Algebraic invariants of graphs; a study based on computer exploration

Nicolas M. Thiéry

Laboratoire de Mathématiques Discrètes
Université Lyon I, 43 bd du 11 novembre
69622 Villeurbanne Cedex
nthiery@users.sourceforge.net
http://www.mines.edu/~nthiery/

Abstract

We consider the ring $\mathcal{I}_n$ of polynomial invariants over weighted graphs on n vertices. Our primary interest is the use of this ring to define and explore algebraic versions of isomorphism problems of graphs, such as Ulam's reconstruction conjecture.

There is a huge body of literature on invariant theory which provides both general results and algorithms. However, there is a combinatorial explosion in the computations involved and, to our knowledge, the ring $\mathcal{I}_n$ has only been completely described for $n \leq 4$.

This led us to study the ring $\mathcal{I}_n$ in its own right. We used intensive computer exploration for small n, and developed `PerMuVAR`, a library for `MuPAD`, for computing in invariant rings of permutation groups.

We present general properties of the ring $\mathcal{I}_n$, as well as results obtained by computer exploration for small n, including the construction of a medium sized generating set for $\mathcal{I}_5$. We address several conjectures suggested by those results (low degree system of parameters, unimodality), for $\mathcal{I}_n$ as well as for more general invariant rings. We also show that some particular sets are not generating, disproving a conjecture of Pouzet related to reconstruction, as well as a lemma of Grigoriev on the invariant ring over digraphs. We finally provide a very simple minimal generating set of the field of invariants.

Introduction

Let $\mathbb{K}$ be a field of characteristic zero, n be a positive integer, and $\{x_{\{1,2\}}, \dots, x_{\{n-1,n\}}\}$ be a set of $\binom{n}{2}$ variables indexed by the pairs $\{i, j\}$ of $\{1, \dots, n\}$. The symmetric group $\mathfrak{S}_n$ acts naturally on those variables by

$$\sigma \cdot x_{\{i,j\}} := x_{\{\sigma(i),\sigma(j)\}}.$$

Let $\mathbb{K}[x_{\{i,j\}}]$ be the ring of polynomials in $x_{\{i,j\}}$. We study the subring $\mathcal{I}_n := \mathbb{K}[x_{\{i,j\}}]^{\mathfrak{S}_n}$ of the polynomials which remain invariant under the action of $\mathfrak{S}_n$.

Our motivation comes from graph theory and in particular from graph reconstruction. Pouzet [21, 22] formulated an algebraic reconstruction conjecture for $\mathcal{I}_n$, which implies Ulam's famous reconstruction conjecture for weighted graphs [2]. We disprove Pouzet's conjecture. Kocay proposed a similar conjecture, by introducing the *algebra of subgraphs* [19, 3]. This algebra is a quotient of $\mathcal{I}_n$; however this quotient is not graded, and we cannot apply our method to disprove Kocay's conjecture.

The ring $\mathcal{I}_n$ can also be used to study the shape of sets of vectors [1]. Our primary goal is to construct complete systems of invariants (systems that separate weighted graphs up to isomorphism), and in particular minimal generating sets of $\mathcal{I}_n$.

In § 1, we introduce the representation $\mathcal{G}_n$ of the symmetric group $\mathfrak{S}_n$ over the vector space $\mathcal{V}_n$ of weighted graphs on n vertices, and the associated invariant ring $\mathcal{I}_n$. We review classical results and tools provided by invariant theory (finite generation, grading, Hilbert series). Since $\mathcal{G}_n$ is a permutation group, there is a combinatorial interpretation of the invariant ring, and a reasonably fast algorithm for computing the Hilbert series. We also review some general properties of minimal generating sets, and the definition of the smallest degree bound $\beta(\mathcal{I}_n)$.

§ 2 is devoted to generating sets of $\mathcal{I}_n$. We provide a finite generating set. By studying the Hilbert series, we show that two other sets are not generating, disproving Pouzet's conjecture. We also prove that, for many common monomial orders, $\mathcal{I}_n$ has no finite SAGBI basis.

Finding a good degree bound is crucial. In § 3, we recall how Hironaka decompositions of $\mathcal{I}_n$ can be used to obtain the degree bound $\beta(\mathcal{I}_n) \leq \binom{\binom{n}{2}}{2} - \mu_n$, where μ_n is a non-negative $O(n)$ integer. We calculate μ_n by constructing minimal multigraphs without odd automorphisms.

In § 4, we try to refine the degree bound by constructing low degree systems of parameters. The study of the Hilbert series for $n \leq 21$, combined with a conjecture of Mallows and Sloane, suggests the existence of a system of parameters composed of invariants of degrees $1, 2, \dots, n, 2, 3, \dots, \binom{n-1}{2}$. This would give $\beta(\mathcal{I}_n) \leq \binom{\binom{n-1}{2}}{2} - \mu_n$. We propose a natural construction for such a low degree system of parameters, and check its validity for $n \leq 5$ using a Gröbner basis computation. Unfortunately, this computation is intractable for $n \geq 6$. Such a system of parameters seems to have nearly optimally low degrees; therefore, this technique cannot be refined much further in order to get better degree bounds.

§ 5 is devoted to the computation of minimal generating sets. For $n = 4$, a minimal generating set was first constructed by hand by Aslaksen, Chan et Gulliksen [1]; it can now be computed in a few seconds by invariant theory software (e.g. Kemper's packages in `Maple` [16] or `Magma` [17]). However, for $n \geq 5$, these software packages are unable to compute even partial minimal generating sets. We wrote

This article was formally reviewed following the procedures described in THIS BULLETIN, **32**(2), issue 124, 1998, pp 5–6.

PerMuVAR [32], a library of invariant theory routines for MuPAD, which uses the usual algorithms [29, 17], but is specialized for permutation groups. This allows us to go a step further: for $n = 5$, we compute a partial minimal generating set, containing 57 polynomials of degree ≤ 9[1]. This suggests a much better degree bound: $\beta(\mathcal{I}_n) = \binom{n}{2} - 1$.

In § 6, we prove that the invariant ring $\mathcal{I}_n$ is Gorenstein when n is even. This fact could be used to accelerate the computations of Hironaka decompositions [32].

We introduce in § 7 the chain product (a naive interpretation of Stanley-Reisner rings [11]). This allows for faster computations of generating sets at the expense of non-minimality [32]: we obtain a generating set of $\mathcal{I}_5$ containing about one thousand polynomials of degree ≤ 22.

In § 8 the projective limit $\mathcal{I}_\infty$ is used to obtain results about $\mathcal{I}_n$; this includes the lower bound $\beta(\mathcal{I}_n) \geq \lfloor \frac{n}{2} \rfloor$.

§ 9 presents various unimodality properties revealed by computer exploration, for $\mathcal{I}_n$ as well as for more general invariant rings.

Grigoriev [14] introduces a related invariant ring over digraphs. In § 10, we apply the Hilbert series tool of § 2 to disprove lemma 1 of [14]. We also provide a simple counter-example. Finally, in § 11, we study the field of invariants. Grigoriev [14] gives a non-constructive proof for the existence of a small generating set of the field of invariants (the proof of the degree bound is incorrect though, since it relies on lemma 1 of [14]). We construct such a small generating set, composed of the elementary symmetric polynomials and a very simple invariant of degree 2; to the contrary of Grigoriev's assertion, it is not a complete system of invariants. We also derive a minimality property of the invariant ring, by using basic Galois theory on the field of invariants.

The results presented in this paper are part of the Ph. D. thesis [30] of the author. We refer to this document for the detailed proofs.

1 The invariant ring over graphs

1.1 Valuated graphs as a vector space

Let V be a $\mathbb{K}$-vector space of finite dimension m, and G be a finite subgroup of $\mathrm{GL}(V)$. Tacitly, we interpret G as a group of $m \times m$ matrices or as a representation on V. Two vectors $\mathbf{v}$ and $\mathbf{w}$ are *isomorphic*, or in the same G*-orbit* (for short *orbit*), if $\sigma \cdot \mathbf{v} = \mathbf{w}$ for some $\sigma \in G$.

Let n be a positive integer. We consider labelled, undirected graphs on the vertices $\{1, \ldots, n\}$, without loops, and whose edges are weighted in $\mathbb{K}$. A *simple graph* is a graph with weights in $\{0, 1\}$, and a *multigraph* is a graph with weights in $\mathbb{N}$. For any pair $\{i, j\}$, let $\mathbf{e}_{\{i,j\}}$ be the simple graph with one single edge $\{i, j\}$. The set of all graphs is a $\mathbb{K}$-vector space $\mathcal{V}_n$ of dimension $m := \binom{n}{2}$ with basis $\{\mathbf{e}_{\{1,2\}}, \ldots, \mathbf{e}_{\{n-1,n\}}\}$. Indeed, any graph $\mathbf{g}$ can be written uniquely as $\mathbf{g} := \sum g_{\{i,j\}} \mathbf{e}_{\{i,j\}}$, where $g_{\{i,j\}}$ is the weight of the edge $\{i, j\}$. Let $\{x_{\{1,2\}}, \ldots, x_{\{n-1,n\}}\}$ be the dual basis ($x_{\{i,j\}}(\mathbf{g})$ is the weight $g_{\{i,j\}}$ of the graph $\mathbf{g}$ on the edge $\{i, j\}$).

