Discrete Mathematics and Theoretical Computer Science Proceedings **AA (DM-CCG)**, 2001, 315–328

Computing Minimal Generating Sets of Invariant Rings of Permutation Groups with SAGBI-Gröbner Basis

Nicolas M. Thiéry

Laboratoire de Mathématiques Discrètes, Université Lyon I, 43 bd du 11 novembre, 69622 Villeurbanne Cedex, France
e-mail : `nthiery@mines.edu`, `http://www.mines.edu/~nthiery/`

received January 30, 2001, *revised April 10, 2001*, *accepted April 16, 2001.*

We present a characteristic-free algorithm for computing minimal generating sets of invariant rings of permutation groups. We circumvent the main weaknesses of the usual approaches (using classical Gröbner basis inside the full polynomial ring, or pure linear algebra inside the invariant ring) by relying on the theory of SAGBI-Gröbner basis. This theory takes, in this special case, a strongly combinatorial flavor, which makes it particularly effective.

Our algorithm does not require the computation of a Hironaka decomposition, nor even the computation of a system of parameters, and could be parallelized. Our implementation, as part of the library `PerMuVAR` for `MuPAD`, is in many cases much more efficient than the other existing software.

Keywords: Invariant Theory, Permutation Group, Discrete Mathematics, Minimal Generating Set, Hironaka Decomposition, SAGBI-Gröbner basis, `PerMuVAR`, `MuPAD`.

---

1 Introduction

Invariant rings of permutation groups arise regularly in discrete mathematics. For example, the study of an algebraic version of Ulam's reconstruction conjecture proposed by Pouzet [Pou77, PT00] led us to consider the invariant ring I_N over graphs [Thi00] on N nodes, and to try to construct generating sets of I_N, as they form complete sets of invariants for weighted graphs.

There is a substantial body of literature on invariant theory which provides both general results [Sta79, Smi95] and algorithms [Stu93]. In [GS84], combinatorial constructions of Hironaka decompositions of invariant rings of certain permutation groups are described; SAGBI basis for invariant rings of permutation groups are investigated in [Göb98]. There is also a strong trend of development of computational invariant theory [Kem93, Kem98, DK97].

Nevertheless, there is a combinatorial explosion and even the computation of a minimal generating system for I_5 requires, so far, specially hand crafted code [Thi00, Kem00]. Our impression is that the usefulness of invariant theory in discrete mathematics strongly depends on the improvement of the existing computational tools, in particular for calculating minimal generating sets in the case of permutation groups.

In this article, we present a new characteristic-free algorithm for computing minimal generating sets of invariant rings of permutation groups. For many groups, our implementation is much more efficient *in practice* than the other existing software. In particular, it allows for computations (or at least partial computations) with some groups which were out of reach.

We review in Section 2 the basic properties of invariant rings of permutation groups, as well as the usual algorithms for computing minimal generating sets. Most of them rely on the computation of a suitable Gröbner basis; however, this computation can be impractical even for relatively small invariant rings like I_6 (group of size $6! = 720$ acting on 15 variables). The fundamental reason is that Gröbner basis break all symmetries, and lead to costly calculations inside the full polynomial ring.

In order to keep the symmetries, our approach is to use *SAGBI-Gröbner basis* instead: following the introduction of SAGBI basis (Subalgebra Analogs of Gröbner Basis for Ideals) by Robbiano and Sweedler [RS90] and Kapur and Madlener [KM89], the theory of SAGBI-Gröbner basis has been developed by Miller [Mil98] for ideals of subalgebras of polynomial rings. SAGBI basis of invariant rings of permutation groups have been extensively studied by Goebel [Göb98] but, to the best of our knowledge, SAGBI Gröbner basis had never been used before in this context. To focus on combinatorial aspects, we only present in Section 3 SAGBI-Gröbner basis in the special case of invariant rings of permutation groups; we call them *invariant Gröbner basis* to emphasize that they do not break the symmetries. The fundamental objects are the initial monomials, which play the same role for invariant polynomials as integer partitions do for symmetric polynomials. We provide a Buchberger-like criterion to skip *a priori* the computation of unnecessary S-pairs, and give an algorithm for computing Hironaka decompositions.

In Section 4, we concentrate on our main goal: computing minimal generating sets of invariant rings of permutation groups. We derive from the computation of a suitable invariant Gröbner basis an algorithm to compute directly the elements of degree d of a minimal generating set. This algorithm only requires a precomputation of a partial SAGBI basis up to degree d whose cost is, in practice, negligible compared to full cost of the computation. This algorithm is characteristic free, could be parallelized, and its complexity is well constrained. It also does not require the computation of a system of parameters, though knowing the existence of such a system with low degrees can help by improving the *a priori* degree bound. An implementation is available as part of the library `PerMuVAR` for the computer algebra system `MuPAD`.

We conclude in Sections 5 and 6 with a comparative benchmark, and some remarks for further development.

2 The ring of invariants of a permutation group

This section describes the basic properties of the invariant ring of a permutation group. For a more general introduction, with a strong computational flavor, see [Kem98]. Whenever possible, notations follow [CLO97, Stu93, Göb98].

Let $\mathbb{K}$ be a field. Let $x_1, \ldots, x_n$ be n variables, and $\mathbb{K}[x_1, \ldots, x_n]$ be the ring of polynomials in those variables. Let G be a subgroup of the symmetric group $\mathfrak{S}_n$, acting on the n variables by $\sigma.x_i := x_{\sigma(i)}$. This action extends naturally to an action of G on $\mathbb{K}[x_1, \ldots, x_n]$. An *invariant polynomial*, or *invariant*, is a polynomial $f \in K[x_1, \ldots, x_n]$ such that $\sigma \cdot f = f$ for all $\sigma \in G$. The *invariant ring* $I(G)$ is the set of all invariants.

