


J. Symbolic Computation (1999) **27**, 171–184
Article No. jsco.1998.0247
Available online at <http://www.idealibrary.com> on 



An Algorithm to Calculate Optimal Homogeneous Systems of Parameters

GREGOR KEMPER[†]

IWR, Universität Heidelberg, Im Neuenheimer Feld 368, 69 120 Heidelberg, Germany

When a homogeneous system of parameters f_1, \dots, f_n is chosen for a graded algebra A , it is important for subsequent computations that the degrees, $\deg(f_i)$, are as small as possible. More precisely, one would like the product or the sum of the degrees to be minimal, depending on the application.

This article investigates which degree vectors can occur as the degrees of a homogeneous system of parameters. From this, an algorithm is derived which constructs an optimal homogeneous system of parameters. Here the notion of what is considered as *optimal* is part of the input. An important application is the case where A is the invariant ring of a finite linear group. There is an implementation of the algorithm in Magma which applies to this case.

© 1999 Academic Press

Introduction

If A is a graded commutative algebra of Krull dimension n over a field K which is also the homogeneous part of degree 0 of A , then by Noether's normalization lemma there exists a homogeneous system of parameters (from now on abbreviated *hsop*) for A . This is a system $f_1, \dots, f_n \in A$ of homogeneous elements such that A is a finitely generated module over $B := K[f_1, \dots, f_n]$. An equivalent condition is that the Krull dimension of $A/(f_1, \dots, f_n)$ is zero. It follows that the f_i are algebraically independent over K . A hsop is by no means uniquely determined by A , and neither are its degrees $d_1 = \deg(f_1), \dots, d_n = \deg(f_n)$. When choosing a hsop for A , it is of crucial importance that the d_i will become as small as possible. This is illustrated by the following considerations: in the case that A is Cohen–Macaulay (i.e. A is a free module over B), the rank of A as a module over B is given by the product $\deg(A) \cdot \prod_{i=1}^n d_i$, where $\deg(A)$ is the coefficient of $(1-t)^{-n}$ in the Laurent expansion of the Hilbert series $H(A, t)$ of A about $t = 1$. Moreover, in this case the maximal degree of a free generator of A over B is $a(A) + \sum_{i=1}^n d_i$, where $a(A)$ is the degree of $H(A, t)$ as a rational function in t . So we see that it is important to keep the product or the sum of the d_i as small as possible, depending on the context. A related problem has been studied by Eisenbud and Sturmfels (1994). In that paper, the goal is to find a hsop which is as *sparse* as possible. Furthermore, only the case of standard graded algebras is considered, i.e. the case where A is generated by its degree 1 elements.

[†]E-mail: Gregor.Kemper@iwr.uni-heidelberg.de

Quite a few algorithms have been proposed to calculate hsop's, most of them in the context that A is the invariant ring of a finite group G . For a discussion, see Sturmfels (1993) or Kemper (1996). In the latter paper, the author gave an algorithm which chooses the f_i one by one, making sure each time that $\dim(A/(f_1, \dots, f_i)) = n - i$. When f_1, \dots, f_i have been chosen, the strategy is to produce a homogeneous element f_{i+1} of minimal degree such that $\dim(A/(f_1, \dots, f_{i+1})) = n - i - 1$. The main content of the algorithm is the technique by which such an f_{i+1} can be found. This involves a primary decomposition of the ideal (f_1, \dots, f_i) , or at least a factorizing Buchberger algorithm. Let us call this algorithm the *successive algorithm*. It has been noted by Decker *et al.* (1998) that the successive algorithm can be altered in such a way that it no longer requires any factorization. Nevertheless, the main problem with the *successive algorithm* is that it does not always produce optimal hsop's. Two examples for this phenomenon were given by Kemper (1996). We provide simpler examples here, which give a clearer idea of what can go wrong.

EXAMPLE 1. Consider the invariant ring $A = K[V]^G$, where $K = \mathbb{C}$ and G is the group of order 18 generated by

$$\begin{pmatrix} \zeta_9 & 0 \\ 0 & -\zeta_9^3 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}) \quad \text{with} \quad \zeta_9 = e^{2\pi i/9}.$$

The successive algorithm would choose the first invariant of positive degree as f_1 , which is $f_1 = x_1^3 x_2^2$. Now an invariant f_2 of minimal degree such that $\dim(A/(f_1, f_2)) = 0$ is $f_2 = x_1^{18} + x_2^{18}$. Hence the successive algorithm would obtain a hsop of degrees 5 and 18. But a better hsop is given by $f_1 = x_2^6$ and $f_2 = x_1^9$, which the successive algorithm would have missed.

This example was inspired by a similar one given by Müller-Quade and Beth (1996).

This example has shown that the successive algorithm may be “too greedy” at small degrees, resulting in large degrees in the end. There are more complicated instances of this phenomenon, and experience indicates that problems of this kind become much more frequent as one tries to calculate more complicated invariant rings. A package for calculating invariant rings has been implemented in the computer algebra system Magma (see Bosma *et al.* (1997)) during and after a visit of the author to Sydney. In a first version of this package, we tried to overcome the “too greedy” problem by having a loop over degree vectors (d_1, \dots, d_n) , ordered by growing values of $\prod_{i=1}^n d_i$, with a variant of the successive algorithm which only tries to find a hsop of degrees d_1, \dots, d_n for each degree vector (d_1, \dots, d_n) . In the above example, the degree vector $(6, 9)$ would be treated before $(5, 18)$, and the algorithm would terminate after being successful for $(6, 9)$. Let us call this algorithm the *trial and error algorithm*.

