Algorithms for fundamental invariants and equivariants

Evelyne Hubert, Erick Rodriguez Bazan

Algorithms for fundamental invariants and equivariants
(of finite groups)

Evelyne Hubert*[1,2] and Erick Rodriguez Bazan[1,2]

[1]Université Côte d'Azur, France
[2]Inria Méditerranée, France

Abstract

For a finite group, we present three algorithms to compute a generating set of invariant simultaneously to generating sets of basic equivariants, *i.e.,* equivariants for the irreducible representations of the group. The first construction applies solely to reflection groups and consists in applying symmetry preserving interpolation, as developed by the same authors, along an orbit in general position. The second algorithm takes as input primary invariants and the output provides not only the scondary invariants but also free bases for the modules of basic equivariants. The third algorithm proceeds degree by degree, determining the fundamental invariants as forming the H-basis of the ideal of the Nullcone, and the fundamental equivariants as constituting the symmetry adapted basis of an invariant complement. Remarkably, the here presented algorithms are the very first algorithms to compute both the fundamental invariants and the fundamental equivariants simultaneously. Fundamental equivariants allow to assemble symmetry adapted bases of higher degrees, and these are essential ingredients in exploiting and preserving symmetry in computations. They appear within algebraic computation and beyond, in physics, chemistry and engineering.

Keywords: finite groups; representation theory; polynomial invariants; equivariants; symmetry adapted bases; H-basis. **MSC:** 13A50 20C30 68W30 13P10

Contents

*Evelyne.Hubert@inria.fr

1 Introduction

Symmetry is ubiquitous in science and art and underlies a number of mathematical endeavors as for instance invariant theory and representation theory. Preserving and exploiting symmetry in computations has relied on both the use of invariants, and equivariants, as well as symmetry adapted bases of polynomial rings. They are relevant in combinatorics [Sta79, TY93], dynamical systems [CL00, Gat00, GSS88], cryptography [LRS16, Mes91], global optimization [GP04, RTAL13], cubatures and multivariate interpolation [CH15, RH21, RH22], solving polynomial systems [FR09, FS13, Gat90, HL12, HL16], and more widely in physics, chemistry, and engineering [FS92, MZ01, MZF92]. Symmetry adapted bases are made of *basic equivariants*, and these form finitely generated modules over the invariant ring. The purpose of this article is to offer algorithms to compute relevant sets of generators of these modules, together with generators for the ring of invariants. We shall call these generators the *fundamental equivariants and invariants*.

One can always compute symmetry adapted bases of polynomial rings degree by degree with linear algebra operations thanks to explicit projection operators [Ser77]. More efficient generative approaches are desirable. Symmetry adapted bases were formed combinatorially for some classical families of finite groups [ATY97, Spe35] or are determined explicitly for some representations of relevance in applications, as for instance [CCP08, CCDP15, DPZ15, FK77, Mug72].

The computation of invariants of group actions has been an active topic since the 19th century. Celebrated mathematicians have left their marks on the subject and textbooks reporting major progress still appeared relatively recently [DK15, Stu07]. Semi-invariants and equivariants may appear in the construction of invariants [GY03, GHP19] and are sometimes more pertinent or simpler to work with. Despite their relevance, the few algorithms to compute equivariants [Gat96, Sta79] are not as well developed.

As any polynomial equivariant can be written in terms of basic equivariants, *i.e.,* equivariants for the irreducible representations of the group, our algorithms thus fill a void in the subject. The fundamental equivariants appear as symmetry adapted bases of an invariant complement, in the polynomial ring, of an ideal generated by invariants.

We develop three algorithms. The first one applies to reflection groups. These latter enjoy extensive properties [BG85, Che55, Kan01]. The fundamental invariants are then algebraically independent and the fundamental equivariants are free bases of the modules of basic equivariants, over the ring of invariants. Their computation can be approached either as $\mathfrak{G}$-harmonic polynomials or from the cyclic structure of the covariant algebra. Yet it is a rather remarkable observation that the invariants and equivariants can simply be obtained as a direct application of symmetry preserving ideal interpolation as developed in [RH22]. Interpolating along an orbit in general position : the fundamental equivariants are read from the basis of the interpolation space, while the invariants are read from the H-basis of the ideal of the orbit. It is this original idea that we expanded on to compute the fundamental invariants and equivariants of any finite groups.

The second construction, in essence, takes as input a set of primary invariants $h_1, \dots, h_n$ and computes a set of secondary invariants together with basic equivariants that form free bases for their modules over $\mathbb{C}[h_1, \dots, h_n]$. This provides us with a Hironaka decomposition of the polynomial ring and hence this may be the most practical set of fundamental invariants and equivariants to assemble higher degree symmetry adapted bases.

The third algorithm computes simultaneously minimal sets of fundamental invariants and equivariants. It constructs, degree by degree, a H-basis of the Nullcone ideal. This H-basis forms a minimal set of fundamental invariants. The fundamental equivariants form a symmetry adapted basis of an invariant complement of the Nullcone ideal and this basis is contructed alongside degree by degree. Dividing the size of the matrices involved in the linear algebra operations at each degree is key to the efficiency of the algorithm. This is obtained by examining the equivariance of the underlying maps and using symmetry adapted bases: the matrices are then block diagonal and intrisic redundancies are disclosed. As King's algorithm (2013) to compute invariants (solely) this algorithm foregoes the use of Molien's series found in earlier algorithms.

All three algorithms rely on the knowledge of symmetry adapted bases of polynomials up to some degree. In return, we can identify fundamental equivariants and thus higher degree symmetry adapted bases can be assembled easily, without resorting to projection operators. This assembly is particularly straightforward with the output of the first and second algorithm when we have a Hironaka decomposition of the polynomial ring.

Section 2 formalizes the link between symmetry adapted bases and fundamental equivariants. In Section 3 we recall the premises of our algorithms: zero dimensional ideals, interpolation and H-bases. In Section 4, we show that the symmetry preserving ideal interpolation algorithm in [RH22] can be straightforwardly applied to compute the fundamental invariants and equivariants of a reflection group. In Section 5, given a set of primary invariants (or superset of these) $\{h_1, \ldots, h_n\}$, we apply the algorithms in [RH21, RH22] to compute both a set of secondary invariants and free bases of basic equivariants, then seen as $\mathbb{C}[h_1, \ldots, h_n]$-modules. The ideas of these two constructions brings us, in Section 6, to an independent algorithm to compute simultaneously minimal sets of fundamental invariants and equivariants for any finite group. The examples we present all along the paper were computed with our implementation in Maple of the algorithms presented.

The base field in this paper is $\mathbb{C}$ for simplicity of presentation. The algorithms can be extended to work over $\mathbb{R}$ or any other subfield of $\mathbb{C}$. As discussed in the conclusion, the constructions can also be adapted to any field the characteristic of which does not divide the order of the group (a.k.a. the non modular case).

2 Symmetry adapted bases and basic equivariants

Symmetry adapted bases are an essential tool to take advantage of symmetry in algebraic computations; the main reason for that is the fact that the matrix of a $\mathfrak{G}$-morphism is block diagonal in symmetry adapted bases [FS92]. In polynomial rings, symmetry adapted bases can be understood to consist of *basic* equivariants. Basic equivariants form modules over the invariant ring which allows for finite presentation. We recall these notions, their connections, and preliminary results about them.

We deal with a finite group $\mathfrak{G}$. We note $\mathfrak{r}^{(1)}, \ldots, \mathfrak{r}^{(\mathfrak{n})}$ the inequivalent irreducible matrix representations of $\mathfrak{G}$ over $\mathbb{C}$; $\mathfrak{n}_\ell$ the dimension of $\mathfrak{r}^{(\ell)}$. All along the article $\mathfrak{r}^{(1)}$ is understood to be the trivial representation.

2.1 Symmetry adapted bases

A representation $\mathfrak{r} : \mathfrak{G} \to \mathrm{GL}(V)$, where V is a m-dimensional $\mathbb{C}$-vector space, can be decomposed into irreducible representations, $\mathfrak{r} = m_1\mathfrak{r}^{(1)} \oplus \ldots \oplus m_\mathfrak{n}\mathfrak{r}^{(\mathfrak{n})}$. Hence, the representation space V admits a basis in which the representation matrices are $\operatorname{diag}\left(\mathrm{I}_{m_\ell} \otimes \mathfrak{r}^{(\ell)}(g) \mid 1 \le \ell \le \mathfrak{n}\right)$, for $g \in \mathfrak{G}$. Assume that

$$\mathcal{Q} = \bigcup_{\ell=1}^{\mathfrak{n}} \mathcal{Q}^{(\ell)}, \text{ with } \mathcal{Q}^{(\ell)} = \left\{\left[q_{i1}^{(\ell)}, \ldots, q_{i\mathfrak{n}_\ell}^{(\ell)}\right] \mid 1 \le i \le m_\ell\right\} \tag{1}$$

is such a basis. A *symmetry adapted basis* is then obtained by reordering the components of $\mathcal{Q}^{(\ell)}$ as $\left\{\left[q_{1j}^{(\ell)}, \ldots, q_{m_\ell j}^{(\ell)}\right] \mid 1 \le j \le \mathfrak{n}_\ell\right\}$. One then shows, as a consequence of Schur's lemma, that the matrix of an equivariant endomorphism in a symmetry adapted basis is block diagonal, with blocks of size m_ℓ appearing with multiplicity $\mathfrak{n}_\ell$ [FS92]. Despite this fact, in this paper it is more practical to present the symmetry adapted bases as in (1) though this differs from the convention adopted in [RH21, RH22] that we shall refer to.

The decomposition into irreducible representations is not unique but the decomposition into *isotypic components* is canonical: $V = \bigoplus_{\ell=1}^{n} V^{(\ell)}$ where $V^{(\ell)}$ is equivalent to m_ℓ times the irreducible representation $\mathfrak{r}^{(\ell)}$.

The *character* of $\mathfrak{r}$ is the function $\chi : \mathfrak{G} \to \mathbb{C}$ given $\chi(g) = \mathrm{trace}(\mathfrak{r}(g))$. If $\chi^{(\ell)}$ is the character of $\mathfrak{r}^{(\ell)}$ we have:

$$m_\ell = \frac{1}{|\mathfrak{G}|} \sum_{g \in \mathfrak{G}} \chi^{(\ell)}(g^{-1})\, \chi(g)$$

and a projection on $V^{(\ell)}$ is given by [Ser77, Chapter 2]:

$$\begin{array}{rccl} \pi^{(\ell)} : & V & \to & V^{(\ell)} \\ & v & \mapsto & \sum_{g \in \mathfrak{G}} \chi^{(\ell)}(g^{-1})\, \mathfrak{r}(g)(v). \end{array}$$

The construction of a symmetry adapted basis is basically given by [Ser77, Chapter 2, Proposition 8] that we reproduce here for ease of reference.

