1 = j_2$. □

Note that it can be shown that the implication in Lemma 22 is not valid if $\gcd(d, l) \neq 1$.

Lemma 23. *Let m, n and l be positive integers, such that $d = \gcd(m, n)$ and $\gcd(l, d) = 1$. Let $n' = n/d$ and $m' = m/d$. Suppose that the linear Diophantine equation:*

$$i_1 n + j_1 m + k_1 l = i_2 n + j_2 m + k_2 l \tag{8}$$

has a non-trivial solution $[(i_0, j_0, 0), (0, 0, d)]$, where $0 \leq i_0 < m'$ and $0 \leq j_0 < n'$. Then all T-polynomials have low representations if the T-polynomials corresponding to $[(i_0, j_0, 0), (0, 0, d)]$ and $[(0, n', 0), (m', 0, 0)]$ have low representations.

Proof. First we note (the "triangle lemma") that if $[a, b]$ and $[b, c]$ are solutions of (8) such that $T(a, b)$ and $T(b, c)$ have low representations, then so does $T(a, c)$. In order to prove this, recall our convention that if $a = (a_1, \ldots, a_l) \in \mathbb{N}^l$ then $f^a = \prod_{i=1}^{l} f_i^{a_i}$. Now the statement follows from:

$$T(a, c) = f^a - f^c = (f^a - f^b) + (f^b - f^c) = T(a, b) + T(b, c).$$

Assume that the T-polynomials corresponding to $[(i_0, j_0, 0), (0, 0, d)]$ and $[(0, n', 0), (m', 0, 0)]$ have low representations. Let $[(i_1, j_1, k_1), (i_2, j_2, k_2)]$ be an arbitrary fixed solution of (8). If both $k_1 > 0$ and $k_2 > 0$, then we can subtract a suitable multiple of $[(0, 0, 1), (0, 0, 1)]$ to obtain at least one of $k_1 = 0$ or $k_2 = 0$. In the case that both are zero we can use Lemma 9 to reduce to the case of the T-polynomial corresponding to $[(0, n', 0), (m', 0, 0)]$. In the case that one of the k_i's is non-zero we may assume, after transposing if necessary, that $k_2 > 0$ and $k_1 = 0$, so the equation reduces to:

$$k_2 l = (i_1 - i_2)n + (j_1 - j_2)m.$$

This implies $d \mid k_2$, so there exists an integer k with $k_2 = kd$. Let $a = (i_1, j_1, 0)$, $b = (i_2 + ki_0, j_2 + kj_0, 0)$ and $c = (i_2, j_2, kd)$. Then

$$[a, b] = [(i_1, j_1, 0), (i_2 + ki_0, j_2 + kj_0, 0)]$$

and from Lemma 9 the T-polynomial corresponding to this has a low representation. The other pair:

$$\begin{aligned} [b, c] &= [(i_2 + ki_0, j_2 + kj_0, 0), (i_2, j_2, kd)] \\ &= [(i_2, j_2, 0), (i_2, j_2, 0)] + k[(i_0, j_0, 0), (0, 0, d)] \end{aligned}$$

also has a low representation as can be seen by applying the triangle lemma repeatedly and using the assumption that $[(i_0, j_0, 0), (0, 0, d)]$ has a low representation and that $[(i_2, j_2, 0), (i_2, j_2, 0)]$ obviously does. A final application of the triangle lemma implies that $[a, c] = [(i_1, j_1, 0), (i_2, j_2, kd)]$ has a low representation as claimed. □

Now we are ready to prove the main result of this section:

Theorem 24. *Suppose the polynomial h is the remainder after subduction of the polynomial $f^{m'} - g^{n'}$, i.e.,*

$$f^{m'} - g^{n'} = \sum_{(i,j)} \alpha_{(i,j)} f^i g^j + h, \tag{9}$$

where $in + jm < mn/d$ for all terms in the sum. If $\deg(h) = l$ and $\gcd(l, d) = 1$ then $\{f, g, h\}$ is a SAGBI basis.