Now there are also examples where the trial and error algorithm fails to produce an optimal hsop, and again these become more frequent and more complex as the algebras A get more complicated. Possibly the simplest example of this kind is the following.

EXAMPLE 2. Consider the invariant ring A of the group of order 9 generated by

$$\begin{pmatrix} \zeta_9 & 0 & 0 \\ 0 & \zeta_9^2 & 0 \\ 0 & 0 & \zeta_9^6 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{C})$$

with the same notation as in Example 1. It turns out that an optimal hsof is of degrees $(3, 5, 9)$, given by

$$f_1 = x_3^3, \quad f_2 = x_1x_2^4, \quad f_3 = x_1^9 + x_2^9.$$

Suppose that the trial and error algorithm was working on the degree vector $(3, 5, 9)$ but picked $f_1 = x_1x_2x_3 \in A$ as the first member of a would-be hsof. The invariants of degree 5 are spanned by $x_1x_2^4$ and $x_2^3x_3^2$, hence no invariant of degree 5 can reduce the dimension of $A/(f_1)$, so with this choice of an f_1 the degree vector $(3, 5, 9)$ would be abandoned. In fact, a hsof of smallest degrees starting with $x_1x_2x_3$ is

$$f_1 = x_1x_2x_3, \quad f_2 = x_1^3x_2^3 + x_3^6, \quad f_3 = x_1^9 + x_2^9.$$

This example shows that being too greedy is not the only problem with the successive algorithm. Failures to produce optimal hsof's may also arise from unlucky choices of f_i .

Obviously, it is much harder to overcome the problem of unlucky choices of f_i . Müller-Quade and Beth (1996) proposed a variant of the successive algorithm which chooses the f_i "sufficiently generic".

The purpose of this paper is to develop an algorithm which is guaranteed to produce an optimal hsof. Here the notion of what is considered as an optimal degree vector (d_1, \dots, d_n) is variable and forms part of the input. The algorithm works for any graded algebra A which is computable in the sense of Definition 4, with invariant rings of finite groups as prominent examples. For this class of algebras, the algorithm has been implemented as a part of the invariant theory package of Magma. An implementation in Mathematica was done by Thomas Bayer[†]. The algorithm does not use any primary decomposition or factorizing Buchberger algorithm, and it turns out to be about equally fast and in many cases faster than the successive algorithm as well as the trial and error algorithm.

1. The Existence of a Homogeneous System of Parameters of Given Degrees

In this section, $A = \bigoplus_{d=0}^{\infty} A_d$ is a graded commutative algebra over a field $K = A_0$. Given degrees $d_1, \dots, d_n \in \mathbb{N}$, we are interested in the question whether there exists a hsof $f_1, \dots, f_n \in A$ such that $\deg(f_i) = d_i$. First of all, we show that being a hsof is an open condition on f_1, \dots, f_n .

PROPOSITION 1. *Suppose that A has Krull dimension n and let $d_1, \dots, d_k \in \mathbb{N}$. Then the set*

$$S = \{(f_1, \dots, f_k) \in A_{d_1} \times \dots \times A_{d_k} \mid \dim(A/(f_1, \dots, f_k)) = n - k\}$$

is a Zariski open subset of $A_{d_1} \times \dots \times A_{d_k}$.

PROOF. There is a presentation $A = K[x_1, \dots, x_m]/I$ with a homogeneous ideal $I \triangleleft R := K[x_1, \dots, x_m]$. Suppose that $f_1, \dots, f_k \in R$ such that $(\bar{f}_1, \dots, \bar{f}_k) := (f_1 + I, \dots, f_k + I) \in S$. We will prove the proposition by showing that a neighborhood of $(\bar{f}_1, \dots, \bar{f}_k)$ is contained in S .

[†]For information, please contact Thomas Bayer at Thomas.Bayer@risc.uni-linz.ac.at.

First, we choose homogeneous $f_{k+1}, \dots, f_n \in R$ such that $\dim(A/(\bar{f}_1, \dots, \bar{f}_n)) = 0$. Set $J := (f_1, \dots, f_n) \triangleleft R$, so that $\dim(R/(I + J)) = 0$. Then for any prime ideal $P \triangleleft R$ containing I with $\dim(R/P) = n$ and for any minimal prime $Q \triangleleft R$ containing J , we have $\dim(R/(P + Q)) = 0$. But P and Q are homogeneous (see, for example, Eisenbud (1995, Proposition 3.12)), so $\dim(R/(P + Q)) \geq n + \dim(R/Q) - m$ (see Hartshorne (1977, Proposition. 7.1)), and it follows that $\dim(R/J) \leq m - n$. Let $g_1, \dots, g_r \in I$ be a maximal sequence of homogeneous elements of I such that $d := \dim(R/J + (g_1, \dots, g_r)) \leq m - n - r$. Then there exists a prime $P \triangleleft R$ over $J + (g_1, \dots, g_r)$ with $\dim(R/P) = d$ such that $I \subset P$. Hence $I + J \subset P$, which implies $d = 0$, so we have extended f_1, \dots, f_n by $g_1, \dots, g_r \in I$ to a hsop for R , and in particular $r = m - n$.

