COMPUTING COMBINATORIAL DECOMPOSITIONS OF RINGS

by

Bernd Sturmfels[1] and Neil White[2]

[1] *Research Institute for Symbolic Computation*
Johannes-Kepler-Universität Linz
4040 Linz, AUSTRIA

[2] *Department of Mathematics,*
University of Florida,
Gainesville, FL 32611; U.S.A.

1. Introduction

This article deals with a topic on the borderline of commutative ring theory, computer algebra and combinatorics. We study canonical decompositions of commutative Noetherian rings. These techniques are based on earlier results of Rees [Ree], Stanley [St2], and Baclawski & Garsia [BGa], and they generalize the well-known Hironaka decomposition of Cohen-Macaulay rings. Here it is our main objective to give explicit algorithms for computing these decompositions.

Classes of rings for which such decompositions are known include coordinate rings of Grassmann varieties and Schubert varieties [Bac], Stanley-Reisner rings of simplicial polytopes [KKl], Partition rings [Gar] or the letter-place algebra of invariant theory [DKR].

An axiomatic theory generalizing these important examples has been developed by Baclawski [Bac], deConcini, Eisenbud, and Procesi [DEP],[Eis]. These authors define a *Hodge algebra* or an *algebra with straightening law* to be an algebra together with a specified normal form mapping, called the *straightening algorithm.* Given such a straightening law, then many structural questions about the ring can be reduced to easier problems about monomial ideals.

This raises a natural question. Given an arbitrary k-algebra R, does there exist a straightening algorithm for R, and, if so, how can we find it ? The answer is simple and encouraging. There is a well-known and rather efficient algorithm for computing straightening laws which is implemented in all major computer algebra systems, namely B. Buchberger *Gröbner basis algorithm.* In Sections 2 and 3 we will briefly summarize some basic concepts of Gröbner basis theory and its applications. For details we refer to [Bu1],[Bu2],[Bu3],[SSw],[Stu] and the references given there. The connection between Buchberger's method and the classical straightening algorithm has been worked out in detail in our earlier paper [SWh].

We now outline the results of the present paper. As a first application of the interplay of Gröbner bases theory and combinatorics we give a new and constructive proof for the existence of *Stanley decompositions* of k-algebras. This result provides a general algorithmic solution to a problem of Cushman related to normal forms of nilpotent vector fields [Cus], generalizing the specific results in in [BCS] and [CSW].

As has been pointed out by Billera, Cushman & Sanders [BCS], Stanley decompositions are closely related to the well-known Hironaka criterion for Cohen-Macaulayness. Yet, Stanley decompositions (as defined below) are not a generalization of *Hironaka decompositions* because they are not invariant under linear changes of variables. The existence of an invariant decomposition generalizing the Hironaka decomposition of Cohen-Macaulay rings to arbitrary rings has been first proved by Rees [Ree]. The resulting *Rees decomposition* have been recently extended and applied to combinatorics by Baclawski & Garsia [BGa].

As a main result of this paper we give an explicit algorithm for computing a Rees decomposition of an arbitrary graded k-algebra. This algorithm generalizes to modules over polynomial rings.

In Section 5 we exploit the fact that our Rees decomposition algorithm yields a decision procedure for Cohen-Macaulayness. Indeed, the given input ring is Cohen-Macaulay if and only if the output is a Hironaka decomposition. In particular, we will consider an extension of the algorithm where the ring is divided by a regular sequence with indeterminant coefficients. This method can be used to compute sufficient algebraic conditions for a sequence of linear forms to be regular.

In Section 6 we apply our methods to obtain Hironaka decompositions for a very important class of Cohen-Macaulay rings, namely invariant rings of finite group actions. More precisely, we give explicit algorithms based on Buchberger's Gröbner bases method for

(a) computing a finite set $\{I_1, \ldots, I_k\}$ of fundamental invariants for the action of a finite group on a polynomial ring *("first fundamental theorem")*,

(b) computing an ideal basis for the syzygies among the I_j *("second fundamental theorem")*, and

(c) expressing an arbitrary invariant I as polynomial function in the I_j.

The method for (a) uses classical ideas as well as modern results of Kempf [Ke1],[Ke2], Hochster, Eagon and Roberts [HoE],[HoR], and it generalizes to infinite reductive algebraic groups provided the Reynolds operator and the nullcone are given effectively.

2. Stanley decompositions and Gröbner bases

Throughout this paper k will denote a field of characteristic 0. By a *k-algebra* we mean a commutative ring with unit which is finitely generated as an algebra over k. Given such a k-algebra R, then we can write $R = k[\mathbf{x}]/I$ where I is an ideal in the polynomial algebra $k[\mathbf{x}]$ freely generated by n indeterminants $\mathbf{x} := (x_1, x_2, \ldots, x_n)$. If I is generated by homogeneous polynomials then R is a *graded* k-algebra (with respect to the usual grading induced from $k[\mathbf{x}]$).

At this point we need to interject a word of caution. While the above statement "we can write ..." is certainly true from an inconstructive mathematical point of view, things can be very difficult computationally whenever R is not given in terms of ideal generators for I. For example, if R is a finitely generated subring of $k[\mathbf{x}]$, then we need the syzygy computation in Algorithm 3.7 to obtain generators for I. In the case of invariant rings in Section 6 we have even less a priori information, and it is the job to find ring generators first. In the present section we shall assume that ideal generators $f_1, \ldots, f_m$ for I are explicitly given.

The set of non-negative integers is abbreviated $\mathbf{N}$, and, by standard abuse of notation, x_i denotes the image of the variable x_i in the residue ring R as well. As usual, the elements of $\mathbf{N}^n$ are identified with the monomials $\mathbf{x}^\alpha$ in the polynomial ring $k[\mathbf{x}]$ via

$$\mathbf{x}^\alpha \quad := \quad x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \ \ldots \ \cdot x_n^{\alpha_n} \quad \text{for} \quad \alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbf{N}^n.$$

A *Stanley decomposition* of the k-algebra R is a representation as the direct sum of k-vector spaces

$$R \quad = \quad \bigoplus_{\alpha \in \mathbf{F}} \mathbf{x}^\alpha \, k[\mathbf{X}_\alpha] \tag{1}$$

where $\mathbf{F}$ is a <u>finite</u> subset of $\mathbf{N}^n$ and where each $\mathbf{X}_\alpha$ is a subset of the variables $\{x_1, x_2, \ldots, x_n\}$. As a first motivation let us note how certain fundamental invariants of graded k-algebras can be read off from the representation (1).

Proposition 2.1. *Let R be a graded k-algebra with Stanley decomposition (1), and let d be the maximum of the numbers $|\mathbf{X}_\alpha|$, $\alpha \in \mathbf{F}$. Then*

(1) d is the Krull dimension of R, and

(2) the Hilbert series of R is given by

$$H(R\,;\lambda) \quad = \quad \sum_{\alpha \in \mathbf{F}} \left[\, \lambda^{|\alpha|} \,/\, (1-\lambda)^{|\mathbf{X}_\alpha|} \,\right].$$

Proposition 2.1 follows from the results in Stanley [St3].

Example 2.2. Let R be the quotient of the polynomial ring $k[x_1, x_2, x_3, x_4]$ by the ideal $< x_1x_3,\, x_2x_4 >$, i.e., R is the Stanley-Reisner ring of a quadrangle. A Stanley decomposition of R is given by

$$R \quad = \quad k[x_1, x_2] \ \oplus\ x_3\, k[x_2, x_3] \ \oplus\ x_4\, k[x_3, x_4] \ \oplus\ x_1x_4\, k[x_1, x_4].$$

Hence R is a 2-dimensional ring with Hilbert series $H(R, \lambda) = \frac{1+2\lambda+\lambda^2}{(1-\lambda)^2}$. Another Stanley decomposition of R is

$$\begin{aligned} R \quad = \quad & k \ \oplus\ x_1k[x_1] \ \oplus\ x_2k[x_2] \ \oplus\ x_3k[x_3] \ \oplus\ x_4k[x_4] \ \oplus \\ & x_1x_2k[x_1, x_2] \ \oplus\ x_2x_3k[x_2, x_3] \ \oplus\ x_3x_4k[x_3, x_4] \ \oplus\ x_1x_4k[x_1, x_4]. \end{aligned}$$

This example shows that Stanley decompositions are far from being unique. It is the main goal of this section to give an algorithmic proof for the existence of Stanley decompositions.