Throughout the text, we denote objects attached to $\mathcal{V}_n$ by cursive symbols, and objects attached to the generic vector space V by ordinary symbols. Let $\mathfrak{S}_n$ be the symmetric group of all permutations of the n vertices. Our group $\mathcal{G}_n$ is the linear representation of $\mathfrak{S}_n$ defined on the basis of $\mathcal{V}_n$ by $\sigma \cdot \mathbf{e}_{\{i,j\}} := \mathbf{e}_{\{\sigma(i),\sigma(j)\}}$. The notion of isomorphism defined above coincides with the usual notion of isomorphism of graphs. Orbits of labelled graphs are called *unlabelled graphs*. Unless otherwise stated, all graphs are unlabelled.

The representation of $\mathcal{G}_n$ on $\mathcal{V}_n$ splits into three irreducible components: $[n] \oplus [n-1, 1] \oplus [n-2, 2]$, where $[n-2, 2]$ represents the irreducible representation of $\mathfrak{S}_n$ indexed by the partition $\lambda = (n-2, 2)$ of n [1, 10]. The first component has dimension 1 and corresponds to the vector space spanned by the complete graph. The sum $[n] \oplus [n-1, 1]$ of the first two components is of dimension n, and corresponds to the vector space spanned by the n *stars* $\mathbf{E}_1, \ldots, \mathbf{E}_n$, where $\mathbf{E}_i := \sum_{j \neq i} \mathbf{e}_{\{i,j\}}$. This representation is the natural representation of $\mathfrak{S}_n$ by permutation of $\mathbf{E}_1, \ldots, \mathbf{E}_n$. Let $X_1, \ldots, X_n$ be the basis of the dual, defined by $X_i := \sum_{j \neq i} x_{\{i,j\}}$. If $\mathbf{g}$ is a graph, $X_i(\mathbf{g})$ is the degree of the vertex i of $\mathbf{g}$. Finally, the last irreducible component $[n-2, 2]$ is the orthogonal of the two previous components, that is the subspace of all 0*-regular graphs* (graphs where each vertex as degree 0).

1.2 The invariant ring

Recall that if G acts on V, a *complete system of invariants* is a set S of functions such that two elements $\mathbf{v}$ and $\mathbf{w}$ of V are in the same orbit if and only if they give the same value to all functions in S (*i.e.* $p(\mathbf{v}) = p(\mathbf{w})$ for all $p \in S$). Our primary goal is to construct, or at least find information about, complete systems of invariants. We introduce the invariant ring of G which provides a mechanical way to do this. We refer to [27, 29, 5, 26, 17] for classical literature on invariant theory of finite groups. Parts of what follows are strongly inspired by [17].

Let $(x_1, \ldots, x_m)$ be a basis of the dual of V; for $\mathcal{V}_n$, we take $(x_1, \ldots, x_m) := (x_{\{1,2\}}, \ldots, x_{\{n-1,n\}})$. Let $\mathbb{K}[x_1, \ldots, x_m]$ be the ring of polynomials over V. The action of G on V extends naturally to an action of G on $K[x_1, \ldots, x_m]$ by $\sigma \cdot p := p \circ \sigma^{-1}$. An *invariant polynomial*, or *invariant*, is a polynomial $p \in K[x_1, \ldots, x_m]$ such that $\sigma \cdot p = p$ for all $\sigma \in G$. The *invariant ring* $I(G)$ is the set of all invariants. We call $\mathcal{I}_n := I(\mathcal{G}_n)$ the *invariant ring over graphs.* Note that $\sigma \cdot x_{\{i,j\}} := x_{\{i,j\}} \circ \sigma^{-1} = x_{\{\sigma(i),\sigma(j)\}}$.

Obviously, $I(G)$ is a $\mathbb{K}$-algebra. Hilbert's famous theorem states that $I(G)$ is *finitely generated*: there exists a finite set S of invariants 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.*

There exist algorithms to compute (minimal) generating sets, and a basic result of invariant theory states that they are complete systems of invariants. However, this often leads to very intensive computations, and rather large complete systems of invariants.

1.3 Invariant ring of a permutation group

The most famous invariant ring is the ring of symmetric polynomials $I(\mathfrak{S}_m)$, defined by the natural action of $\mathfrak{S}_m$ on the variables $(x_1, \ldots, x_m)$. The fundamental theorem of symmetric polynomials [29, p. 2] states that $I(\mathfrak{S}_m)$ is generated by m algebraically independent symmetric polynomi-

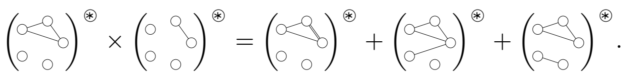
[1] Using *ad hoc* computations, Kemper [18] checked recently that this system was indeed a complete minimal generating set, thus proving that $\beta(\mathcal{I}_5) = 9$.

als, for example the m elementary symmetric polynomials or the first m symmetric power sums.

$\mathcal{G}_n$ is a *permutation group*, since it acts by permuting the variables $x_{\{i,j\}}$; thus, we also view $\mathcal{G}_n$ as a subgroup of the full group $\mathfrak{S}_m$ of the permutations of m variables. This results in several convenient and powerful combinatorial interpretations of invariants:

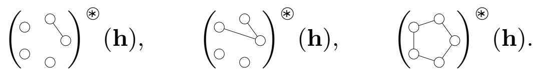
(i) A labelled multigraph $\mathbf{g} := (g_{\{1,2\}}, \dots, g_{\{n-1,n\}})$ can be identified with the monomial $\mathbf{x}^{\mathbf{g}} := x_{\{1,2\}}^{g_{\{1,2\}}} \dots x_{\{n-1,n\}}^{g_{\{n-1,n\}}}$. The *exponential* of $\mathbf{g}$ is the polynomial $\mathbf{x}^{\mathbf{g}^{\circledast}} := \sum_{\mathbf{h}} \mathbf{x}^{\mathbf{h}}$, where $\mathbf{h}$ belongs to the orbit of $\mathbf{g}$. The polynomial $\mathbf{x}^{\mathbf{g}^{\circledast}}$ is invariant, and is well defined even if $\mathbf{g}$ is unlabelled. The exponential therefore identifies unlabelled graphs with some particular invariants. Moreover, the set of all invariants $\mathbf{x}^{\mathbf{g}^{\circledast}}$, where $\mathbf{g}$ is a multigraph, is a vector space basis of $\mathcal{I}_n$. Note that the exponential differs from the usual Reynolds operator * by a multiplicative factor: $\mathbf{x}^{\mathbf{g}^{\circledast}} = |\operatorname{Aut}(\mathbf{g})|(\mathbf{x}^{\mathbf{g}})^*$, where $|\operatorname{Aut}(\mathbf{g})|$ is the size of the automorphism group of $\mathbf{g}$.

(ii) Let $\mathbf{g}_1$ and $\mathbf{g}_2$ be two multigraphs on n vertices. The product $\mathbf{x}^{\mathbf{g}_1{}^{\circledast}}\mathbf{x}^{\mathbf{g}_2{}^{\circledast}}$ is a linear combination of all possible superpositions of $\mathbf{g}_1$ and $\mathbf{g}_2$ (with, at times, counter-intuitive coefficients). For instance:



Let $n' > n$, and consider the multigraphs $\overline{\mathbf{g}}_1$ and $\overline{\mathbf{g}}_2$ obtained by adding $n' - n$ isolated vertices to $\mathbf{g}_1$ and $\mathbf{g}_2$. New superpositions, which fit in n' vertices but not in n vertices, may appear in the product $\mathbf{x}^{\overline{\mathbf{g}}_1{}^{\circledast}}\mathbf{x}^{\overline{\mathbf{g}}_2{}^{\circledast}}$. However, the use of a modified Reynolds operator ensures that the coefficients in the linear combination do not change. This makes the product somewhat independent of n (see § 8).

(iii) If $\mathbf{g}$ and $\mathbf{h}$ are simple graphs, $\mathbf{x}^{\mathbf{g}^{\circledast}}(\mathbf{h})$ counts the number $s(\mathbf{g}, \mathbf{h})$ of subgraphs of $\mathbf{h}$ isomorphic to $\mathbf{g}$. The following invariants can be used to count respectively the number of edges, the number of pairs of adjacent edges and the number of Hamiltonian cycles of $\mathbf{h}$:



Manipulations of the quantities $s(\mathbf{g}, \mathbf{h})$ are the cornerstone of several results on reconstruction of graphs [2]; for the use of these algebraic considerations see [23].

1.4 Grading, Hilbert series and degree bound

Powerful properties of an invariant ring are its grading and the associated Hilbert series. As a $\mathbb{K}$-vector space, $I(G)$ is not finite dimensional. However, since the action of G preserves the degree of polynomials, $I(G)$ decomposes into the direct sum of its homogeneous components:

$$I(G) = \bigoplus_{d=0}^{\infty} I(G)_d,$$

where $I(G)_d$ is the finite dimensional vector space of all homogeneous invariants of degree d. The Hilbert series of $I(G)$ is the generating series of its dimensions:

$$H(I(G), z) := \sum_{d=0}^{\infty} z^d \dim I(G)_d.$$

For general finite groups of matrices, this series can be computed by averaging over the group, through Molien's formula. However, since $\mathcal{G}_n$ is a permutation group, the set of all invariants $\mathbf{x}^{\mathbf{g}^{\circledast}}$, where $\mathbf{g}$ is a multigraph with d edges is a vector space basis of $\mathcal{I}_{n,d}$. Therefore, computing $H(\mathcal{I}_n, z)$ reduces to a Pólya enumeration of multigraphs with respect to the number of edges [27]. Recall that the conjugacy classes C_λ of $\mathfrak{S}_n$ are indexed by the partitions λ of n. Let σ be a permutation of the vertices in C_λ. The cycle type of the induced permutation of the edges is easily computed from the cycle type of σ, *i.e.* from the partition λ [15]. We denote by $l_1(\lambda), \dots, l_m(\lambda)$ this cycle type. Then,

$$H(\mathcal{I}_n, z) = \frac{1}{n!} \sum_{\lambda} |C_\lambda| \frac{1}{\prod(1 - z^i)^{l_i(\lambda)}},$$

where the sum is over all partitions λ of n. This provides an algorithm whose complexity is about $O(n^4 \exp(n^{0.8}))$. Concretely, we can compute $H(\mathcal{I}_n, z)$ for $n \leq 21$. It is sometimes useful to consider the multigraded Hilbert series, where each grading corresponds to one of the three irreducible components of the representation $\mathcal{G}_n$. We can compute this multigraded Hilbert series for $n \leq 15$.