Now for $(f'_1, \dots, f'_k) \in R_{d_1} \times \dots \times R_{d_k}$ we have

$$\begin{aligned} \dim(R/(g_1, \dots, g_{m-n}, f'_1, \dots, f'_k, f_{k+1}, \dots, f_n)) = 0 &\iff \\ \text{Res}(g_1, \dots, g_{m-n}, f'_1, \dots, f'_k, f_{k+1}, \dots, f_n) \neq 0, \end{aligned}$$

where $\text{Res}(g_1, \dots, g_{m-n}, f'_1, \dots, f'_k, f_{k+1}, \dots, f_n)$ is the resultant (see Gelfand *et al.* (1994, p. 426)). The right-hand side of the equivalence is an open condition on (f'_1, \dots, f'_k) which is satisfied for $f'_i = f_i$, and the left-hand side implies that $(\bar{f}'_1, \dots, \bar{f}'_k) \in S$. Now the natural morphism $\phi: X := R_{d_1} \times \dots \times R_{d_k} \rightarrow A_{d_1} \times \dots \times A_{d_k} =: Y$ splits (existence of complements in vector spaces), and $\psi: Y \rightarrow X$ with $\phi \circ \psi = \text{id}_Y$ can be chosen such that $\psi(\bar{f}_1, \dots, \bar{f}_k) = (f_1, \dots, f_k)$. We have found an open subset $U \subset X$ containing (f_1, \dots, f_k) with $\phi(U) \subset S$, hence $\psi^{-1}(U) \subset \phi(U) \subset S$ is open in Y and contains $(\bar{f}_1, \dots, \bar{f}_k)$. This completes the proof. \square

I thank Antoine Colin for drawing my attention to multivariate resultants, which are used in the above proof. One of the referees of this paper pointed out that one can also prove Proposition 1 by using the semicontinuity of the fiber dimension. However, the explicit proof given above is more useful for the following discussion:

The most interesting case is $k = n$. In the proof we have used the non-vanishing of the resultant $\text{Res}(f_1, \dots, f_n)$ as a criterion for $(f_1, \dots, f_n) \in S$. For practical computations, the resultant is not very useful as it cannot be calculated explicitly. It is only known that for each i it is a polynomial of degree $d_1 \cdots d_{i-1} d_{i+1} \cdots d_n$ in the coefficients of f_i . So one could prove that there is no hsop f_1, \dots, f_n with $\deg(f_i) = d_i$ by choosing so many particular f_1, \dots, f_n that it is impossible that the resultant specializes to zero for all of them without being the zero-polynomial. The minimum number of specializations would be

$$1 + \prod_{i=1}^n d_i^{\dim(A_{d_1}) + \dots + \dim(A_{d_{i-1}}) + \dim(A_{d_{i+1}}) + \dots + \dim(A_{d_n})},$$

which is enormous even for very small problems since $\dim(A_{d_i})$ is approximated by a polynomial of degree $n - 1$ in d_i . To prove that no hsop with degrees d_1, \dots, d_n exists, one would have to perform the above number of Gröbner basis computations. The following theorem provides a more useful criterion for the existence of f_1, \dots, f_n .

THEOREM 2. *Let $A = \bigoplus_{d=0}^{\infty} A_d$ be a graded commutative algebra over an infinite field $K = A_0$ and let $n \in \mathbb{N}_0$ and $d_1, \dots, d_k \in \mathbb{N}$. Then the following conditions are equivalent:*

- (a) *There exist homogeneous $f_1, \dots, f_k \in A$ with $\deg(f_i) = d_i$ such that*

$$\dim(A/(f_1, \dots, f_k)) \leq n - k.$$

(b) For each subset $M \subset \{1, \dots, k\}$ we have

$$\dim \left(A / \left(\bigcup_{i \in M} A_{d_i} \right) \right) \leq n - |M|.$$

If K is a finite field, then the implication “(a) \Rightarrow (b)” still holds.

PROOF. First we prove that (a) implies (b). Suppose that for some $M \subset \{1, \dots, k\}$ we had

$$\dim(A/(f_i \mid i \in M)) > n - |M|.$$

Then by Krull’s principal ideal theorem

$$\dim(A/(f_1, \dots, f_k)) > n - |M| - (k - |M|) = n - k$$

in contradiction to assumption (a). Hence

$$\dim \left(A / \left(\bigcup_{i \in M} A_{d_i} \right) \right) \leq \dim(A/(f_i \mid i \in M)) \leq n - |M|.$$

Now we prove “(b) \Rightarrow (a)” by induction on k . If $k = 0$, then (b) for $M = \emptyset$ says that $\dim(A) \leq n$, hence (a) follows trivially. We now assume that $k > 0$, and for $M \subset \{1, \dots, k\}$ we write

$$d_A(M) := \dim \left(A / \left(\bigcup_{i \in M} A_{d_i} \right) \right).$$

Let $N \subset \{1, \dots, k - 1\}$ and let $P \triangleleft A$ be a prime ideal containing $(\cup_{i \in N} A_{d_i})$ with $\dim(A/P) = n - |N|$. (Such primes only exist if $d_A(N) = n - |N|$.) Since $d_A(N \cup \{k\}) < n - |N|$, A_{d_k} cannot be contained in P , in other words, $A_{d_k} \cap P$ is a proper subspace of A_{d_k} . Since K is infinite, there exists $f_k \in A_{d_k}$ which is contained in no such prime ideal P for any $N \subset \{1, \dots, k - 1\}$. We set $A' = A/(f_k)$, $n' = n - 1$, $k' = k - 1$, and check that condition (b) is satisfied for A' , n' and k' : For $N \subset \{1, \dots, k'\}$,

$$d_{A'}(N) = \dim \left(A / \left(\bigcup_{i \in N} A_{d_i} \right) + (f_k) \right) \leq n - |N| - 1 = n' - |N|,$$

since f_k lies outside of every prime ideal over $(\cup_{i \in N} A_{d_i})$ of dimension $n - |N|$. Now by induction, there exist $f_1, \dots, f_{k-1} \in A$ with $\deg(f_i) = d_i$ and $\dim(A'/(f_1 + (f_k), \dots, f_{k'} + (f_k))) \leq n' - k' = n - k$, which implies (a). \square

EXAMPLE 3. To see that the assumption that K is an infinite field cannot be dropped from Theorem 2, consider the example

$$A = \mathbb{F}_2[xy + xz, xy + yz, xyz, x^4, y^4, z^4] \leq \mathbb{F}_2[x, y, z].$$

It is easily checked that the degree vector $(d_1, d_2, d_3) = (2, 3, 4)$ satisfies the conditions of Theorem 2(b). But since the degree-2 part of A consists only of the polynomials $0, xy + xz, xy + yz, xz + yz$, there exists no hsop $f_1, f_2, f_3 \in A$ with $\deg(f_i) = d_i$.