Theorem 2.3. *Every finitely generated k-algebra admits a Stanley decomposition.*

Our proof of Theorem 2.3 consists of two steps. First, we will assume that the ideal I is generated by monomials. In that case the problem is purely combinatorial, and it is not difficult to give an algorithm for computing Stanley decompositions. In the second step we apply Gröbner bases theory to reduce the general case to the previous one.

Lemma 2.4. *Let $R = k[\mathbf{x}]/I$ where I is a monomial ideal. Then R has Stanley decomposition.*

Proof. A natural partial order "$<$" on $\mathbf{N}^n$ is defined by setting $\gamma < \delta$ whenever the vector $\delta - \gamma \in \mathbf{N}^n$ is non-zero and has only non-negative entries. Suppose that I is generated by $\{\mathbf{x}^{\beta_1}, \mathbf{x}^{\beta_2}, \ldots, \mathbf{x}^{\beta_m}\}$ where $\beta_i = (\beta_{i1}, \beta_{i2}, \ldots, \beta_{in}) \in \mathbf{N}^n$.

A Stanley decomposition for the ring $R = k[\mathbf{x}]/I$ is obtained as follows. Consider the set of $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbf{N}^n$ such that

$$\gamma \not\geq \beta_1 \quad \wedge \quad \gamma \not\geq \beta_2 \quad \wedge \quad \ldots \quad \wedge \quad \gamma \not\geq \beta_m. \tag{2}$$

The corresponding monomials form a k-vector space basis for the algebra R. Hence we have the decomposition

$$R \quad = \quad \bigoplus_{\gamma \text{ satisfies } (2)} \mathbf{x}^{\gamma}\, k. \tag{3}$$

If R is finite-dimensional over k, then (3) is already a Stanley decomposition. Otherwise, we have to regroup the infinite direct sum (3) into finitely many terms. To do so, we observe that (2) is equivalent to

$$
\begin{array}{rl}
& (\,\gamma_1 < \beta_{11} \;\vee\; \gamma_2 < \beta_{12} \;\vee\; \ldots \;\vee\; \gamma_n < \beta_{1n}\,) \\
\wedge & (\,\gamma_1 < \beta_{21} \;\vee\; \gamma_2 < \beta_{22} \;\vee\; \ldots \;\vee\; \gamma_n < \beta_{2n}\,) \\
\wedge & \qquad \ldots \qquad \ldots \qquad \ldots \\
\wedge & (\,\gamma_1 < \beta_{m1} \;\vee\; \gamma_2 < \beta_{m2} \;\vee\; \ldots \;\vee\; \gamma_n < \beta_{1n}\,)
\end{array}
\tag{4}
$$

Using a disjunctive normal form algorithm, the conjunction (4) can be rewritten as a finite exclusive disjunction (4') of n-ary conjunctions of certain basic expressions. These basic expressions are either inequalities "$\gamma_j \geq \alpha_j$" or equations "$\gamma_j = \alpha_j$", for suitable $\alpha_j \in \mathbf{N}$.

One such conjunction of basic expressions is indexed by a vector $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{N}^n$. Let $\mathbf{X}_\alpha$ be the set of variables x_j such that γ_j appears in an inequality "$\gamma_j \geq \alpha_j$" and not in an equation "$\gamma_j = \alpha_j$". Finally, let $\mathbf{F}$ denote the finite set of all $\alpha \in \mathbf{N}^n$ indexing the conjunctions in the exclusive disjunction (4'). This implies that (3) is equivalent to the Stanley decomposition (1), and the proof of Lemma 2.4 is complete. $\triangle$

The transformation from (4) to (4') is a finite (hence computable) problem. Yet, it seems to be a non-trivial combinatorial task to find an optimal algorithm for this transformation.

We now describe how Theorem 2.3 is derived from Lemma 2.4. First we must introduce Gröbner bases. A total order "$\prec$" on $\mathbf{N}^n$ is *admissible* if the zero vector is the infimum, and if $\alpha \prec \beta$ implies $\alpha + \gamma \prec \beta + \gamma$ for all $\alpha, \beta, \gamma \in \mathbf{N}^n$. Note that every admissible order "$\prec$" refines the above partial order "$<$".

In the following we fix an admissible order "$\prec$" on $\mathbf{N}^n$, or, equivalently, on the set of monomials in $k[\mathbf{x}]$. Given any polynomial $p \in k[\mathbf{x}]$, we write $lead(p)$ for the maximal monomial with non-zero coefficient in p, called the *leading monomial* of p (with respect to "$\prec$").

Let $I \subset k[\mathbf{x}]$ be any ideal. The *initial ideal* $Init(I)$ associated with I is the monomial ideal generated by $\{\, lead(f) \mid f \in I\}$. A subset $G = \{g_1, g_2, \ldots, g_k\}$ of I is said to be a *Gröbner basis* for I (w.r.t "$\prec$") if the initial ideal $Init(I)$ is generated by $\{lead(g_1), lead(g_2), \ldots, lead(g_k)\}$. Gordan's lemma, stating that "$<$" has no infinite antichains [KRo], implies the existence of a finite Gröbner basis G and the fact that G generates I as an ideal.

An important property of Gröbner bases is that they provide a simple normal form algorithm for the residue classes modulo I. As in shown in [SWh], this normal form algorithm generalizes the classical *straightening algorithm* for the coordinate rings of Grassmann varieties.

In the language of Hodge algebras [DEP], the monomials in the initial ideal $init(I)$ are *non-standard* in $R = k[\mathbf{x}]/I$ while the monomials not in $init(I)$ are called *standard*. Every non-standard monomial $\mathbf{x}^\alpha$ is thus expressible modulo I as a unique k-linear combination $\sum c_{\alpha\beta}\,\mathbf{x}^\beta$ of standard monomials.

The cornerstone of Gröbner bases theory is B. Buchberger's algorithm for computing the *reduced Gröbner basis*

$$\left\{\ \mathbf{x}^\alpha - \sum_{\mathbf{x}^\beta \text{standard}} c_{\alpha\beta}\ \mathbf{x}^\beta \quad | \quad \mathbf{x}^\alpha \ \text{minimally non-standard}\ \right\}$$

with respect to a given order "$\prec$" from an arbitrary generating set of an ideal I in $k[\mathbf{x}]$. Buchberger's original procedure from 1965 (see [Bu1]) has been improved many times since, and today quite efficient implementations are available in many computer algebra systems such as MACSYMA, SCRATCHPAD, MAPLE, ... [Bu2].

We now complete the proof of Theorem 2.3 by showing the following easy lemma.

Lemma 2.5. *Let*

$$k[\mathbf{x}]\,/\,init(I) \quad = \quad \bigoplus_{\alpha\in\mathbf{F}} \mathbf{x}^\alpha\, k[\mathbf{X}_\alpha]$$

be a Stanley decomposition of the residue ring modulo the monomial ideal $init(I)$. Then we have the same Stanley decomposition

$$k[\mathbf{x}]\,/\,I \quad = \quad \bigoplus_{\alpha\in\mathbf{F}} \mathbf{x}^\alpha\, k[\mathbf{X}_\alpha]$$

for the residue ring modulo the ideal I.