Given an integer $d \geq 1$, let $\mathbb{K}[I(G)_{<d}]$ be the subalgebra of $I(G)$ generated by invariants of degree $< d$, and $\mathbb{K}[I(G)_{<d}]_d$ its homogeneous component of degree d. Set $\mathrm{s}_0(I(G)) := 0$ and $\mathrm{s}_d(I(G)) := \dim I(G)_d - \dim \mathbb{K}[I(G)_{<d}]_d$. The generating series $\mathrm{s}(I(G), z) := \sum_{d=0}^{\infty} z^d \, \mathrm{s}_d(I(G))$ is a polynomial of degree $\beta(I(G))$.

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

Lemma 1.1. *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 having 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, $|S_d| = \mathrm{s}_d(I(G))$.

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 consider only homogeneous generating sets, since non-homogeneous generating sets are not much smaller than homogeneous ones.

The Hilbert series provides a simple necessary condition to test if a set S of homogeneous invariants is generating. The following proposition is valid for any graded algebra A, where A_0 is the ground field $\mathbb{K}$. We stress the importance of the homogeneity of the invariants. A series $s(z)$ is *dominated* by a series $t(z)$ if the coefficients of $s(z)$ are upper-bounded term by term by the coefficients of $t(z)$.

Condition 1.2. *Let $S := (p_1, \dots, p_t)$ be a homogeneous generating set, with respective degrees $(d_1, \dots, d_t)$. Then, the Hilbert series $H(I(G), z)$ is dominated by the series*

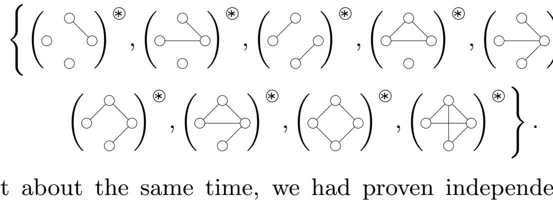
$$F(d_1, \dots, d_t, z) := \frac{1}{(1 - z^{d_1}) \dots (1 - z^{d_t})}.$$

Proof. As a vector space, the homogeneous component $I(G)_d$ is generated by the set of all the homogeneous products $p_1^{\lambda_1} \dots p_t^{\lambda_t}$ whose degree $d_1\lambda_1 + \dots + d_t\lambda_t$ is d; those products are counted by the series $F(d_1, \dots, d_t, z)$. □

This apparently weak condition is in fact very powerful. In particular, it leads to the proof of theorem 2.3, and to the disproving of Grigoriev's lemma 1 of [14] (see § 10).

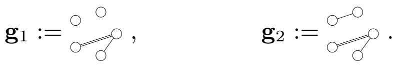
2 Generating sets of $\mathcal{I}_n$

For $n = 1, 2, 3$, the invariant ring is the ring of symmetric polynomials; the elementary symmetric polynomials form a minimal generating set. For $n = 4$, Aslaksen et al. [1] constructed by hand the following minimal generating set:



At about the same time, we had proven independently a similar result through a Gröbner basis computation with CoCoA [4], using theorem 2.7.9 of [29]. However, our set was not minimal since we had not removed the invariant $\mathbf{x}^{\mathbf{c}\circledast}$ where $\mathbf{c}$ is the complete graph. The set above can now be computed in about one second with Kemper's implementation of `Invar` in `Magma` [17].

We now provide a large, but reasonable, finite generating set of $\mathcal{I}_n$. A multigraph is *quasi-connected* if it has, at most, one non-trivial connected component. For example, $\mathbf{g}_1$ below is quasi-connected, but not $\mathbf{g}_2$:



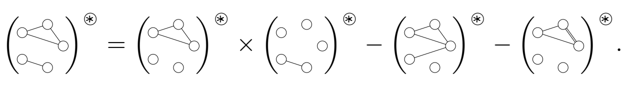
Proposition 2.1. *(i) The homogeneous component $\mathcal{I}_{n,d}$ has for vector space basis the set of all invariants $\mathbf{x}^{\mathbf{c}_1\circledast} \cdots \mathbf{x}^{\mathbf{c}_k\circledast}$, where each $\mathbf{c}_i$ is a quasi-connected multigraph with n_i non-isolated vertices and d_i edges, and where $n_1 + \dots + n_k \leq n$ and $d_1 + \dots + d_k = d$.*

(ii) The invariant ring $\mathcal{I}_n$ is generated by the set of all homogeneous invariants $\mathbf{x}^{\mathbf{g}\circledast}$, where $\mathbf{g}$ is a quasi-connected multigraph with at most $\beta(\mathcal{I}_n)$ edges.

Proof. (i) Let $\mathbf{g}$ be a multigraph with n vertices and $k > 1$ non-trivial connected components $\mathbf{c}_1, \dots, \mathbf{c}_k$. Let $\overline{\mathbf{c}}_1, \dots, \overline{\mathbf{c}}_1$ be the quasi-connected multigraphs on n vertices obtained by adding isolated vertices to the $\mathbf{c}_i$. Obviously, $n_1 + \dots + n_k \leq n$, and $d_1 + \dots + d_k = d$. Then:

$$\mathbf{x}^{\mathbf{g}\circledast} = \mathbf{x}^{\overline{\mathbf{c}}_1\circledast} \cdots \mathbf{x}^{\overline{\mathbf{c}}_k\circledast} - \sum_i \mathbf{x}^{\mathbf{h}_i\circledast},$$

where the $\mathbf{h}_i$ are multigraphs with strictly less than k non-trivial connected components. For example:



By induction on the number k of non-trivial connected components, $\mathbf{g}$ is a linear combination of products $\mathbf{x}^{\overline{\mathbf{c}}_1\circledast} \cdots \mathbf{x}^{\overline{\mathbf{c}}_k\circledast}$. In fact, we just inverted a triangular linear system with ones on the diagonal, and uniqueness follows.

(ii) Use (i) and the definition of $\beta(\mathcal{I}_n)$. □

Obviously, in order to get a usable generating set, it is essential to have a good bound for $\beta(\mathcal{I}_n)$.

We tried to use the technique of SAGBI basis. This is a powerful tool, which generalizes Gröbner basis techniques for rings instead of ideals [24]. The main drawback is that there exist invariant rings with no finite SAGBI basis; this seems to be the case for $\mathcal{I}_n$, at least for many common monomial orders.

Theorem 2.2. *There are no finite SAGBI basis for $\mathcal{I}_n$ if the monomial order is either lexicographic, degree lexicographic, or degree reverse lexicographic with the $n - 1$ smallest variables corresponding to adjacent edges.*

Proof. We prove in each case that there is an infinite number of irreducible initial monomials (an initial monomial is irreducible if it cannot be written as product of two smaller initial monomials). For the lexicographic order, we can alternatively use Göbel's characterization of permutation groups with finite SAGBI basis [13]. □

The following theorem states that some sets are not generating. (i) disproves a tempting generalization of the fundamental theorem of symmetric functions, whereas (ii) disproves Pouzet's conjecture [21], which would have implied Ulam's reconstruction conjecture.

Theorem 2.3. *(i) For $n \geq 5$, the set of all invariants $\mathbf{x}^{\mathbf{g}\circledast}$, where $\mathbf{g}$ is a simple graph, do not generate $\mathcal{I}_n$.*

(ii) For $11 \leq n \leq 18$, the set of all invariants $\mathbf{x}^{\mathbf{g}\circledast}$, where $\mathbf{g}$ is a multigraph with at least one isolated vertex, do not generate $\mathcal{I}_n$.

Proof. (i) For $n = 5, 6, 7, 8$, simple graphs can be counted with respect to the number of edges using Pólya enumeration [15]. The coefficient of degree $d = 4$ of the series $S(d_1, \dots, d_t)$ is strictly smaller than that of the Hilbert series. Therefore, condition 1.2 applies. For $n \geq 9$, no new isomorphism types of multigraphs with less than 4 edges appears, so the coefficient of degree 4 of both series is the same as for $n = 8$. Condition 1.2 again applies.

(ii) By an argument similar to the proof of proposition 2.1, we have only to consider the set of all invariants $\mathbf{x}^{\mathbf{g}\circledast}$, where $\mathbf{g}$ is a multigraph with a unique non-trivial connected component, which is of size $< n$. Those multigraphs can be counted from the total number of multigraphs by using a technique similar to that described in [15, § 4.2, p. 90]. For $11 \leq n \leq 18$, computations of both series shows that condition 1.2 fails. □

We could not check (ii) for $n > 18$ since the computation were intractable. However, the results for $n \leq 18$ strongly suggest that, for $d \approx 4n - 24$, the ratio between the coefficients of degree d of the two series is bounded by an expression of the form $\exp(-an) + 0.17$. This could probably be confirmed by an asymptotic study, and we conjecture that (ii) is true for any $n \geq 11$.