The situation is changed if we pass from A to $\mathbb{F}_4 \otimes_{\mathbb{F}_2} A$: If $\mathbb{F}_4 = \mathbb{F}_2[\zeta]$, then

$$f_1 = xy + xz + \zeta(xy + yz), \quad f_2 = xyz, \quad f_3 = x^4 + y^4 + z^4$$

forms a hsop.

REMARK 3. In concrete examples some of the conditions contained in (b) of Theorem 2 will usually become redundant. However, none of the conditions can be omitted “globally” in the following sense: given $n \in \mathbb{N}$ and $M \subset \{1, \dots, n\}$, there exists a graded algebra A and numbers $d_1, \dots, d_n \in \mathbb{N}$ such that M is the only subset of $\{1, \dots, n\}$ for which (b) is violated. Indeed, take A to be the polynomial algebra with indeterminates x_1, \dots, x_{n-m+1} where $m = |M|$, and assign the degree 2 to each of the x_i 's. Moreover, choose

$$d_i = \begin{cases} 1, & \text{if } i \in M, \\ 2, & \text{if } i \notin M. \end{cases}$$

Hence $(\cup_{i \in M} A_{d_i}) = 0$, so

$$\dim \left(A / \left(\bigcup_{i \in M} A_{d_i} \right) \right) = n - m + 1 > n - |M|.$$

Conversely, let $N \subset \{1, \dots, n\}$ be a subset violating condition (b). Suppose that there exists $i \in N \setminus M$. Then $d_i = 2$, so $(\cup_{i \in M} A_{d_i}) = (x_1, \dots, x_{n-m+1})$ and

$$\dim \left(A / \left(\bigcup_{i \in N} A_{d_i} \right) \right) = 0 \leq n - |N|,$$

in contradicton to the hypothesis. Hence $N \subset M$ and therefore

$$\dim \left(A / \left(\bigcup_{i \in N} A_{d_i} \right) \right) = n - m + 1,$$

which is larger than $n - |N|$ iff $|N| = m$. Hence $N = M$ as claimed.

The important point is that condition (b) in the above theorem can be checked algorithmically provided that dimensions of ideals in A and bases for homogeneous components of A can be calculated, which is the case if A is given by a presentation, for instance. The evaluation of condition (b) then involves the calculation of 2^k Gröbner bases, but this number can be reduced by forming the ideal products

$$I_j = \prod_{\substack{M \subset \{1, \dots, k\} \\ |M|=j}} \left(\bigcup_{i \in M} A_{d_i} \right).$$

Then (b) is equivalent to

$$\dim(A/I_j) \leq n - j \quad \text{for } j = 0, \dots, k.$$

This reduces the number of Gröbner basis calculations to $k + 1$, but each calculation will be much harder. In the actual algorithm, there will be a high probability that much fewer and easier Gröbner basis calculations will be necessary.

A rough algorithm can be seen already now: run through all degree vectors (d_1, \dots, d_n) ordered (for example) by rising products $d_1 \cdots d_n$ and check condition (b) from Theorem 2 until it is satisfied for (d_1, \dots, d_n) . Then the above proof says how a hsop f_1, \dots, f_n having degrees d_i can be obtained recursively. Since this is done for the first degree vector which satisfies the criterion, the resulting hsop will always be optimal.

2. The Algorithm

Our algorithm will have to calculate generators for homogeneous components A_d of A and dimensions of ideals in A . We make the following definition:

DEFINITION 4. A graded commutative algebra A over a field $K = A_0$ is called *computable* if

- (a) there is an algorithm to calculate generators of A_d (as a vector space over K) for a given $d \in \mathbb{N}$, and
- (b) given by an ideal basis for a homogeneous ideal $I \trianglelefteq A$ there is an algorithm to calculate $\dim(A/I)$.

Note that if A is computable, then so is $A/(f)$ for a homogeneous $f \in A$. Every graded algebra which is given by a finite presentation is computable. Further, if A satisfies condition (a) and can be embedded into a graded algebra R which is finitely generated as an A -module and given by a finite presentation, then A is computable by the following proposition. This applies if A is the invariant ring of a finite group, since homogeneous components can be calculated by application of the Reynolds-operator (if available) or by a simple linear algebra method (see Kemper (1996)) and the polynomial algebra is integral over A .

PROPOSITION 5. *Let $A \leq R$ be commutative rings such that R is finitely generated as an A -module, and let $I \triangleleft A$ be an ideal such that A/I is of finite Krull dimension. Then*

$$\dim(A/I) = \dim(R/(I)),$$

where $(I) \triangleleft R$ is the ideal in R generated by I .