Proposition 2.1 *The linear maps $\pi_{ij}^{(\ell)} : V \to V$, for $1 \le i, j \le \mathfrak{n}_\ell$, defined by*

$$\pi_{ij}^{(\ell)}(v) = \sum_{g \in \mathfrak{G}} [\mathfrak{r}^{(\ell)}(g^{-1})]_{ji}\, \mathfrak{r}(g)(v)$$

satisfy the following properties:

1. *For every $1 \le i \le \mathfrak{n}_\ell$, the map $\pi_{ii}^{(\ell)}$ is a projection; it is zero on the isotypic components $V^{(k)}$, $k \ne \ell$. Its image $V^{(\ell,i)}$ is contained in $V^{(\ell)}$ and*

$$V^{(\ell)} = V^{(\ell,1)} \oplus \cdots \oplus V^{(\ell,\mathfrak{n}_\ell)} \quad \text{while} \quad \pi^{(\ell)} = \sum_{i=1}^{\mathfrak{n}_\ell} \pi_{ii}^{(\ell)}. \tag{2}$$

2. *For every $1 \le i, j \le \mathfrak{n}_\ell$, the linear map $\pi_{ij}^{(\ell)}$ is zero on the isotypic components $V^{(k)}$, $k \ne \ell$, as well as on the subspaces $V^{(\ell,k)}$ for $k \ne j$; it defines an isomorphism from $V^{(\ell,j)}$ to $V^{(\ell,i)}$.*

3. *For any $v \in V$ and $1 \le k \le \mathfrak{n}_\ell$ consider $v_i = \pi_{ik}^{(\ell)}(v) \in V^{(\ell,i)}$ for all $1 \le i \le \mathfrak{n}_\ell$. If nonzero, $v_1, \ldots, v_{\mathfrak{n}_\ell}$ are linearly independent and generate an invariant subspace of dimension $\mathfrak{n}_\ell$. For each $g \in \mathfrak{G}$, we have*

$$\mathfrak{r}(g)(v_j) = \sum_{i=1}^{\mathfrak{n}_\ell} \mathfrak{r}_{ij}^{(\ell)}(g)(v_i) \quad \forall i, j = 1, \ldots, \mathfrak{n}_\ell.$$

If the representation $\mathfrak{r}$ is actually defined over $\mathbb{R}$, we can also compute real symmetry adapted bases whose components are in correspondence with the irreducible representations over $\mathbb{R}$. This can be obtained by combining conjugate pairs of irreducible representations over $\mathbb{C}$ and is detailed for instance in [RH21].

2.2 Equivariants

The representation space we are concerned with in this section is the polynomial ring in n variables $\mathbb{C}[\mathrm{x}] = \mathbb{C}[x_1, \ldots, x_n]$. We consider the representation $\rho : \mathfrak{G} \to \mathrm{GL}(\mathbb{C}[\mathrm{x}])$ induced by a representation $\varrho : \mathfrak{G} \to \mathbb{C}^n$, *i.e.*, $\rho(g)(p) = p \circ \varrho(g^{-1})$, for $p \in \mathbb{C}[\mathrm{x}]$, $g \in \mathfrak{G}$. For a row vector $\mathrm{q} = [q_1, \ldots, q_m] \in \mathbb{C}[\mathrm{x}]^m$ of polynomials we write $\rho(g)(\mathrm{q})$ for the row vector $[\rho(g)(q_1), \ldots, \rho(g)(q_m)] \in \mathbb{C}[\mathrm{x}]^m$.

The representation $\rho : \mathfrak{G} \to \mathrm{GL}(\mathbb{C}[\mathrm{x}])$ leaves invariant the finite dimensional subspace $\mathbb{C}[\mathrm{x}]_d$ spanned by the homogeneous polynomials of degree d. The isotypic components of $\mathbb{C}[\mathrm{x}]_d$ are denoted $\mathbb{C}[\mathrm{x}]_d^{(\ell)}$. We write

$$\mathbb{C}[\mathrm{x}] = \bigoplus_{d \in \mathbb{N}} \mathbb{C}[\mathrm{x}]_d = \bigoplus_{d \in \mathbb{N}} \bigoplus_{\ell=1}^{\mathfrak{n}} \mathbb{C}[\mathrm{x}]_d^{(\ell)}, \qquad \mathbb{C}[\mathrm{x}]^{(\ell)} = \bigoplus_{d \in \mathbb{N}} \mathbb{C}[\mathrm{x}]_d^{(\ell)}, \qquad \mathbb{C}[\mathrm{x}] = \bigoplus_{\ell=1}^{\mathfrak{n}} \mathbb{C}[\mathrm{x}]^{(\ell)};$$

and

$$\mathbb{C}[\mathrm{x}]_d^{(\ell)} = \bigoplus_{i=1}^{\mathfrak{n}_\ell} \mathbb{C}[\mathrm{x}]_d^{(\ell,i)}, \qquad \mathbb{C}[\mathrm{x}]^{(\ell,i)} = \bigoplus_{d\in\mathbb{N}} \mathbb{C}[\mathrm{x}]_d^{(\ell,i)}, \qquad \mathbb{C}[\mathrm{x}]^{(\ell)} = \bigoplus_{i=1}^{\mathfrak{n}_\ell} \mathbb{C}[\mathrm{x}]^{(\ell,i)}.$$

An *invariant polynomial*, or simply *invariant*, is a polynomial $p \in \mathbb{C}[\mathrm{x}]$ such that $\rho(g)(p) = p$ for all $g \in \mathfrak{G}$. The $\mathbb{C}$-vector space of invariants is $\mathbb{C}[\mathrm{x}]^{(1)}$. But the invariants also form a ring, which is denoted $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$. The infinite dimensional isotypic components $\mathbb{C}[\mathrm{x}]^{(\ell)}$, and their components $\mathbb{C}[\mathrm{x}]^{(\ell,i)}$, are $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-modules: if $p \in \mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$, then $\pi_{ij}^{(\ell)}(pq) = p\,\pi_{ij}^{(\ell)}(q)$ for any $q \in \mathbb{C}[\mathrm{x}]$.

More generally, if $\mathfrak{r} : \mathfrak{G} \to \mathrm{GL}_m(\mathbb{C})$ is a m-dimensional matrix representation of $\mathfrak{G}$, an $\mathfrak{r}$*-equivariant* is a row vector $\mathrm{q} \in \mathbb{C}[\mathrm{x}]^m$ such that $\rho(g)(\mathrm{q}) = \mathrm{q}\,\mathfrak{r}(g)$, where the left-hand side is a vector-matrix multiplication. The set of all $\mathfrak{r}$-equivariants forms a $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-module that we denote $\mathbb{C}[\mathrm{x}]_{\mathfrak{r}}^{\mathfrak{G}}$. A set of $\mathfrak{r}$-equivariants $\mathcal{Q} = \{\mathrm{q}_1, \dots, \mathrm{q}_m\}$ is generating for $\mathbb{C}[\mathrm{x}]_{\mathfrak{r}}^{\mathfrak{G}}$ as a $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-module if any other $\mathfrak{r}$-equivariant q can be written as a linear combination of elements of $\mathcal{Q}$ over $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$: $\mathrm{q} = a_1\,\mathrm{q}_1 + \dots + a_m\,\mathrm{q}_m$, with $a_i \in \mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$.

We call *basic equivariant* an $\mathfrak{r}^{(\ell)}$-equivariant, for some $1 \le \ell \le \mathfrak{n}$. Hence a symmetry adapted basis of any invariant subspace of $\mathbb{C}[\mathrm{x}]$ consists of basic equivariants. Furthermore the $\mathfrak{r}$-equivariants, for any matrix representation $\mathfrak{r} : \mathfrak{G} \to \mathrm{GL}_m(\mathbb{C})$, are linear combinations of basic equivariants. Indeed, let $\mathrm{q} \in \mathbb{C}[\mathrm{x}]^m$ be an $\mathfrak{r}$-equivariant and $\mathrm{P} \in \mathbb{C}^{m\times m}$ be an invertible matrix such that $\mathrm{P}^{-1}\,\mathfrak{r}(g)\,\mathrm{P} = \mathrm{diag}\left(I_{m_\ell} \otimes \mathfrak{r}^{(\ell)}(g) \mid 1 \le \ell \le \mathfrak{n}\right)$ for all $g \in \mathfrak{G}$. Then $\mathrm{q}\,\mathrm{P}$ is a $(m_1\mathfrak{r}^{(1)} \oplus \dots \oplus m_{\mathfrak{n}}\mathfrak{r}^{(\mathfrak{n})})$-equivariant, *i.e.,* its components are basic equivariants.

Sets $\mathcal{Q}^{(1)}$ of invariants and $\mathcal{Q}^{(\ell)}$, $2 \le \ell \le \mathfrak{n}$, of $\mathfrak{r}^{(\ell)}$-equivariants are called *fundamental* if they generate, repectively, the ring $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$ and the $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-modules $\mathbb{C}[\mathrm{x}]_{\mathfrak{r}^{(\ell)}}^{\mathfrak{G}}$.

We conclude this section by formalizing the correspondances between the $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-modules $\mathbb{C}[\mathrm{x}]_{\mathfrak{r}^{(\ell)}}^{\mathfrak{G}}$ and the isotypic components $\mathbb{C}[\mathrm{x}]^{(\ell)}$ of $\mathbb{C}[\mathrm{x}]$. On then sees that a set of fundamental equivariants generates $\mathbb{C}[\mathrm{x}]$ as a $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-module.

Proposition 2.2 *For $1 \le \ell \le \mathfrak{n}$ and any $1 \le k \le \mathfrak{n}_\ell$, the $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-linear maps*

$$\begin{array}{rccc} \phi_k : & \mathbb{C}[\mathrm{x}]_{\mathfrak{r}^{(\ell)}}^{\mathfrak{G}} & \to & \mathbb{C}[\mathrm{x}]^{(\ell,k)} \\ & [q_1, \dots, q_{\mathfrak{n}_\ell}] & \mapsto & q_k \end{array} \qquad \textit{and} \qquad \begin{array}{rccc} \Phi_k : & \mathbb{C}[\mathrm{x}]^{(\ell,k)} & \to & \mathbb{C}[\mathrm{x}]_{\mathfrak{r}^{(\ell)}}^{\mathfrak{G}} \\ & q & \mapsto & \left[\pi_{1k}^{(\ell)}(q), \dots, \pi_{\mathfrak{n}_\ell k}^{(\ell)}(q)\right] \end{array}$$

are well defined and inverse of each other.

PROOF: The fact that ϕ_k and Φ_k are $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-linear is an easy observation from the definition of the maps $\pi_{ji}^{(\ell)}$. We first show that the images of ϕ_k and Φ_k are correctly described.

Let $\mathrm{q} = [q_1, \dots, q_{\mathfrak{n}_\ell}]$ be an $\mathfrak{r}^{(\ell)}$-equivariant. By definition of equivariance $\mathrm{q} = \rho(g)(\mathrm{q})\,\mathfrak{r}^{(\ell)}(g)^{-1}$. Hence

$$\mathrm{q} = [\rho(g)(q_1), \dots, \rho(g)(q_{n_\ell})]\,\mathfrak{r}^{(\ell)}(g^{-1}) = \left[\sum_{j=1}^{\mathfrak{n}_\ell} \mathfrak{r}_{j1}^{(\ell)}(g^{-1})\rho(g)(q_j), \dots, \sum_{j=1}^{\mathfrak{n}_\ell} \mathfrak{r}_{j\mathfrak{n}_\ell}^{(\ell)}(g^{-1})\rho(g)(q_j)\right].$$

Summing over $g \in \mathfrak{G}$ we see

$$|\mathfrak{G}|\,\mathrm{q} = \left[\sum_{j=1}^{\mathfrak{n}_\ell}\sum_{g\in\mathfrak{G}} \mathfrak{r}_{j1}^{(\ell)}(g^{-1})\rho(g)(q_j), \dots, \sum_{j=1}^{\mathfrak{n}_\ell}\sum_{g\in\mathfrak{G}} \mathfrak{r}_{j\mathfrak{n}_\ell}^{(\ell)}(g^{-1})\rho(g)(q_j)\right] = \frac{|\mathfrak{G}|}{\mathfrak{n}_\ell}\left[\sum_{j=1}^{\mathfrak{n}_\ell} \pi_{1j}^{(\ell)}(q_j), \dots, \sum_{j=1}^{\mathfrak{n}_\ell} \pi_{\mathfrak{n}_\ell j}^{(\ell)}(q_j)\right].$$

Since $\pi_{jk}^{(\ell)} \circ \pi_{kl}^{(\ell)} = \pi_{jl}^{(\ell)}$ we can write

$$\mathrm{q} = \frac{1}{\mathfrak{n}_\ell}\left[\sum_{j=1}^{\mathfrak{n}_\ell} \pi_{11}^{(\ell)} \circ \pi_{1j}^{(\ell)}(q_j), \dots, \sum_{j=1}^{\mathfrak{n}_\ell} \pi_{\mathfrak{n}_\ell 1}^{(\ell)} \circ \pi_{1j}^{(\ell)}(q_j)\right] = \left[\pi_{11}^{(\ell)}(\hat{q}), \dots, \pi_{\mathfrak{n}_\ell 1}^{(\ell)}(\hat{q})\right], \tag{3}$$

where $\hat{q} = \frac{1}{\mathfrak{n}_\ell}\sum_{j=1}^{\mathfrak{n}_\ell}\pi_{1j}^{(\ell)}(q_j)$. It follows that $\phi_k(\mathrm{q}) \in \mathbb{C}[\mathrm{x}]^{(\ell,k)}$.