Remark 25. If we remove the condition that h is the remainder after subduction of the polynomial $f^{m'} - g^{n'}$, then the theorem would no longer be valid. This can be seen from the following example:

Let $f = x^6 + 3x^3$, $g = x^4 + 2x$ and $h = x^3 + x^2$, then the T-polynomial $f^2 - g^3$ subduces to $-x^2$, which cannot be subduced further; thus $\{f, g, h\}$ is not a SAGBI basis.

Proof of Theorem 24. For simplicity assume that f and g are monic. Regard the commutative algebra on three generators f, g, h and one relation:

$$f^{m'} - g^{n'} = \sum_{in+jm<m'n=n'm} \alpha_{(i,j)} f^i g^j + h.$$

Define an order on the monomials as follows:

$$f^{i_1} g^{j_1} h^{k_1} > f^{i_2} g^{j_2} h^{k_2}$$

if and only if $i_1 n + j_1 m + k_1 l > i_2 n + j_2 m + k_2 l$ or in the case of equality if the left monomial is larger than the right in terms of lex using $f > g > h$.

Since the algebra is commutative the single polynomial:

$$f^{m'} - g^{n'} - \sum_{in+jm<m'n=n'm} \alpha_{(i,j)} f^i g^j - h \tag{10}$$

constitutes a Gröbner basis. Consider $D(f, g)$ as a polynomial in f, g (and h) and Gröbner reduce it w.r.t. our only relation. The result $R(f, g, h) = \sum \gamma_{(i,j,k)} f^i g^j h^k$ will be a polynomial which contains only monomials $f^i g^j h^k$ where $i < m'$, $k \le d$. The inequality $i < m'$ follows from the fact that the leading term of the polynomial (10) is $f^{m'}$, so any factor f^s where $s \ge m'$ can be reduced. To prove that $k \le d$ we simply note that every time a factor h appears during the reduction, a factor $f^{m'}$ disappears. Because the maximal power of f was $f^m = f^{m'd}$, the number d is the highest possible power of h that can appear during the reduction process. Also note that since f^m is the only term in $D(f, g)$ containing d factors $f^{m'}$ the only monomial of h-degree d will be h^d.

If we replace f, g, h by $f(x), g(x), h(x)$ in $R(f, g, h)$ we get zero, so we have an identity between $f(x), g(x)$ and $h(x)$. In particular the terms of highest degree in $R(f(x), g(x), h(x))$ must cancel; thus two $\{f, g, h\}$-monomials $f(x)^i g(x)^j h(x)^k$ must have the same maximal degree. According to Lemma 22 the only two such $\{f, g, h\}$-monomials that can have the same degree are $f(x)^{i_1} g(x)^{j_1}$ and $f(x)^{i_2} g(x)^{j_2} h(x)^d$ for some $i_1, i_2 < m'$, j_1, j_2. As we noted before, the only $\{f, g, h\}$-monomial of h-degree d

is $h(x)^d$; therefore $i_2 = j_2 = 0$. Since all other terms of $R(f(x), g(x), h(x))$ have strictly lower degree, we can rewrite the equality $R(f(x), g(x), h(x)) = 0$ as

$$\alpha f(x)^{i_1} g(x)^{j_1} - \beta h(x)^d = \sum_{(i,j,k) \notin \{(i_1, j_1, 0), (0,0,d)\}} \gamma_{(i,j,k)} f^i g^j h^k$$

for some $\alpha, \beta \neq 0$. This is the sought low representation.

Since there exist low representations for the pairs

$$[(m', 0, 0), (0, n', 0)], \qquad [(i_1, j_1, 0), (0, 0, d)]$$

and this, according to Lemma 23, implies that all critical pairs have low representations, we may apply Theorem 10 to conclude that $\{f, g, h\}$ is a SAGBI basis. □

There is a partial converse to the main theorem:

Theorem 26. *Let h be the (non-zero) subduced remainder of the T-polynomial $f^{m'} - g^{n'}$ and $\{f, g, h\}$ be a SAGBI basis. If $p = \gcd(m, n)$ is a prime, then p and $l = \deg(h)$ are relatively prime.*

Proof. To prove this theorem, assume that $\{f, g, h\}$ is SAGBI and that $p = \gcd(m, n)$ is a prime dividing l. As in the proof of Theorem 15 we combine the tower law and Lemma 13:

$$n = [K(x) : K(f)] = [K(x) : K(f, g)][K(f, g) : K(f)],$$
$$m = [K(x) : K(g)] = [K(x) : K(f, g)][K(f, g) : K(g)].$$

Thus $[K(x) : K(f, g)]$ divides $\gcd(m, n) = p$, and since we have assumed that p is prime: $[K(x) : K(f, g)] = p$ or $[K(x) : K(f, g)] = 1$.