PROOF. Let $P \triangleleft A$ be a prime ideal containing I with $\dim(A/P) = \dim(A/I)$. Then there exists a prime ideal $Q \triangleleft R$ such that $Q \cap A = P$ (see, for example, Benson (1993, Theorem 1.4.4)). This gives an inclusion $A/P \hookrightarrow R/Q$, and R/Q is finite over A/P , hence

$$\dim(A/I) = \dim(A/P) = \dim(R/Q) \leq \dim(R/(I)),$$

as (I) is contained in Q . Now take a prime $Q \triangleleft R$ containing (I) such that $\dim(R/Q) = \dim(R/(I))$. Then $P := (Q \cap A) \triangleleft A$ is a prime ideal containing I , and the inclusion $A/P \hookrightarrow R/Q$ yields

$$\dim(R/(I)) = \dim(R/Q) = \dim(A/P) \leq \dim(A/I).$$

Now the assertion follows. \square

In the previous section, a rough algorithm for the construction of an optimal hsop f_1, \dots, f_n was already stated. This algorithm requires $2^{n+1} - 1$ Gröbner basis calculations with the recursion for calculating the f_i taken into account, provided that there occur no unlucky choices of degree vectors (d_1, \dots, d_n) or f_i . But since being a hsop is an open condition (Proposition 1), it makes sense to proceed as follows: if we have a degree vector (d_1, \dots, d_n) of which we can assume the existence of a hsop f_1, \dots, f_n with $\deg(f_i) = d_i$, then we take random elements $f_i \in A_{d_i}$ and test the condition $\dim(A/(f_1, \dots, f_n)) = 0$. In many cases, this condition will be verified, and we obtain a hsop by performing just one

Gröbner basis calculation. If this first guess fails, we try to use a variant of Algorithm 3 in Kemper (1996) which chooses the f_i successively such that the dimension of $A/(f_1, \dots, f_i)$ decreases in each step, without “looking further into the future” by taking additional conditions from Theorem 2(b) into account. In other words, we want to bring in more of the conditions from Theorem 2(b) dynamically and only if the need arises. This way, we will probabilistically minimize the number of Gröbner basis calculations and at the same time obtain an algorithm which is guaranteed to yield an optimal hso.

The algorithm uses a loop over a finite dimensional vector space V over K , so we have to explain how such a loop is performed: First, a basis (or a system of generators) b_1, \dots, b_m of V is chosen. Then we distinguish two cases:

- (a) K is infinite: Then an injective map $\iota: \mathbb{N}_0 \hookrightarrow K$ is chosen. Now we loop over all vectors $(k_1, \dots, k_m) \in \mathbb{N}_0^m$ in the order given by a total-degree term order on \mathbb{N}_0^m (starting with small (k_1, \dots, k_m)), and for each (k_1, \dots, k_m) we have a vector $\iota(k_1) \cdot b_1 + \dots + \iota(k_m) \cdot b_m$. If $f \in K[V]$ is a nonzero polynomial, then the loop will reach a $v \in V$ with $f(v) \neq 0$ after a finite number of steps. This assures termination in the context of our algorithm.
- (b) K is a finite field. Then we choose a bijection $\iota: \{0, \dots, q-1\} \rightarrow K$ and loop over all vectors $(k_1, \dots, k_m) \in \{0, \dots, q-1\}^m$ ordered by a total-degree term order on \mathbb{N}_0^m restricted to $\{0, \dots, q-1\}^m$. As above, this gives a loop over V .

We can now state the core algorithm (presented as Algorithm 1 on the following page) which takes a degree vector (d_1, \dots, d_m) as an argument and returns $f_1, \dots, f_m \in A$ with $\deg(f_i) = d_i$ and $\dim(A/(f_1, \dots, f_m)) = n - m$ if such f_i exist.

To see what happens in Algorithm 1, let us first look at the case where the ground field K is infinite. At the beginning of the main loop, the parameter k has a value such that it is known that there exist $f_1, \dots, f_k \in A$ with $\deg(f_i) = d_i$ and $\dim(A/(f_1, \dots, f_k)) \leq n - k$, except for the case $k = 0$, where it is not certain that $\dim(A) \leq n$. Now Theorem 2 is used to select an $f_1 \in A_{d_1}$ such that f_1 can be extended to a sequence f_1, \dots, f_k with the above properties. In the case $k = 0$, a random $f_1 \in A_{d_1} \setminus \{0\}$ is taken. Thus the value R returned by the recursive call of the algorithm will be a list from $A/(f_1)$ (in which case the algorithm finishes successfully) or a number $R \geq k$. In the latter case, k is set to $R + 1$, i.e. the algorithm will from now on try to find an f_1 which is extendable further than the previous one. Before searching such an f_1 , its existence is checked by using Theorem 2. It is known from the value returned by the recursive call that there exist f_1, \dots, f_{k-1} of degrees d_1, \dots, d_{k-1} with $\dim(A/(f_1, \dots, f_{k-1})) \leq n - k + 1$, so if no f_1 which is extensible to a sequence of k elements exists, then k is indeed minimal such that no sequence f_1, \dots, f_k with the desired properties exists. The only ambiguity occurs if the returned value R is 0, i.e. $\dim(A/(f_1)) > n - 1$. Then we must distinguish the cases $\dim(A) > n$ and $\dim(A) \leq n$. In the first case, zero is returned and in the second case one.

The only difference in the case that K is a finite field is that only the implication “(a) \Rightarrow (b)” from Theorem 2 can be used and hence no f_1 might be found by the loop although the condition at the end of the loop was satisfied. Then the loop runs through all elements of $A_{d_1} \setminus \{0\}$, and the algorithm comes to the correct conclusion that no f_1, \dots, f_k with the desired properties exist.

Hence the value of k gives the current degree of “foresight” with which Algorithm 1 operates. It is kept as small as possible to avoid unnecessary dimension tests, but as high

Algorithm 1. Try to find a hstop of given degrees.