Now let $q \in \mathbb{C}[\mathrm{x}]^{(\ell,k)}$. By Proposition 2.1.3 we have $\rho(g)\left(\pi_{jk}^{(\ell)}(q)\right) = \sum_{i=1}^{n_\ell}\mathfrak{r}_{ij}^{(\ell)}(g)\pi_{ik}^{(\ell)}(q)$ so that

$$\rho(g)\left(\Phi_k(q)\right) = \left[\sum_{i=1}^{n_\ell}\mathfrak{r}_{i1}^{(\ell)}(g)\pi_{ik}^{(\ell)}(q), \dots, \sum_{i=1}^{n_\ell}\mathfrak{r}_{in_\ell}^{(\ell)}(g)\pi_{ik}^{(\ell)}(q)\right]$$

$$= \left[\pi_{1k}^{(\ell)}(q), \dots, \pi_{\mathfrak{n}_\ell k}^{(\ell)}(q)\right]\mathfrak{r}^{(\ell)}(g) = \Phi_k(q)\,\mathfrak{r}^{(\ell)}(g).$$

Hence $\Phi_k(q) \in \mathbb{C}[\mathrm{x}]_{\mathfrak{r}^{(\ell)}}^{\mathfrak{G}}$.

To conclude we show that $\phi_k \circ \Phi_k$ and $\Phi_k \circ \phi_k$ are the identity maps. Let $\mathrm{q} = [q_1, \dots, q_{n_\ell}] \in \mathbb{C}[\mathrm{x}]_{\mathfrak{r}^{(\ell)}}^{\mathfrak{G}}$. By Equation (3) there exists $\hat{q} \in \mathbb{C}[\mathrm{x}]$ such that $\mathrm{q} = \left[\pi_{11}^{(\ell)}(\hat{q}), \dots, \pi_{\mathfrak{n}_\ell 1}^{(\ell)}(\hat{q})\right]$. Hence $\Phi_k \circ \phi_k(\mathrm{q}) = \Phi_k\left(\pi_{k1}^{(\ell)}(\hat{q})\right) = \left[\pi_{1k}^{(\ell)} \circ \pi_{k1}^{(\ell)}(\hat{q}), \dots, \pi_{\mathfrak{n}_\ell k}^{(\ell)} \circ \pi_{k1}^{(\ell)}(\hat{q})\right] = \mathrm{q}$. If now $q \in \mathbb{C}[\mathrm{x}]^{(\ell,k)}$ then $\pi_{kk}^{(\ell)}(q) = q$ so that $\phi_k \circ \Phi_k(q) = q$. □

Corollary 2.3 *For $1 \le \ell \le \mathfrak{n}$, consider a set $\mathcal{Q} = \{\mathrm{q}_1, \dots, \mathrm{q}_m\}$ of $\mathfrak{r}^{(\ell)}$-equivariants, with $\mathrm{q}_i = [q_{i1}, \dots, q_{i\mathfrak{n}_\ell}]$. Considering $\mathbb{C}[\mathrm{x}]_{\mathfrak{r}^{(\ell)}}^{\mathfrak{G}}$, $\mathbb{C}[\mathrm{x}]^{(\ell,k)}$, and $\mathbb{C}[\mathrm{x}]^{(\ell)}$ as $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-modules, the following statements are equivalent:*

1. *$\mathcal{Q}$ is a generating set for $\mathbb{C}[\mathrm{x}]_{\mathfrak{r}^{(\ell)}}^{\mathfrak{G}}$*
2. *for any given $1 \le k \le \mathfrak{n}_\ell$, $\{q_{ik} \mid 1 \le i \le m\}$ is a generating set for $\mathbb{C}[\mathrm{x}]^{(\ell,k)}$*
3. *$\{q_{ik} \mid 1 \le k \le n_\ell,\ 1 \le i \le m\}$ is a generating set for $\mathbb{C}[\mathrm{x}]^{(\ell)}$.*

PROOF:
1. ⇒ 2. Let $q \in \mathbb{C}[\mathrm{x}]^{(\ell,k)}$. Since $\Phi_k(q) \in \mathbb{C}[\mathrm{x}]_{\mathfrak{r}^{(\ell)}}^{\mathfrak{G}}$, there exist $h_1, \dots, h_m \in \mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$ such that $\Phi_k(q) = \sum_{i=1}^m h_i \mathrm{q}_i$. Applying ϕ_k on both sides we obtain $q = \sum_{i=1}^m h_i \phi_k(\mathrm{q}_i) = \sum h_i q_{ik}$.

2. ⇒ 1. Take $\mathrm{q} \in \mathbb{C}[\mathrm{x}]_{\mathfrak{r}^{(\ell)}}^{\mathfrak{G}}$. Since $\phi_k(\mathrm{q}) \in \mathbb{C}[\mathrm{x}]^{(\ell,k)}$ there are invariant polynomials $h_1, \dots, h_m$ such that $\phi_k(\mathrm{q}) = \sum_{i=1}^m h_i q_{ik}$. Applying Φ_k on both sides we obtain $\mathrm{q} = \sum_{i=1}^m h_i \Phi_k(q_{ik})$ and therefore $\Phi_k(q_{1k}) = \mathrm{q}_1, \dots, \Phi_k(q_{mk}) = \mathrm{q}_m$ form a generating set for $\mathbb{C}[\mathrm{x}]_{\mathfrak{r}^{(\ell)}}^{\mathfrak{G}}$.

2. ⇒ 3. Since $\mathbb{C}[\mathrm{x}]^{(\ell)} = \bigoplus_{j=1}^{\mathfrak{n}_\ell}\mathbb{C}[\mathrm{x}]^{(\ell,j)}$, and $\pi_{jk}^{(\ell)} : \mathbb{C}[\mathrm{x}]^{(\ell,k)} \to \mathbb{C}[\mathrm{x}]^{(\ell,j)}$ is $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-linear and bijective, and $\pi_{jk}^{(\ell)}(q_{ik}) = q_{ij}$.

3. ⇒ 2. Since $\pi_{kk}^{(\ell)} : \mathbb{C}[\mathrm{x}]^{(\ell)} \to \mathbb{C}[\mathrm{x}]^{(\ell,k)}$ is $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-linear and surjective, and $\pi_{kk}^{(\ell)}(q_{ij})$ equals to q_{ik} or 0 according to whether $j = k$ or not. □

3 Zero dimensional ideals, H-bases and interpolation

This is a section with the premises for our constructions of fundamental invariants and equivariants. It somewhat recapitulates the ingredients and results of [RH21, RH22].

We consider the polynomial ring $\mathbb{C}[\mathrm{x}] = \mathbb{C}[x_1, \dots, x_n]$ in n variables and its subspaces $\mathbb{C}[\mathrm{x}]_d$ of homogeneous polynomials of degree d, and $\mathbb{C}[\mathrm{x}]_{\le d} = \oplus_{e=0}^d \mathbb{C}[\mathrm{x}]_e$.

3.1 Orthogonality

$\mathbb{C}[x]$ is naturally endowed with the *apolar product* that can be defined, for $p, q \in \mathbb{C}[x]$, as $\langle p, q\rangle = \bar{p}(\partial)q$. In the monomial basis, this is spelt out as $\langle \sum_\alpha p_\alpha x^\alpha, \sum_\alpha q_\alpha x^\alpha\rangle = \sum_\alpha \alpha! \bar{p}_\alpha q_\alpha$. If $\mathcal{P} = \{p_1, p_2, \ldots\}$ is a basis of $\mathbb{C}[x]$ we note $\mathcal{P}^\dagger$ the dual basis, that is, the basis $\{p_1^\dagger, p_2^\dagger, \ldots\}$ such that $\langle p_i^\dagger, p_j\rangle = \delta_{ij}$. For instance, the dual basis of the monomial basis $\{x^\alpha \,|\, \alpha \in \mathbb{N}^n\}$ is $\{\frac{1}{\alpha!}x^\alpha \,|\, \alpha \in \mathbb{N}^n\}$. The choice of the apolar product as the inner product is crucial to later exploit symmetry.

At many places we shall invoke the orthogonal complement of a subspace $Q = \langle q_1, \ldots, q_r\rangle$ in a subspace P of $\mathbb{C}[x]$ with basis $\mathcal{P} = \{p_1, p_2, \ldots p_m\}$. One way to compute it is to consider the matrix A whose columns are the coefficients of the q_i in $\mathcal{P}$. A nonzero row vector $[a_1, \ldots, a_m]$ is in the left kernel of A iff $\bar{a}_1\bar{p}_1^\dagger + \ldots + \bar{a}_m p_m^\dagger$ is in the orthogonal complement of Q in P. A basis for the left kernel of A is for instance obtained through a QR-decomposition [GVL96]. To avoid the notational complication between $\mathcal{P}$ and $\mathcal{P}^\dagger$, we shall mostly work with an orthonormal polynomial basis.

3.2 Zero-dimensional ideals and interpolation.

As expanded on in [CLO05], some properties of the variety of an ideal J in $\mathbb{C}[x]$ can be understood from the structure of the quotient algebra $\mathbb{C}[x]/J$. For instance, if $\mathbb{C}[x]/J$ is a finite dimensional $\mathbb{C}$-vector space then the variety of J consists only of points. Such ideals are said to be *zero-dimensional.* When appropriately counted with multiplicities, the number of these points is the dimension of $\mathbb{C}[x]/J$. A basis $\mathcal{Q}$ of a direct complement of J in $\mathbb{C}[x]$ can be identified with a basis of $\mathbb{C}[x]/J$.

We write $\mathbb{C}[x]^*$ for the set of linear forms on $\mathbb{C}[x]$. If r is the dimension of $\mathbb{C}[x]/J$ then J can be described as the orthogonal of a r-dimensional $\mathbb{C}$-vector subspace Λ of $\mathbb{C}[x]^*$ of dimension r: $J = \Lambda^\perp = \cap_{\lambda\in\Lambda} \ker \lambda$. We shall consider in this article two such descriptions.

First, when J is radical, its variety consists of r simple zeros $\xi_1, \ldots, \xi_r \in \mathbb{C}^n$. Then $J = \cap_{i=1}^r \ker \mathrm{e}_{\xi_i}$ where $\mathrm{e}_\xi : \mathbb{C}[x] \to \mathbb{C}$ is the evaluation at $\xi \in \mathbb{C}^n$.