Obviously, $I(G)$ is a $\mathbb{K}$-algebra. Its structure is simpler in the *non-modular case*, that is when the characteristic of the field does not divide the order of the group (e.g. in characteristic 0). However, more results extend to the modular case as in the more general case of matrix groups.

The image $\sigma.m$ of a monomial m by any element σ of G is a monomial. The *automorphism group* of m is the subgroup $\mathrm{Aut}(m) := \{\sigma \in G \mid \sigma.m = m\}$. Let $m^{\circledast} := \sum_{m' \in \{\sigma.m \mid \sigma \in G\}} m'$ be the invariant obtained by summing the monomials in the orbit of m (note that, in the non-modular case, $m^{\circledast} = |\mathrm{Aut}(m)|\, m^*$, where * is the usual Reynolds operator). Such invariants are called *orbit sums*. The set of all orbit sums is a vector space basis of $I(G)$, so any invariant can be uniquely written as a linear combination of orbit sums.

The invariant ring $I(G)$ is a graded algebra, and the finite set of all orbit sums of degree d is a vector space basis of the homogeneous component $I(G)_d$ of degree d of $I(G)$. The *Hilbert series* $H(I(G),z) := \sum z^d \dim I(G)_d$ can be computed via a Pólya enumeration, since $\dim I(G)_d$ is the number of monomials of degree d (*i.e.* of functions from $\{1,\dots,n\}$ into $\mathbb{N}$) enumerated up to an isomorphism [Sta79].

2.1 Generating sets

The famous theorem of Hilbert states that $I(G)$ is *finitely generated*: there exists a finite set of invariants S such that any invariant can be expressed as a polynomial combination of invariants in S. We call S a *generating set*. If no proper subset of S is generating, S is a *minimal generating set*. Since $I(G)$ is finitely generated, there exists a degree bound d such that $I(G)$ is generated by the set of all invariants of degree at most d. We denote by $\beta(I(G))$ the *smallest degree bound*.

Given an integer $d \geq 1$, let $\mathbb{K}[I(G)_{<d}]$ be the subalgebra of $I(G)$ generated by the invariants of degree $< d$, and $\mathbb{K}[I(G)_{<d}]_d$ its homogeneous component of degree d. Invariants of $\mathbb{K}[I(G)_{<d}]_d$ are called *decomposable*, since they can be expressed as sums and products of invariants of strictly smaller degree. $\mathbb{K}[I(G)_{<d}]_d$ will be referred as the space of decomposable invariants of degree d. Set $s_0(I(G)) := 0$ and $s_d(I(G)) := \dim I(G)_d - \dim \mathbb{K}[I(G)_{<d}]_d$. The generating series $s(I(G),z) := \sum_{d=0}^{\infty} z^d s_d(I(G))$ is a polynomial of degree $\beta(I(G))$.

A set S is *homogeneous* if its elements are homogeneous. The following lemma, valid for any *graded connected algebra* A (graded algebra such that $A_0 = \mathbb{K}$) summarizes some general properties of generating sets.

Lemma 1. *Let S be a generating set of $I(G)$.*

(i) $I(G)$ has a homogeneous minimal generating set composed of at most $|S|\beta(I(G))$ invariants of degree at most $\beta(I(G))$.

(ii) Assume S is homogeneous, and let S_d be the set of all invariants of S with degree d. Then, S is a minimal homogeneous generating set if, and only if, for all d, S_d is a vector space basis of a direct factor of $\mathbb{K}[I(G)_{<d}]_d$ in $I(G)_d$. In particular, $|S_d| = s_d(I(G))$.

Proof. (i) For each $p \in S$ and d, let p_d be the homogeneous component of degree d of p. Since $I(G)$ is graded, it is generated by the set $\{p_d \mid p \in S, 1 \leq d \leq \beta(I(G))\}$.

(ii) Use the grading and basic linear algebra. □

From (i), it is not very restrictive to only consider homogeneous generating sets, since non-homogeneous generating sets are not much smaller than homogeneous ones.

2.2 Classical algorithms for computing minimal generating sets

The basic principle of the classical algorithms is to construct generating sets degree by degree, from 1 up to the best degree bound known so far. Since the complexity of the computations involved increases quickly with the degree, the quality of the *a priori* degree bound is crucial. In the non-modular case, Noether's degree bound $\beta(I(G)) \leq |G|$ hold [Smi95, Fle00] (see also [Sch89, DH00] for refinements).

In all characteristic we also have $\beta(I(G)) \leq \binom{n}{2}$ [GS84, Göb96]. Finally, when $I(G)$ is Cohen-Macaulay, typically in the non-modular case, better *a priori* degree bounds can often be obtained from the knowledge of a system of parameter.

So, in the non-modular case, the usual approach is to compute such a system of parameters $(\theta_1, \ldots, \theta_n)$ of the invariant ring, and to take advantage of the existence of a Hironaka decomposition by computing secondary invariants and, while doing so, selecting the secondary invariants that are *irreducible* (*i.e.* that cannot be expressed as products of lower degree secondary invariants). The irreducible secondary invariants together with the primary invariants form a minimal generating set (some primary invariants may need to be removed). We refer to [Kem98] for details, as well as for an extended algorithm for the modular case.