3 Decomposition of Hironaka

The smallest degree bound $\beta(\mathcal{I}_n)$ and furthermore the polynomial $\mathrm{s}(\mathcal{I}_n, z)$ contains important information about the invariant ring, which would be very useful when the computation of a minimal generating set is intractable. But so far, we don't know how to calculate them except by explicitly computing such a minimal generating set.

Invariant theory provides only some bounds on $\beta(\mathcal{I}_n)$ and $\mathrm{s}(\mathcal{I}_n, z)$ [25, 6]. Noether's theorem [29, p. 27] yields: $\beta(\mathcal{I}_n) \leq |\mathcal{G}_n| = n!$, which is not very informative. A much better bound exists for permutation groups: $\beta(\mathcal{I}_n) \leq \binom{m}{2} = \binom{\binom{n}{2}}{2}$ [11]. However, our computations for small n shows that this is still a rather loose bound. This section introduces the tools that produce this bound, and possibly even better bounds.

A set of m homogeneous invariants $(\theta_1, \dots, \theta_m)$ of $I(G)$ is called a *homogeneous system of parameters* or, for short, a *system of parameters* if the invariant ring $I(G)$ is finitely generated over its subring $\mathbb{K}[\theta_1, \dots, \theta_m]$. That is, if there exist a finite number of invariants $(\eta_1, \dots, \eta_t)$ such that the invariant ring is the sum of the subspaces $\eta_i.\mathbb{K}[\theta_1, \dots, \theta_m]$. By Noether's normalization lemma, there always exists a system of parameters for $I(G)$. Moreover, $I(G)$ is *Cohen-Macaulay*, which means that $I(G)$ is a free-module over any system of parameters. So, if the set $(\eta_1, \dots, \eta_t)$ is minimal for inclusion, $I(G)$ decomposes into a direct sum:

$$I(G) = \bigoplus_{i=1}^{t} \eta_i.\mathbb{K}[\theta_1, \dots, \theta_m].$$

This decomposition is called a *Hironaka decomposition* of the invariant ring. The θ_i are called *primary invariants*, and the η_i *secondary invariants* (in algebraic combinatorics literature, the θ_i are some times called *quasi-generators* and the η_i *separators* [11]). It should be emphasized that primary and secondary invariants are not uniquely determined, and that being a primary or secondary invariant is not an intrinsic property of an invariant p, but rather express the role of p in a particular generating set.

The primary and secondary invariants together form a generating set. From the degrees $(d_1, \dots, d_m)$ of the primary invariants $(\theta_1, \dots, \theta_m)$ and the Hilbert series we can compute the number t and the degrees $(e_1, \dots, e_t)$ of the secondary invariants $(\eta_1, \dots, \eta_t)$ by the formula:

$$z^{e_1} + \cdots + z^{e_t} = (1 - z^{d_1}) \cdots (1 - z^{d_m}) H(I(G), z). \tag{1}$$

Assuming $d_1 \leq \cdots \leq d_m$ and $e_1 \leq \cdots \leq e_t$, it can be proved that:

$$\begin{aligned} t &= \frac{d_1 \cdots d_m}{|G|}, \\ e_t &= d_1 + \cdots + d_m - m - \mu, \\ \beta(I(G)) &\leq \max(d_m, e_t), \end{aligned} \tag{2}$$

where μ is the smallest degree of a polynomial p such that $\sigma \cdot p = \det(\sigma)p$ for all $\sigma \in G$ [27, Proposition 3.8].

For example, if G is the symmetric group $\mathfrak{S}_m$, the m elementary symmetric polynomial (or the m first symmetric power sums) form a system of parameters, $t = 1$, $e_t = 0$ and $\eta_1 = 1$. This is consistent with the fundamental theorem of symmetric polynomials.

More generally, for $\mathcal{G}_n$ as well as for any permutation group, the elementary symmetric polynomials still form a system of parameters. This yields the following information on $\mathcal{I}_n$.

Proposition 3.1. *For $n \geq 4$, consider the system of parameters of $\mathcal{I}_n$ composed of the elementary symmetric polynomials, and let $(e_1, \dots, e_t)$ be the degrees of secondary invariants. Then,*

$$t = \frac{m!}{|\mathcal{G}_n|} = \frac{\binom{n}{2}!}{n!},$$

$$e_t = \binom{m}{2} - \mu_n = \binom{\binom{n}{2}}{2} - \mu_n,$$

$$\beta(\mathcal{I}_n) \leq \binom{\binom{n}{2}}{2} - \mu_n,$$

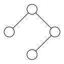
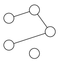
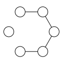
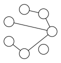
where $\mu_n = 0$ if n is even, and $\mu_n = \lceil \frac{3}{4}(n-1) \rceil$ otherwise.

For example, $\beta(\mathcal{I}_4) \leq 15$, $\beta(\mathcal{I}_5) \leq 42$ and $\beta(\mathcal{I}_6) \leq 104$.

Proof. We only have to check the value of μ_n. When n is even, $\det(\sigma) = 1$ for all $\sigma \in \mathcal{G}_n$. Therefore, $p := 1$ verifies the condition $\sigma \cdot p = \det(\sigma)p$ for all $\sigma \in \mathcal{G}_n$. We note that this is generally true for any Gorenstein ring (see § 6 and [27, § 8]). When n is odd, the sign of a permutation of the edges is the sign of the corresponding permutation of the vertices. Then, the smallest degree μ_n of a polynomial p such that $\sigma \cdot p = \operatorname{sign} \sigma p$ is the smallest number of edges of multigraph with no odd automorphism. The following lemma completes the proof. □

Lemma 3.2. *The smallest number of edges of a multigraph $\mathbf{g}_n$ on $n \geq 4$ vertices without odd automorphism is $\lceil \frac{3}{4}(n-1) \rceil$.*

Proof. Such multigraphs can be constructed for any n as follows:

- $\mathbf{g}_4 :=$  ; $\mathbf{g}_5 :=$  ; $\mathbf{g}_6 :=$  ; $\mathbf{g}_7 :=$  ;
- $\mathbf{g}_{4k}$ is composed of k copies of $\mathbf{g}_4$ ($3k$ edges);
- $\mathbf{g}_{4k+1}$ is composed of k copies of $\mathbf{g}_4$ and an isolated vertex ($3k$ edges);
- $\mathbf{g}_{4k+2}$ is composed of $k-1$ copies of $\mathbf{g}_4$ and one copy of $\mathbf{g}_6$ ($3k+1$ edges);
- $\mathbf{g}_{4k+3}$ is composed of $k-1$ copies of $\mathbf{g}_4$ and one copy of $\mathbf{g}_7$ ($3k+2$ edges).

The minimality of the number of edges of such multigraphs can be proved by induction over n. □

So, the knowledge of a system of parameters and of the Hilbert series provides both an upper bound on $\beta(\mathcal{I}_n)$, as well as bounds on the coefficients of $\mathrm{s}(\mathcal{I}_n, z)$. Unfortunately, our experience has shown that generating sets composed of primary and secondary invariants are far from minimal (see Figures 4 and 2), so those bounds are quite loose. Moreover, to our knowledge, those bounds are the only obtainable information about a minimal generating set, without actually computing it.

4 Low degrees systems of parameters

We now search for a low degrees system of parameters for $\mathcal{I}_n$, in order to improve the bound on $\beta(\mathcal{I}_n)$. Equation (1) can guide our quest by suggesting possible degrees. Indeed, there can only exist a system of parameters of degrees $(d_1, \dots, d_m)$ if the expression $(1 - z^{d_1}) \cdots (1 - z^{d_m}) H(I(G), z)$ is a polynomial with positive integer coefficients. It has even been conjectured by Mallows and Sloane [20, 7] that the converse is true: if $(1 - z^{d_1}) \cdots (1 - z^{d_m}) H(I(G), z)$ is a polynomial with positive integer coefficient, then there exists a system of parameters of degrees $(d_1, \dots, d_m)$. A counter-example has been found, but the conjecture still holds if the representation of G over V is irreducible, or when using a multigraded Hilbert series (one grading for each irreducible component) [7, p. 5].

By tweaking the Hilbert series for $n \leq 21$, and the multigraded Hilbert series for $n \leq 15$, we find that the degree sequence $(1, \dots, n,\ 2, \dots, \binom{n-1}{2})$ always produces a polynomial with positive integer coefficient. We also proved that, for any n, this degree sequence produces a polynomial. We are therefore somewhat confident with the following conjecture:

Conjecture 4.1. *For all $n \geq 3$, there exists a system of parameters for $\mathcal{I}_n$ of degrees $(1, \dots, n,\ 2, \dots, \binom{n-1}{2})$. As a direct consequence, $\beta(\mathcal{I}_n) \leq \binom{n}{2} + \binom{\binom{n-1}{2}}{2} - \mu_n$.*

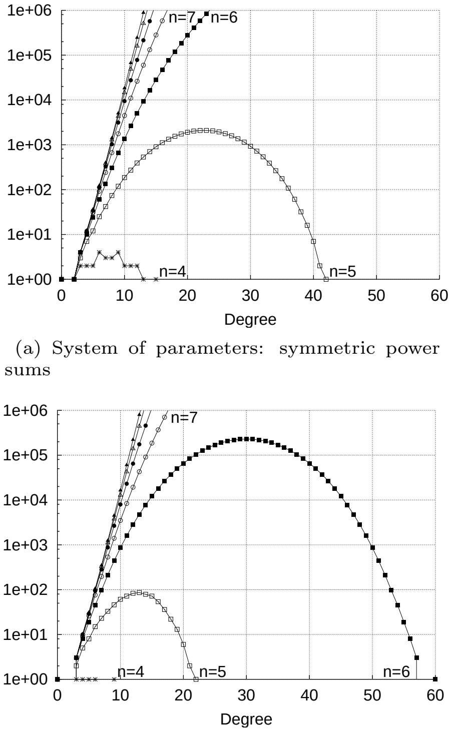
For example, $\beta(\mathcal{I}_4) \leq 9$, $\beta(\mathcal{I}_5) \leq 22$ and $\beta(\mathcal{I}_6) \leq 60$, which are much smaller degree bounds than those provided by proposition 3.1. Figure 1 displays the number of secondary invariants depending on the system of parameters.