The second scenario is when we have a basis $\mathcal{Q} = \{q_1, \ldots, q_r\}$ of a direct complement of J in $\mathbb{C}[x]$. This allows us to define uniquely $\lambda_1, \ldots, \lambda_r \in \mathbb{C}[x]^*$ by the equation:

$$p \equiv \lambda_1(p)q_1 + \ldots + \lambda_r(p)q_r \mod J, \qquad p \in \mathbb{C}[x].$$

Then $J = \Lambda^\perp$, where $\Lambda = \langle \lambda_1, \ldots, \lambda_r\rangle_{\mathbb{C}}$. This is in particular relevant when we have a Gröbner basis $\mathcal{B}$ of J, according to some term order. The terms $\mathcal{Q} = \{x^{\alpha_1}, \ldots, x^{\alpha_r}\}$ that are not multiples of the leading terms of $\mathcal{B}$ form a basis of $\mathbb{C}[x]/J$ and the associated forms $\lambda_1, \ldots, \lambda_r$ are computable by Hironaka division [CLO15].

Conversely, if Λ is a r-dimensional subspace of $\mathbb{C}[x]^*$ and $J = \cap_{\lambda\in\Lambda} \ker \lambda$ is an ideal, then [RH22, Section 2], $\mathcal{Q}$ is a basis of $\mathbb{C}[x]/J$ if and only if $\langle \mathcal{Q}\rangle_{\mathbb{C}}$ is an *interpolation space* for Λ, that is: for any linear map $\phi : \Lambda \to \mathbb{C}$, there is a single $q \in \langle \mathcal{Q}\rangle_{\mathbb{C}}$ such that $\lambda(p) = \phi(\lambda)$ for all $\lambda \in \Lambda$. In these conditions, the *least interpolation space* [DBR92, RH21], is the orthogonal complement of J^0 with respect to the apolar product [RH22, Proposition 2.7].

3.3 H-bases

On one hand, *Gröbner bases* are the most established and versatile representations of polynomial ideals [CLO15]. They are defined after a term order is fixed and one then focuses on the leading terms of the polynomials and the initial ideal of J. The basis of choice for $\mathbb{C}[x]/J$ then consists of the monomials. On the other hand, monomial bases are incompatible with most symmetries and hence we turn our attention to H-bases, where one focuses on the leading homogeneous forms instead of the leading terms. These were introduced in [Mac16] and revisited in [MS00].

For a nonzero polynomial p in $\mathbb{C}[\mathrm{x}]=\mathbb{C}[x_1,\ldots,x_n]$ we shall denote p^0 the *leading form* of p, *i.e.,* the homogeneous polynomial of $\mathbb{C}[\mathrm{x}]$ such that $\deg(p-p^0)<\deg(p)$. For a set $\mathcal{P}\subset\mathbb{C}[\mathrm{x}]$, $\mathcal{P}^0$ is the set of the leading forms of the elements in $\mathcal{P}$. If J is an ideal in $\mathbb{C}[\mathrm{x}]$, then J^0 is a homogeneous ideal in $\mathbb{C}[\mathrm{x}]$. We have $\dim\mathbb{C}[\mathrm{x}]/J=\dim\mathbb{C}[\mathrm{x}]/J^0$ and if $\mathcal{Q}$ is a linearly independent set of homogeneous polynomials s.t. $\mathbb{C}[\mathrm{x}]=J^0\oplus\langle\mathcal{Q}\rangle_{\mathbb{C}}$ then $\mathbb{C}[\mathrm{x}]=J\oplus\langle\mathcal{Q}\rangle_{\mathbb{C}}$ [MS00, Theorem 8.6].

Definition 3.1 *A finite set $\mathcal{H}:=\{h_1,\ldots,h_m\}\subset\mathbb{C}[\mathrm{x}]$ is a* H-basis *of the ideal $J:=\langle h_1,\ldots,h_m\rangle$ if one of the two equivalent conditions holds:*

- $J^0=\left\langle h_1^0,\ldots,h_m^0\right\rangle$;
- *for all $p\in J$, there exist $g_1,\ldots g_m$ such that* $p=\sum_{i=1}^{m}h_ig_i$ and $\deg(h_i)+\deg(g_i)\le\deg(p), i=1,\ldots,m.$

Any ideal has a finite H-basis since Hilbert basis theorem ensures that J^0 has a finite basis.

We shall now introduce the concepts of minimal, orthogonal and reduced H-basis.

Definition 3.2 *Given a row vector $\mathrm{h}=[h_1,\ldots,h_m]\in\mathbb{C}[\mathrm{x}]^m$ of homogeneous polynomials and a degree d, we define the Sylvester map to be the linear map*

$$\begin{array}{rccl}\psi_{d,\mathrm{h}}: & \mathbb{C}[\mathrm{x}]_{d-d_1}\times\ldots\times\mathbb{C}[\mathrm{x}]_{d-d_m} & \to & \mathbb{C}[\mathrm{x}]_d\\ & \mathrm{f}=[f_1,\ldots,f_m]^t & \to & \sum_{i=1}^{m}f_i\,h_i=\mathrm{h}\cdot\mathrm{f}\end{array}$$

where $d_1,\ldots,d_m$ are the respective degrees of $h_1,\ldots,h_m$. If $\mathcal{H}=\{h_1,\ldots,h_n\}$ then $\Psi_d(\mathcal{H})$ shall denote the image of $\psi_{d,\mathrm{h}}$, i.e.,

$$\Psi_d(\mathcal{H})=\left\{\sum_{i=1}^{m}f_i\,h_i\;\middle|\;f_i\in\mathbb{C}[\mathrm{x}]_{d-\deg(h_i)}\right\}\subset\mathbb{C}[\mathrm{x}]_d.$$

If $\mathcal{H}$ is a set of polynomials, we shall use the notation $\mathcal{H}_d^0$ for the set of the degree d elements of $\mathcal{H}^0$. In other words $\mathcal{H}_d^0=\mathcal{H}^0\cap\mathbb{C}[\mathrm{x}]_d$.

Definition 3.3 *We say that a H-basis $\mathcal{H}$ is minimal if, for any $d\in\mathbb{N}$, $\mathcal{H}_d^0$ is linearly independent and*

$$\Psi_d\left(J_{d-1}^0\right)\oplus\left\langle\mathcal{H}_d^0\right\rangle_{\mathbb{C}}=J_d^0. \tag{4}$$

When minimal, $\mathcal{H}$ is said to be orthogonal if $\left\langle\mathcal{H}_d^0\right\rangle_{\mathbb{C}}$ is the orthogonal complement of $\Psi_d\left(J_{d-1}^0\right)$ in J_d^0. Then the reduced *H-basis associated to $\mathcal{H}$ is defined by $\widetilde{\mathcal{H}}=\left\{h-\widetilde{h}\mid h\in\mathcal{H}^0\right\}$ where, for $h\in\mathbb{C}[\mathrm{x}]$, $\tilde{h}$ is the projection of h on the orthogonal complement of J^0 parallel to J.*

3.4 Symmetry

We consider the representation $\rho:\ \mathfrak{G}\ \to\ \mathrm{GL}(\mathbb{C}[\mathrm{x}])$ induced by a unitary representation $\varrho:\mathfrak{G}\to\mathfrak{U}_n(\mathbb{C})$, *i.e.,* $\rho(g)(p)=p\circ\varrho(g^{-1})$, for $p\in\mathbb{C}[\mathrm{x}]$, $g\in\mathfrak{G}$. The dual representation is denoted $\rho^*:\ \mathfrak{G}\ \to\ \mathrm{GL}(\mathbb{C}[\mathrm{x}]^*)$, with $\rho^*(g)(\lambda)(p)=\lambda\left(\rho(g^{-1})(p)\right)$.

The apolar product has the property that, for $a:\mathbb{C}^n\to\mathbb{C}^n$ a linear map, $\langle p,q\circ a\rangle=\left\langle p\circ\bar{a}^t,q\right\rangle$. Hence for a unitary representation ϱ, the apolar product is invariant, *i.e.,* $\langle\rho(g)(p),\rho(g)(q)\rangle=\langle p,q\rangle$. It is actually no loss of generality to assume the representation on $\mathbb{C}^n$ unitary. Indeed, for $\varrho:\mathfrak{G}\to\mathrm{GL}_n(\mathbb{C})$, we can construct an invariant inner product, for instance by averaging over the group the natural inner product. Then, in a basis orthonormal w.r.t. this invariant inner product, the representation becomes unitary.

Invariance is preserved in the constructions we reviewed in this section: the homogeneous subspace $\mathbb{C}[\mathrm{x}]_d$ are invariant, and thus, if an ideal J is invariant, so are the leading form ideal J^0 together with its orthogonal complement, as well as $J^\perp = \{\lambda \in \mathbb{C}[x]^* \,|\, \lambda(p) = 0 \ \forall p \in J\}$. Conversely if $\Lambda \subset \mathbb{C}[x]^*$ is invariant, so is $\Lambda^\perp \subset \mathbb{C}[\mathrm{x}]$. On then sees that if J is invariant it admits a *symmetry adapted H-basis*, that is, a reduced H-basis that consists of basic equivariants.

A key to exploiting symmetry in algorithms is to exhibit the equivariance of the linear maps involved in the constructions. Their matrices can then be block diagonalized, with identical blocks being repeated according to the dimensions of the irreducible representations of the group. For ideal interpolation [RH22], two maps are relevant: the Vandermonde operator, to obtain a basis of an interpolation space, and the Sylvester map, introduced in Definition 3.2, to obtain the H-basis of the ideal. For the purpose of the algorithm in Section 6, we shall recall the equivariance of this latter.

Proposition 3.4 *[RH22, Proposition 5.2] Consider $\Theta : \mathfrak{G} \to \mathrm{GL}_m(\mathbb{C})$ and $\mathrm{h} = [h_1, \ldots, h_m] \in \mathbb{C}[x]_{d_1} \times \ldots \times \mathbb{C}[x]_{d_m}$ such that $\mathrm{h} \circ \vartheta(g^{-1}) = \mathrm{h} \cdot \Theta(g)$, for all $g \in G$. For any $d \in \mathbb{N}$, the map $\psi_{d\,\mathrm{h}}$ is $\tau - \rho$ equivariant, i.e., $\psi_{d\,\mathrm{h}} \circ \tau(g) = \rho(g) \circ \psi_{d\,\mathrm{h}}$, for the representation τ on $\mathbb{C}[\mathrm{x}]_{d-d_1} \times \ldots \times \mathbb{C}[\mathrm{x}]_{d-d_m}$ defined by $\tau(g)(\mathrm{f}) = \Theta(g) \cdot \mathrm{f} \circ \varrho(g^{-1})$.*

For $e \in \mathbb{N}$ and $1 \le \ell \le \mathfrak{n}$ we introduce the representations

$$\tau_e^{(\ell)} : \mathfrak{G} \to \mathrm{GL}_n(\mathbb{C}[\mathrm{x}]_e^{\mathfrak{n}_\ell}), \quad \text{given by} \quad \tau_e^{(\ell)}(g)(\mathrm{f}) = \mathfrak{r}^{(\ell)}(g) \cdot \mathrm{f} \circ \varrho(g^{-1}).$$

If $\mathcal{H}$ consists of basic equivariants, $\mathcal{H} = \bigcup_{\ell=1}^{\mathfrak{n}} \{\mathrm{h}_i^{(\ell)} \,|\, 1 \le i \le m_\ell\}$, we see that $\Psi_d(\mathcal{H})$ is the sum of the images of $\psi_{d\,\mathrm{h}_i^{(\ell)}}$, which is $\tau_e^{(\ell)}$-equivariant, with $e = d - \deg \mathrm{h}_i^{(\ell)}$. According to [FS92, Theorem 2.5], recalled as [RH22, Proposition5.4], the matrix of $\psi_{d\,\mathrm{h}_i^{(\ell)}}$ in $\tau_e^{(\ell)}-$ and ρ_d- symmetry adapted bases of $\mathbb{C}[\mathrm{x}]_e^{\mathfrak{n}_\ell}$ and $\mathbb{C}[\mathrm{x}]_d$ respectively is

$$\mathrm{diag}\left(\mathrm{I}_{\mathfrak{n}_k} \otimes A_{\ell,i}^{(k)} \mid k = 1 \ldots \mathfrak{n}\right)$$

where $A_{\ell,i}^{(k)}$ is a matrix with dimensions the mutiplicities of $\mathfrak{r}^{(k)}$ in $\mathbb{C}[\mathrm{x}]_e^{\mathfrak{n}_\ell}$ and $\mathbb{C}[\mathrm{x}]_d$.