The critical part of this approach is the computations modulo the ideal $\langle\theta_1, \ldots, \theta_n\rangle$ generated by the system of parameters in $I(G)$. Most invariant theory libraries [Kem93, Kem98] do a precomputation of a Gröbner basis B of $\langle\theta_1, \ldots, \theta_n\rangle$, and then use normal form reduction modulo B. However, the precomputation of B often fails, even for quite small permutation group. Moreover, this computation breaks the symmetries, since B is a Gröbner basis of the ideal generated by the primary invariants in $\mathbb{K}[x_1, \ldots, x_n]$, and not in $I(G)$. The normal form $\overline{p}^B$ of an invariant is not necessarily an invariant, and cannot be stored efficiently as linear combination of orbit sums. This induces a high overhead on the remaining linear algebra operations.

Hence, we looked for analogs of Gröbner basis that would not break the symmetries.

3 Invariant Gröbner basis

3.1 Monomial orders and SAGBI basis

We assume that the reader is familiar with the usual definitions of Gröbner basis [CLO97, KR00] and SAGBI basis [RS90]. Unless explicitly stated, we only consider homogeneous invariants, and homogeneous ideals of $I(G)$.

Throughout the rest of this paper, we assume a monomial order $<$ has been fixed. For a polynomial p, denote respectively by $\mathrm{LM}(p)$, $\mathrm{LT}(p)$, and $\mathrm{LC}(p)$ the leading monomial, leading term, and leading coefficient of p with respect to $<$. Of course, $\mathrm{LT}(p) = \mathrm{LC}(p)\mathrm{LM}(p)$. By extension, for any set B of polynomials, define $\mathrm{LM}(B) := \{\mathrm{LM}(p) \mid p \in B\}$ and $\mathrm{LT}(B) := \{\mathrm{LT}(p) \mid p \in B\}$.

A monomial in $\mathrm{LM}(I(G))$ is called *initial*. By the properties of monomial orders, the leading term of a product pq is the product of the leading terms of p and q, and it follows that the product of two initial monomials is initial. The vector space $\langle\mathrm{LT}(I(G))\rangle$ spanned by the elements of $\mathrm{LT}(I(G))$ is thus an algebra, called the *initial algebra* of $I(G)$.

A subset B of $I(G)$ is called a *SAGBI basis* of G if $\mathrm{LT}(B)$ generates $\langle\mathrm{LT}(I(G))\rangle$ as an algebra. As with usual Gröbner basis, there is a general reduction algorithm, as well as Buchberger-like characterization and algorithm to compute SAGBI basis. However, for invariant rings of permutation groups, there are a much simpler and purely combinatorial algorithms. This is best described in the context of the *initial poset*.

3.2 The initial poset

The set $\mathrm{LM}(I(G))$ is a monoid, and its elements can be ordered by divisibility: given two initial monomials p and q, *p divides q*, denoted $p \prec q$, if there exists an initial monomial r such that $q = pr$. The partially ordered set $P^G := (\mathrm{LM}(I(G)), \prec)$ is called the *initial poset* of $I(G)$.

This is a generalization of the poset $P := (\mathrm{LM}(\mathbb{K}[x_1,\ldots,x_m]),|)$ of all monomials of $\mathbb{K}[x_1,\ldots,x_m]$ ordered by divisibility. The poset P plays a fundamental role in the theory of Gröbner basis. For example, the existence of finite Gröbner basis is a direct consequence of Dickson's lemma: any subset of P has a finite number of minimal elements, *i.e.* P is a well quasi ordering. The initial poset P^G plays the same role for SAGBI-Gröbner basis.

Remark 3.1. The following basic operations are comparatively cheap for permutation groups:

1. Test if a monomial m is initial.
2. Return an initial monomial m' isomorphic to m.
3. Compute the size of the automorphism group of m.
4. Compute the orbit of m.
5. Compute all the initial monomials of a given degree.

Naive algorithms can be obtained by running through the group. In the case of `PerMuVAR`, they are implemented as an external optimized C++ library `GLIP` (`http://glip.sourceforge.net`). It would be beyond the scope of this article to describe more efficient algorithms based on Shreier-Simms chains representation of permutation groups [KS98].

Using those operations, invariants can be stored and manipulated as linear combinations of orbit sums $m^{\mathfrak{G}}$, where $m \in \mathrm{LM}(I(G))$. This saves memory up to a factor of $1/|G|$, especially since most monomials do not have symmetries. The cost of calculating additions and multiplications of invariants is also reduced by about the same factor.

We can now state an effective characterization of SAGBI basis. A monomial $p \in \mathrm{LM}(I(G))$ is *irreducible* if p is minimal for $\prec$.

Proposition 1. *A subset B of $I(G)$ is a SAGBI basis of $I(G)$ if, and only if, $\mathrm{LT}(B)$ contains all the irreducible monomials of $\mathrm{LM}(I(G))$. The set of all irreducible initial monomials is the unique minimal reduced SAGBI basis of $I(G)$.*

Using this proposition, and operation 5 of remark 3.1, the unique minimal reduced SAGBI basis can be computed degree by degree using an Eratosthenes sieve in the initial poset.

Remark 3.2. The leading coefficient of any invariant in the unique minimal reduced SAGBI basis is 1. It follows that this SAGBI basis is independent of the base field (in the modular case, some non-leading terms may disappear), and can actually be defined for a base ring instead.