Next, we construct a reasonable system of parameters and check its validity for $n = 3, 4, 5$, which proves conjecture 4.1 for those values. We note that Dixmier [7] constructed a system of parameters with degrees $(2, 3, 4, 5, 6)$ for the representation $[3, 2]$ of $\mathfrak{S}_5$, and proved its validity by hand. By using the decomposition of the representation $\mathcal{G}_5$ into $[5] + [4, 1] + [3, 2]$, this also provides a system of parameters with the expected degrees.

The form of the degree sequence suggests starting from the $\binom{n}{2}$ first symmetric power sums, and replacing the last $n - 1$ degrees $(\binom{n-1}{2} + 1, \dots \binom{n}{2})$ by some invariants of degree $2, \dots, n$. Moreover, since the representation splits into $[n] \oplus [n-1, 1]$ and $[n-2, 2]$ (see § 1.1), we get a system of parameters for the invariant ring of the whole representation, by taking systems of parameters for the invariant rings of each components and putting them together. Recall that the first component is the natural representation of $\mathfrak{S}_n$ by permutations of the stars $(\mathbf{E}_1, \dots, \mathbf{E}_n)$. So, the invariant ring over this component is the ring of symmetric polynomials in the dual variables $(X_1, \dots, X_n)$, and the n first symmetric power sums in the X_i form a system of parameters for this component. Note that, up to a constant 2, the first symmetric power sum in the X_i is equal to the first symmetric power sum in the $x_{\{i,j\}}$. All this leads to the following conjecture:

Conjecture 4.2. *If $n \geq 3$, the following system of invariants is a system of parameters for $\mathcal{I}_n$.*

$$x_{\{1,2\}} + \dots + x_{\{n-1,n\}}, \quad \dots, \quad x_{\{1,2\}}^{\binom{n-1}{2}} + \dots + x_{\{n-1,n\}}^{\binom{n-1}{2}},$$
$$X_1 + \dots + X_n, \quad \dots, \quad X_1^n + \dots + X_n^n.$$



(a) System of parameters: symmetric power sums

(b) Conjectured system of parameters

Figure 1: Number of secondaries per degree

Proposition 4.3. *Conjecture 4.2 holds for $3 \leq n \leq 5$.*

This is immediate for $n = 3$, since the component $[n-2, 2]$ is trivial. To test the conjecture for other small cases, we used the following general characterization:

Caracterisation 4.4 ([29]). *A set of m homogeneous invariants $(\theta_1, \dots, \theta_m)$ is a system of parameters if and only if $\mathbf{v} = 0$ is the only common zero of the θ_i:*

$$\theta_1(\mathbf{v}) = \dots = \theta_m(\mathbf{v}) = 0 \Rightarrow \mathbf{v} = 0$$

For $n = 4$, this characterization is enough to prove conjecture 4.2 by hand.

For $n \geq 5$, we can try to check conjecture 4.2 as follow: compute a Gröbner basis for the θ_i, and verify that for each variable $x_{\{i,j\}}$ there is a polynomial in the Gröbner basis whose leading term is of the form $x_{\{i,j\}}^k$ (see [29, Subroutine 2.5.2]; this is both a necessary and sufficient condition for the radical of the ideal generated by the θ_i to be the irrelevant ideal).

For $n = 3, 4$, the direct computation of this Gröbner basis takes less than one second, but for $n = 5$ it seems to be intractable and fails. However, some equivalent Gröbner basis can be computed in about one minute, by using a suitable linear change of basis which respects the decomposition of the representation. The verification of characterization 4.4 is then straightforward.

For $n = 6$, even with the same linear change of basis and using `FGb` [9], the computation is intractable. In fact, the growth of the Gröbner basis seems to follow nearly the worst possible theoretical case [12].

Finally, as a by-product of the computation of minimal generating sets with PerMuVAR, we checked that for $n \leq 8$ and for the low-degree homogeneous components, the ring of invariants is indeed a free-module over $\mathbb{K}[\theta_1, \ldots, \theta_m]$. This gives some confidence in conjecture 4.2, but so far we are unable to prove it.

If the above construction of a system of parameters is correct, we believe it to be nearly optimal: there exist no general construction of systems of parameters with lower degrees. Indeed, we calculated, for small values of n, the smallest degree sequence allowed by the multigraded Hilbert series. For $3, 4, 5$, the degrees conjectured above are optimal. For $n \geq 6$, it was usually possible to divide some of the degrees by 2 or 3. For example, for $n = 6$ and 7 the best degree sequences are respectively $(1, \ldots, 6,\ 2, \ldots, 7, \frac{8}{2}, \frac{9}{3}, \frac{10}{2})$ and $(1, \ldots, 7,\ 2, \ldots, 7, \frac{8}{2}, 9, \ldots, 13, \frac{14}{2}, 15)$. We have not noticed any regularity in these case by case optimizations. Therefore, we don't think this technique can be refined much further in order to get better degree bounds.

5 Computing minimal generating sets

Since we can not get more *a priori* information on homogeneous minimal generating sets of $\mathcal{I}_n$, we proceed with explicitly computing them. The computations are very intensive (even for $n = 5$) but give some feeling of the size and degree of minimal generating sets. The bounds given by Hironaka decompositions seem very loose.

The basic principle of the classical algorithms is to construct generating sets degree by degree, from 1 up to the best degree bound known. Since the complexity of the computations involved usually increases quickly with increasing degree, the quality of the degree bound is crucial. One can 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).

Most software [16] relies on a precomputation of a Gröbner basis of the system of parameters to greatly speed up the rest of the computations. However, with $\mathcal{I}_n$ this precomputation is very hard, if not impossible (see § 4). Software that do not rely on this precomputation uses linear algebra on the homogeneous component of degree d of the whole ring of polynomials, whose dimension grows quickly with increasing d, and fail early.

Since our group is a permutation group, invariants can be stored as linear combinations of invariants $\mathbf{x}^{\mathbf{g}^{\circledast}}$. This saves a lot of memory (up to a factor of $1/|\mathcal{G}_n|$ for monomials without symmetries, which happens to be the case for most of them). This data structure also allows for the same linear algebra operations inside the homogeneous component of degree d of the invariant ring which is considerably smaller. We therefore implemented our own invariant theory software PerMuVAR which takes advantage of the particular properties of permutation groups [32]. We chose the computer algebra system MuPAD, which is freely available (but alas not open source software), and allows modularity through object oriented programming. Moreover, MuPAD's dynamic modules will allow for rewriting critical sections in a very efficient language like C++.

A sketch of the algorithm follows. We denote by $\langle \theta_1, \ldots, \theta_m \rangle_d$ the homogeneous component of degree d of the ideal generated by $(\theta_1, \ldots, \theta_m)$ in $I(G)$.

Algorithm 5.1 (Computing secondary invariants)
Input: a system of parameters $(\theta_1, \ldots, \theta_m)$ and a function nextInvariant(d) which iterates through a set of invariants of degree d spanning $I(G)_d$ as a vector space.
Output: (irreducible) secondary invariants.

```
for d from 1 to $e_t$ do
  // Compute secondary invariants for degree d
  secondaries [d]:=[ ]; // Secondary invariants
  irreducibles [d]:=[ ]; // Irreducible secondaries
  // Compute a basis L of $\langle \theta_1, \ldots, \theta_m \rangle_d$
  L:=[ ];
  for p product of a previous secondary and a non-trivial product of the $\theta_i$ do
    insert p into L;
  end for
  // Extend L to a basis of $\mathbb{K}[I(G)_{<d}]_d$
  for p product of previous secondaries do
    if p is not in the vector space spanned by L then
      insert p into secondaries [d];
      insert p into L;
    end if
  end for
  // Construct the irreducible secondaries
  while p:=nextInvariant (d) do
    if p is not in the vector space spanned by L then
      insert p into secondaries [d]
      insert p into irreducibles [d]
      insert p into L
    end if
  end while
end for
```

Some comments about this algorithm are in order:

(i) In the last loop, the Hilbert series provides a stopping condition, since the number of secondary invariants is known. To maintain efficiency, the elements of L are mutually reduced by Gauss elimination. Testing if p is in the vector space generated by L amounts to reducing it modulo L; inserting it into L amounts to further reducing the elements of L by p. Therefore, this algorithm is essentially a step by step matrix inversion by Gauss elimination, and the cost for each degree is about $(\dim I(G)^3_d$.

(ii) The main waste of memory and time in this algorithm is the explicit computation of the vector space basis L of $\langle \theta_1, \ldots, \theta_m \rangle_d$. It would be nice to work directly in the quotient of $I(G)$ by the ideal $\langle \theta_1, \ldots, \theta_m \rangle$, as in the algorithm based on a Gröbner basis precomputation. This approach is further developed in [31].

(iii) By properly keeping track of the reductions in L, we can determine which primary invariants should be removed in order to obtain a minimal generating set. In addition, by properly choosing the nextInvariant function, we can check whether a given set of invariants is generating, and if not construct counter-examples.