Proof. By a well-known result Gröbner bases theory, the normal form procedure versus a Gröbner basis of I defines an isomorphism from $k[\mathbf{x}]/I$ onto the k-vector space freely generated by the standard monomials $\{\,\mathbf{x}^\beta \mid \mathbf{x}^\beta \notin init(I)\,\}$. In other words, we have an explicit k-vector space isomorphism between the residues algebras $k[\mathbf{x}]/I$ and $k[\mathbf{x}]/init(I)$. Since Stanley decompositions are invariant under this isomorphism, Lemma 2.5 and hence Theorem 2.3 follows. Note that $k[\mathbf{x}]/I$ and $k[\mathbf{x}]/init(I)$ are, in general, not isomorphic as k-algebras (see Example 5.1). $\triangle$

Observe that the k-vector space isomorphism promised by Theorem 2.3 is realized by the normal form (straightening) map versus the Gröbner basis of I. This section will be closed with an example illustrating the above results. An explicit Stanley decomposition of rank 2 bracket algebras has recently been obtained by Cushman, Sanders & White [CSW]. We use Gröbner bases and cyclic straightening [KRo] to give an alternative Stanley decomposition for [CSW, Example 2].

Example 2.6. (A Stanley decomposition of a rank 2 bracket algebra)

Let $k\big[[12],\ldots,[45]\big]$ be the polynomial algebra freely generated by ten indeterminants *brackets* $[12],[13],[14],[15],[23],[24],[25],[34],[35],[45]$. The *bracket ring* is the quotient $B := k\big[[12],\ldots,[45]\big]\,/\,I$ by the ideal I generated by the polynomials

$$\begin{aligned}&\underline{[13][24]} - [12][34] - [14][23]\,,\ \underline{[13][25]} - [12][35] - [15][23]\,,\ \underline{[14][25]} - [12][45] - [15][24]\,,\\ &\underline{[14][35]} - [13][45] - [15][34]\,,\ \underline{[24][35]} - [23][45] - [25][34].\end{aligned} \tag{5}$$

It follows from the results in [SWh] and [KRo] that the polynomials in (5) form a Gröbner basis for I with respect to the *cyclic tableaux order* on the monomials in $k\big[[12],\ldots,[45]\big]$. ¿From this we can derive a Stanley decomposition for B as follows. The initial ideal $init(I)$ is generated by the underlined leading monomials

$$[13][24]\,,\quad [13][25]\,,\quad [14][25]\,,\quad [14][35]\,,\quad [24][35], \tag{6}$$

called the (cyclic) non-standard monomials in B. By Lemma 2.5 it is sufficient to find a Stanley decomposition of the simpler ring $B_0 := k\big[[12],\ldots,[45]\big]\,/\,init(I)$. To simplify things further, we divide B_0 by the brackets not occuring in (6), that is, we first compute a Stanley decomposition for $B_0' := B_0\,/ < [12],[23],[34],[45],[15] >$. We observe that B_0' is the Stanley-Reisner ring of a pentagon. Generalizing the first decomposition of the quadrangle ring in Example 2.2, we get $B_0' =$

$$k\big[[13],[14]\big] \oplus [24]\,k\big[[14],[24]\big] \oplus [25]\,k\big[[24],[25]\big] \oplus [35]\,k\big[[25],[35]\big] \oplus [35][13]\,k\big[[35],[13]\big]$$

Hence the bracket algebra has the Stanley decomposition $B =$

$$
\begin{aligned}
& k[\,[13],[14]\,,\,[12],[23],[34],[45],[15]\,] && \oplus \\
[24]\ & k[\,[14],[24]\,,\,[12],[23],[34],[45],[15]\,] && \oplus \\
[25]\ & k[\,[24],[25]\,,\,[12],[23],[34],[45],[15]\,] && \oplus \\
[35]\ & k[\,[25],[35]\,,\,[12],[23],[34],[45],[15]\,] && \oplus \\
[35][13]\ & k[\,[35],[13]\,,\,[12],[23],[34],[45],[15]\,].
\end{aligned}
$$

3. Some commutative algebra subroutines using Gröbner bases

In the following we summarize nine commutative algebra "subroutines" based on Buchberger's method which will be applied in the following sections. Most of these algorithms are well-known in Gröbner basis theory, and appropriate references are given. Whenever the monomial order is unspecified, any admissible order will work for the Gröbner bases computation.

Two of the most frequently used admissible orders are the *purely lexicographical order* "$>_{pl}$" and the *reverse lexicographical order* "$>_{rl}$". These are defined as follows.

We begin by assuming that an order is given on the variables, $x_1 > x_2 > \ldots > x_n$. We then put $\mathbf{x}^\alpha >_{pl} \mathbf{x}^\beta$ if there exists $i, 1 \leq i \leq n$, such that $\alpha_j = \beta_j$ for all $j < i$, and $\alpha_i > \beta_i$. In contrast to "$>_{pl}$", the reverse lexicographic order "$>_{rl}$" is a linear extension of the natural grading on $k[\mathbf{x}]$. We define $\mathbf{x}^\alpha >_{rl} \mathbf{x}^\beta$ if $\sum \alpha_i > \sum \beta_i$, or if $\sum \alpha_i = \sum \beta_i$ and there exists $i, 1 \leq i \leq n$, such that $\alpha_j = \beta_j$ for all $j > i$, and $\alpha_i < \beta_i$.

Subroutine 3.1. (Ideal intersection [Bu3])

Input : $f_1, f_2, \ldots, f_m, g_1, g_2, \ldots, g_k \in k[\mathbf{x}]$.
Problem : Let $I := < f_1, \ldots, f_m >$ be the ideal generated by the f_i's, and let $J := < g_1, \ldots, g_k >$ be the ideal generated by the g_i's. Find generators for the ideal $I \cap J$.
Solution : Let G be a Gröbner basis of

$$< f_1 z, f_2 z, \ldots, f_m z\,,\, g_1(1-z), g_2(1-z), \ldots, g_k(1-z) >,$$

where z is a new variable, and we use purely lexicographical order induced from $x_1 > x_2 > \ldots > x_n > z$. Then $G' := G \cap k[x_1, \ldots, x_n]$ is a Gröbner basis of $I \cap J$.

Subroutine 3.2. (Ideal quotient by a principal ideal [Bu3])

Input : $f_1, f_2, \ldots, f_m, g \in k[\mathbf{x}]$.

Problem : Let $I := < f_1, \ldots, f_m >$ be the ideal generated by the f_i's. Find $I : g$, which by definition is $\{ h \in k[\mathbf{x}] : gh \in I \}$.

Solution : Since $g\,(I : g) = I \cap < g >$, we use Subroutine 3.1 to find a Gröbner basis G of $I \cap < g >$. Then $G' := \{ h/g : h \in G \}$ is a Gröbner basis of $I : g$.

Subroutine 3.3. (Ideal quotient by a principal ideal, alternate version [Bay])

Input : Homogeneous polynomials $f_1, f_2, \ldots, f_m, g \in k[\mathbf{x}]$.

Problem : Let $I := < f_1, \ldots, f_m >$ be the ideal generated by the f_i's. Find $I : g$.

Solution : Let G be a Gröbner basis of $< f_1, f_2, \ldots, f_m, g - z >$, where z is a new variable, and we use reverse lexicographical order induced from $x_1 > x_2 > \ldots, > x_n > z$. Let $G' = \{h/z : h \in G, h \,\text{is a multiple of}\, z\}$. Replace any remaining occurances of z in elements of G' by g. Then G' is a Gröbner basis of $I : g$.

Subroutine 3.4. (Ideal quotient [Bu3])

Input : $f_1, f_2, \ldots, f_m\,,\, g_1, g_2, \ldots, g_k \in k[\mathbf{x}]$.

Problem : Let $I := < f_1, \ldots, f_m >$, and let $J := < g_1, \ldots, g_k >$. Find the ideal $I : J$, which is $\{ h \in k[\mathbf{x}] : hJ \subseteq I \}$.

Solution : $I : J = (I : g_1) \cap \ldots \cap (I : g_k)$. Use Subroutines 3.1 and 3.2.

Subroutine 3.5. (Radical containment [Bu2, Theorem 2.5.1])

Input : $f_1, f_2, \ldots, f_m, g \in k[\mathbf{x}]$.