If G is the trivial group, the irreducible elements are the variables $x_1,\ldots,x_k$, which also form the minimal reduced SAGBI basis of $I(G)$. If G is a permutation group, and $<$ is the lexicographic order, the n monomials $x_1\ldots x_k$ with $1 \leq k \leq n$ are irreducible. If G is the symmetric group $\mathfrak{S}_n$, those are the only irreducible monomials, and the elementary symmetric polynomials form the minimal reduced SAGBI basis of $I(S_n)$. For the alternating group A_3 acting on the variables x,y,z, the situation is more complicated, as any monomial of the form $x^k z^{k-1}$ is also irreducible. It follows that there can be an infinite number of irreducible monomials: Dickson's lemma does not generalize to the invariant case.

In [Göb98], Göbel proves that, for the lexicographic order, there is a finite number of irreducible monomials if, and only if, G is a direct product of symmetric groups. Another equivalent condition is that all irreducible monomials are multilinear (a monomial $x_1^{d_1}\ldots x_m^{d_m}$ is *multilinear* if $d_i \leq 1$ for all i). He also shows that it is enough to compute the irreducible monomials up to degree $\frac{n^2(n_1)}{2}$, since the irreducible monomials of higher degree can be obtained by a suitable scaling.

Note that $\mathrm{LM}(I(G))$ is not factorial. For example, if G is the alternating group A_3 acting on the variables x,y,z, and $<$ is the lexicographic order, the monomial $m = x^3yz$ can be written in two different ways as product of irreducible monomials: $m = (xyz)(x)(x)$ or $m = (x^2z)(xy)$.

A *least common multiple* (LCM) of p and q is an initial monomial r such that $p \prec r$, $q \prec r$ and r is minimal with this property. Consider again $G = A_3$, and take $p = xyz$ and $q = xy$. Then, x^3yz is a LCM of p and q, but so are also x^4yz^2 and x^5yz^3. Actually, any monomial of the form $x^{k+2}yz^k$, with $k > 1$ is a LCM of p and q. Not only is the LCM of two monomials not necessarily unique, but there may be an infinite number of them.

Problems 3.3.
1. Generate all the irreducible monomials of a given degree d;
2. Generate all the LCMs of a given degree d of two initial monomials;
3. Determine if two initial monomials have a finite number of LCMs.

So far, `PerMuVAR` solves problem 1 and 2 by a brute force Eratosthenes sieve. Those steps are not yet time critical, but there ought to be better algorithms.

3.3 Invariant division algorithm

The key of invariant Gröbner basis is a little modification of the usual division algorithm.

Algorithm 3.4 (Invariant division algorithm).

Input: *An invariant f and a family of invariants $F = (f_1, \dots, f_k)$.*
Output: *An invariant remainder $\overline{f}^F$ of f on division by F.*
while $f \neq 0$ ***do***
  for $g \in F$ ***do***
    $m := \frac{\mathrm{LM}(f)}{\mathrm{LM}(g)}$;
    if *m is a monomial and m is initial* ***then***
      $f := f - \frac{\mathrm{LC}(f)}{\mathrm{LC}(g)} m^{\circledast} g$;
      restart main loop;
    end if
  end for
  exit main loop;
end while
return(f);

Let's run the algorithm on a few examples. Consider the ring $I(\mathfrak{S}_2)$ of symmetric polynomials on two variables x,y, where the monomials are ordered lexicographically with $x > y$. Take $f := x^2 + y^2$, and $F = (x+y)$. We have $\mathrm{LM}(f) = x^2$, $\mathrm{LM}(x+y) = x$, and $m = x$. With the usual division algorithm we would compute $f := f - x(x+y)$, and get $y^2 - xy$ which is not invariant. Here, we compute $f := f - x^{\circledast}(x+y)$ instead, which yields $f = x^2 + y^2 - (x+y)(x+y) = -2xy$: invariance is preserved! Now, $\mathrm{LM}(f) = -2xy$ and $m = y$, so running the loop once more would yield $f := f - y^{\circledast}(x+y) = -2xy + 2(x+y)(x+y) = 2x^2 + 2xy + 2y^2$. Notice that the term x^2 has been recreated, so we may suspect that the algorithm is going to run forever. What is happening here is that the monomial m is not initial, and replacing m by $m^{\circledast}$ generates extra terms of higher order. To avoid this, there is an extra condition "m is initial" on line 3. Thus, in the above example, the algorithm stops with the result $\overline{f}^F = -2xy$.

With those points in mind, it is obvious that the algorithm always terminates, that the remainder $\overline{f}^F$ of f on division by F is invariant, and that $\overline{f}^F - f \in \langle F \rangle$. However, uniqueness of the result is not guaranteed; for example, the rest of $f := x^2 + y^2$ on division by $(x^2+y^2, x+y)$ can be either 0 or $-2xy$, depending on whether the algorithm starts with $g := x^2+y^2$ or $g := x+y$. Worst, the rest of $f := xy$ on division by $F := (x^2+y^2, x+y)$ alway yields $\overline{f}^F = xy$, whereas xy belongs to the ideal generated by $(x^2+y^2, x+y)$. On the other hand, there are systems such as $F := (xy, x+y)$, for which the result is always unique, and for which $\overline{f}^F = 0$ if, and only if, f is in the ideal generated by F. As with the usual division algorithm, this motivates the introduction of Gröbner basis.