For $n = 5$, we could only compute a partial minimal generating set S_5 up to degree 10, whereas the best a priori degree bound is $\beta(\mathcal{I}_n) \leq 22$. However, $s_{10}(\mathcal{I}_n) = 0$ (*i.e.* a minimal generating set contains no invariant of degree 10), and Figure 2 strongly suggested that $s_d(\mathcal{I}_n) = 0$ for any $d \geq 10$. This has been checked by Kemper [18], using *ad hoc* computations, thus proving that S_5 is a minimal generating set (see § 9 for a possible alternative approach). Therefore, $\beta(\mathcal{I}_4) = 5$, and $\beta(\mathcal{I}_5) = 9$.

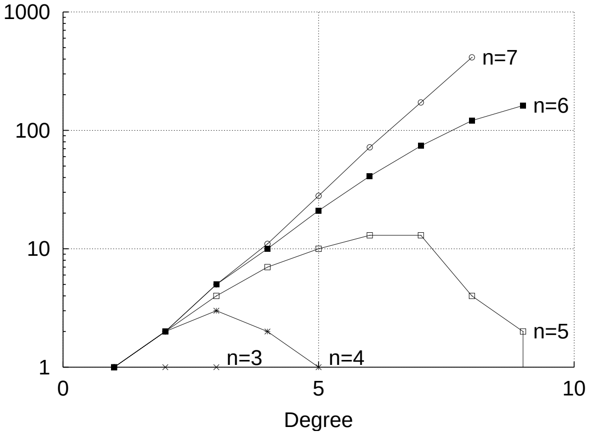


Figure 2: $s_d(\mathcal{I}_n)$: number of invariants per degree d in a minimal generating set of $\mathcal{I}_n$

Conjecture 5.2. *If $n \geq 4$, $\beta(\mathcal{I}_n) = \binom{n}{2} - 1$.*

6 The Gorenstein property

In this section, we show that the invariant ring $\mathcal{I}_n$ is Gorenstein when n is even, which indicates several duality properties of $\mathcal{I}_n$. In particular, $e_t = d_1 + \cdots + d_m - m$ and there are as many secondary invariants of degree $e_t - d$ and degree d. Actually, this could be used to considerably speed up the construction of secondary invariants [32].

Lemma 6.1. *(i) Let σ be a permutation of the vertices, that is an element of $\mathfrak{S}_n$, and $\overline{\sigma}$ be the corresponding permutation of the edges in $\mathcal{G}_n$. Then:*

$$\begin{aligned} \operatorname{sign}(\overline{\sigma}) &= \operatorname{sign}(\sigma) && \textit{if } n \textit{ is odd}, \\ \operatorname{sign}(\overline{\sigma}) &= 1 && \textit{if } n \textit{ is even}. \end{aligned}$$

(ii) If n is even, $\mathcal{G}_n$ is a subgroup of the special linear group $\mathrm{SL}(V)$.

(iii) If n is odd, the representation of $\mathfrak{S}_n$ on the irreducible component $[n-2, 2]$ is a subgroup of $\mathrm{SL}(V)$.

Proof. (i) If σ is a transposition of 2 vertices, then $\overline{\sigma}$ exchanges $n-2$ pairs of edges, and $\operatorname{sign}(\overline{\sigma}) = (-1)^{n-2}$.

(iii) Take $\sigma \in \mathfrak{S}_n$, and M the matrix of the representation of σ on the component $[n-2, 2]$. The determinant of the representation of σ on $\mathcal{V}_n$ is $\operatorname{sign}(\overline{\sigma})$, whereas the sign of the representation of σ on the other component $[n] \oplus [n-1, 1]$ is $\operatorname{sign}(\sigma)$ (natural representation of $\mathfrak{S}_n$). Therefore, $\det(M) = \operatorname{sign}(\overline{\sigma}) / \operatorname{sign}(\sigma) = 1$, if n is odd. □

Then, Watanabee's theorem [27, § 8] applies.

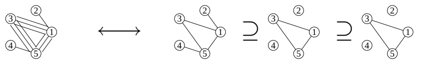
Theorem 6.2. *(i) When n is even, $\mathcal{I}_n$ is Gorenstein.*

(ii) When n is odd, the invariant ring over the irreducible component $[n-2, 2]$ is Gorenstein.

7 The chain product

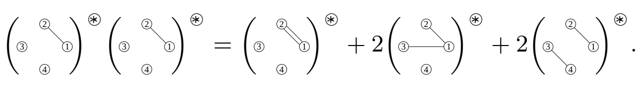
We have discussed the power of the grading of the invariant ring. We now define another product on the invariant ring $\mathcal{I}_n$, called the *chain product*, which preserves a finer grading and has a nice computational behavior. Most algebraic properties of the invariant ring with respect to the chain product transfer back to the usual product. We only construct and use the chain product for $\mathcal{I}_n$, but it generalizes to any permutation group [32].

Let $\mathbf{g}$ be a multigraph. As in the following example, it can be interpreted as a superposition of simple graphs $\mathbf{g}_1, \mathbf{g}_2, \cdots, \mathbf{g}_k$, where $\mathbf{g}_1 \supseteq \mathbf{g}_2 \supseteq \cdots \supseteq \mathbf{g}_k$:

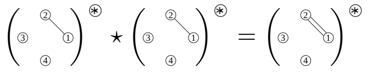


Thus, $\mathbf{g}$ can be identified with the *multichain* (*i.e.* chain with repetitions) $C(\mathbf{g}) := \mathbf{g}_1 \supseteq \mathbf{g}_2 \supseteq \cdots \supseteq \mathbf{g}_k$ of simple graphs. The *shape* $\lambda(\mathbf{g})$ of $\mathbf{g}$ is the decreasing sequence of the sizes of the simple graphs in $C(\mathbf{g})$. Here, $\lambda(\mathbf{g}) = (5, 3, 3)$. A polynomial is called *finely-homogeneous* if all its monomials have the same shape. Since two monomials $\mathbf{x}^{\mathbf{g}}$ and $\mathbf{x}^{\mathbf{g}'}$ in the same $\mathfrak{S}_n$-orbit have the same shape, any invariant decomposes into a sum of finely-homogeneous invariants. Therefore, the shape defines a fine grading on the invariant ring $\mathcal{I}_n$, and we denote by $\mathcal{I}_{n,(5,3,3)}$ the *finely homogeneous component* of $\mathcal{I}_n$ for the shape $(5, 3, 3)$.

The usual product does not preserve this grading:



The *chain product* $\mathbf{x}^{\mathbf{g}} \star \mathbf{x}^{\mathbf{h}}$ of two monomials $\mathbf{x}^{\mathbf{g}}$ and $\mathbf{x}^{\mathbf{h}}$ is the usual product of $\mathbf{x}^{\mathbf{g}}$ and $\mathbf{x}^{\mathbf{h}}$ if the two multichains $C(\mathbf{g})$ and $C(\mathbf{h})$ can be merged into another multichain, and zero otherwise. The chain product extends to invariants, and yields for example:



The chain product preserves the fine grading of the invariant ring, since the shape $\mathbf{x}^{\mathbf{g}} \star \mathbf{x}^{\mathbf{h}}$ can be obtained by merging the shapes of $\mathbf{g}$ and $\mathbf{h}$.

The invariant ring $\mathcal{I}_n$ together with the chain product is actually isomorphic to the Stanley-Reisner ring of the poset of unlabelled graphs on n vertices ordered by subgraph. Stanley-Reisner rings of posets have been intensively studied, in particular by Garsia and Stanton [11] to construct Hironaka decompositions of invariant rings of certain permutation groups. We did not succeed in using this theoretical framework to get a Hironaka decomposition of $\mathcal{I}_n$. The need of taking the elementary symmetric polynomials as a system of parameters causes the main difficulty. Indeed, this is not a low degree system of parameters and there are too many secondary invariants. However, even our naive point of view of the Stanley-Reisner ring as an alternative product on $\mathcal{I}_n$ yields dramatic speed ups of the computations.

The following proposition is the heart of this technique.

Proposition 7.1 ([11]). *A Hironaka decomposition of $\mathcal{I}_n$ for the chain product, is also a Hironaka decomposition of $\mathcal{I}_n$ for the usual product.*

The key of the proof is that, if p and q are finely homogeneous, the maximal finely homogeneous component of pq is exactly $p \star q$. The result follows by induction over the fine grading. We used the same principle to prove a similar result on generating sets.

Proposition 7.2. *A generating set of $\mathfrak{I}_n$ for the chain product is a generating set of $\mathfrak{I}_n$ for the usual product.*

In all our examples, however, minimal generating sets for the chain product were far from being minimal for the usual product.

The elementary symmetric polynomials form a system of parameters for the chain product. We do not know if there are other systems of parameters, since the usual characterization from proposition 4.4 does not apply for the chain product. In particular, the symmetric power sums do not form a system of parameters for the chain product. They are not even algebraically independent since $\sum x_{\{i,j\}}^k = \left(\sum x_{\{i,j\}}\right)^k$. Given the size of the minimal generating sets we computed, there are no systems of parameters for the chain product with degrees as low as in conjecture 4.1.

In [32], we describe how to use this product for faster computations. Practically, we could push the computation of a partial minimal generating set S for $\mathfrak{I}_5$ up to the degree 22 instead of only 10. This is a significant progress, considering that the dimension of $\mathfrak{I}_{5,22}$ is 174403, whereas the dimension of $\mathfrak{I}_{5,10}$ is only 974. Unfortunately, we cannot use a low-degrees system of parameters, so the degree bound is 42 instead of 22. This means that there is still a lot of work to do to get a full minimal generating set for the chain product. On the other hand, this partial computation yields a generating set for the usual product, since $\beta(\mathfrak{I}_5) \leq 22$.