In the first case Theorem 15 tells us that $\{f, g\}$ is a SAGBI basis, so $h = 0$ contrary to our assumption.

In the second case we have $K(x) = K(f, g)$, and this implies that x can be written as a quotient of two polynomials from $K[f, g]$. Since $\{f, g, h\}$ is SAGBI, all elements of $K[f, g] = K[f, g, h]$ have degree divisible by p, so in particular the quotient of two elements has degree divisible by p, contradiction. □

This converse does not hold if $\gcd(m, n)$ is not prime, as the following example shows:

Example 27. Let $f = x^8 + 2x^2$, $g = x^{12} + 3x^6$, then $g^2 - f^3$ subduces to $h = x^6$. Then $\{f, g, h\}$ is a SAGBI basis despite the fact that $d = \gcd(12, 8) = 4$ and $\deg(h) = 6$ have a common factor. Note that $\{f, g, h\}$ in this example is a SAGBI basis, but not a minimal one.

6. An example

In this section we shall take a closer look at subalgebras $K[f, g]$, where f is of degree 6 and g is of degree 4. From Theorem 20 we know that if the degrees of f and g are relatively prime then $\{f, g\}$ form a SAGBI basis. To get a better understanding of what is going on in the case where the degrees of the polynomials have a common factor we examine the "smallest" such instance in detail. The characteristic of the underlying field plays an essential role here as the following example shows:

Example 28. Let K be a field of characteristic 2 and let $f = x^6 + x$ and $g = x^4$. Then $f^2 - g^3 = 2x^7 + x^2 = x^2$ and hence $x^2 \in K[f, g]$. Moreover, $x = f - (x^2)^3$, so in this case $K[f, g] = K[x]$.

As mentioned in the introduction, it follows from the important epimorphism theorem by Abhyankar and Moh (1973a,b, 1975) that this can never happen when the characteristic of the field does not divide $d = \gcd(n, m)$, that is when the characteristic is different from 2 in our case.

Let us first concentrate on the situation when the field has characteristic different from 2. From Theorem 24 we know that if h is of odd degree then $\{f, g, h\}$ is a SAGBI basis. Since h is the remainder after subduction of $f^2 - g^3$ it must have one of the following degrees: 11, 9, 7, 5, 3, 2, 1. It turns out that h never has degree 1 or 2, but let us return to that question later. The following list of examples shows that h can have any of the degrees 11, 9, 7, 5 and 3:

Example 29. If $f = x^6$ and $g = x^4 + x^3$ then $h = f^2 - g^3 = -3x^{11} - 3x^{10} - x^9$.

Example 30. If $f = x^6$ and $g = x^4 + x$ then $h = f^2 - g^3 = -3x^9 - 3x^6 - x^3$.

Example 31. If $f = x^6 + x$ and $g = x^4$ then $h = f^2 - g^3 = 2x^7 + x^2$.

Example 32. If $f = x^6 + 3x^3 + x^2$ and $g = x^4 + 2x$ then $h = f^2 - g^3 - 2g^2 + 3f - g = -2x^5 + x^3 - 5x^2 - 2x$.

Example 33. If $f = x^6 + 3x^4 + 3x^3$ and $g = x^4 + 4x^2 + 2x$ then $h = f^2 - g^3 + 6fg - 3g^2 + 19f + 3g = x^3 + 6x$.