3.4 Invariant Gröbner basis

Let I be an ideal of $I(G)$. For the sake of simplicity, we assume that I is homogeneous. The extension to the non-homogeneous case raises no difficulty. The vector space $\langle \mathrm{LT}(I) \rangle$ spanned by $\mathrm{LT}(I)$ is actually an ideal of $\langle \mathrm{LT}(I(G)) \rangle$, and is called the *initial ideal* of $\mathrm{LT}(I)$. A subset B of I is an *invariant Gröbner basis of the ideal I* if $\mathrm{LT}(B)$ generates the initial ideal $\langle \mathrm{LT}(I) \rangle$ as an ideal over $\langle \mathrm{LT}(I(G)) \rangle$. It is a *partial invariant Gröbner Basis up to degree d* of I if $\mathrm{LM}(B)$ generates $\langle \mathrm{LT}(I) \rangle$ up to the degree d. A family $F = (f_1, \dots, f_k)$ of invariants is an *invariant Gröbner basis* if it is an invariant Gröbner basis of the ideal $I := \langle f_1, \dots, f_k \rangle$ it generates.

For example, let's check that $B := (xy, x+y)$ is an invariant Gröbner basis of the maximal ideal $I(\mathfrak{S}_2)_+$ of symmetric polynomials of positive degree. Take $p \in I(\mathfrak{S}_2)_+$. Its leading term is of the form $x^k y^l$, with $k \geq l$ and $k > 1$. If $l = 0$, $\mathrm{LT}(p)/\mathrm{LT}(x+y) = x^{k-1}$ is initial, and if $l > 0$, $\mathrm{LT}(p)/\mathrm{LT}(xy) = x^{k-1}y^{l-1}$ is also initial. So $\mathrm{LT}(B)$ indeed generates $\langle \mathrm{LT}(I(\mathfrak{S}_2)_+) \rangle$. It is also a SAGBI basis of $I(\mathfrak{S}_2)$, which is not a coincidence. In general, B is a SAGBI basis of $I(G)$ if, and only if, B is an invariant Gröbner basis of the maximal ideal $I(G)_+$.

A monomial m of $\langle \mathrm{LT}(I(G)) \rangle$ is *standard* if $m \notin \langle \mathrm{LT}(I) \rangle$. The orbit sum $m^{\circledast}$ of a standard monomial m is called a *standard invariant*. As usual, $I(G)$ is the direct sum of I and of the vector space spanned by the standard invariants. More precisely, for all d, the homogeneous component $I(G)_d$ is the direct sum of I_d and of the vector space spanned by the standard invariants of degree d. It follows that a remainder $\overline{F}^B$ of an invariant f on invariant division by B is necessarily the unique linear combination of standard invariants such that $f - \overline{f}^B \in I$. The invariant $\overline{f}^B$ is called the *normal form* of f, and is 0 if, and only if, $f \in I$. If moreover f is homogeneous, f and $\overline{f}^B$ have the same degree.

Finally, the definition of the unique *reduced* invariant Gröbner basis of I is straightforward.

3.5 Invariant Buchberger characterization and algorithm

The next step is to obtain a Buchberger like characterization. Let g_1 and g_2 be two invariants, and let r be a LCM of $\mathrm{LM}(g_1)$ and $\mathrm{LM}(g_1)$. Let $p_1 := \frac{r}{\mathrm{LM}(g_1)}$, $p_2 := \frac{r}{\mathrm{LM}(g_2)}$ and $S(g_1, g_2, r) := \mathrm{LC}(g_2) g_1 p_1^{\circledast} - \mathrm{LC}(g_1) g_2 p_2^{\circledast}$. Clearly, the leading monomial cancels in $S(g_1, g_2, r)$, which creates a new leading monomial. The invariant $S(g_1, g_2, r)$ is called a S-pair of g_1 and g_2.

Proposition 2 (Invariant Buchberger's characterization). *Let $I := \langle f_1, \dots, f_k \rangle$ be an ideal of $I(G)$, and let B be a subset of I containing $f_1, \dots, f_k$. Then, B is a Gröbner basis of I if, and only if, for any S-pair s*

of two invariants of B, the remainder of s on division by B is zero.

This characterization is not effective. Indeed, given two invariants g_1 and g_2 of B, there may be an infinite number of LCMs and thus of S-pairs.

Algorithm 3.5 (Invariant Buchberger's algorithm).

Input: *a set of invariants* $F = (f_1, \dots, f_k)$.
Output: *a Gröbner basis* B *of* $I = \langle F \rangle$*, with* $F \subset B$.
  $B := F$;
  repeat
    $B' := B$;
    for all *S-pair* $s := S(b_1, b_2, r)$ *of any two elements* $\{b_1, b_2\}$ *of* B' ***do***
      $s := \overline{s}^B$;
      if $s \neq 0$ ***then***
        $B := B \cup \{s\}$;
      end if
    end for
  until $B = B'$
  return(B);

The proof of partial correctness raises no difficulties. However, this algorithm may not terminate, since there are ideals of $I(G)$ without finite invariant Gröbner basis. Moreover, even if at some point a finite Gröbner basis B is obtained, the implicit Buchberger's characterization test may not terminate.

On the other hand, the algorithm can be modified to effectively produce a partial invariant Gröbner basis up to a given degree using the following algorithm to augment a partial invariant Gröbner basis up to degree $d-1$ into a partial invariant Gröbner basis up to degree d.

Algorithm 3.6 (Augmentation of a partial invariant Gröbner basis).