3.5 Algorithms

The goal in this article is to identify generating sets of invariants and equivariants. The algorithm for ideal interpolation with symmetry presented in [RH22] is at the heart of our two first constructions, in Section 4 and 5. It also inspired our third algorithm, in Section 6. We recall here the input and output of this algorithm, with the vocabulary that is consistent with the main thread of the present article.

Just as it will be the case of the further three constructions, we shall need symmetry adapted bases up to a certain degree d. They can be obtained by the projections introduced in Section 2.1. An upper bound on this degree is known at the start of each algorithm, but the termination of the algorithms is based on other criteria that might prove the needed degree to be much smaller. For Algorithm 3.5 the upper bound is $r = \dim \Lambda$. Yet it is more likely that we only need to go up to a degree d such that $r \le \dim \mathbb{C}[\mathrm{x}]_{\le d}$. The termination criterion is that the Vandermonde matrix on $\mathbb{C}[\mathrm{x}]_{\le d}$ is of full row rank.

Algorithm 3.5 ***Ideal Interpolation with Symmetry*** *[RH22, Algorithm 3]*

Input:

- $\mathcal{L} = \bigcup_{\ell=1}^{\mathfrak{n}} \mathcal{L}^{(\ell)}$ *a symmetry adapted basis (s.a.b.) for Λ, a r-dimensional subspace of $\mathbb{C}[x]^*$.*
- $\mathcal{P} = \bigcup_{\ell=1}^{\mathfrak{n}} \bigcup_{d=1}^{r} \mathcal{P}_d^{(\ell)}$ *an orthonormal graded s.a.b of $\mathbb{C}[\mathrm{x}]_{\le r}$*

- $\mathcal{M}_d^{(\ell)}$ *the s.a.b for the representations* $\tau_d^{(\ell)}$ *on* $(\mathbb{C}[\mathrm{x}]_d)^{\mathfrak{n}_\ell}$, $1 \le \ell \le \mathfrak{n}$, $1 \le d \le r-1$

Output:

- $\mathcal{H}$ *a symmetry adapted H-basis for* $J := \bigcap_{\lambda \in \Lambda} \ker \lambda$
- $\mathcal{Q} = \bigcup_{\ell=1}^{\mathfrak{n}} \mathcal{Q}^{(\ell)}$ *a s.a.b of the orthogonal complement of* J^0.

Though the algorithm calls for the symmetry adapted bases of $(\mathbb{C}[\mathrm{x}]_d)^{\mathfrak{n}_\ell}$ for the representations $\tau_d^{(\ell)}$, in the applications we make of it, in Section 4 and Section 5, we only need $\tau_d^{(1)}$. Hence only $\mathcal{P}$ is actually needed.

4 Fundamental equivariants & invariants by interpolation

A reflection group is a subgroup of $\mathrm{GL}_n(\mathbb{C})$ that is generated by matrices that have precisely one eigenvalue different from 1. In this section we show that we can deduce fundamental invariants and equivariants for such group actions from the solution of an ideal interpolation problem as computed in [RH22, Algorithm 3], whose input and output are recalled in Section 3.5.

Reflection groups enjoy extensive properties [BG85, Che55, Kan01]. The most well known is the fact that their rings of invariants $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$ are polynomial, *i.e.,* are generated by algebraically independent homogeneous invariants. Concomitantly, if N is the ideal generated by the invariants of positive degree, a.k.a. the ideal of the Nullcone, the representation induced on the *covariant algebra* $\mathbb{C}[\mathrm{x}]/N$ is equivalent to the regular representation of $\mathfrak{G}$. The beautiful properties of reflection groups offer several approaches to compute, first, the invariants whose degrees can be unequivocally read on the Molien series, and then the fundamental equivariants either as $\mathfrak{G}$-harmonic polynomials or from the cyclic structure of the covariant algebra. For some classical reflection groups, the fundamental equivariants can be determined through a combinatorial approach [ATY97, Spe35].

In this section we wish to make the rather remarkable observation that the fundamental invariants and equivariants, can be obtained as a direct application of ideal interpolation with symmetry as performed by [RH22, Algorithm 3]. We just need to interpolate along an orbit in general position. This observation was the starting point for the results in this paper.

We start with two propositions which are not specific to reflection groups. They lead to the key lemma that is restricted to reflection groups. After another technical lemma we can state the theorem that explains how to apply Algorithm 3.5 to obtain the fundamental invariants and equivariants.

Proposition 4.1 *For* $\xi \in \mathbb{C}^n$*, consider the* evaluation map $\mathrm{e}_\xi : \mathbb{C}[\mathrm{x}] \to \mathbb{C}$ *and let* $J = \bigcap_{g \in \mathfrak{G}} \ker \mathrm{e}_{g\cdot\xi}$ *in* $\mathbb{C}[\mathrm{x}]$ *be the radical ideal of the orbit of* ξ*. Then* $\langle h - \mathrm{e}_\xi(h) \,|\, h \in \mathbb{C}[\mathrm{x}]^{\mathfrak{G}} \rangle \subset J$.

PROOF: $\mathrm{e}_{g\cdot\xi}\left(h - \mathrm{e}_\xi(h)\right) = 0$ for all $h \in \mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$ and $g \in \mathfrak{G}$. □

The isotropy subgroup $\mathfrak{G}_\xi$ of $\xi \in \mathbb{C}^n$ is the set of elements of $\mathfrak{G}$ that leave ξ invariant: $\mathfrak{G}_\xi = \{\, g \in \mathfrak{G} \,|\, g\cdot\xi = \xi \,\}$

Proposition 4.2 *If* $J = \bigcap_{g \in \mathfrak{G}} \ker \mathrm{e}_{g\cdot\xi}$ *then the induced representation on* $\mathbb{C}[\mathrm{x}]/J$ *is equivalent to the permutation representation of* $\mathfrak{G}$ *associated to* $\mathfrak{G}/\mathfrak{G}_\xi$.

PROOF: The ideal $J = \bigcap_{g \in \mathfrak{G}} \ker \mathrm{e}_{g\cdot\xi}$ is invariant under the action of $\mathfrak{G}$. There is thus an action of $\mathfrak{G}$ induced on $\mathbb{C}[\mathrm{x}]/J$ that is well defined.

Let $g_1, \ldots, g_r$ be representatives for the classes of $\mathfrak{G}/\mathfrak{G}_\xi$. Denoting $\xi_i = \varrho(g_i)(\xi)$ we have that $\xi_i \neq \xi_j$ for $i \neq j$ and $\{\xi_1, \ldots, \xi_r\}$ is the orbit of ξ and hence the zero set of J. Therefore for every $g \in \mathfrak{G}$ there exists a permutation $\sigma(g)$ of $\{1, \ldots, r\}$ such that $\varrho(g)(\xi_i) = \xi_{\sigma(g)(i)}$.

Let $f_1, \ldots, f_r$ be polynomial such $f_i(\xi_j) = \delta_{ij}$. Such polynomials can be found via interpolation and we prove next that they form a basis of $\mathbb{C}[\mathrm{x}]/J$. This latter is of dimension r hence we only need to prove that they are linearly independent modulo J. Let $a_1, \ldots, a_r \in \mathbb{C}$ such that $f = \sum_{i=1}^{r} a_i f_i \in J$. Then for any $1 \leq i \leq r$, $a_i = \mathrm{e}_{\xi_i}(f) = 0$.

For any $1 \leq i, j \leq r$ we have

$$\rho(g)(f_i)(\xi_j) = f_i \circ \varrho(g^{-1})(\xi_j) = f_i\left(\xi_{\sigma(g^{-1})(j)}\right) = f_{\sigma(g)(i)}(\xi_j).$$

It follows that $\rho(g)(f_i) - f_{\sigma(g)(i)}$ vanishes on the orbit of ξ and thus $\rho(g)(f_i) - f_{\sigma(g)(i)} \in J$. Hence, in the basis $f_1, \ldots, f_r$, the induced matrix representation of $\mathfrak{G}$ on $\mathbb{C}[\mathrm{x}]/J$ is given by the permutation σ. □

In particular, if $\mathfrak{G}_\xi$ is restricted to the identity then the induced representation on $\mathbb{C}[\mathrm{x}]/J$ is equivalent to the regular representation of $\mathfrak{G}$ and thus has dimension $|\mathfrak{G}|$.

Lemma 4.3 *Assume $\mathfrak{G}$ is a reflection group and $\xi \in \mathbb{C}^n$ such that $\mathfrak{G}_\xi$ is restricted to the identity and define the ideal $J = \bigcap_{g\in\mathfrak{G}} \ker \mathrm{e}_{g\cdot\xi} \in \mathbb{C}[\mathrm{x}]$. Then J^0 is the ideal of the Nullcone, i.e., the ideal generated by all the homogeneous invariants of positive degree.*

PROOF: Let N be the ideal generated by all the homogeneous invariants of positive degree. From Proposition 4.1 it follows that $N \subset J^0$. $\mathfrak{G}$ being a reflection group, by [Che55] or [Kan01, Theorem 24-1], $\mathbb{C}[\mathrm{x}]/N$ is equivalent to the regular representation and thus of dimension $|\mathfrak{G}|$. By Proposition 4.2, $\mathbb{C}[\mathrm{x}]/J$ is also of dimension $|\mathfrak{G}|$, and thus so is $\mathbb{C}[\mathrm{x}]/J^0$. Since $\mathbb{C}[\mathrm{x}]/J^0$ and $\mathbb{C}[\mathrm{x}]/N$ have the same dimension while $N \subset J^0$, we can conclude $J^0 = N$. □

Lemma 4.4 *Let J be an ideal generated by k homogeneous invariants of positive degree. Then any homogeneous orthogonal H-basis of J consists of invariant polynomials, and of at most k of them.*

PROOF: We write $J_d = J \cap \mathbb{C}[\mathrm{x}]_d$ and $J_{\leq d} = J \cap \mathbb{C}[\mathrm{x}]_{\leq d}$ and similarly for $\mathcal{H}$ a set of homogeneous invariants generating J. Recalling Definition 3.2, we have $J_d = \Psi_d(\mathcal{H}_{<d}) + \langle \mathcal{H}_d \rangle_{\mathbb{C}}$.

We show that for any degree d, any basis for the orthogonal complement Q_d of $\Psi_d(J_{<d})$ in J_d consists of homogeneous invariants in numbers less or equal to the cardinal of $\mathcal{H}_d$.