Function TryDegrees($A, n, [d_1, \dots, d_m]$)

Input: A computable graded algebra A , a number $n \in \mathbb{N}_0$, and a list $[d_1, \dots, d_m]$ with $d_i \in \mathbb{N}$ and $d_1 \leq \dots \leq d_m$.

Output: Either a list $[f_1, \dots, f_m]$ with $f_i \in A$ homogeneous, $\deg(f_i) = d_i$ and $\dim(A/(f_1, \dots, f_m)) \leq n - m$, or the smallest $k \in \{0, \dots, m\}$ such that no $f_1, \dots, f_k \in A$ exist with $\deg(f_i) = d_i$ and $\dim(A/(f_1, \dots, f_k)) \leq n - k$.

Begin

Set $k := 0$;

if $m > 0$ **then** set $V := A_{d_1}$ **else** set $V := \{0\}$ **end if**;

for $f_1 \in V \setminus \{0\}$ **do**

if $k > 0$ **then**

for $M \subset \{2, \dots, k\}$ **do**

if $\dim\left(A/(f_1) + \left(\bigcup_{i \in M} A_{d_i}\right)\right) > n - |M| - 1$ **then next** f_1

end if

end for

end if;

Set $R := \text{TryDegrees}(A/(f_1), n - 1, [d_2, \dots, d_m])$;

if $R = [f_2 + (f_1), \dots, f_m + (f_1)]$ with $f_i \in A$ homogeneous **then return**
 $[f_1, \dots, f_m]$

end if;

if $R \geq k$ **then**

 Set $k := R + 1$;

for $M \subset \{1, \dots, k\}$ **do**

if $\dim\left(A/\left(\bigcup_{i \in M} A_{d_i}\right)\right) > n - |M|$ **then break** “for f_1 ” **end if**

end for

end if

end for;

if $k \leq 1$ **then**

if $\dim(A) > n$ **then** set $k := 0$

else set $k := 1$

end if

end if;

if $m = 0$ **and** $k = 1$ **then** set $k := []$ **end if**;

return k

end.

Algorithm 2. Calculate an optimal hsop.

Function HomogeneousParameterSystem(A, S)

Input: A graded algebra A which is computable in the sense of Definition 4, and a next-best function S (see 2).

Output: A list $[f_1, \dots, f_n]$ with $f_i \in A$ homogeneous and $\dim(A/(f_1, \dots, f_n)) = 0$, which is optimal in the following sense: If $S^e(1, \dots, 1) = (\deg(f_1), \dots, \deg(f_n))$ with $e \in \mathbb{N}_0$ and if there exists a hsop f'_1, \dots, f'_n for A with $S^{e'}(1, \dots, 1) = (\deg(f'_1), \dots, \deg(f'_n))$, then $e' \geq e$.

Begin

Set $n := \dim(A)$;

Set $(d_1, \dots, d_n) := (1, \dots, 1)$;

repeat

Test if (d_1, \dots, d_n) can be the degree vector of a hsop for A by applying those of the restrictions mentioned above which are available for this particular algebra A .

if (d_1, \dots, d_n) meets all these restrictions **then**

Set $R := \text{TryDegrees}(A, n, [d_1, \dots, d_n])$;

if R is a list **then return** R

end if;

end if;

Set $(d_1, \dots, d_n) := S(d_1, \dots, d_n)$;

end repeat;

end.

as necessary to ensure termination. A variant of the algorithm is to pass this foresight value to the lower recursion levels. This is done in the actual implementation in Magma. It is also important to remember the results of all dimension calculations performed in the course of the algorithm in order to avoid double calculations.

As mentioned at the beginning of this section, our approach of trying random elements of A_{d_i} as a hsop before checking conditions from Theorem 2(b) only makes sense if we have a fairly good guess of a degree vector (d_1, \dots, d_n) , or, equivalently, strong restrictions on degree vectors of hsop's. For example, if there exists a hsop with degrees d_1, \dots, d_n , then the Hilbert series $H(A, t) = \sum_{d=0}^{\infty} \dim_K(A_d) \cdot t^d$ takes the form

$$H(A, t) = \frac{f(t)}{(1 - t^{d_1}) \cdots (1 - t^{d_n})}$$

with $f \in \mathbb{Z}[t]$. This poses severe restrictions on (d_1, \dots, d_n) , and in fact the smallest d_i for which a representation of the above form exists will in many cases be correct. $H(A, t)$ is known by Molien's formula if A is the invariant ring of a permutation group or a finite linear group G such that $\text{char}(K) \nmid |G|$, or by a Gröbner basis calculation and the algorithm of Bayer and Stillman (1992) if A is given by a finite presentation, for instance.

Another restriction which is applicable in general is given by

PROPOSITION 6. *Let $A = \sum_{d=0}^{\infty} A_d$ be a graded commutative algebra of Krull-dimension n over a field $K = A_0$, and set $J_d = (\cup_{i=1}^d A_i) \triangleleft A$. If there exists a hsop f_1, \dots, f_n for A of degrees $d_1 \leq d_2 \leq \dots \leq d_n$, then*

$$d_i \geq \min\{d \mid \dim(A/J_d) \leq n - i\}.$$

PROOF. The result follows from

$$\dim(A/J_{d_i}) \leq \dim(A/(f_1, \dots, f_i)) = n - i. \quad \square$$

It is quite easy to calculate $\dim(A/J_d)$ for $d = 1, 2, \dots$ until the value zero is reached. In many cases, setting $d_i = \min\{d \mid \dim(A/J_d) \leq n - i\}$ provides a good guess for degrees of a hsop. Example 1 shows that this guess is not always correct, since in that example d_1 would be set to 5 and d_2 to 9.