Question : Let $I := < f_1, \ldots, f_m >$. Is $g \in Rad(I)$ (the radical of I) ?

Solution : Let G be a Gröbner basis of $< f_1, f_2, \ldots, f_m\,,\, gz - 1 >$, where z is a new variable. $g \in Rad(I)$ if and only if $1 \in G$.

Subroutine 3.6. Solvability of homogeneous equations [Bu1, Method 6.9]

Input : <u>Homogenous</u> polynomials $f_1, f_2, \ldots, f_m \in k[\mathbf{x}]$.

Question : Is there a <u>non-zero</u> vector $\mathbf{x} \in \bar{k}^n$ such that $f_1(\mathbf{x}) = f_2(\mathbf{x}) = \ldots = f_m(\mathbf{x}) = 0$. Here $\bar{k}$ denotes the algebraic closure of k.

Solution : Compute a Gröbner basis G of the ideal $I := < f_1, f_2, \ldots, f_m >$. We have $Rad(I) = < x_1, x_2, \ldots, x_n >$ (i.e., there is no non-zero solution) if and only if a monomial of the form $x_i^{j_i}$ occurs among the leading terms in G for every i, for $1 \le i \le n$.

Subroutine 3.7. (Algebraic Dependence [Bu2],[Stu])

Input : $F := \{f_1, f_2, \ldots, f_m\} \subset k[\mathbf{x}]$, where $m \le n$, considered as subset of the field $k(\mathbf{x})$.
Questions : Is F algebraically dependent over k ? If so, find an m-variate polynomial P such that $P(f_1, f_2, \ldots, f_m) = 0$ in $k(\mathbf{x})$.
Solution : Introduce m new "slack" variables $\mathbf{y} := (y_1, \ldots, y_m)$, and compute a Gröbner basis G of $\{f_1 - y_1, f_2 - y_2, \ldots, f_m - y_m\}$ with respect to purely lexicographical order induced from $x_1 > \ldots > x_n > y_1 > \ldots > y_m$. Let $G' := G \cap k[\mathbf{y}]$. F is algebraically independent if and only of $G' = \emptyset$. On the other hand, if $P(\mathbf{y}) \in G'$, then $P(f_1, \ldots, f_m) = 0$ in $k[\mathbf{x}]$.

Subroutine 3.8. (Containment in subrings [SSw],[Stu])

Input : $f_1, f_2, \ldots, f_m,\ g \in k[\mathbf{x}]$.
Question : Is g contained in the subring $k[f_1, \ldots, f_m]$ of $k[\mathbf{x}]$? If so, find an m-variate polynomial Q such that $g = Q(f_1, f_2, \ldots, f_m)$ in $k[\mathbf{x}]$.
Solution : Compute the Gröbner basis G as in Subroutine 3.7, and let $Q \in k[\mathbf{x}, \mathbf{y}]$ be the unique normal form of g with respect to G. Then $g \in k[f_1, \ldots, f_m]$ if and only if Q is contained in $k[\mathbf{y}]$. In that case we have the identity $g = Q(f_1, f_2, \ldots, f_m)$ in $k[\mathbf{x}]$.

While the Subroutines 3.1 to 3.8 are well known in Gröbner basis theory, we will close this section with a subroutine which (to the best of our knowledge) has not yet been considered in the literature. It is a generalization of Subroutine 3.3.

Subroutine 3.9. (Free module over a subring of variables)

Input : Homogeneous polynomials $f_1, f_2, \ldots, f_m \in k[x_1, \ldots, x_n\,,\ z_1, \ldots, z_d] =: k[\mathbf{x}, \mathbf{z}]$.
Question : Let $I := < f_1, \ldots, f_m >$, and consider the graded k-algebra $R := k[\mathbf{x}, \mathbf{z}]/I$. Is R a free module over the subring $k[\mathbf{z}]$ generated by the z_i ?
Solution : Let G be a reduced Gröbner basis for I with respect to reverse lexicographical order induced from $x_1 > \ldots > x_n > z_1 > \ldots > z_d$. Then R is a free $k[\mathbf{z}]$-module if and

only if the leading monomials of all elements of G are contained in $k[\mathbf{x}]$. If so, then the subset of standard monomials in $k[\mathbf{x}]$ forms a free basis for R as a $k[\mathbf{z}]$-module.

For completeness we include a proof of correctness for Subroutine 3.9. The monomials in $k[\mathbf{x}, \mathbf{z}]$ will be identified with the elements of $\mathbf{N}^n \times \mathbf{N}^d$. Let $Std \subset \mathbf{N}^n \times \mathbf{N}^d$ denote the set of standard monomials versus G, and let $Std_{\mathbf{x}} \subset \mathbf{N}^n$ denote the subset of standard monomials only containing $x_1, \ldots, x_n$. The above criterion that the leading monomials of all polynomials in G are in $k[\mathbf{x}]$ is equivalent to the condition $Std = Std_{\mathbf{x}} \times \mathbf{N}^d$.

If this condition is satisfied, then we have the k-vector space decomposition

$$R \quad = \quad \bigoplus_{(\alpha,\beta) \in Std} \mathbf{x}^\alpha \, \mathbf{z}^\beta \, k \quad = \quad \bigoplus_{\alpha \in Std_{\mathbf{x}}} \mathbf{x}^\alpha \, k[\mathbf{z}],$$

and hence $Std_{\mathbf{x}}$ is a free $k[\mathbf{z}]$-module basis for R.

Conversely, let R be a free $k[\mathbf{z}]$-module, and let $g \in G$. We need to show that $lead_{rl}(g) \in k[\mathbf{x}]$. We assume the contrary, namely $lead_{rl}(g) = \mathbf{x}^\alpha \mathbf{z}^\beta$ with $\beta \neq 0$. By the properties of the reverse lexicographic order, this implies that every monomial in g contains some z_i, and we can write

$$g \quad = \quad \sum_{\gamma,\delta} c_{\gamma\delta} \, \mathbf{x}^\gamma \mathbf{z}^\delta \quad \in \quad G$$

where $c_{\gamma\delta} \in k$ and where the sum ranges only over non-zero δ. Consider the above sum as an identity in the $k[\mathbf{z}]$-module R.

By the *cancellation property* for free modules over graded algebras [Bac, Prop. 2.3], there exists an index $\hat{\gamma}$ such that $\mathbf{x}^{\hat{\gamma}} = \sum_{\delta, \gamma \neq \hat{\gamma}} \hat{c}_{\gamma\delta} \, \mathbf{x}^\gamma \mathbf{z}^\delta$ in R. Let $\hat{g} := \mathbf{x}^{\hat{\gamma}} - \sum_{\delta, \gamma \neq \hat{\gamma}} \hat{c}_{\gamma\delta} \, \mathbf{x}^\gamma \mathbf{z}^\delta$ be the corresponding element in I. Clearly $lead(\hat{g}) \geq_{rl} \mathbf{x}^{\hat{\gamma}}$, and, by the properties of the reverse lexicographic order, this implies $lead(\hat{g}) = \mathbf{x}^\gamma$ for some $\mathbf{x}^\gamma \mathbf{z}^\delta$, $\delta \neq 0$, occuring in the expansion of g.

Thus the non-standard monomial $\mathbf{x}^\gamma$ properly divides a monomial in g. This is a contradiction to the assumption that g is contained in the <u>reduced</u> Gröbner basis G. This completes the proof of correctness for Subroutine 3.9. $\triangle$

4. Rees decompositions

Let $R = k[\mathbf{x}]/I$ be a (finitely generated) k-algebra, where I is a homogeneous ideal with respect to the usual grading. Then R is a graded k-algebra which is generated by homogeneous elements of degree one. Let d be the Krull dimension of R. A *Rees decomposition* of R consists of a d-tuple of homogeneous elements of R, $(\theta_1, \theta_2, \ldots, \theta_d)$, which form a homogeneous system of parameters for R, a finite sequence $(\eta_1, \eta_2, \ldots, \eta_N)$ of homogeneous elements of R, and an index function $f : [1, N] \to [0, d]$ such that:

(1) every element of R may be uniquely expressed in the form

$$\sum_{j=1}^{N} \eta_j \, p_j(\theta_1, \theta_2, \ldots, \theta_{f(j)}),$$

where p_j is a polynomial in $f(j)$ variables,

(2) for every j, $\quad \eta_j < \theta_{f(j)+1}, \ldots, \theta_d > \subseteq < \theta_1, \ldots, \theta_{f(j)} >$.