Let us now prove that h cannot be of degree 1 or 2. One way to do so is to calculate h when f and g are polynomials of degrees 6 and 4 with arbitrary coefficients and then show that every choice of coefficients for f and g that satisfy the equations we get from setting the coefficients of x^{11}, x^9, x^7, x^5 and x^3 to zero also makes the coefficients of x^2 and x vanish. The computation is quite short and straightforward, but provides little understanding of what is going on. Instead we will give a proof inspired by an algorithm presented in Richman (1986). This algorithm takes two univarite polynomials f and g as input and from them constructs polynomials $h_0, h_1, h_2 \ldots h_{N-1}$, where $N = [K(f, g) : K(g)]$ is the degree of the field extension $K(f, g)/K(g)$, such that $h_i \in f^i + K[g]f^{i-1} + \cdots + K[g]f + K[g]$. In Richman (1986) it is also claimed that all h_i have incongruent degrees modulo $\deg(g)$. However, the proof of this property seems to be incomplete, as pointed out by Kang (1991). (For a hint of the significance of this property, see the proof of the proposition below.) Therefore we will not assume that the degrees of the h_i's are incongruent modulo $\deg(g)$, but rather verify this explicitly for the specific polynomials under consideration.

Proposition 34. *Let f and g be monic polynomials of degree* 6 *and* 4 *respectively over a field of characteristic different from two and let h be the unique polynomial of the form $f^2 - g^3 + \alpha fg + \beta g^2 + \gamma f + \delta g + \epsilon$ that has no terms of degree* 10, 8, 6, 4 *or* 0 *($\alpha, \beta, \gamma, \delta, \epsilon \in K$). Then h cannot be of degree* 1 *or* 2.

Proof. Let us first show that h cannot be of degree 1 using Richman's algorithm to produce elements h_0, h_1, h_2 and h_3 and then verifying that they all have incongruent degrees modulo 4.

Assume that h is of degree 1. Let $h_0 = 1$, $h_1 = f$ and $h_2 = h = f^2 - g^3 + \alpha fg + \beta g^2 + \gamma f + \delta g + \epsilon$. Then $h_3 = hf = f^3 - fg^3 + \alpha f^2 g + \beta fg^2 + \gamma f^2 + \delta fg + \epsilon f$ is of degree 7. Now it is easy to show that $K[f, g] = K[g] + K[g]f + K[g]f^2 + K[g]f^3 = K[g]h_0 + K[g]h_1 + K[g]h_2 + K[g]h_3$. In other words h_0, h_1, h_2, h_3 is a $K[g]$-basis for $K[f, g]$. The advantage of choosing a basis with elements of incongruent degrees modulo the degree of g is that for any element $p = p_0(g)h_0 + p_1(g)h_1 + p_2(g)h_2 + p_3(g)h_3$ the degrees of the leading terms of the summands must all be different, so that the leading term of p equals the leading term of the summand $p_j(g)h_j$ with $\deg(h_j) \equiv \deg(p)$ modulo $\deg(g)$. In our case we immediately get a contradiction from the fact that $p = h^2$ is an element in $K[f, g]$ of degree 2, but then its leading term must equal that of $p_1(g)h_1$ which is of degree at least 6.

To prove that h cannot be of degree 2 we use an argument similar to the one above, but now the degrees of f and h are congruent modulo $\deg(g)$ so using them both in our basis would prevent it from having the desired incongruence property. To overcome this difficulty we modify the basis elements h_i somewhat.

Assume that h is of degree 2. If $h = sx^2 + tx$ we perform the substitution $y = x - t/2s$ to get rid of the coefficient of x in h. (Note that we are using that the characteristic is different from 2 here.) Such a substitution does not affect the degrees occurring in the subalgebra $K[f, g]$, while simplifying our analysis. Hence we may assume from now on that $h = sx^2$ for some non-zero s.