Proposition 7.3. *The computed set S is a generating set of $\mathfrak{I}_5$ for the usual product. However, S has more than one thousand invariants of degree up to* 22.

To conclude, the usual product allowed us to compute a small set, with is minimal, but not necessarily generating, whereas the chain product allowed us to compute a set which is generating, but far from being minimal.

8 The invariant ring for $n = \infty$

In this section, we study the projective limit $\mathfrak{I}_\infty$ of the invariant ring, and get back some information on $\mathfrak{I}_n$.

A multigraph $\mathbf{g}$ on $n' \leq n$ non-isolated vertices can be identified with a multigraph on n vertices by adding $n - n'$ isolated vertices. This defines $\mathbf{x}^{\mathbf{g}\circledast}$ in $\mathfrak{I}_n$. The set B_n of all invariants $\mathbf{x}^{\mathbf{g}\circledast}$, where $\mathbf{g}$ is a multigraph on less than n non-isolated vertices, is obviously a vector space basis of $\mathfrak{I}_n$. For $n' \leq n$, let $\Phi_{n'}$ be the linear projection from $\mathfrak{I}_n$ to $\mathfrak{I}_{n'}$ which maps $\mathbf{x}^{\mathbf{g}\circledast}$ (in $\mathfrak{I}_n$) to 0 if $\mathbf{g}$ has strictly more than n' non-isolated vertices, and to $\mathbf{x}^{\mathbf{g}\circledast}$ (in $\mathfrak{I}_{n'}$) otherwise. Our definition of the exponential (see § 1.3) makes it a surjective morphism of graded algebra. The projective limit of $\mathfrak{I}_n$:

$$\mathfrak{I}_1 \overset{\Phi_1}{\twoheadleftarrow} \mathfrak{I}_2 \overset{\Phi_2}{\twoheadleftarrow} \cdots \twoheadleftarrow \mathfrak{I}_n \overset{\Phi_n}{\twoheadleftarrow} \cdots \twoheadleftarrow \mathfrak{I}_\infty,$$

defines a graded algebra $\mathfrak{I}_\infty$, with a canonical vector space basis $B_\infty := \{\mathbf{x}^{\mathbf{g}\circledast}\}$ indexed by the multigraphs $\mathbf{g}$ on a finite number of non-isolated vertices.

Proposition 8.1. *(i) $\mathfrak{I}_\infty$ is the free polynomial ring over $C := \{\mathbf{x}^{\mathbf{g}\circledast} \mid \mathbf{g}$ is connected$\}$.*

(ii) The canonical morphism of graded algebra $\Phi_n : \mathfrak{I}_\infty \twoheadrightarrow \mathfrak{I}_n$ is an isomorphism up to the degree $\lfloor \frac{n}{2} \rfloor$.

Proof. (i) Following the proof of proposition 2.1 (ii), C generates $\mathfrak{I}_\infty$. Now, let $g_1, \dots, g_k$ be $k > 0$ connected multigraphs. In the product $\mathbf{x}^{\mathbf{g}_1\circledast} \cdots \mathbf{x}^{\mathbf{g}_k\circledast}$, there is a term $\mathbf{x}^{\mathbf{h}\circledast}$ with coefficient 1, where $\mathbf{h}$ is the disconnected multigraph whose connected components are precisely the g_i. This term is a marker of the product $\mathbf{x}^{\mathbf{g}_1\circledast} \cdots \mathbf{x}^{\mathbf{g}_k\circledast}$ in any non-trivial polynomial combination of elements of S. The algebraic independence follows.

Any multigraph with d edges and no isolated vertices has less than $2d$ vertices. (ii) follows. □

Corollary 8.2. $\beta(\mathfrak{I}_n) \geq \lfloor \frac{n}{2} \rfloor$.

This lower bound is loose: for $n \leq 5$, we know that $\beta(\mathfrak{I}_n) \geq \binom{n}{2} - 1$ and for $11 \leq n \leq 18$, it follows from theorem 2.3 (ii) that $\beta(\mathfrak{I}_n) \geq n - 2$. We expect that refining this technique will yield much better lower bounds.

By (ii), the Hilbert series $H(\mathfrak{I}_\infty, z)$ is the limit of the Hilbert series $H(\mathfrak{I}_n, z)$ as n goes to infinity, and by (i)

$$H(\mathfrak{I}_\infty, z) = \prod_{d=1}^{\infty} \frac{1}{(1 - z^d)^{n_d}},$$

where n_d is the number of connected multigraphs with d edges. We do not know how to directly compute $H(\mathfrak{I}_n, z)$, or whether there exists a closed form formula. The only asymptotic studies we have seen in the literature deal with n fixed and d going to infinity [15].

9 Unimodality

A startling fact revealed by our computations of minimal generating sets (MGS) lies in Figure 2, which shows the coefficients of $\mathrm{s}(\mathfrak{I}_n, z)$. For $n \leq 4$ and most likely for $n = 5$, this polynomial is *unimodal*: the coefficients first increase with the degree, and then decrease down to 0.

Conjecture 9.1. *The polynomial $\mathrm{s}(\mathfrak{I}_n, z)$ is unimodal.*

This would prove that the partial minimal generating set we computed for $n = 5$ is generating, and provide a very nice stopping condition for algorithm 5.1.

To figure out which properties of $\mathfrak{G}_n$ could be useful to prove this conjecture, we extend it to general groups of matrices. A finite subgroup G of $\mathrm{GL}(V)$ is *MGS-unimodal* if the polynomial $\mathrm{s}(I(G), z)$ is unimodal.

Problem 9.2. *Characterize MGS-unimodal groups.*

Not all groups are MGS-unimodal. Indeed, let G be the subgroup of $\mathrm{GL}(\mathbb{C}^2)$ generated by the matrix

$$M := \begin{bmatrix} j & 0 \\ 0 & \overline{j} \end{bmatrix},$$

where j and $\overline{j}$ are the two non-trivial third roots of unity. Obviously, (x_1x_2, x_1^3, x_2^3) is a minimal generating set of $I(G)$, and $\mathrm{s}(G, z) = z + 0z^2 + 2z^3$, which is not unimodal.

Whereas the irreducible representations of the symmetric group are thoroughly described, their invariants rings are barely known. In an amazing but very technical paper [7], Dixmier has been able to construct by hand minimal generating sets for several irreducible representations of $\mathfrak{S}_n$, including all the irreducible representations of $\mathfrak{S}_1, \dots, \mathfrak{S}_5$, except $[3,1,1]$. It follows that the representations $[n]$,$[n-1,1]$, $[2,2]$ and $[3,2]$ are MGS-unimodal, whereas the representations $[2,1^{n-2}]$ for $n \geq 4$ and $[2,2,1]$ are not. This proves the existence non-MGS-unimodal irreducible representations of the symmetric group.

The trivial group, the full symmetric group and multisymmetric polynomials are MGS-unimodal. We checked with PerMuVAR that several other small permutation groups are MGS-unimodal. It's tempting to conjecture that all permutation groups are MGS-unimodal, since they give rise to a lot of unimodality properties (see [28]; note that, as opposite to here, the corresponding series are always either log-concave or symmetric). However, for $n \geq 4$, the alternating group $\mathcal{A}_n$ is not MGS-unimodal. Indeed, $I(\mathcal{A}_n)$ is generated by the elementary symmetric polynomials of degrees $1, \dots, n$ together with the Van-der-Monde determinant $\prod_{i<j}(x_i - x_j)$ of degree $\binom{n}{2}$.

Figure 1 also shows that, up to $n = 21$, the generating series of the secondary invariants is unimodal (except at $d = 0$ and possibly $d = e_t$), and very smooth.

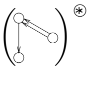
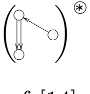
Conjecture 9.3. *Let G be a permutation group, and $(\theta_1, \dots, \theta_m)$ be a system of parameters of $I(G)$. Then, the generating series of the secondary invariants is unimodal, except for $d = 0$ and possibly $d = e_t$.*

We recall that this series can be computed directly from the Hilbert series. Therefore a careful study of the Hilbert series might yield a simple proof of this conjecture.

10 The invariant ring over digraphs

In [14], Grigoriev introduced a related invariant ring, the *invariant ring over digraphs* (digraphs are directed graphs, with loops). The definition is similar to the one for the invariant ring over graphs, but there are n^2 variables $(x_{1,1}, x_{1,2}, \dots, x_{n,n})$, indexed by the pairs (i,j) of $\{1, \dots, n\}$. The action of $\mathfrak{S}_n$ is then defined by $\sigma \cdot x_{i,j} := x_{\sigma(i),\sigma(j)}$. In this section, we denote by $\overrightarrow{\mathcal{I}_n}$ the invariant ring over *digraphs*. More generally, Grigoriev defined the invariant ring over oriented k-hypergraphs, with n^k variables indexed by k-uples of $\{1, \dots, n\}$.

Lemma 1 of [14] states that $\overrightarrow{\mathcal{I}_n}$ is generated by the invariants $\mathbf{x}^{\mathbf{g}^{\circledast}}$, where $\mathbf{g}$ is a simple digraph. The proof is said to be an easy generalization of the usual proof of the fundamental theorem of symmetric functions. This surprised us, since we proved this was false in $\mathcal{I}_n$ (theorem 2.3 (ii)). Therefore, we checked the condition 1.2, which failed even for $n = 3$ and degree 5. We then ran PerMuVAR to try to compute a minimal generating set using only simple digraphs. It failed as expected, and produced the two following very small invariants, which are not generated by simple digraphs:

()$^{\circledast}$, ()$^{\circledast}$.