Rees decompositions were first studied by Rees [Ree] in the more general case of non-graded k-algebras. They were studied extensively in the graded case and related to the Stanley-Reisner ring of the chain complex of a poset by Baclawski and Garsia [BGa], who assumed only that each x_i has positive grade. We need the stronger assumption that R is generated by homogeneous elements of degree one in order to prove the following stronger version of a lemma of Baclawski and Garsia. Let R_+ denote the set of elements of R of positive degree and $A(r)$ the annihilator of r in R for any $r \in R$. Given any subset S of R, we write HS for the set of homogeneous elements of S and S_i for the set of homogeneous elements of degree i in S.

Lemma 4.1. *Assume that for every homogeneous η in HR_+, $A(\eta) \neq R_+$. Then there exists a non zero-divisor in R_1. Furthermore, if R_1 is identified with k^q as a vector space, then the non zero-divisors contain a non-empty Zariski-open subset of k^q.*

Proof of Lemma 4.1. We proceed as in Baclawski-Garsia [BGa, Lemma 2.2], to see that $Z(R)$, the set of zero-divisors in R, is contained in

$$A(\eta_1) \cup A(\eta_2) \cup \ldots \cup A(\eta_p)$$

for some finite number of elements $\eta_1, \eta_2, \ldots, \eta_p$ of HR_+. Thus

$$Z(R)_1 \quad \subseteq \quad A(\eta_1)_1 \cup A(\eta_2)_1 \cup \ldots A(\eta_p)_1,$$

but each $A(\eta_i)_1$ is a proper vector subspace of the vector space R_1. Since we are working over an infinite field, the Lemma follows.

We now describe an algorithm to compute a Rees decomposition of R.

Algorithm 4.2.

Input : $f_1, f_2, , \ldots, f_m \in k[\mathbf{x}]$.

Problem : Find a Rees decomposition of $R = k[\mathbf{x}]/I$ where $I = < f_1, f_2, \ldots, f_m >$.

1. Initialize $j := 1, h := 0$.
2. If $I = < x_1, \ldots, x_n >$, then set $N := j$, $\eta_j := 1 \in k$, $d := h$ and EXIT.
3. Using Subroutine 2.4, with $M = < x_1, x_2, \ldots, x_n >$, compute $J = I : M$. Note that J is homogeneous and its elements annihilate R_+. Use the Gröbner basis normal form subroutine to determine whether any of the computed generators of J is not an element of I. If so, GO TO 4. If not, GO TO 5.
4. Set η_j equal to the element of $J - I$ found in 3. Set $f(j) := h, I := I + < \eta_j >$, and $j := j + 1$. GO TO 2.
5. Set $h := h + 1$. Randomly pick a homogeneous element of degree 1, $\theta_h = a_{1,h}x_1 + \ldots + a_{n,h}x_n$. In particular, $a_{1,h}, \ldots, a_{n,h}$ may be picked by random number generation in the interval $[0, 1]$ in the rationals. Determine whether $I : \theta_h = I$, or equivalently, whether $A(\theta_h) = (I : \theta_h)/I$ is zero.

   This will be true with probability 1 by Lemma 4.1, but if not, repick θ_h until it is true. Set $I := i + < \theta_h >$. GO TO 2.

The proof that Algorithm 4.2 terminates with a Rees decomposition of R (with probability 1) is just the constructive analogue to the proof provided in Baclawski and Garsia [BGa, Theorem 2.1]. Moreover, our algorithm gives the extra condition that the θ_h's are of degree 1.

We remark that the number of θ's found before the first η is found is the common length of all R-sequences in R, in other words, the *depth* of R.

Example 4.3. We apply Algorithm 4.2 to the ideal $I = < x^4, x^2z, y^2 > \subseteq k[x, y, z]$. In Step 4, we find the annihilator $\eta_1 = x^3y$, the unique choice of an element from the computed Gröbner basis of J which is not in I. Updating I to $< x^4, x^3y, x^2z, y^2 >$, we similarly find successively $\eta_2 = x^2y$, $\eta_3 = x^3$, $\eta_4 = x^2$, with $f(1) = \ldots = f(4) = 0$. I is now $< x^2, y^2 >$, and we now find $I : M = I$.

In Step 5, suppose we now pick the non-zerodivisor $\theta_1 = x + y + z$. We now cycle through Step 4 some more, finding $\eta_5 = xy, \eta_6 = x, \eta_7 = y$, and finally $\eta_8 = 1$, with $f(5) = \ldots = f(8) = 1$. We conclude that a Rees decomposition of R is

$$R = x^2\ k \ \oplus\ x^3\ k \ \oplus\ x^2y\ k \ \oplus\ x^3y\ k \ \oplus\ 1\ k[\theta_1] \ \oplus\ x\ k[\theta_1] \ \oplus\ y\ k[\theta_1] \ \oplus\ xy\ k[\theta_1].$$

We can now immediately read off the Hilbert series for R, namely

$$H(R;\lambda) \quad = \quad t^2 + 2t^3 + t^4 \ + \ \frac{1 + 2t + t^2}{1 - t}.$$

We now wish to point out that the above algorithm for Rees decompositions can be done just as easily for the more general case of a finitely generated graded module over $k[\mathbf{x}]$. We chose not to present it that way to make it easier for non-algebraists to read. If M is such a module, then Lemma 4.1 now says that if for every homogeneous η in HM_+, $A(\eta) \neq R_+$, then there exists an element of R_1 which is a non zero-divisor on M. The algorithm proceeds as above, updating M by $M/ < \eta >$ if $A(\eta) = R_+$, and by $M/k[\theta]M$ if θ is a non zero-divisor. Gröbner basis routines for computing with modules over polynomial rings are straightforward generalizations of the ones for polynomial rings themselves, and are implemented in some systems, such as MACAULAY.

5. Hironaka decompositions of Cohen-Macaulay rings

In this section we will discuss decompositions of a special class of rings which is of particular interest in combinatorics. A graded k-algebra R is said to be *Cohen-Macaulay* if $depth(R) = dim(R)$. In other words, R is Cohen-Macaulay if the index function f generated by our Rees decomposition Algorithm 4.2 is constant and hence equal to the dimension $d := dim(R)$ of the ring in question. The equivalence of this algorithmic definition to other characterizations of Cohen-Macaulayness is the well-known Hironaka's criterion .

Let us look more closely at the performance of Algorithm 4.2 when applied to a Cohen-Macaulay ring. In the first d iterations only Step 5 is executed, and a regular sequence $(\theta_1, \theta_2, \ldots, \theta_d)$ of homogeneous elements of degree 1 is found. Then the algorithm proceeds with the zero-dimensional graded ring $R' := R / < \theta_1, \theta_2, \ldots, \theta_d >$, and from now on only Step 4 is executed, finding N successive annihilators $\eta_1, \ldots, \eta_N$. The resulting Rees decomposition expresses R as a free $k[\theta_1, \theta_2, \ldots, \theta_d]$-module with basis $\{\eta_1, \ldots, \eta_N\}$. Note that at this point the set of separators $\{\eta_1, \ldots, \eta_N\}$ can be replaced by any other k-vector space basis for R'. In particular, we may pick N separators all of which are monomials. It is the objective of this section to study this special form of Rees decompositions for Cohen-Macaulay rings.