Without loss of generality we may also assume that f and g have the forms:

$$f = x^6 + a_5x^5 + a_3x^3 + a_2x^2 + a_1x,$$
$$g = x^4 + b_3x^3 + b_2x^2 + b_1x.$$

To see this we note that if for example $a_4 \neq 0$ then we may replace our generators f and g by the generators $f - a_4g$ and g of $K[f, g]$ and hence we may assume that f has no term of degree 4. Note that this procedure does not change h:

$$\begin{aligned} h &= f^2 - g^3 + \alpha fg + \beta g^2 + \gamma f + \delta g + \epsilon \\ &= (f - a_4g)^2 - g^3 + (\alpha + 2a_4)(f - a_4g)g + (\beta + a_4(\alpha + a_4))g^2 \\ &\quad + \gamma(f - a_4g) + (\delta + \gamma a_4)g + \epsilon. \end{aligned}$$

Thus if $f' = f - a_4g$ the unique polynomial of the form $f'^2 - g^3 + \alpha' f'g + \beta' g^2 + \gamma' f' + \delta' g + \epsilon'$ that has no terms of degree 10, 8, 6, 4 or 0 is still h. Similarly if $a_0 \neq 0$ or $b_0 \neq 0$ we can replace f by $f - a_0$ or g by $g - b_0$ without altering h or $K[f, g]$.

For future use we note that since h is of degree less than 11 the coefficient $2a_5 - 3b_3$ of x^{11} in $f^2 - g^3$ must be equal to zero. Let us now construct our $K[g]$-basis. First we look at the case when $b_3 \neq 0$. Let $h_0 = 1$ and $h_2 = h$ as before and let $h_3 = hf - sg^2 \in f^3 + K[g]f^2 + K[g]f + K[g]$. The coefficient of x^7 in h_3 is $s(a_5 - 2b_3)$ which is non-zero. Moreover, $h_1 = sf - hg$ is of degree 5, since the coefficient of x^5 is $s(a_5 - b_3)$. It is straightforward to check that h_0, h_1, h_2, h_3 generates $K[f, g]$ as a $K[g]$-module, and as above the h_i have the convenient property of having incongruent degrees modulo $\deg(g)$.

We obtain a contradiction by noting that $g - h^2/s^2$ is an element of degree 3 in $K[f, g]$ while the only basis element of degree congruent to 3 mod 4 is h_3 of degree 7.

Let us now return to the case $b_3 = 0$. The conditions for $f^2 - g^3 + 3b_2 fg$ being of degree at most 8 are $2a_5 = 0$ and $-3b_1 - a_5^3 + 2a_3 + 3b_2 a_5 = 0$ or equivalently $a_5 = 0$ and $a_3 = \frac{3b_1}{2}$. The coefficients of x^3 in $\widetilde{h_3} = h_1 + sb_2 g$ and x^5 in $\widetilde{h_1} = h_3 + 2sb_2 f$ become $\frac{sb_1}{2}$ and $-\frac{sb_1}{2}$, respectively. If $b_1 \neq 0$ this gives a contradiction in the same way as above: $\{h_0, \widetilde{h_1}, h_2, \widetilde{h_3}\}$ is a $K[g]$-basis of $K[f, g]$ with elements of degrees that are incongruent modulo $\deg(g)$, but the leading term of $g - \frac{h^2}{s^2} - \frac{b_2 h}{s} = b_1 x \in K[f, g]$ is of degree 1. Otherwise $b_1 = 0$, in which case $h = sx^2$ cannot hold since if the coefficient $2a_1$ of x^7 in h equals zero this also makes the coefficient a_1^2 of x^2 in h (and hence the whole of h) vanish. □

When the characteristic of the field is 2, h can have any of the possible degrees 11, 9, 7, 5, 3 and 2, but not 1. That the degree cannot be 1 can be seen in the same way as for other characteristics, and that the other degrees are possible is clear from Examples 28, 29, 30 and 33 together with the following ones:

Example 35. If $f = x^6 + x^5$ and $g = x^4 + x$ are polynomials over a field of characteristic 2 then $h = f^2 - g^3 - fg = x^7 + x^3$.

Example 36. If $f = x^6 + x^5$ and $g = x^4 + x^2$ are polynomials over a field of characteristic 2 then $h = f^2 - g^3 - g^2 - f = x^5 + x^4$.

In this section we have seen that, when the characteristic of K is different from 2, $K[f, g]$, where $\deg(f) = 6$ and $\deg(g) = 4$, always has a SAGBI basis $\{f, g, h\}$, where h is the subduced remainder of the T-polynomial $f^2 - g^3$. This follows from Proposition 34 and Theorem 24. In the case when $\mathrm{char}(K) = 2$ and $\deg(h) = 2$ we cannot apply Theorem 24, so $\{f, g, h\}$ is not necessarily a SAGBI basis, cf. Example 28. This points to the importance of the characteristic of the underlying field in the construction of SAGBI bases.