A further general restriction on the degree vector (d_1, \dots, d_n) of a hsop is that $\deg(A) \cdot d_1 \cdots d_n \in \mathbb{N}$. Note that $\deg(A) = 1/|G|$ if A is the invariant ring of a finite group G , so we get the condition that $d_1 \cdots d_n$ must be multiple of $|G|$. Also, in this case the least common multiple of d_1, \dots, d_n must be a multiple of the exponent of G by Campbell *et al.* (1997), Kemper (1998). More restrictions can arise from the knowledge of several coefficients $\dim_K(A_d)$ of the Hilbert series and from previous runs of Algorithm 1. If Algorithm 1 has returned a number k when called with a degree vector d_1, \dots, d_n , then no extension of d_1, \dots, d_k can lead to a hsop.

We already mentioned in the introduction that how an optimal hsop is to be defined depends on the context. We now formulate an algorithm for the calculation of an optimal hsop which leaves it to the user to define the notion of optimal. More precisely, the user submits a so-called *next-best function* as an argument to the algorithm, i.e. a function $S: \mathbb{N}_{\text{asc}}^n := \{(d_1, \dots, d_n) \in \mathbb{N}^n \mid d_1 \leq \dots \leq d_n\} \rightarrow \mathbb{N}_{\text{asc}}^n$ such that for any $(d_1, \dots, d_n) \in \mathbb{N}_{\text{asc}}^n$ there is an $e \in \mathbb{N}_0$ with $(d_1, \dots, d_n) = S^e(1, \dots, 1)$, where S^e is the e -fold application of S . A typical choice for such a next-best function would be as follows: Given (d_1, \dots, d_n) , take the set of all $(d'_1, \dots, d'_n) \in \mathbb{N}_{\text{asc}}^n$ such that $\prod_{i=1}^n d'_i = \prod_{i=1}^n d_i$ and order this set by a total-degree term order. If (d_1, \dots, d_n) is not the greatest element in the resulting set, set $S(d_1, \dots, d_n)$ to be its successor. If it is the greatest element, take the smallest vector from the subset of $\mathbb{N}_{\text{asc}}^n$ consisting of the elements with product $1 + \prod_{i=1}^n d_i$ as $S(d_1, \dots, d_n)$.

With these preparations we can state Algorithm 2, which yields an optimal hsop for any computable graded algebra.

3. Implementation and Performance

There are several reasons why it does not make much sense to study the algorithm given in Section 2 in terms of complexity. The most important one is that it involves the calculation of Gröbner bases, which will dominate the complexity and make the behavior seem much worse than it practically is. The same is true for the successive algorithm and the trial and error algorithm (see in the Introduction). It is also quite hard to give estimates for the number of Gröbner basis calculations and the sizes of their inputs since the degree vectors d_1, \dots, d_n which the algorithm will try are not known in advance. In terms of average or probabilistic complexity, it can be said that the algorithm contains

Table 1. Running times for various algorithms that compute hsop's.

Example	Algorithm 2 (this article)	Successive algorithm	Trial and error algorithm	Dade's algorithm
Z_{18}	(6, 9) 0.180 sec.	(5, 18) 0.540 sec.	(6, 9) 0.160 sec.	(6, 9) 0.01 sec.
Z_9	(3, 5, 9) 0.610 sec.	(3, 6, 9) 0.819 sec.	(3, 6, 9) 0.510 sec.	(3, 9, 9) 0.01 sec.
S_3^2	(1, 1, 2, 2, 3, 3) 0.270 sec.	(1, 1, 2, 2, 3, 6) 0.179 sec.	(1, 2, 2, 2, 3, 3) 0.250 sec.	(1, 1, 3, 3, 6, 6) 0.02 sec.
A_5	(3, 5, 8, 12) 1.370 sec.	(3, 3, 12, 20) 19.760 sec.	(3, 5, 8, 12) 43.739 sec.	FAIL
$Z_4 \times Z_2$	(2, 2, 4) 0.179 sec.	(2, 2, 4) 0.119 sec.	(2, 2, 4) 0.110 sec.	(2, 2, 4) 0.01 sec.
Q_8^2	(2, 4, 4, 4) 0.440 sec.	(2, 4, 4, 4) 0.209 sec.	(2, 4, 4, 4) 0.169 sec.	(8, 8, 8, 8) 0.01 sec.
S_3^4	$(4 \times 1, 4 \times 2, 4 \times 3)$ 47.850 sec.	$(4 \times 1, 4 \times 2, 2 \times 3, 2 \times 6)$ 160.409 sec.	$\geq (2 \times 1, 5 \times 2, 5 \times 3)$ $\geq 337:09$ min.	$(4 \times 1, 4 \times 3, 4 \times 6)$ 0.039 sec.
$W_3(F_4)$	(2, 4, 18, 24) 115.869 sec.	(2, 4, 18, 24) 125.090 sec.	(2, 4, 18, 24) 81.769 sec.	FAIL

one Gröbner basis calculation if the ground field is infinite, but again this is misleading since in many interesting examples, bad choices of degree vectors as well as particular invariants f_i do happen. Hence, the only reasonable way to assess the performance of the algorithm is to run it on some typical examples and compare the running times with those of other algorithms.

For doing such experiments, I used an implementation of Algorithm 2 in the computer algebra system Magma, which applies to the case where A is the invariant ring of a finite linear group. This implementation is available as part of the new invariant theory package of Magma. The successive algorithm and the trial and error algorithm (see in the Introduction) were also implemented in Magma. Another interesting algorithm for constructing hsop's of invariant rings of finite groups is Dade's algorithm, which takes products over orbits of suitable linear polynomials as the members of a hsop, (see Stanley (1979)). This algorithm may fail if the ground field K has too few elements. A hsop produced by Dade's algorithm will have degrees of the same order of magnitude as $|G|$, so it is usually far from optimal, but Dade's algorithm does not involve any Gröbner bases and hence is quicker than the other algorithms discussed here. In the experiments this algorithm was performed in Magma in such a way that the resulting hsop's were optimal among those that could be obtained by Dade's algorithm. In all cases a Sun Ultraspac workstation was used. Table 1 contains the results.