  `augmentGBasis`$:=$ ***proc***(B,d)
Input: *an integer* $d \geq 1$ *and a partial invariant Gröbner basis* B *of an ideal* $I\langle F \rangle$ *up to degree* $d-1$*, with* $F = (f_1, \dots, f_n) \subset B$.
Output: *an invariant Gröbner basis* B *of* $I = \langle F \rangle$ *up to degree d, with* $F \subset B$ *and the list of the standard monomials of degree d.*
  `standard`$:= []$;
  M:=[initial monomials of degree d of $I(G)$*, sorted decreasingly w.r.t.* $<$*];*
  for all $m \in M$ ***do***
    $S := \{b \in B \mid \mathrm{LT}(b) \prec m\}$;
    if $|S| = 0$ ***then***
      `standard`$:=$ `standard`$\cup \{m\}$; $\{$*m is a standard monomial*$\}$
    else if $|S| = 1$ ***then***
      $\{$*m is already in* $\langle \mathrm{LT}(B) \rangle$$\}$
    else
      $\{$*m gives rise to some S-pairs*$\}$
      Let b_1 *be an element of S.*

for all $b_2 \in S - \{b_1\}$ **do**
$s := \overline{S(b_1, b_2, m)}^B$;
if $s \neq 0$ **then**
$B := B \cup \{s\}$;
end if
end for
end if
end for
return(B, `standard`);

As for usual Gröbner basis computations, it is critical to improve Buchberger's characterization to skip as much as possible the computation of S-pairs which reduce to zero. The following proposition is an adaptation of Buchberger's first and second criteria.

Proposition 3. *Let m and S be as defined on line 4 of algorithm 3.6. The algorithm is still correct if S is restricted as follow. Remove any monomial b such that $2\deg(b) > \deg(m)$. If S still contains two monomials $b_1 < b_2$ such that $m = b_1 b_2$, further remove b_2 (criterion 1). Finally, let ρ be the relation on S defined by $b_1 \rho b_2$ if m is not a LCM of b_1 and b_2; let ρ^* be the transitive closure of ρ; replace S by a set of representatives of the equivalence classes of ρ (criterion 2).*

Also as with usual Gröbner basis [Fau99], much faster implementations are obtained by replacing the Buchberger's step-by-step reductions of S-pairs by Gauss elimination on the matrices M_d of all syzygies of each degree d.

3.6 An algorithm for computing secondary invariants

In this subsection, we assume $I(G)$ is Cohen-Macaulay, which is always true in the non-modular case. Recall that our goal is to compute secondary invariants and minimal generating systems of $I(G)$.

Proposition 4. *Let $\theta_1, \dots, \theta_n$ be a system of parameters of $I(G)$, and $\langle \theta_1, \dots, \theta_n \rangle$ be the ideal of $I(G)$ they generate. Then, the standard invariants w.r.t. $\langle \theta_1, \dots, \theta_n \rangle$ form a system of secondary invariants of $I(G)$.*

With this proposition, our goal becomes to compute standard invariants, and to have a procedure for rewriting any invariant as a linear combination of standard invariants. The ideal we consider is graded and zero-dimensional, with a finite number of standard monomials of degrees $e_1, \dots, e_t$. Moreover, any homogeneous invariant p of degree $d > e_t$ is rewritten as $\overline{p}^I = 0$. Therefore, the computation of a partial Gröbner basis up to the degree e_t yields the standard monomials, as well as the procedure for rewriting invariants as linear combination of standard monomials.

Algorithm 3.7 (Computation of secondary invariants).

Input: *A system of parameters $F = (f_1, \dots, f_n)$ of $I(G)$*
Output: *A Gröbner basis B of $I = \langle F \rangle$ up to degree $d_{\max}$, with $F \subset B$, and the secondary invariants.*
$B := F$; `standard` $:= []$;
for $d := 1, \dots, d_{\max}$ **do**
$(B, \mathtt{secondaries}_d) := \mathtt{augmentGBasis}(B, d)$;
`secondaries` $:=$ `secondaries` $\cup$ $\mathtt{secondaries}_d$;
$\{$*Insert code here*$\}$

end for
return$(B,$`secondaries`$)$;

Any piece of code can be inserted in algorithm 3.7, for incremental use of the standard invariants and the Gröbner basis. For example, assume that the following lines are inserted:

$L := [\,]$;{L will be kept row reduced versus $<$}
for p product of standard monomials of degree $< d$ **do**
  $p := \overline{p}^B$;
  if p is not in the vector space spanned by L **then**
    Insert p into L;
  end if
end for
`irreducibles` $:=$ `irreducibles` $\cup \{m^{\circledast}, m$ is standard and $m \notin \mathrm{LM}(L)\}$

Then, the procedure computes all the standard monomials (*i.e.* the secondary invariants), and produces, as a by-product, a set `irreducibles` of irreducible secondary invariants.

4 Direct computation of minimal generating sets

The key idea for directly computing the elements of degree d of a minimal generating set is fairly simple. Let I be the ideal generated by invariants of positive degree $< d$. The homogeneous component of degree d of I coincides with the vector space $\mathbb{K}[I(G)_{<d}]_d$ of decomposable invariants of degree d. Let S be the set of irreducible monomials of $I(G)$ of positive degree $< d$. Then, S generates I, and is a partial invariant Gröbner basis of I up to degree $d-1$. Hence, `augmentGBasis`(S,d) yields a partial invariant Gröbner basis of I up to degree d, and the standard invariants form a minimal generating set at degree d.

The only prerequisite is the computation of the structure of the initial poset up to degree d, *i.e.* the partial minimal reduced SAGBI basis up to degree d.

This yields the desired algorithm:

Algorithm 4.1 (Computation of a minimal generating set).