A *Hironaka decomposition* of a graded k-algebra R is a representation as the direct sum of k-vector spaces

$$R \quad = \quad \bigoplus_{\alpha \in \mathbf{F}} \mathbf{x}^\alpha \, k[\theta_1, \theta_2, \ldots, \theta_d] \tag{7}$$

where $\mathbf{F}$ is a <u>finite</u> subset of $\mathbf{N}^n$ and where each θ_i is homogeneous of degree 1. By the above arguments, R admits a Hironaka decomposition if and only if R is Cohen-Macaulay.

Example 5.1. Consider the ideal $I := < (x+y)^2, x^2 - y^2, xz >$ in $k[x, y, z]$. The quotient ring is Cohen-Macaulay, and using Algorithm 4.2 we could find the Hironaka decomposition

$$k[x, y, z]/I \quad = \quad k[y+z] \, \oplus \, x\, k[y+z] \, \oplus \, z\, k[y+z].$$

The initial ideal of I with respect to purely lexicographic order from $x > y > z$ is given by $init(I) = < x^2, xy, xz, zy^2 >$. We see that x is a zero-divisor in the one-dimensional ring $k[x,y,z]/init(I)$. Hence $k[x,y,z]/init(I)$ is not Cohen-Macaulay although $k[x,y,z]/I$ is Cohen-Macaulay.

This example shows that the question whether a k-algebra $k[\mathbf{x}]/I$ is Cohen-Macaulay cannot be reduced to the monomial ideal algebra $k[\mathbf{x}]/init(I)$. Hence finding Rees and Hironaka decompositions of Cohen-Macaulay rings necessarily requires methods which are different from our Stanley decomposition algorithm in Section 2.

In the following we suggest a decision procedure for Cohen-Macaulayness and for computing Hironaka decompositions which is expected to perform better than the general purpose Algorithm 4.2. First we remark that it is not too difficult to find the Krull dimension d of R, for example by our methods in Section 2.

Algorithm 5.2.

Input: $f_1, f_2, \ldots, f_m \in k[\mathbf{x}]$, generating an ideal I.
Problem: Decide whether $R = k[\mathbf{x}]/I$ is a d-dimensional Cohen-Macaulay ring, and, if so, construct a Hironaka decomposition.

1. Pick a generic $n \times d$ matrix $(a_{ij})_{1\le i\le n, 1\le j\le d}$ over k, and abbreviate

$$\theta_1 := \Sigma_{i=1}^n a_{i1} x_i \ , \quad \theta_2 := \Sigma_{i=1}^n a_{i2} x_i \ , \quad \ldots , \quad \theta_n := \Sigma_{i=1}^n a_{in} x_i. \tag{8}$$

2. Introduce d new variables $\mathbf{z} := (z_1, \ldots, z_d)$. Compute a reduced Gröbner basis $\mathcal{G}$ with respect to reverse lexicographic order induced from $z_1 < z_2 < \ldots < z_d < x_1 < x_2 < \ldots < x_n$ for the ideal

$$J \quad := \quad I \ + \ < \theta_1 - z_1, \theta_2 - z_2, \ldots, \theta_d - z_d > \qquad \text{in} \quad k[\mathbf{x}, \mathbf{z}].$$

3. Does the leading monomial of some element in $\mathcal{G}$ contain a new variable z_i ? If so; STOP: R is not a free $k[\theta_1, \ldots, \theta_d]$-module. Otherwise, proceed with Step 4.
4. Let $\mathbf{F}$ be the set of $\alpha \in \mathbf{N}^n$ such that $\mathbf{x}^\alpha$ is standard (i.e. not a multiple of the leading monomial of some element in $\mathcal{G}$). If $\mathbf{F}$ is infinite, then STOP: R is an infinite-dimensional free $k[\theta_1, \ldots, \theta_d]$-module. If $\mathbf{F}$ is finite, then R is a d-dimensional Cohen-Macaulay ring with Hironaka decomposition (7).

The correctness of Algorithm 5.2 follows from the our correctness proof of Subroutine 3.9. The Gröbner basis $\mathcal{G}$ computed by Algorithm 5.2 can be used to find the Hironaka representation of any given polynomial in R. The normal form of any $P \in k[\mathbf{x}]$ versus $\mathcal{G}$

is an expression of the form $\sum_{\alpha\in\mathbf{F}} \mathbf{x}^\alpha\, p_\alpha(z_1,\ldots,z_d) \in k[\mathbf{x},\mathbf{z}]$. This gives us the desired identity

$$P(\mathbf{x}) \quad = \quad \sum_{\alpha\in\mathbf{F}} \mathbf{x}^\alpha\, p_\alpha(\theta_1,\theta_2,\ldots,\theta_d) \qquad \text{in} \quad k[\mathbf{x}].$$

It would be desirable to have such a normal form algorithm for the Rees decomposition of Section 4.

The following variant of Algorithm 5.2 provides even more information. Suppose that the coefficients a_{ij} of the parameters θ_i are not in k but algebraically independent transcendentals over k. Let $k' := k(a_{11},\ldots,a_{nd})$ denote the corresponding field extension of transcendence degree nd over k. Now execute Step 1 and Step 2 of Algorithm 5.2 with respect to the ring $k'[\mathbf{x},\mathbf{z}]$. Let $\mathcal{G}'$ denote the resulting reduced Gröbner basis. Recall that in a reduced Gröbner basis all leading monomials have coefficient 1. During this computation we have to divide through several polynomials $d(a_{11},\ldots,a_{nd})$ in the transcendentals a_{ij}. We keep track of these denominators, and we let $D(a_{11},\ldots,a_{nd})$ denote their product. The following observation is straightforward.

Proposition 5.3. *Suppose that R is a ring of depth $\geq d$. Then (8) defines a regular sequence for all $(a_{11},\ldots,a_{nd}) \in k^{nd}$ with $D(a_{11},\ldots,a_{nd}) \neq 0$.*

The method of Proposition 5.3 for computing genericity conditions is particularly useful in studying of Stanley-Reisner rings of simplicial complexes. In that case the indeterminant coefficients a_{ij} represent the vertex coordinates of an embedding of the simplicial complex in questions, and the condition $D \neq 0$ guarantees the genericity of that embedding with respect to certain algebraic questions. Possible applications of this computation include the rigidity theory of triangulated manifolds [WWh] and Billera's homology theory of smooth splines [Bil].

6. Hironaka decompositions of invariant rings of finite groups

In this section we give a practical algorithm using Gröbner bases for finding a fundamental set of invariants for the action of a finite group Γ on $k[\mathbf{x}]$. As a byproduct, our algorithm will generate an explicit Hironaka decomposition for the invariant ring $k[\mathbf{x}]^\Gamma$.

Let Γ be a finite group acting linearly on the polynomial ring $k[\mathbf{x}]$, and let $k[\mathbf{x}]^\Gamma$ be the subring of invariant polynomials. The invariant ring $k[\mathbf{x}]^\Gamma$ is the image of $k[\mathbf{x}]$ under the *Reynolds operator*

$$\begin{aligned} {}^* \;: k[\mathbf{x}] &\rightarrow k[\mathbf{x}]^\Gamma \\ f \mapsto f^* &:= \frac{1}{|\Gamma|}\sum_{\sigma\in\Gamma}\sigma(f). \end{aligned} \tag{9}$$

Note that * is an $k[\mathbf{x}]^\Gamma$-module homomorphism and that the restriction of * to $k[\mathbf{x}]^\Gamma$ is the identity. (Recall that k was assumed to have characteristic zero.)

By Hilbert's classical finiteness theorem [Hil] there exists a finite set $\mathcal{F} \subset k[\mathbf{x}]$ of *fundamental invariants*, i.e. the invariant subring $k[\mathbf{x}]^\Gamma = k[\mathcal{F}]$ is finitely generated. Another classical result due to E. Noether [Noe] states that the elements of $\mathcal{F}$ may be chosen of degree less than or equal to the group order $|\Gamma|$, which implies the existence of a finite yet impractical algorithm for computing such a set $\mathcal{F}$.

