Preliminary Manuscript

1988-02-29

EFFICIENT COMPUTATION OF FUNDAMENTAL INVARIANTS – AN APPROACH USING BUCHBERGER'S GRÖBNER BASES METHOD

BERND STURMFELS* AND NEIL WHITE*†

Abstract. We outline feasible 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 thm.)*, (b) computing an ideal basis for the syzygies among the I_j *(second fundamental thm.)*, 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, Hochster, Eagon and Roberts, and it generalizes to infinite reductive algebraic groups provided a computable Reynolds operator and ideal generators for the nullcone are given.

1. Introduction. Let Γ be a finite group acting linearly on the polynomial ring $R := \mathbb{C}[x_1, x_2, \ldots, x_n]$, and let R^Γ be the subring of invariant polynomials. A *Reynolds operator* for the invariant ring R^Γ is given by

$$(1) \qquad \begin{array}{ccccc} {}^* : R & \to & R^\Gamma & & \\ f & \mapsto & f^* & := & \dfrac{1}{|\Gamma|} \displaystyle\sum_{\sigma \in \Gamma} \sigma(f). \end{array}$$

In other words, * is an R^Γ-module homomorphism such that $^*|_{R^\Gamma}$ is the identity on the invariant ring R^Γ.

By Hilbert's classical finiteness theorem [Hil] there exists a finite set $\mathcal{F} \subset R$ of *fundamental invariants*, i.e. the invariant subring $R^\Gamma = \mathbb{C}[\mathcal{F}]$ 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].

In Section 3 we summarize the method described in [Ke2] from a computer algebra point of view. As Kempf points out, "this algorithm uses some commutative algebra which

*Institute for Mathematics and its Applications, University of Minnesota, Vincent Hall 514, 206 Church Street S.E., Minneapolis, MN 55455, U.S.A.

†Department of Mathematics, University of Florida, Gainesville, FL 32611, U.S.A.

is now on the level of computer programmable calculations" [Ke2, pp.82], but he gives no hint as to how to actually implement certain techniques from commutative algebra, such as testing algebraic dependence or containment in (modules over) subrings of R.

It is the objective of the present note to close that gap by showing that all necessary steps can be programmed easily using B. Buchberger's Gröbner bases method. This approach seems very promising from a practical point of view since Gröbner bases are implemented in many widely available computer algebra systems.

2. Four commutative algebra subroutines based on Gröbner bases.

Let us briefly recall some basic definitions concerning Gröbner bases. For a detailed account on computational algebraic geometry and its applications we refer to Buchberger [Bu1], [Bu2] and the references given there. All definitions and results in this section remain valid when C is replaced by an arbitrary field.

A total order "<" on the power products $x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$ in the polynomial ring $R = \mathbb{C}[x_1, x_2, \dots, x_n]$ is called *admissible* if $p \neq 1 \Rightarrow 1 < p$, and $p < q \Rightarrow pr < qr$ for all power products p, q, r. Given any $g \in R$, we write $lead(g)$ for the leading term of g, that is, the maximal (w.r.t "<") power product with non-zero coefficient in g. The *initial ideal* $Init(I)$ associated with an ideal $I \subset R$ is the monomial ideal generated by $\{ lead(f) \mid f \in I\}$. A set $G = \{g_1, g_2, \dots, g_k\}$ of generators for I is said to be a *Gröbner bases* for I with respect to the order "<" if the initial ideal $Init(I)$ is generated by $\{lead(g_1), lead(g_2), \dots, lead(g_k)\}$. As is customary, we assume the elements of G to have leading coefficient 1. An important property of Gröbner bases is that they provide a fast normal form algorithm for the residue classes modulo I. The first algorithm to compute Gröbner bases, given by B. Buchberger in 1965 (see [Bu1]), has been refined many times since, and today quite efficient implementations are available in many computer algebra systems [Bu2].

One of the most frequently used admissible order is the *purely lexicographical order* induced from a given variable order, say $x_1 < x_2 < \dots < x_n$. That ordering is defined by $x_1^{i_1}\dots x_n^{i_n} < x_1^{h_1}\dots x_n^{h_n}$ if there exists m, $1 \leq m \leq n$, with $i_m < h_m$ and for all $j > m$, $i_j = h_j$.

In the following we summarize four commutative algebra "subroutines" based on Buchberger's method which will be applied to invariant theory in the next section. Whenever the monomial order is unspecified, any admissible order will work for the Gröbner bases computation.

SUBROUTINE 2.1. (Radical containment [Bu2, Theorem 2.5.1])

Input : $f_1, f_2, \dots, f_m, g \in R$.