Each entry in the table contains the degree vector of the hsop obtained by the corresponding algorithm and the running time (in seconds). The examples considered are:

- Z_{18} : The cyclic group of order 18 from Example 1.
- Z_9 : The cyclic group of order 9 from Example 2.
- S_3^2 : The permutation group $G \leq S_6$ generated by $(1, 2)(4, 5)$ and $(1, 2, 3)(4, 5, 6)$, with \mathbb{Q} as the ground field. In other words, the second vector invariants of the natural representation of S_3 are considered. This is Example 5(a) from Kemper (1996), where a bad choice of polynomials of degrees 2 and 3 leads to unnecessarily high degrees in the trial and error and in the successive algorithms.
- A_5 : The “first A_5 in $SL_4(\mathbb{F}_2)$ ” of Adem and Milgram (1994, p. 116). This is Example 5(b) from Kemper (1996), where the successive algorithm is too greedy in degree 3.
- $Z_4 \times Z_2$: The abelian group $G \leq GL_3(\mathbb{C})$ of order 8 generated by the diagonal matrices

$$\begin{pmatrix} 1 & & \\ & 1 & \\ & & i \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix}.$$

This is an example of Stanley (see Sloane (1977)), where

$$H(\mathbb{C}[V]^G, t) = \frac{1}{(1 - t^2)^3},$$

but there is no hsop of degrees $(2, 2, 2)$.

- Q_8^2 : The irreducible linear representation of degree 2 of the quaternion group $G = Q_8$ of order 8 on $V = \mathbb{C}^2$, given by the matrices

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

We consider the second vector invariants, i.e. $A = \mathbb{C}[V \oplus V]^G$. The interesting aspect of this example is that an optimal hsop for A cannot be obtained by putting together optimal hsop’s for both copies of V .

- S_3^4 : The fourth vector invariants of the natural representation of $G = S_3$ over \mathbb{Q} . In other words, we consider the permutation group in S_{12} generated by $(1, 2)(4, 5)(7, 8)$ $(10, 11)$ and $(1, 2, 3)(4, 5, 6)(7, 8, 9)(10, 11, 12)$. Here the trial and error algorithm was interrupted after more than 5 hours.
- $W_3(F_4)$: The 3-modular reduction of the Weyl group of type F_4 . This is historically the first example of a reflection group whose invariant ring is not isomorphic to a polynomial algebra.

From these example we see that Algorithm 2 is often quicker and never much slower than the successive or the trial and error algorithm. In many cases, it yields hsop’s of better degrees. In conclusion one can say that is not only a theoretic improvement of the existing algorithms (as it is guaranteed to produce optimal hsop’s), but also a practical one.

References

Adem, A., Milgram, R. J. (1994). *Cohomology of Finite Groups*. New York, Springer.
 Bayer, D., Stillman, M. (1992). Computation of Hilbert functions. *J. Symb. Comput.*, **14**, 31–50.
 Benson, D. J. (1993). *Polynomial Invariants of Finite Groups*, Lond. Math. Soc. Lecture Note Ser. 190. Cambridge, Cambridge University Press.
 Bosma, W., Cannon, J. J., Playoust, C. (1997). The Magma algebra system I: the user language. *J. Symb. Comput.*, **24**, 235–265.

- Campbell, H. E. A., Geramita, A. V., Hughes, I. P., Smith, G. G., Wehlau, D. L. (1997). Hilbert functions of graded algebras. *The Curves Seminar at Queen's*, Volume XI: in *Queen's Papers in Pure and Applied Math.*, **105**, 60–74.
- Decker, W., Heydtmann, A. E., Schreyer, F.-O. (1998). Generating a Noetherian normalization of the invariant ring of a finite group. *J. Symb. Comput.*, **25**, 727–731.
- Eisenbud, D. (1995). *Commutative Algebra with a View Toward Algebraic Geometry*. New York, Springer.
- Eisenbud, D., Sturmfels, B. (1994). Finding sparse systems of parameters. *J. Pure Appl. Algebra*, **94**, 143–157.
- Gelfand, I. M., Kapranov, M. M., Zelevinsky, A. V. (1994). *Discriminants, Resultants and Multidimensional Determinants*. Boston, MA, Birkhauser.
- Hartshorne, R. (1977). *Algebraic Geometry*. New York, Springer.
- Kemper, G. (1996). Calculating invariant rings of finite groups over arbitrary fields. *J. Symb. Comput.*, **21**, 351–366.
- Kemper, G. (1998). Lower degree bounds for modular invariants and a question of I. Hughes. *Transformation Groups*, **3**, 135–144.
- Müller-Quade, J., Beth, T. (1996). Homogeneous systems of parameters of minimal degree. Karlsruhe, EISS Preprint.
- Sloane, N. J. A. (1977). Error-correcting codes and invariant theory: new applications of a nineteenth-century technique. *Amer. Math. Monthly*, **84**, 82–107.
- Stanley, R. P. (1979). Invariants of finite groups and their applications to combinatorics. *Bull. Am. Math. Soc.*, **1**, 475–511.
- Sturmfels, B. (1993). *Algorithms in Invariant Theory*. New York, Springer.

Originally Received 20 August 1997
Accepted 27 August 1998