Let m be the dimension of a complement of $\Psi_d(\mathcal{H}_{<d})$ in J_d. Then $m \leq \mathrm{card}(\mathcal{H}_d)$. We can select $h_1, \ldots, h_m \in \langle \mathcal{H}_d \rangle \subset \mathbb{C}[\mathrm{x}]_d^{\mathfrak{G}}$ s.t. $J_d = \Psi_d(\mathcal{H}_{<d}) \oplus \langle h_1, \ldots, h_m \rangle_{\mathbb{C}}$.

Consider $q_1, \ldots, q_m$ any basis of Q_d. There is then a nonsingular matrix $(a_{ij}) \in \mathbb{C}^{m\times m}$ such that $q_i = \sum a_{ij} h_j + r_i$ where $r_i \in \Psi_d(\mathcal{H}_{<d})$. Since $\Psi_d(J_{<d})$, J_d and Q_d are invariant, the polynomial $q_i - \pi^{(1)}(q_i) = r_i - \pi^{(1)}(r_i)$ belongs to $Q_d \cap \Psi_d(\mathcal{H}_{<d})$. It therefore is 0, *i.e.*, $q_i = \pi^{(1)}(q_i)$, that is to say $q_i \in \mathbb{C}[\mathrm{x}]_d^{\mathfrak{G}}$. □

Theorem 4.5 *Consider $\mathfrak{G} \subset \mathrm{GL}_n(\mathbb{C})$ a reflection group and take $\xi \in \mathbb{C}^n$ with $\mathfrak{G}_\xi = \{I_n\}$. Define*

- $J = \bigcap_{g\in\mathfrak{G}} \ker \mathrm{e}_{g\cdot\xi}$, *and*
- $\mathcal{Q} = \bigcup_{\ell=1}^{\mathrm{n}} \mathcal{Q}^{(\ell)}$ *a symmetry adapted basis of the orthogonal complement of J^0.*

Then :

- *Any reduced H-basis of J is given by a set $\{h_1 - \mathbb{e}_\xi(h_1), \ldots, h_n - \mathbb{e}_\xi(h_n)\}$ where $\{h_1, \ldots, h_n\}$ is a set of homogeneous invariants generating $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$;*
- *$\mathcal{Q}^{(1)} = \{1\}$ and, for $2 \le \ell \le \mathfrak{n}$, $\mathcal{Q}^{(\ell)}$ consists of precisely $\mathfrak{n}_\ell$ $\mathfrak{r}^{(\ell)}$-equivariants $\mathrm{q}_1^{(\ell)}, \ldots, \mathrm{q}_{\mathfrak{n}_\ell}^{(\ell)}$ freely generating $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}_{\mathfrak{r}^{(\ell)}}$ as a $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-module. Writing $\mathrm{q}_i^{(\ell)} = \left[q_{i1}^{(\ell)}, \ldots, q_{i\mathfrak{n}_\ell}^{(\ell)}\right]$, for $1 \le i \le \mathfrak{n}_\ell$, we have*

$$\mathbb{C}[\mathrm{x}] = \bigoplus_{\ell=1}^{\mathfrak{n}} \bigoplus_{i,j=1}^{\mathfrak{n}_\ell} \mathbb{C}[\mathrm{x}]^{\mathfrak{G}}\, q_{ij}^{(\ell)}.$$

PROOF: When $\mathfrak{G}$ is a reflection group, $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$ is generated by n algebraically independent homogeneous invariants [Che55], [Kan01, Theorem 18-1]. The ideal N generated by all homogeneous invariants of positive degree is a zero dimensional ideal and thus any of its H-basis cannot have less then n elements. It thus follows from Lemma 4.4, that a reduced H-basis of N consists of exactly n homogeneous invariants.

By Lemma 4.3, $N = J^0$. Hence $\mathcal{H}$ is a H-basis of J iff $\mathcal{H}^0$ is a H-basis of N. It follows from Lemma 4.4 that, for any orthogonal H-basis $\mathcal{H}$ of J, $\mathcal{H}^0 = \{h_1, \ldots, h_n\}$ where $h_1, \ldots, h_n$ form a generating set of homogeneous invariants. With Proposition 4.1 we can conclude that the shape of a reduced H-basis is as stated.

By Lemma 4.3 $J^0 = N$, and thus $\mathbb{C}[\mathrm{x}] = N \oplus \langle \mathcal{Q} \rangle_{\mathbb{C}}$ since $\mathcal{Q}$ spans the orthogonal complement of J^0. Nakayama's lemma for graded algebra [Kan01, Lemma 17-5] thus implies that

$$\mathbb{C}[\mathrm{x}] = \sum_{\ell=1}^{\mathfrak{n}} \sum_{k=1}^{\mathfrak{n}_\ell} \left(\sum_{i}^{\mathfrak{n}_\ell} \mathbb{C}[\mathrm{x}]^{\mathfrak{G}}\, q_{ik}^{(\ell)} \right).$$

By [Kan01, Lemma 18-3] the set $\left\{ q_{ik}^{(\ell)} \mid 1 \le \ell \le \mathfrak{n},\ 1 \le i, k \le \mathfrak{n}_\ell \right\}$ is furthermore algebraically independent when $\mathfrak{G}$ is a reflection group. Moreover $\mathbb{C}[\mathrm{x}]^{(\ell,1)} = \sum_i^{\mathfrak{n}_\ell} \mathbb{C}[\mathrm{x}]^{\mathfrak{G}}\, q_{1i}^{(\ell)}$, and thus Proposition 2.3 implies that $\mathcal{Q}^{(\ell)} = \left\{ \left[q_{i1}^{(\ell)}, \ldots, q_{i\mathfrak{n}_\ell}^{(\ell)} \right] \mid 1 \le i \le \mathfrak{n}_\ell \right\}$ is a freely generating $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}_{\mathfrak{r}^{(\ell)}}$ as a $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-module. ◻

Example 4.6 *The dihedral group $\mathfrak{D}_m$ is the group of order $2m$ generated by two elements s_1 and s_2 satisfying the relationships $s_1^2 = s_2^2 = (s_1 s_2)^m = 1$. The representation ϱ of $\mathfrak{D}_8$ given by*

$$\varrho(s_1) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad \varrho(s_2) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$$

is a reflection group. $\mathfrak{D}_8$ has 7 inequivalent irreducible representations, four of dimension 1 and three of dimension 2 [Ser77, Section 5.3].

Applying Algorithm 3.5 to $\Lambda = \langle \mathbb{e}_{g \cdot \xi} \mid g \in \mathfrak{G} \rangle$ where $\xi = {}^t[a, b]$ we obtain the following H-basis $\mathcal{H}$ of $J = \Lambda^\perp$ and s.a.b $\mathcal{Q} = \bigcup_{\ell=1}^7 \mathcal{Q}^{(\ell)}$ of the orthogonal complement of J^0

$$\mathcal{H} = \left\{ x^2 + y^2 - (a^2 + b^2),\ x^8 - 28x^6y^2 + 70x^4y^4 - 28x^2y^6 + y^8 - \left(a^8 - 28a^6b^2 + 70a^4b^4 - 28a^2b^6 + b^8\right) \right\}$$

$$Q^{(1)} = \{1\}, \quad Q^{(2)} = \left\{ xy\left(x^6 - 7x^4y^2 + 7x^2y^4 - y^6\right) \right\}, \quad Q^{(3)} = \left\{ x^4 - 6x^2y^2 + y^4 \right\}, \quad Q^{(4)} = \left\{ xy\left(x^2 - y^2\right) \right\},$$
$$Q^{(5)} = \left\{ [x, y],\ \left[x\left(x^6 - 21x^4y^2 + 35x^2y^4 - 7y^6\right), y\left(-7x^6 + 35x^4y^2 - 21x^2y^4 + y^6\right) \right] \right\},$$
$$Q^{(6)} = \left\{ \left[x^2 - y^2, 2xy\right],\ \left[x^6 - 15x^4y^2 + 15x^2y^4 - y^6, 2xy\left(3x^4 - 10x^2y^2 + 3y^4\right) \right] \right\},$$
$$Q^{(7)} = \left\{ \left[x\left(x^2 - 3y^2\right), y\left(3x^2 - y^2\right) \right],\ \left[x\left(-x^4 + 10x^2y^2 - 5y^4\right), y\left(5x^4 - 10x^2y^2 + y^4\right) \right] \right\}.$$

As Theorem 4.5 asserts $\mathcal{H}^0 = \left\{ x^2 + y^2,\ x^8 - 28x^6x^2 + 70x^4y^4 - 28x^2y^6 + y^8 \right\}$ is a generating set for $\mathbb{C}[\mathrm{x}]^{\mathfrak{D}_8}$ and, for $2 \le \ell \le 7$, $Q^{(\ell)}$ is a set of free generators for the $\mathfrak{r}^{(\ell)}$-equivariants.

Next example illustrates that Theorem 4.5 fails when not applied to a reflection group. In such cases, fundamental invariants and equivariants can be computed with the algorithm in Section 6.

Example 4.7 *Consider the representation of $\mathfrak{D}_6$ given by*

$$\varrho(s_1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \text{ and } \varrho(s_2) = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} & 0 \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Contrary to the standard representation of $\mathfrak{D}_6$ in the plane, this is not a reflection group since -1 is a double eigenvalue of $\varrho(s_1)$.

The output of Algorithm 3.5 applied to $\Lambda = \langle \mathrm{e}_{g\cdot\xi} \mid g \in \mathfrak{G} \rangle$ consists of a symmetry adapted H-basis $\mathcal{H} = \bigcup_{\ell=1}^{6} \mathcal{H}^{(\ell)}$ of J and a s.a.b. $\mathcal{Q} = \bigcup_{\ell=1}^{6} \mathcal{Q}^{(\ell)}$ of the orthogonal complement of J^0. For $\xi = {}^t[a, b, c]$

$$\mathcal{Q}^{(1)} = \{1\}, \quad \mathcal{Q}^{(2)} = \{z\}, \quad \mathcal{Q}^{(3)} = \left\{x^3 - 3xy^2\right\}, \quad \mathcal{Q}^{(4)} = \left\{3x^2y - y^3\right\},$$
$$\mathcal{Q}^{(5)} = \{[x, y], [yz, -xz]\}, \mathcal{Q}^{(6)} = \left\{[x^2 - y^2, 2xy], [2xyz, y^2z - x^2z]\right\},$$

and

$$\mathcal{H}^{(1)} = \left\{x^2 + y^2 - (a^2 + b^2), z^2 - c^2\right\},$$
$$\mathcal{H}^{(2)} = \varnothing, \quad \mathcal{H}^{(3)} = \left\{a\left(a^2 - b^2\right)yz\left(3x^2 - y^2\right) - bc\left(3a^2 - b^2\right)x\left(x^2 - y^2\right)\right\},$$
$$\mathcal{H}^{(4)} = \left\{b\left(b^2 - 3a^2\right)xz\left(x^2 - 3y^2\right) - ac\left(a^2 - 3b^2\right)y\left(y^2 - 3x^2\right)\right\}, \quad \mathcal{H}^{(5)} = \varnothing,$$
$$\mathcal{H}^{(6)} = \Big\{\Big[-c\left(a^2 + b^2\right)^2\left(x^4 - 6x^2y^2 + y^4\right) + 4ab\left(3a^2 - b^2\right)\left(a^2 - 3b^2\right)xyz + c\left(a^2 - b^2\right)\left(a^4 - 14a^2b^2 + b^4\right)\left(x^2 - y^2\right),$$
$$2c\left(a^2 + b^2\right)^2 xy\left(x^2 - y^2\right) - ab\left(3a^2 - b^2\right)\left(a^2 - 3b^2\right)\left(x^2 - y^2\right)z + c\left(a^2 - b^2\right)\left(a^4 - 14a^2b^2 + b^4\right)xy\Big]\Big\}$$

$\mathcal{Q}$ has 12 elements, as predicted by Proposition 4.2. Yet we shall see in Example 6.4 that a minimal set of fundamental equivariants has 22 elements.