Question : Let $I := < f_1, \dots, f_m >$ *be the ideal generated by the* f_i*'s. Is* $g \in Rad(I)$ *(the radical of* I*) ?*

Solution : Let G *be a Gröbner basis of* $< f_1, f_2, \dots, f_m, gz - 1 >$, *where* z *is a new*

variable. $g \in Rad(I)$ *if and only if* $1 \in G$.

SUBROUTINE 2.2. Solvability of homogeneous equations [Bu1, Method 6.9]

Input : Homogenous *polynomials* $f_1, f_2, \ldots, f_m \in R$.

Question : Is there a non-zero *vector* $\mathbf{x} \in \mathbb{C}^n$ *such that* $f_1(\mathbf{x}) = f_2(\mathbf{x}) = \ldots = f_m(\mathbf{x})$.

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 power product of the form* $x_i^{j_i}$ *occurs among the leading terms in* G *for every* i, *for* $1 \leq i \leq n$.

Remark : An alternative but worse solution would be applying Subroutine 2.1 with $g := x_i$ *for all* $i = 1, 2, \ldots, n$.

SUBROUTINE 2.3. (Algebraic Dependence [Bu2],[Stu])

Input : $F := \{f_1, f_2, \ldots, f_m\} \subset R$, *where* $m \leq n$, *considered as subset of the field* $\mathbb{C}(x_1, \ldots, x_n)$.

Questions : Is F *algebraically dependent over* $\mathbb{C}$ *? If so, find an* m*-variate polynomial* P *such that* $P(f_1, f_2, \ldots, f_m) = 0$ *in* R.

Solution : Introduce m *new "slack" variables* $y_1, \ldots, y_m$, *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* $y_1 < \ldots < y_m < x_1 < \ldots < x_n$. *Let* $G' := G \cap \mathbb{C}[y_1, \ldots, y_m]$. F *is algebraically independent if and only of* $G' = \emptyset$. *On the other hand, if* $P(y_1, \ldots, y_m) \in G'$, *then* $P(y_1, \ldots, y_m) = 0$ *in* R.

SUBROUTINE 2.4. (Containment in subrings [Stu, Prop. 5.1])

Input : $f_1, f_2, \ldots, f_m, g \in R$.

Question : Is g *contained in the subring* $\mathbb{C}[f_1, \ldots, f_m]$ *of* R *? If so, find an* m*-variate polynomial* Q *such that* $g = Q(f_1, f_2, \ldots, f_m)$ *in* R.

Solution : Compute the Gröbner basis G *as in 2.3, and let* $Q(x_1, \ldots, x_n, y_1, \ldots, y_m)$ *be the unique normal form of* g *with respect to* G. *Then* $g \in \mathbb{C}[f_1, \ldots, f_m]$ *if and only if* Q *is independent of the* x_i*'s, i.e.* $Q = Q(y_1, \ldots, y_m)$. *In that case we have the identity* $g = Q(f_1, f_2, \ldots, f_m)$.

3. Computing fundamental invariants.

We describe the basic steps in the computation of a finite set of fundamental invariants for action of a finite group Γ on R. Most algebraic results underlying these steps are well known in invariant theory. For details the reader is refered to Dieudonné & Carrell [DiC], Kempf [Ke1],[Ke2], Sloane [Slo], Stanley [Sta], and the references given there. We summarize the algebraic results needed for the special case of a finite group in order to give a correctness proof for the proposed algorithm.

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 (1), and the ideal of the nullcone equals $M := < x_1, x_2, \ldots, x_n >$, i.e., it is the maximal ideal generated by the coordinate functions. The latter fact is proved in Lemma 3.3. We order the set of nonconstant monomials in R by any admissible linear extension of the total degree : $m_1 < m_2 < m_3 < m_4 < \ldots$.

ALGORITHM 3.1.

0. *Let* $t := 0$ *and* $\mathcal{Q} := \{\}$.
1. *Repeat* $t := t+1$ *until* $m_t^* \neq 0$ *and* $m_t^* \notin Rad(< \mathcal{Q} >)$ *(using SUBROUTINE 2.1).*
2. *Let* $\mathcal{Q} := \mathcal{Q} \cup \{m_t^*\}$. *If* $Rad(< \mathcal{Q} >) \neq M$ *go to 1 (using SUBROUTINE 2.2).*
3. *If* $\mathcal{Q}$ *is algebraically independent over* $\mathbb{C}$ *(using SUBROUTINE 2.3).*
   - 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* $\mathcal{S} := \{1\}$, *and let bound* $:= \sum_{i=1} degree(P_i) - n$.
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* R^Γ *as a ring.*
6. *If* $m_t^* \notin \mathbb{C}[\mathcal{P} \cup \mathcal{S}]$ *(using SUBROUTINE 2.4)*
   - 6.1 *then let* $\mathcal{S} := \mathcal{S} \cup \{m_t^*\}$. *Go to 5.*

Let us outline a proof of correctness for Algorithm 3.1.