These counter-examples to lemma 1 of [14] can also easily be checked by hand.

This was disappointing. Indeed, the invariant ring $\mathcal{I}_n$ is the quotient ring of $\overrightarrow{\mathcal{I}_n}$ by the ideal generated by $x_{i,i} = 0$ and $x_{i,j} = x_{j,i}$. Therefore, we could have used lemma 1 to prove that $\mathcal{I}_n$ is generated by the invariants where each variable appears with degree at most 2. This would provide a pretty good degree bound $\beta(\mathcal{I}_n) \leq 2\binom{n}{2}$. Moreover, we could use this together with computations of partial minimal generating sets to prove that $\mathcal{I}_5$ is generated by the invariants $\mathbf{x}^{\mathbf{g}^{\circledast}}$, where $\mathbf{g}$ is a multigraph with at least one isolated vertex, result of interest for the reconstruction problem.

Most of the results on $\mathcal{I}_n$ apply as well for $\overrightarrow{\mathcal{I}_n}$, but since the number of variables is greater, the computations are even harder than for $\mathcal{I}_n$, even if we ignore loops.

11 The field of invariant fractions

The *field of invariants* $\mathbb{K}(x_{\{i,j\}})^{\mathfrak{S}_n}$ is the subfield of all rational fractions of $\mathbb{K}(x_{\{i,j\}})$ which remain invariant under the action of the group. The following classical lemma is valid for any finite group of matrices.

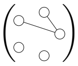
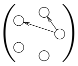
Lemma 11.1. *The field of invariant is exactly the field of fractions of the invariant ring.*

Proof. By averaging over the group, write any invariant fraction as $\frac{p}{q}$ where p and q are invariant polynomials. □

In [14], Grigoriev used basic Galois theory to prove the existence of a generating set of the field of invariants composed of $m + 1$ invariants of degree less than m. The principle is to first take the m elementary symmetric polynomials, and to consider the subfield of symmetric fractions. Since the ground field $\mathbb{K}$ has characteristic zero (this would be also the case for any normal ground field, like a finite field), the primitive element theorem applies: there exist a primitive element p which generates the field of invariants over the field of symmetric fractions. Therefore, the m elementary symmetric polynomials together with p generates the field of invariants.

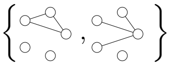
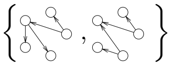
However, Grigoriev did not provide a way to construct such an element. Moreover, the proof that it could be chosen of degree less than m was incorrect, since it relied on lemma 1 of [14] which we disproved in § 10.

Theorem 11.2. *Let $n \geq 4$. The field of invariants over graphs (respectively over digraphs) is generated by the elementary symmetric polynomials together with:*

$p :=$ ()$^{\circledast}$, *respectively* $p :=$ ()$^{\circledast}$.

Proof. Key fact: in both cases a permutation of the edges belongs to the group if and only if it leaves p invariant. □

Grigoriev also stated that such a generating set would be a complete system of invariants. This is incorrect since, unlike a generating set of the field of the invariant ring, a generating set of the field of fraction is not necessarily a complete system of invariants. For example, our generating sets do not separate the following pairs of non-isomorphic graphs:

{  } ; {  }.

In some cases, the field of invariants can be used to indirectly apply Galois theory on the invariant ring.

Theorem 11.3. *If $n \neq 4, 5, 6, 8$, there is no intermediate invariant ring of matrix group between the ring of symmetric polynomials (respectively the ring of alternate polynomials for n even) and the ring of invariants $\mathcal{I}_n$.*

Proof. For $n \neq 4, 5, 6, 8$, the group $\mathcal{G}_n$ is a maximal proper subgroup of the symmetric group $\mathfrak{S}_m$ (respectively the alternate group $\mathcal{A}_m$ for n even) [8]. Basic Galois theory then proves the theorem for the field of invariants, and lemma 11.1 transfers it back to the invariant ring. □

12 Conclusion

Invariant theory provides both very general tools and algorithms to study the invariant ring $\mathcal{I}_n$ over graphs. Unfortunately, the computer exploration of small cases appears to be very hard and shows that those tools and algorithms lack accuracy and efficiency for our particular invariant ring. However, we could still obtain a few results, formulate conjectures related to $\mathcal{I}_n$, and solve a problem arising from graph theory.

Acknowledgments

This research was partially funded by the Région Rhône-Alpes. We gratefully thank A. Garsia, J-C. Faugère and N. Wallach for the time invested trying to compute a Gröbner basis for conjecture 4.2. In particular, discussions with A. Garsia where very helpful, and raised decisive ideas. Finally, we would like to thank M. Pouzet for introducing and guiding us through this beautiful subject.

References

[1] Aslaksen, H., Chan, S.-P., and Gulliksen, T. Invariants of S_4 and the shape of sets of vectors. *Appl. Algebra Engrg. Comm. Comput. 7*, 1 (1996), 53–57.

[2] Bondy, J. A. A graph reconstructor's manual. In *Surveys in combinatorics, 1991 (Guildford, 1991)*, vol. 166 of *London Math. Soc. Lecture Note Ser.* Cambridge Univ. Press, Cambridge, 1991, pp. 221–252.

[3] Cameron, P. J. Stories from the age of reconstruction. *Congr. Numer. 113* (1996), 31–41. Festschrift for C. St. J. A. Nash-Williams.

[4] Capani, A., Niesi, G., and Robbiano, L. Cocoa, a system for doing computations in commutative algebra. Available via anonymous ftp from: cocoa.dima.unige.it.

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

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

[7] Dixmier, J. Sur les invariants du groupe symétrique dans certaines représentations. II. In *Topics in invariant theory (Paris, 1989/1990)*, vol. 1478 of *Lecture Notes in Math.* Springer, Berlin, 1991, pp. 1–34.

[8] Faradzev, I. A., Ivanov, A. A., Klin, M. H., and Woldar, A. J., Eds. *Investigations in algebraic theory of combinatorial objects.* Kluwer Academic Publishers Group, Dordrecht, 1994.

[9] Faugère, J.-C. A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure Appl. Algebra 139*, 1-3 (1999), 61–88. Effective methods in algebraic geometry (Saint-Malo, 1998).

[10] Fulton, W., and Harris, J. *Representation theory*, vol. 129 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1991 - 1996. A first course, Readings in Mathematics.

[11] Garsia, A. M., and Stanton, D. Group actions of Stanley - Reisner rings and invariants of permutation groups. *Adv. in Math. 51*, 2 (1984), 107–201.

[12] Garsia, A. M., and Wallach, N. Personnal communication, Feb. 1999.

[13] Göbel, M. A constructive description of SAGBI bases for polynomial invariants of permutation groups. *J. Symbolic Comput. 26*, 3 (1998), 261–272.

[14] Grigoriev, D. J. Two reductions of the graph isomorphism to problems for polynomials. *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) 88* (1979), 56–61, 237–238. Studies in constructive mathematics and mathematical logic, VIII.

[15] Harary, F., and Palmer, E. M. *Graphical enumeration.* Academic Press, New York, 1973.

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

[17] Kemper, G. Computational invariant theory. *Queen's Papers in Pure and Applied Math.* (Feb. 1998).

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

[19] Kocay, W. L. Some new methods in reconstruction theory. In *Combinatorial mathematics, IX (Brisbane, 1981).* Springer, Berlin, 1982, pp. 89–114.

[20] Mallows, C. L., and Sloane, N. J. A. On the invariants of a linear group of order 336. *Proc. Cambridge Philos. Soc. 74* (1973), 435–440.

[21] Pouzet, M. Quelques remarques sur les résultats de Tutte concernant le problème de Ulam. *Publ. Dép. Math. (Lyon) 14*, 2 (1977), 1–8.

[22] Pouzet, M. Note sur le problème de Ulam. *J. Combin. Theory Ser. B 27*, 3 (1979), 231–236.

[23] Pouzet, M., and Thiéry, N. M. Algebraic invariants of graphs and reconstruction. *Discrete Mathematics* (2001). In preparation.

[24] Robbiano, L., and Sweedler, M. Subalgebra bases. In *Commutative algebra (Salvador, 1988).* Springer, Berlin, 1990, pp. 61–87.

[25] Schmid, B. J. Finite groups and invariant theory. In *Topics in invariant theory (Paris, 1989/1990)*. Springer, Berlin, 1991, pp. 35–66.

[26] Smith, L. Polynomial invariants of finite groups. A survey of recent developments. *Bull. Amer. Math. Soc. (N.S.) 34*, 3 (1997), 211–250.

[27] Stanley, R. P. Invariants of finite groups and their applications to combinatorics. *Bull. Amer. Math. Soc. (N.S.) 1*, 3 (1979), 475–511.

[28] Stanley, R. P. Log-concave and unimodal sequences in algebra, combinatorics, and geometry. In *Graph theory and its applications: East and West (Jinan, 1986)*. New York Acad. Sci., New York, 1989, pp. 500–535.

[29] Sturmfels, B. *Algorithms in invariant theory.* Springer-Verlag, Vienna, 1993.

[30] Thiéry, N. M. *Invariants algébriques de graphes et reconstruction; une étude expérimentale.* PhD thesis, Université Lyon I, June 1999. N° d'ordre: 167-99.

[31] Thiéry, N. M. Computing minimal generating sets of invariant rings of permutation groups with SAGBI-Gröbner basis. In *International conference DM-CCG, Discrete Models - Combinatorics, Computation and Geometry, Paris, July 2-5 2001* (2001). Submitted.

[32] Thiéry, N. M. `PerMuVAR`, a library for computing in invariant rings of permutation groups. *Journal of Symbolic Computations* (2001). In preparation.