In a recent article G.R. Kempf summarizes the state of the art concerning the computation of invariants [Ke2]. Classical ideas are combined with a recent theorem of Hochster, Eagon and Roberts [HoR],[HoE] to yield an algorithm for computing a fundamental system of *primary* and *secondary* invariants. A very nice and elementary exposition on the invariant theory of finite groups and its applications to coding theory is found in N.J.A. Sloane [Slo].

Most algebraic results used in this section are well known in invariant theory; see Dieudonné & Carrell [DiC], Kempf [Ke1],[Ke2], Sloane [Slo], Stanley [St1], and the references given there. In order to prove the correctness of the proposed algorithm we shall summarize the algebraic results needed for the special case of a finite group.

We mention parenthetically that the computation generalizes in a straightforward manner to infinite reductive algebraic groups provided the Reynolds operator * and the ideal of the nullcone are given effectively. In the finite case, the Reynolds operator * is computed using formula (9), and the ideal of the nullcone equals the irrelavant ideal

$M \ := < x_1, x_2, \ldots, x_n >$. This fact is proved in Lemma 6.3. Fix an admissible order $m_1 < m_2 < m_3 < m_4 < \ldots$ which refines the total degree ordering on the set $\mathbf{N}^n$ of monomials in $k[\mathbf{x}]$.

Algorithm 6.1.

Input : A subroutine realizing the Reynolds operator $^* \ : \ k[\mathbf{x}] \to k[\mathbf{x}]^\Gamma$ of a finite subgroup Γ of $GL(k^n)$.

Problem : Find a Hironaka decomposition for the invariant ring $k[\mathbf{x}]^\Gamma$.

0. Let $t := 0$ and $\mathcal{Q} := \emptyset$.
1. Repeat $t := t+1$ until $m_t^* \neq 0$ and $m_t^* \notin Rad(< \mathcal{Q} >)$ (using Subroutine 3.5).
2. Let $\mathcal{Q} \ := \ \mathcal{Q} \cup \{m_t^*\}$. If $Rad(< \mathcal{Q} >) \ \neq \ M$ then go to Step 1 (using Subroutine 3.6).
3. If $\mathcal{Q}$ is algebraically independent over k (using Subroutine 3.7).
   - 3.1. then $\mathcal{P} \ := \ \mathcal{Q}$;
   - 3.2. else modify the set $\mathcal{Q}$ to an algebraically independent set $\mathcal{P}$ of invariants with $Rad(< \mathcal{P} >) \ = \ M$ (see below).
4. Write $\mathcal{P} \ = \ \{P_1, P_2, \ldots, P_n\}$, let $\mathcal{S} := \{1\}, t := 0$, and set $bound \ := \ \sum_{i=1}^n degree(P_i) - n$.
5. Let $t := t+1$. If $degree(m_t) \ > \ bound$ then STOP. In that case $\mathcal{P}$ and $\mathcal{S}$ are primary and secondary invariants respectively (see below), and their union generates $k[\mathbf{x}]^\Gamma$ as a ring.
6. If $m_t^* \notin k[\mathcal{P} \cup \mathcal{S}]$ (using Subroutine 3.8) then let $\mathcal{S} \ := \ \mathcal{S} \ \cup \ \{m_t^*\}$. Go to 5.

In the following we outline a proof of correctness for Algorithm 6.1.

Proposition 6.2. *Algorithm 6.1 terminates with finite sets* $\mathcal{P} \ = \ \{P_1, P_2 \ldots, P_n\}$ *(the primary invariants) and* $\mathcal{S} = \{S_1, S_2 \ldots, S_k\}$ *(*$the secondary invariants, where S_1 \ = 1$*) such that the invariant ring* $k[\mathbf{x}]^\Gamma$ *is a free* $k[\mathcal{P}]$*-module with basis* $\mathcal{S}$*. In other words, for any* $f \ = \in k[\mathbf{x}]^\Gamma$*, there exist* <u>*unique*</u> *polynomials* $f_i \in k[\mathbf{x}]$ *such that*

$$f \ = \ \sum_{i=1}^{k} f_i(P_1, \ldots, P_n) \cdot S_i.$$

This implies the Hironaka decomposition $k[\mathbf{x}]^\Gamma \ = \ \oplus_{s \in \mathcal{S}} \, s \, k[\mathcal{P}]$.

Lemma 6.3. *Let I^Γ denote the ideal in $k[\mathbf{x}]$ generated by all homogeneous invariants of degree ≥ 1. Then $Rad(I^\Gamma) = M$.*

Proof of Lemma 6.3. Note that I^Γ is generated by the (infinite) set $\{m_1^*, m_2^*, m_3^*, m_4^*, \ldots\}$, that is, I^Γ a subset of irrelevant ideal M. Let $\bar{k}$ denote the algebraic closure of the field k. By Hilbert's Nullstellensatz, it is sufficient to show that the zero set $\mathcal{V}(I^\Gamma)$ of I^Γ in $\bar{k}^n$ is contained in $\mathcal{V}(M) = \{0\}$. More precisely, we shall prove that $\mathbf{x} \neq 0$ implies $\mathbf{x} \notin \mathcal{V}(I^\Gamma)$ for any $\mathbf{x} \in \bar{k}^n$

Suppose $\mathbf{x} \neq 0$. The underlying representation of Γ over k^n maps every $\sigma \in \Gamma$ onto an invertible matrix, and we have $0 \notin \Gamma\mathbf{x} = \{\sigma\mathbf{x} \in \bar{k}^n \mid \sigma \in \Gamma\}$. The set $\Gamma\mathbf{x}$ is Zariski closed in $\bar{k}^n$ because the group Γ is assumed to be finite. Hence there exists a polynomial function $f \in k[\mathbf{x}]$ such that $f(0) = 0$ and $f(\sigma\mathbf{x}) = 1$ for all $\sigma \in \Gamma$.

Symmetrizing the polynomial f, we obtain an invariant f^* which is contained in I^Γ because $f^*(0) = 0$. On the other hand we have $f^*(\mathbf{x}) = \frac{1}{|\Gamma|}\sum_{\sigma\in\Gamma} f(\sigma\mathbf{x}) = 1$, and thus $\mathbf{x} \notin \mathcal{V}(I^\Gamma)$. $\triangle$

Lemma 6.3 shows that the condition in step 2 will eventually be satisfied. Indeed, the resulting set $\mathcal{P}$ will be optimal with respect to degree. If $\mathcal{P}$ is algebraically independent, then it contains precisely n elements. If this is not the case, we can perform step 3.2 as follows.

First delete successively elements $p \in \mathcal{P}$ with $p \in Rad(< \mathcal{P} \setminus \{p\} >)$ (using Subroutine 3.5). Only if the resulting set $\mathcal{P}$ has still more than n elements, (which will probably rarely be the case), then we can proceed as suggested in [Ke2, Theorem 3]: We replace the elements of $\mathcal{P}$ by appropriate powers in order for all invariants in $\mathcal{P}$ to have the same degree. Pick randomly $n \cdot |\mathcal{P}|$ rational coefficients to form n linear combinations of the $p_i \in \mathcal{P}$, and replace the old $\mathcal{P}$ by these. By Hilbert's normalization theorem these will be algebraically independent with probability 1. To make sure, go to step 3.

A somewhat more efficient version of Algorithm 6.1 would be to not set $t = 0$ in Step 4, keep the deleted elements of $\mathcal{P}$ to process for inclusion in $\mathcal{S}$, and then proceed with processing m_t^* as before.

The correctness of the remaing steps and thus the proof of Proposition 6.2 follows now from the following theorem which combines the the Hochster–Eagon–Roberts theorem on the Cohen-Macauleyness of $k[\mathbf{x}]^\Gamma$ [HoR],[HoE] with a degree bound given by G. Kempf [Ke2]. For more details see Kempf's exposition in [Ke1].