7. Ideas for further development

The calculations in the next natural example, when $n = 8, m = 6$, exhibit behaviour similar to that when $n = 6, m = 4$. In zero characteristic the polynomial $h(x)$ which we get in the subduction process never has degree 10, although degree 9 is possible. In characteristic two the situation is different; $h(x)$ can have degree 10 as can be seen from the example:

$$f(x) = x^8 + x^4, g(x) = x^6 + x,$$

where the SAGBI basis also contains the polynomials

$$x^{10} + x^4 + x^2 + x, \qquad x^{11} + x^7 + x^5 + x^4 + x^3 + x, \qquad x^{13} + x^3 + x^2 + x.$$

Hence the characteristic of the field influence the vanishing of coefficients both here and when $n = 6, m = 4$. On the other hand, the identity derived from the resultant, that we

used in the proof of Theorem 20, shows that certain coefficients vanish when the generating polynomials are of relatively prime degrees, and this identity is valid in all characteristics. We therefore suspect that a different type of identity is needed to explain what happens in the case when the degrees of the generators have a common factor.

The absence of polynomials of degree 10 could be explained using the algorithm in Richman (1986, Section 3), but as mentioned earlier there are unfortunately some gaps in the proof of the correctness of this algorithm, as was pointed out by Kang (1991). It would be interesting to see if Richman's algorithm can be justified.

Acknowledgements

We would like to thank the anonymous referees for their valuable comments and suggestions.

References

Abhyankar, S.S., Moh, T.T., 1973a. Newton–Puiseux expansion and generalized Tschirnhausen transformation. I, II. J. Reine Angew. Math. 260, 47–83.

Abhyankar, S.S., Moh, T.T., 1973b. Newton–Puiseux expansion and generalized Tschirnhausen transformation. I, II. J. Reine Angew. Math. 261, 29–54.

Abhyankar, S.S., Moh, T.T., 1975. Embeddings of the line in the plane. J. Reine Angew. Math. 276, 148–166.

Bourbaki, N., 1990. Algebra. II. In: Elements of Mathematics (translated from the French by Cohn PM and Howie J). Springer-Verlag, Berlin (Chapters 4–7).

Cox, D., Little, J., O'Shea, D., 1997. Ideals, varieties, and algorithms. In: Undergraduate Texts in Mathematics, 2nd edition. Springer-Verlag, New York (An introduction to computational algebraic geometry and commutative algebra).

Kang, M.C., 1991. On Abhyankar-Moh's epimorphism theorem. Amer. J. Math. 113 (3), 399–421.

Kapur, D., Madlener, K., 1989. A completion procedure for computing a canonical basis for a *k*-subalgebra. In: Computers and Mathematics (Cambridge, MA, 1989). Springer, New York, pp. 1–11.

Lausch, H., Nöbauer, W., 1973. Algebra of Polynomials. In: North-Holland Mathematical Library, vol. 5. North-Holland Publishing Co., Amsterdam.

Perron, O., 1927. Algebra I; Die Grundlagen. Walter de Gruyter & Co., Berlin W 10 und Leipzig.

Richman, D.R., 1986. On the computation of minimal polynomials. J. Algebra 103 (1), 1–17.

Robbiano, L., Sweedler, M., 1990. Subalgebra bases. In: Commutative Algebra (Salvador, 1988). In: Lecture Notes in Math., vol. 1430. Springer, Berlin, pp. 61–87.

Sturmfels, B., 1996. Gröbner Bases and Convex Polytopes. In: University Lecture Series, vol. 8. American Mathematical Society, Providence, RI.

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

Torstensson, A., Ufnarovski, V., Öfverbeck, H., 2003. On SAGBI bases and resultants. In: Herzog, J., Vuletescu, V. (Eds.), Commutative Algebra, Singularities and Computer Algebra. In: NATO Science Series II: Mathematics, Physics and Chemistry, vol. 115. Kluwer Academic Publishers, Dordrecht, pp. 241–254.