Input: $d_{\max} \in \mathbb{N}$*: an* a priori *degree bound for* $I(G)$
Output: *a minimal generating set* S *of* $I(G)$
  $S := []$; *B:=[];*
  for $d := 1, \ldots, d_{\max}$ ***do***
    `augmentGBasis`(B,d);
    $S := S \cup \{standardmonomials\}$;
    $B := B \cup$ *`SAGBI`*(d);
  end for
  return(S);

5 Comparative benchmark

We ran systematic computations of minimal generating sets of invariant rings of permutation groups with both `PerMuVAR` and `Magma` [BCP97] (command `FundamentalInvariants`) on Intel Bi-PIII 1 GHz PC's running GNU/Linux. We used as test-bed all the transitive permutation groups on a small number

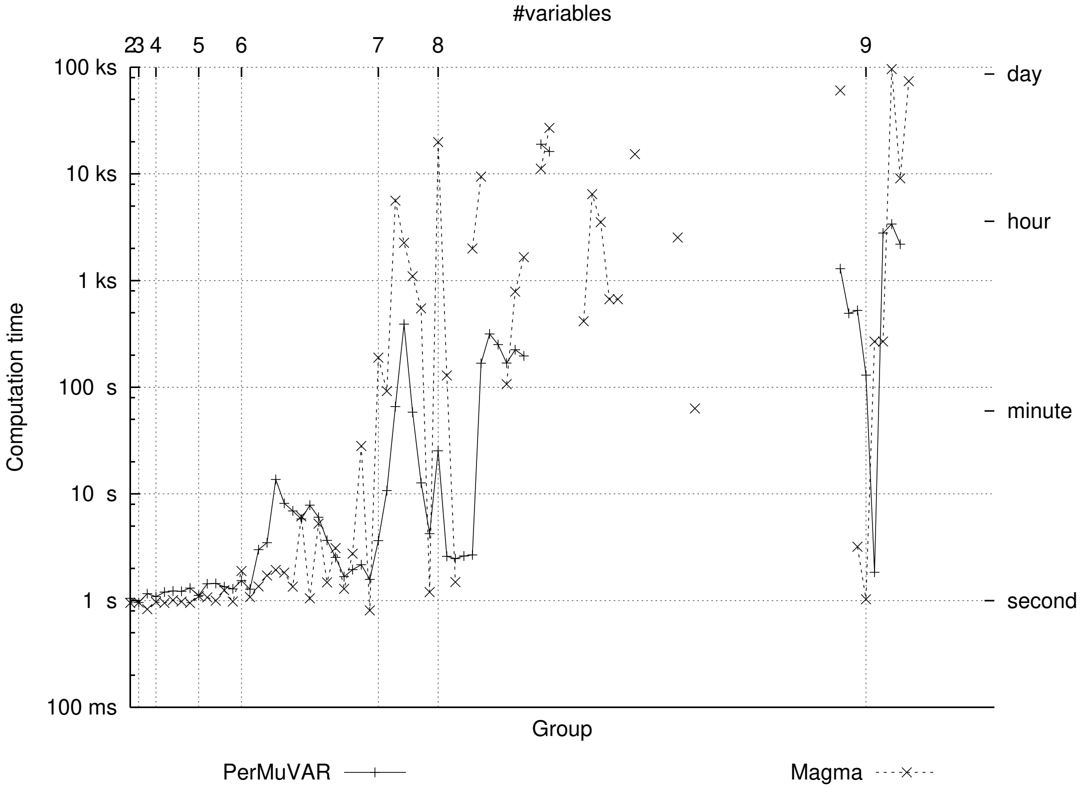

Fig. 1: Computation time for the transitive groups on $1, 2, 3, \ldots$ variables

of variables, as provided by GAP [GAP99]. Non-transitive permutation groups have sharper *a priori* degree bounds, and are usually much easier to compute. Starting from 8 variables many groups are out of reasonable reach; our choice of a 500 Mb memory limit and a 2 days time limit was essentially guided by the availability of computation resources.

Figure 1 summarizes the computation times. The corresponding tables, as well as the logs and results of computations are available on `PerMuVAR`'s web page. We will keep updating this benchmark with memory information, tests of other software as well as new results for groups requiring higher memory and time limits.

`PerMuVAR` and `Magma` appears to be complementary; depending on the group, both can in turn be up to several orders of magnitude faster than the other. Some further comments are still in order, since their practical behavior are completely different.

For `Magma`, the critical step is the computation of a system of parameters and its Gröbner basis, whose difficulty is relatively unpredictable. The actual computation of a minimal generating system is then fairly quick. Our benchmark is slightly unfair with `Magma`: some time could be saved on this second step by avoiding the computation of secondary invariants above the *a priori* degree bound.

On the other hand, for `PerMuVAR`, the difficulty of a computation can be reasonably predicted from the *a priori* degree bound $d_{\max}$, and the dimensions of the homogeneous components of degree $d \leq d_{\max}$. A very rough estimate of the complexity is given by $(\frac{d_{\max}^{n-1}}{|G|})^3$. Practically, and at the time of writing the limit is around homogeneous components of dimension 20000. In particular, one can guess in advance when a full computation is out of reach. In this case, the computation still yields useful partial results. For example, we computed a minimal generating system for the invariant ring over graphs I_n up to degree 17 for $n = 5$ (10 variables, $|G| = 120$, $d_{\max} = 22$), up to degree 12 for $n = 6$ (15 variables, $|G| = 720$, $d_{\max} = 45$), and up to degree 11 for $n = 7$ (21 variables, $|G| = 5040$). This computation leads us to conjecture that $\beta(I_6) = 11$.

6 Further developments

We expect drastic improvement on the efficiency of our implementation through:

- the use of optimized exact sparse linear algebra routines, e.g. from the ALP library [MP00];
- the implementation of the basic operations of remark 3.1 in GAP [GAP97] using Shreier-Sims chains.