Theorem 6.4. [Kempf, Hochster, Eagon, Roberts] *Let $\mathcal{P} = \{P_1, P_2 \ldots, P_n\}$ be a set of algebraically independent invariant generators of I^Γ. Then there exists a finite set of invariants $\mathcal{S}$ of degree bounded by $\sum_{i=1} degree(P_i) - n$ such that $k[\mathbf{x}]^\Gamma$ is a free $k[\mathcal{P}]$-module with basis $\mathcal{S}$.*

We close with a simple example showing how Algorithm 6.1 works and why the distinction between primary and secondary invariants yields the desired Hironaka decomposition.

Example 6.5. Consider the action of the cyclic group $\Gamma = \{1, \delta, \delta^2, \delta^3\}$ of order 4 on $k[x, y]$ which is given by $\delta : x \mapsto y,\ y \mapsto -x$. An admissible total degree order on the monomials is given by

$$x < y < x^2 < xy < y^2 < x^3 < x^2y < xy^2 < y^3 < x^4 < x^3y < \ldots .$$

Clearly $x^* = y^* = 0$. (The underlying linear representation of Γ is irreducible, hence there is no invariant 1-form !). For degree 2 we have $p_1 := (x^2)^* = (y^2)^* = \frac{1}{2}(x^2 + y^2)$ and $(xy)^* = 0$. There are no invariants of degree 3 since $(x^3)^* = (x^2y)^* = (xy^2)^* = (y^3)^* = 0$. Next, we have $p_2 = (x^4)^* = \frac{1}{2}(x^4 + y^4) := p_2$, and the condition in step 2 is satisfied: $Rad(< p_1, p_2 >) = < x, y >$, and *bound* $:= 4$ in step 4. Clearly, $\mathcal{P} = \{p_1, p_2\}$ is algebraically independent.

Let $s_1 := 1$ and consider the next monomial x^3y. We have $s_2 := (x^3y)^* = \frac{1}{2}(x^3y - xy^3)$, and we check that $s_2 \notin k[p_1, p_2, s_1]$, i.e., s_2 cannot be written as a polynomial in p_1, p_2, s_1. For the next monomial x^2y^2 we have $(x^2y^2)^* = x^2y^2 = -p_2 + 2p_1^2$. If not already precomputed, the identities $(xy^3)^* = -(x^3y)^*$, $(y^4)^* = (x^4)^* \in k[p_1, p_2, s_1]$ will be discovered next. Next, in step 5, the *bound* is exceeded, and the program comes to a STOP.

Hence we obtain the Hironaka decomposition $k[\mathbf{x}]^\Gamma = k[p_1, p_2] \oplus s_2\, k[p_1, p_2]$. Using Subroutine 3.7, we find that the syzygy ideal of relations among p_1, p_2 and s_2 is generated by $-s_2^2 + 3p_1^2p_2 - 2p_1^4 - p_2^2$. Geometrically speaking, we have imbedded the orbit space k^2/Γ into affine 3-space k^3 as the hypersurface $z^2 = 3x^2y - 2x^4 - y^2$.

References

[Bac] K. Baclawski, *Rings with lexicographic straightening law*, Advances in Math. **39** (1981) 185–213.

[BGa] K. Baclawski and A.M. Garsia, *Combinatorial decompositions of rings*, Advances in Math. **39** (1981) 155–184.

[Bay] D. Bayer, *The division algorithm and the Hilbert scheme*, thesis, Harvard University, 1982.

[Bil] L.J. Billera, *Homology of smooth splines: Generic triangulations and a conjecture of Strang*, Advances in Math., to appear.

[BCS] L.J. Billera, R. Cushman and J.A. Sanders, *The Stanley decomposition of the harmonic oscillator*, Preprint, 1988.

[Bu1] B. Buchberger, *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*, Aequationes Mathematicae, **4** (1970) 374–383.

[Bu2] B. Buchberger, *Gröbner bases – an algorithmic method in polynomial ideal theory*, Chapter 6 in N.K. Bose (ed.) : "Multidimensional Systems Theory", D. Reidel Publ. Comp., 1985.

[Bu3] B. Buchberger, *Applications of Gröbner bases in non-linear computational geometry*, in J.R. Rice (ed.): Scientific Software, I.M.A. Volumes in Mathematics and its Applications, # 14, Springer, New York, 1988.

[Cus] R. Cushman, *Invariant theory and normal forms of vector fields*, presented at "Invariant Theory and Tableaux", I.M.A. work shop, University of Minnesota, Minneapolis, March 1988.

[CSW] R. Cushman, J.A. Sanders, N. White, *Normal form for the $(2;n)$-nilpotent vectorfield, using invariant theory*, Preprint, 1988.

[DEP] C. De Concini, D. Eisenbud and C. Procesi, *Hodge algebras*, Astérique **91** (1982).

[DiC] J.A. Dieudonné and J.B. Carrell, *Invariant Theory - Old and New*, Academic Press, New York, 1971.

[DKR] P. Doubilet, J.P.S. Kung, and G.C. Rota, *Invariant theory, Young bitableaux, and combinatorics*, Advances in Math. **27** (1978) 63-92.

[Eis] D. Eisenbud, *Introduction to algebras with straightening laws*, in B.R. McDonald (ed.): Ring Theory and Algebra, Proceedings of the third Oklahoma conference, Marcel Dekker, New York, 1980.

[Gar] A. Garsia, *Combinatorial methods in the theory of Cohen-Macaulay rings*, Advances in Math. **38** (1980) 229-266.

[Hil] D. Hilbert, *Über die Theorie der algebraischen Formen*, Math. Annalen **36** (1890) 473–534.

[HoR] M. Hochster and J. Roberts, *Rings of invariants of reductive groups acting on regular rings are Cohen-Macauley*, Advances in Math. **13** (1974) 115-175.

[HoE] M. Hochster and J.A. Eagon, *Cohen-Macauley rings, invariant theory, and the generic perfection of determinantal loci*, American J. Math. **93** (1971) 1020–1058.

[Ke1] G. Kempf, *The Hochster-Roberts theorem of invariant theory*, Michigan Math. J. **26** (1979) 19–32.

[Ke2] G. Kempf, *Computing invariants*, in S.S. Koh (ed.): Invariant Theory, Springer Lecture Notes # 1278, Heidelberg, 1987.

[KKl] B. Kind and P. Kleinschmidt, *Schälbare Cohen-Macaulay-Komplexe und ihre Parametrisierung*, Math. Zeitschrift **167** (1979) 173–179.

[KRo] J.P.S. Kung and G.-C. Rota, *The invariant theory of binary forms*, Bull. American Math. Soc. (new series) **10** (1984) 27–85.

[Noe] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Annalen **77** (1916) 89–92.

[Ree] D. Rees, *A basis theorem for polynomial rings*, Cambridge Phil. Soc. Proc. **52** (1956) 12–16.

[SSw] D. Shannon and M. Sweedler, *Using Gröbner bases to determine subalgebra membership*, Preprint, Cornell University, Ithaca N.Y., 1987.

[Slo] N.J.A. Sloane, *Error-correcting codes and invariant theory: New applications of a nineteenth-century technique*, American Math. Monthly **84** (1977) 82–107.

[St1] R.P. Stanley, *Invariants of finite groups and their applications to combinatorics*, Bulletin Amer. Math. Soc. **1** (1979) 475–511.

[St2] R.P. Stanley, *Linear diophantine equations and local cohomology*, Invent. math. **68** (1982) 175–193.

[St3] R.P. Stanley, *Hilbert functions of graded algebras*, Advances in Math. **28** (1978) 57–83.

[Stu] B. Sturmfels, *Computing final polynomials and final syzygies using Buchberger's Gröbner bases method*, submitted.

[SWh] B. Sturmfels and N. White, *Gröbner bases and invariant theory*, Advances in Math., to appear.

[WWh] W. Whiteley and N. White, *The algebraic geometry of stresses in frameworks*, SIAM J. Alg. Discr. Meth. **4** (1983) 481–511.