In this case $\mathcal{H}^0$ has non invariant elements, as for instance the leading form $yz\left(3x^2 - y^2\right)$ of the single element of $\mathcal{H}^{(3)}$. One can check that this form does not belong to N. Hence $N \subsetneq J^0$. Furthermore $\mathcal{H}^{(1)}$ consists of only 2 elements and thus we can not obtain a fundamental set of invariants directly from $\mathcal{H}$.

Example 4.8 *We consider the tetrahedral group $\mathfrak{T}_h$ defined as the group of symmetry of the tetrahedron whose vertices $[a, b, c] \in \{-1, 1\}^3$ satisfy $abc = -1$. This group is actually a representation of $\mathfrak{S}_4$, generated by s_1, s_2, s_3 satisfying $s_1^2 = s_2^2 = s_3^2 = (s_1s_2)^3 = (s_2s_3)^3 = (s_1s_3)^2 = 1$. It has order 24 and 5 inequivalent irreducible representations whose dimensions are 1, 1, 2, 3, and 3 [Ser77, Section 5.8]. $\mathfrak{T}_h$ is the reflection group given by the representation:*

$$\varrho(s_1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}, \quad \varrho(s_2) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \varrho(s_3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Applying Algorithm 3.5 to $\Lambda = \langle \mathrm{e}_{g\cdot\xi} \mid g \in \mathfrak{T}_h \rangle$ where $\xi = [a, b, c]$ we obtain a H-basis $\mathcal{H}$ of the ideal J of the *orbit of ξ and a symmetry adapted basis $\mathcal{Q} = \bigcup_{\ell=1}^{5} \mathcal{Q}^{(\ell)}$ of the orthogonal complement of J^0:*

$$\mathcal{H} = \left\{x^2+y^2+z^2-(a^2+b^2+c^2),\, xyz-abc,\, x_1^4+x_2^4+x_3^4-\tfrac{3}{5}\left(x^2+y^2+z^2\right)^2-(a^4+b^4+c^4)+\tfrac{3}{5}\left(a^2+b^2+c^2\right)^2\right\}$$

$$Q^{(1)} = \{1\},$$

$$Q^{(2)} = \left\{(y^2-z^2)(z^2-x^2)(x^2-y^2)\right\},$$

$$Q^{(3)} = \left\{\left[\sqrt{3}(2x^2-y^2-z^2), 3(y^2-z^2)\right], \left[\sqrt{3}(2x^4-y^4-z^4-6x^2(y^2+z^2)+12y^2z^2, 3(z^2-y^2)(6x^2-y^2-z^2)\right]\right\}$$

$$Q^{(4)} = \left\{[x,y,z],\, [yz,xz,xy],\, \left[x\left(2x^2-3y^2-3z^2\right), y\left(2y^2-3z^2-3x^2\right), z\left(2z^2-3x^2-3y^2\right)\right]\right\}$$

$$Q^{(5)} = \left\{\left[x(y^2-z^2), y(z^2-x^2), z(x^2-y^2)\right], \left[yz\left(y^2-z^2\right), xz\left(x^2-z^2\right), xy\left(x^2-y^2\right)\right],\right.$$
$$\left.\left[x(z^2-y^2)\left(z^2+y^2-2x^2\right), y(x^2-z^2)\left(x^2+z^2-2y^2\right), z(y^2-x^2)\left(y^2+x^2-2z^2\right)\right]\right\}.$$

By Theorem 4.5, $\mathcal{Q}^{(2)}, \ldots, \mathcal{Q}^{(5)}$ are free bases of the basic equivariant modules $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}_{\mathfrak{r}^{(2)}}, \ldots, \mathbb{C}[\mathrm{x}]^{\mathfrak{G}}_{\mathfrak{r}^{(5)}}$ and the leading forms of $\mathcal{H}$ form a minimal generating set of algebraically independent invariant:

$$\mathcal{H}^0 = \left\{x^2+y^2+z^2,\, xyz,\, x_1^4+x_2^4+x_3^4-\frac{3}{5}\left(x^2+y^2+z^2\right)^2\right\}$$

5 Hironaka decompositions of the equivariant modules

Working with the concepts of *primary and secondary invariants* [Stu07, Section 2.3] allows to have a unique representation of the elements of $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$. Considering additionally a finite number of basic equivariants we obtain unique representations for the elements in the modules $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}_{\mathfrak{r}^{(\ell)}}$. Consequently, forming symmetry adapted bases of $\mathbb{C}[\mathrm{x}]_d$, for any $d \in \mathbb{N}$, becomes a task based on comparing degrees. In this section we show how to determine fundamental invariants and equivariants assuming we have sufficiently many invariants already. When applied to a set of *primary invariants* $h_1, \ldots, h_n$ this construction provides a Hironaka decomposition of $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$, $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}_{\mathfrak{r}^{(\ell)}}$ and $\mathbb{C}[\mathrm{x}]^{(\ell)}$, for $1 \le \ell \le \mathfrak{n}$, as $\mathbb{C}[h]$-modules.

Theorem 5.1 *Consider $\mathcal{H} = \{h_1, \ldots, h_k\} \subset \mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$ a set of homogeneous invariants of positive degree such that the ideal $J = \langle h_1, \ldots, h_k\rangle$ is a zero dimensional.*

Consider $\mathcal{Q} = \bigcup_{\ell=1}^{\mathfrak{n}} \mathcal{Q}^{(\ell)}$ a symmetry adapted basis of the orthogonal complement of J in $\mathbb{C}[\mathrm{x}]$. Then $\mathcal{H} \cup \mathcal{Q}^{(1)}$, $\mathcal{Q}^{(2)}, \ldots, \mathcal{Q}^{(\mathfrak{n})}$ form a fundamental set of invariants and equivariants. More precisely, if $\mathcal{Q}^{(\ell)}$ consists of the $\mathfrak{r}^{(\ell)}$-equivariants $\mathrm{q}_i^{(\ell)} = \left[q_{i1}^{(\ell)}, \ldots, q_{i\mathfrak{n}_\ell}^{(\ell)}\right]$, for $1 \le i \le m_\ell$, then, for $1 \le k \le \mathfrak{n}_\ell$,

$$\mathbb{C}[\mathrm{x}]^{(\ell,k)} = \sum_{i=1}^{m_\ell} \mathbb{C}[h]\, q_{ik}^{(\ell)}, \qquad \mathbb{C}[\mathrm{x}]^{(\ell)} = \bigoplus_{k=1}^{\mathfrak{n}_\ell}\left(\sum_{i=1}^{m_\ell} \mathbb{C}[h]\, q_{ik}^{(\ell)}\right) \quad \text{and} \quad \mathbb{C}[\mathrm{x}] = \bigoplus_{\ell=1}^{\mathfrak{n}}\bigoplus_{k=1}^{\mathfrak{n}_\ell}\left(\sum_{i=1}^{m_\ell} \mathbb{C}[h]\, q_{ik}^{(\ell)}\right).$$

PROOF: We have

$$\mathbb{C}[\mathrm{x}]/J \cong \langle Q\rangle_{\mathbb{C}} = \bigoplus_{\ell=1}^{\mathfrak{n}}\bigoplus_{k=1}^{\mathfrak{n}_\ell}\bigoplus_{i}^{m_\ell} \mathbb{C}\, q_{ik}^{(\ell)}$$

and thus, by Nakayama's lemma for graded algebra [DK15, Lemma 3.7.1],

$$\mathbb{C}[\mathrm{x}] = \sum_{\ell=1}^{\mathfrak{n}}\sum_{k=1}^{\mathfrak{n}_\ell}\left(\sum_{i}^{m_\ell} \mathbb{C}[h]\, q_{ik}^{(\ell)}\right).$$

For all $1 \le \ell \le \mathfrak{n}$ and $1 \le k \le \mathfrak{n}_\ell$, $q_{ik}^{(\ell)}$ belongs to $\mathbb{C}[\mathrm{x}]^{(\ell,k)} = \pi_{kk}^{(\ell)}(\mathbb{C}[\mathrm{x}])$. These subspaces are in direct sum with each other. Hence two subspaces $\left(\sum_i \mathbb{C}[h]\, q_{ik}^{(\ell)}\right)$ for different pairs (ℓ, k) have an intersection restricted to $\{0\}$. We can thus replace the two first $\sum$ by a $\oplus$ so as to obtain the decompositions stated. □

When $\mathcal{H}$ is a generating set of invariants of positive degree, $\mathcal{Q}^{(1)} = \{1\}$ and the $\mathfrak{r}^{(\ell)}$-equivariant $\mathrm{q}_i^{(\ell)}$, $1 \le i \le m_\ell$, generate $\mathbb{C}[\mathrm{x}]_{\mathfrak{r}^{(\ell)}}^{\mathfrak{G}}$-module as a $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-module.

Of particular interest though is the case where $\mathcal{H} = \{h_1, \ldots, h_n\}$ is a set of *primary invariants*, *i.e.,* a set of homogeneous parameters for $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$. Then $\{h_1, \ldots, h_n\}$ are algebraically independent and $\mathbb{C}[h] = \mathbb{C}[h_1, \ldots, h_n]$ is a polynomial algebra. $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$ is a Cohen-Macaulay algebra and the *secondary invariants* $s_1, \ldots, s_m$ are defined to be a free basis of $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$ viewed as a $\mathbb{C}[h]$-module. Any $p \in \mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$ can be written in a unique way as $p = p_1 s_1 + \ldots + p_m s_m$ where $p_i \in \mathbb{C}[h]$. This is a so called Hironaka decomposition of $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$. The following results shows how we can actually compute a Hironaka decomposition of $\mathbb{C}[\mathrm{x}]$ as a $\mathbb{C}[h]$-module.

Theorem 5.2 *Consider $h_1, \ldots, h_n$ a set of primary invariants. Let m be the quotient of $\prod_{i=1}^n \deg(h_i)$ by $|\mathfrak{G}|$. If $\mathcal{Q} = \bigcup_{\ell=1}^{\mathfrak{n}} \mathcal{Q}^{(\ell)}$ is a symmetry adapted basis of the orthogonal complement of the ideal $\langle h_1, \ldots, h_n \rangle$ in $\mathbb{C}[\mathrm{x}]$, then $\mathcal{Q}^{(\ell)}$ consists of $m\, \mathfrak{n}_\ell\ \mathfrak{r}^{(\ell)}$-equivariants $\mathrm{q}_1, \ldots, \mathrm{q}_{m\mathfrak{n}_\ell}$ that form a free basis of $\mathbb{C}[\mathrm{x}]_{\mathfrak{r}^{(\ell)}}^{\mathfrak{G}}$ seen as a $\mathbb{C}[h]$-module. In particular $\mathcal{Q}^{(1)}$ consists of a set of secondary invariants for $h_1, \ldots, h_n$. We have*

$$\mathbb{C}[\mathrm{x}]^{(\ell,k)} = \bigoplus_{i=1}^{m_\ell} \mathbb{C}[h]\, q_{ik}^{(\ell)}, \qquad \mathbb{C}[\mathrm{x}]^{(\ell)} = \bigoplus_{k=1}^{\mathfrak{n}_\ell} \left(\bigoplus_{i=1}^{m_\ell} \mathbb{C}[h]\, q_{ik}^{(\ell)} \right) \quad \text{and} \quad \mathbb{C}[\mathrm{x}] = \bigoplus_{\ell=1}^{\mathfrak{n}} \bigoplus_{k=1}^{\mathfrak{n}_\ell} \left(\bigoplus_{i=1}^{m_\ell} \mathbb{C}[h]\, q_{ik}^{(\ell)} \right).$$

PROOF: By [Stu07, Proposition 2.3.6], $|\mathfrak{G}|$ divides $\prod_{i=1}^n \deg(h_i)$ and the number of secondary invariants m is their quotient. With an argument based on the Molien series of $\mathbb{C}[\mathrm{x}]^{(\ell)}$, [Sta79, Proposition 4.9] proves that $\mathbb{C}[\mathrm{x}]/\langle h_1, \ldots, h_n \rangle$ is equivalent to m times the regular representation of $\mathfrak{G}$. Hence $m{\mathfrak{n}_\ell}^2$ is the dimension of $\mathbb{C}[\mathrm{x}]^{(\ell)}/\langle h_1, \ldots, h_n \rangle \mathbb{C}[\mathrm{x}]^{(\ell)}$ as a $\mathbb{C}$-vector space.