For permutation groups, the minimal generating sets obtained by this algorithm only depends on the characteristic of the field. By running the computation over $\mathbb{Z}$, it will be possible to compute at once minimal generating sets for all characteristics.

The results of our systematic computations for transitive permutation groups will be collected in a database (see e.g. [KKM$^+$00]), and extended to any characteristic. We hope that this database will be a useful tool for, e.g., the systematic study of degree bounds.

7 Acknowledgements

We gratefully thank Lorenzo Robbiano and Jean-Charles Faugère for decisive ideas, as well as the Unité Mixte de Service Médicis, for providing the computational power.

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[CLO97] David Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms*, second ed., Springer-Verlag, New York, 1997, An introduction to computational algebraic geometry and commutative algebra.

[DH00] M. Domokos and P. Hegedüs, *Noether's bound for polynomial invariants for finite groups*, Arch. Math. **74** (2000), 161–167.

[DK97] Harm Derksen and Hanspeter Kraft, *Constructive invariant theory*, Algèbre non commutative, groupes quantiques et invariants (Reims, 1995), Soc. Math. France, Paris, 1997, pp. 221–244.

[Fau99] Jean-Charles Faugère, *A new efficient algorithm for computing Gröbner bases* (F_4), J. Pure Appl. Algebra **139** (1999), no. 1-3, 61–88, Effective methods in algebraic geometry (Saint-Malo, 1998).

[Fle00] P. Fleischmann, *The Noether bound in invariant theory of finite groups*, Adv. Math. **156** (2000), 23–32.

[GAP97] The GAP Group, Lehrstuhl D für Mathematik, RWTH Aachen, Germany and School of Mathematical and Computational Sciences, U. St. Andrews, Scotland, *GAP – Groups, Algorithms, and Programming, Version 4*, 1997.

[GAP99] The GAP Group, Aachen, St Andrews, *GAP – Groups, Algorithms, and Programming, Version 4.1*, 1999.

[Göb96] Manfred Göbel, *Symideal Gröbner bases*, Rewriting techniques and applications (New Brunswick, NJ, 1996), Springer, Berlin, 1996, pp. 48–62.

[Göb98] Manfred Göbel, *A constructive description of SAGBI bases for polynomial invariants of permutation groups*, J. Symbolic Comput. **26** (1998), no. 3, 261–272.

[GS84] A. M. Garsia and D. Stanton, *Group actions of Stanley - Reisner rings and invariants of permutation groups*, Adv. in Math. **51** (1984), no. 2, 107–201.

[Kem93] Gregor Kemper, *The* invar *package for calculating rings of invariants*, IWR Preprint 93-94, University of Heidelberg, 1993.

[Kem98] Gregor Kemper, *Computational invariant theory*, The Curves Seminar at Queen's. Vol. XII (Kingston, ON, 1998), Queen's Univ., Kingston, ON, 1998, pp. 5–26.

[Kem00] Gregor Kemper, *Complete computation of a minimal generating set of the invariant rings over graphs on* 5 *nodes*, personal communication, 2000.

[KKM$^+$00] Gregor Kemper, Elmar Körding, Günter Malle, B. Heinrich Matzat, Denis Vogel, and Gabor Wiese, *A database of invariant rings*, Preprint, University of Heidelberg, Nov 2000.

[KM89] Deepak Kapur and Klaus Madlener, *A completion procedure for computing a canonical basis for a k-subalgebra*, Computers and mathematics (Cambridge, MA, 1989), Springer, New York, 1989, pp. 1–11.

[KR00] Martin Kreuzer and Lorenzo Robbiano, *Computational commutative algebra 1*, Springer Verlag, 2000.

[KS98] D. L. Kreher and D. R. Stinson, *Combinatorial algorithms; generation, enumeration and search*, Discrete mathematics and its applications, CRC Press, 1998.

[Mil98] J. Lyn Miller, *Effective algorithms for intrinsically computing SAGBI-Gröbner bases in a polynomial ring over a field*, Gröbner bases and applications (Linz, 1998), Cambridge Univ. Press, Cambridge, 1998, pp. 421–433.

[MP00] B. Mourrain and H. Prieto, *A framework for symbolic and numeric computations*, Rapport de Recherche 4013, INRIA, Octobre 2000.

[Pou77] Maurice Pouzet, *Quelques remarques sur les résultats de Tutte concernant le problème de Ulam*, Publ. Dép. Math. (Lyon) **14** (1977), no. 2, 1–8.

[PT00] Maurice Pouzet and Nicolas M. Thiéry, *Invariants algébriques de graphes et reconstruction*, Comptes Rendus de l'Académie des Sciences (2000), Soumis.

[RS90] Lorenzo Robbiano and Moss Sweedler, *Subalgebra bases*, Commutative algebra (Salvador, 1988), Springer, Berlin, 1990, pp. 61–87.

[Sch89] Barbara J. Schmid, *Generating invariants of finite groups*, C. R. Acad. Sci. Paris Sér. I Math. **308** (1989), no. 1, 1–6.

[Smi95] Larry Smith, *Polynomial invariants of finite groups*, Research Notes in Mathematics, vol. 6, A K Peters Ltd., Wellesley, MA, 1995.

[Sta79] Richard P. Stanley, *Invariants of finite groups and their applications to combinatorics*, Bull. Amer. Math. Soc. (N.S.) **1** (1979), no. 3, 475–511.

[Stu93] Bernd Sturmfels, *Algorithms in invariant theory*, Springer-Verlag, Vienna, 1993.

[Thi00] Nicolas M. Thiéry, *Algebraic invariants of graphs; a study based on computer exploration*, SIGSAM Bulletin (2000), In print.