PROPOSITION 3.2. *Algorithm 3.1 terminates with finite sets* $\mathcal{P} = \{P_1, P_2 \ldots, P_n\}$ *and* $\mathcal{S} = \{S_1, S_2 \ldots, S_k\}$ $(S_1 = 1)$ *such that the invariant ring* R^Γ *is a free* $\mathbb{C}[\mathcal{P}]$*-module with basis* $\mathcal{S}$. *In other words, for any* $f = \in R^\Gamma$, *there exist unique polynomials* $f_i \in R$ *such that*

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

This implies in particular $R^\Gamma = \mathbb{C}[\mathcal{P} \cup \mathcal{S}]$.

LEMMA 3.3. *Let* I^Γ *denote the ideal in* R *generated by all homogeneous invariants of degree* ≥ 1. *Then* $Rad(I^\Gamma) = M$.

Proof of Lemma 3.3. 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 the radical ideal M. By Hilbert's Nullstellensatz, it is sufficient to show that the zero set $\mathcal{V}(I^\Gamma)$ of I^Γ in $\mathbb{C}^n$ 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 $\mathbf{x} \in \mathbb{C}^n$

Suppose $\mathbf{x} \neq 0$. The underlying representation of Γ over $\mathbb{C}^n$ maps every $\sigma \in \Gamma$ onto an invertible matrix, and we have $0 \notin \Gamma\mathbf{x} = \{\sigma\mathbf{x} \in \mathbb{C}^n \mid \sigma \in \Gamma\}$. The set $\Gamma\mathbf{x}$ is Zariski closed in $\mathbb{C}^n$ because the group Γ is assumed to be finite. Hence there exists a polynomial function $f \in R$ 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 $\mathbf{x} \notin \mathcal{V}(I^\Gamma)$. □

Lemma 3.3 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 succesively elements $p \in \mathcal{P}$ with $p \in Rad(< \mathcal{P} \setminus \{p\} >)$ (using SUBROUTINE 2.1). 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.

At this stage, we pause to ask the following question. If we choose the lexicographically smallest set of m_i^* which are algebraically independent of cardinality n, then is their radical equal to M ? If so, then with that set as $\mathcal{P}$ we need not perform the normalization step, and we avoid the high powers of the previous paragraph.

The correctness of the remaing steps and thus the proof of Proposition 3.2 follows now from the following theorem which combines the the Hochster–Eagon–Roberts theorem on the Cohen-Macauleyness of R^Γ [HoR],[HoE] with a degree bound given by G. Kempf [Ke2]. For more details see Kempf's exposition in [Ke1].

THEOREM 3.4. (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 R^Γ is a free $\mathbb{C}[\mathcal{P}]$-module with basis $\mathcal{S}$.*

Let us see in a very simple example to show how Algorithm 3.1 works and why we distinguish between primary and secondary invariants.

Example 3.5. Consider the action of the cyclic group $\Gamma = \{1, \delta, \delta^2, \delta^3\}$ of order 4 on $R := \mathbb{C}[x, y]$ 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 $s_2 \notin \mathbb{C}[p_1, p_2, s_1]$, 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 $(xy^3)^* = -(x^3y)^*$, $(y^4)^* = (x^4)^* \in \mathbb{C}[p_1, p_2, s_1]$ will be discovered next. Next, in step 5, the *bound* is exceeded, and the program comes to a STOP.

We conclude that $R^\Gamma = \mathbb{C}[p_1, p_2] + \mathbb{C}[p_1, p_2] \cdot s_2$, and we find (using the Gröbner basis computation in SUBROUTINE 2.3) that the syzygy ideal of relations among p_1, p_2 and s_2 is generated by $-s_2^2 + 3p_1^2p_2 - 2p_1^4 - p_2^2$. (Note that s_2 is necessarily integral over $\mathbb{C}[p_1, p_2]$). In other words, we have imbedded the orbit space $\mathbb{C}^2/\Gamma$ into affine 3-space $\mathbb{C}^3$ as the hypersurface $z^2 = 3x^2y - 2x^4 - y^2$.

REFERENCES

[Bu1] 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.

[Bu2] B. Buchberger, *Applications of Gröbner bases in non-linear geometry*, to appear in J.R. Rice (ed.): Scientific Software, I.M.A. Volumes in Mathematics and its Applications, # 14, Springer, New York, to appear..

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

[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.

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

[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.

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

[Stu] B. Sturmfels, *Applications of final polynomials and final syzygies*, Institute for Mathematics and its Appl., University of Minnesota, Preprint # 372, December 1987.