From Theorem 5.1 we have

$$\mathbb{C}[\mathrm{x}] = \bigoplus_{\ell=1}^{\mathfrak{n}} \bigoplus_{k=1}^{\mathfrak{n}_\ell} \sum_{i=1}^{m\mathfrak{n}_\ell} \mathbb{C}[h]\, q_{ik}^{(\ell)}.$$

As $\mathbb{C}[\mathrm{x}]$ is finitely generated over $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$, $h_1, \ldots, h_n$ also form a homogeneous system of parameters for $\mathbb{C}[\mathrm{x}]$. Since $\mathbb{C}[\mathrm{x}]$ is Cohen-Macaulay, $\mathbb{C}[\mathrm{x}]$ is a free $\mathbb{C}[h]$-module. If $\eta_1, \ldots, \eta_k$ is a free basis, then their images in $\mathbb{C}[\mathrm{x}]/\langle h_1, \ldots, h_n \rangle$ span this $m|\mathfrak{G}|$-dimensional vector space. Hence the rank of $\mathbb{C}[\mathrm{x}]$ as a $\mathbb{C}[h]$-module is at least $m|\mathfrak{G}|$. It follows that $\mathcal{Q}$ is a free basis. □

With Algorithm 3.5, the above theorems are seen to be straightforwardly constructive: With any term order, compute a Gröbner basis $\mathcal{B}$ of the homogeneous ideal $J = \langle h_1, \ldots, h_n \rangle$ together with the normal set $\{x^{\alpha_1}, \ldots, x^{\alpha_r}\}$. This defines the computable linear forms $\lambda_1, \ldots, \lambda_r : \mathbb{C}[\mathrm{x}] \to \mathbb{C}$ such that, for any $p \in \mathbb{C}[\mathrm{x}]$, the normal form of p w.r.t. $\mathcal{B}$ is $\lambda_1(p) x^{\alpha_1} + \ldots + \lambda_r(p) x^{\alpha_r}$. Applying Algorithm 3.5 to $\Lambda = \langle \lambda_1, \ldots, \lambda_r \rangle_{\mathbb{C}}$, or alternatively [RH21, Section 5] for the least interpolation space, one computes the desired symmetry adapted basis $\mathcal{Q}$ of the orthogonal complement of J.

The advantage of the above approach is that Gröbner bases implementations are widely available and efficient. Yet, as the input invariants $h_1, \ldots, h_k$ are homogeneous, we could alternatively compute a H-basis and its orthogonal complement with linear algebra operations. Such an approach is taken in next section where we actually compute generating invariants on the fly.

There are actually several algorithms to compute primary invariants. Dade's algorithm [Stu07, Algorithm 2.5.14] constructs primary invariants taking products over $\mathfrak{G}$−orbits of linear forms, such that all the degrees of the computed invariants are divisors of the group order. On the other hand [Kem99, Algorithm 2] looks for a set of primary invariants $\{f_1, \ldots, f_n\}$ that minimizes $\Pi_{i=1}^n \deg(f_i)$, and then $\sum_{i=1}^n \deg(f_i)$. The algorithm iterates according to a pre-order over $\mathbb{N}^n$ and stops when a n-tuple $(d_1, \ldots, d_n)$ is found such that there exist a set of primary invariants with those degrees.

On the other hand [Stu07, Algorithm 2.5.8] and [Gat00, Algorithm 2.1.5] proposed to extract primary invariants from a generating set. They generate invariants of increasing degree whose variety gets smaller each time until a set of algebraically independent homogeneous invariants is found. If the obtained set is composed of n elements, then it is a set of primary invariants. Otherwise sets of n elements weighted over the computed invariant are randomly generated until an algebraically independent set is found. In next section we provide a new algorithm to compute generating set of invariants, together with fundamental equivariants.

Example 5.3 *The cyclic group $\mathfrak{C}_m$ is the group of order m generated by a single element r. If we consider its representation in $\mathbb{C}^n$ given by*

$$\varrho(r) = \mathrm{diag}\left(e^{\frac{2i\pi}{m}}, \ldots, e^{\frac{2i\pi}{m}}\right)$$

$\mathbb{C}[x]^{\mathfrak{C}_m}$ is generated by all terms of degree m [Stu07, Proposition 2.1.5] and $\mathcal{H} = \{x_1^m, \ldots, x_n^m\}$ is a set of primary invariants. $\mathcal{H}$ is also a Gröbner basis with respect to any term order. The normal set consists of the terms $\mathcal{N} = \left\{x^i y^j z^k \mid 0 \le i, j, k \le m-1\right\}$. $\mathfrak{C}_m$ has m inequivalent irreducible representations of dimensions 1 [Ser77, Section 5.1]. For $1 \le \ell \le m$, the fundamental equivariants are given by $\mathcal{Q}^{(\ell)} = \left\{x^i y^j z^k \mid i+j+k = m+1-\ell\right\}$. Observe $\mathcal{N} = \bigcup_{\ell=1}^m Q^{(\ell)}$ and this corroborates Theorem 5.2.

Example 5.4 *The alternating group $\mathfrak{A}_4$ is the subgroup of $\mathfrak{S}_4$ of even permutations on 4 elements. $\mathfrak{A}_4$ has four irreducible representations over $\mathbb{C}$, three of dimension 1 and one of dimension 3 [Ser77, Section 5.7]. The pair of of non trivial one dimensional representations are conjugate to each other. As mentioned in Section 2.1 we can combine them into one real irreducible representation of dimension 2 in order to keep the comptutation and the write up over $\mathbb{R}$.*

Restricting the representation of $\mathfrak{S}_4$ in Example 4.8 to $\mathfrak{A}_4$ we obtain the group $\mathfrak{T}$ of rotational symmetries of the tetrahedron. The fundamental invariants of $\mathfrak{T}_h$ thus provide a set $\mathcal{H}$ of primary invariants for this representation:

$$\mathcal{H} = \left\{x^2+y^2+z^2,\, xyz,\, x^2y^2+x^2z^2+y^2z^2\right\}.$$

The Gröbner basis and the normal set of the ideal generated by $\mathcal{H}$ w.r.t a degree reverse lexicographical order are given by

$$\mathcal{B} = \left\{x^2+y^2+z^2, xyz, y^3z+yz^3, y^4+y^2z^2+z^4, z^5\right\}$$
$$\mathcal{N} = \left\{1, z, y, x, z^2, yz, xz, y^2, xy, z^3, yz^2, xz^2, y^2z, y^3, xy^2, z^4, yz^3, xz^3, y^2z^2, xy^3, yz^4, xz^4, y^2z^3, y^2z^4\right\}.$$

We define the linear forms $\lambda_1, \ldots, \lambda_{24}$ so that the normal form of $p \in \mathbb{C}[\mathrm{x}]$ w.r.t $\mathcal{B}$ is $\lambda_1(p)\, x^{\alpha_1} + \ldots + \lambda_{24}(p) x^{\alpha_{24}}$ where $x^{\alpha_i} \in \mathcal{N}$. Then the output of Algorithm 3.5 applied to $\Lambda = \langle\, \lambda_i \mid 1 \le i \le 24\,\rangle$ computes the secondary invariants $\mathcal{Q}^{(1)}$ and the set of fundamental equivariants $\mathcal{Q}^{(2)}$ and $\mathcal{Q}^{(3)}$ that freely generate $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}_{\mathfrak{r}^{(2)}}$ and $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}_{\mathfrak{r}^{(3)}}$ as $\mathbb{C}[h]$-modules.

$$\mathcal{Q}^{(1)} = \left\{[1], \left[(y^2-z^2)(z^2-x^2)(x^2-y^2)\right]\right\},$$
$$\mathcal{Q}^{(2)} = \left\{\left[2x^2-y^2-z^2, \sqrt{3}(y^2-z^2)\right], \left[\sqrt{6}\left(y^2-x^2\right)\left(6z^2-x^2-y^2\right), (y^2-z^2)(6x^2-y^2+z^2)\right]\right\},$$
$$\begin{aligned}\mathcal{Q}^{(3)} = \Big\{&[x,y,z], [yz,xz,xy], \left[x\left(x^2-3z^2\right), y\left(y^2-3x^2\right), z\left(z^2-3y^2\right)\right],\\ &\left[x\left(y^2-z^2\right), y\left(z^2-x^2\right), z\left(x^2-y^2\right)\right], \left[yz\left(y^2-z^2\right), zx\left(z^2-x^2\right), xy\left(x^2-y^2\right)\right],\\ &\left[2x^3(y^2-z^2)-x(y^4-z^4), 2y^3(z^2-x^2)-y(z^4-x^4), 2z^3(x^2-y^2)-z(x^4-y^4)\right]\Big\}.\end{aligned}$$

6 Simultaneous computation of invariants and equivariants

In this section we present an algorithm that computes, simultaneously, a minimal set of fundamental invariants and equivariants. The fundamental invariants are obtained as the elements of the H-basis $\mathcal{H}$ of the ideal N of the Nullcone and the fundamental equivariants are obtained as a symmetry adapted basis $\mathcal{Q}$ of the orthogonal complement of N in $\mathbb{C}[\mathrm{x}]$. The algorithm proceeds degree by degree. At degree d, a symmetry adapted basis of the orthogonal complement of $\Psi_d(\mathcal{H}_{d-1})$ in $\mathbb{C}[\mathrm{x}]_d$ is the union of $\mathcal{K}_d \subset \mathbb{C}[\mathrm{x}]_d^{(1)}$ and $\mathcal{R}_d \subset \bigoplus_{\ell=2}^{\mathfrak{n}} \mathbb{C}[\mathrm{x}]_d^{(\ell)}$. One adjoins $\mathcal{K}_d$ to $\mathcal{H}_{d-1}$ to form $\mathcal{H}_d$ and $\mathcal{R}_d$ to $\mathcal{Q}_{d-1}$ to form $\mathcal{Q}_d$. Yet, as we first show, the computation of the orthogonal complement of $\Psi_d(\mathcal{H}_{d-1})$ can be split into smaller pieces, with redundancy avoided. The linear algebra operations are thus done over linear spaces of small dimension. At worse the algorithm terminates at $d = |\mathfrak{G}|$, Noether's bound. Yet the main termination criterion is $\Psi_d(\mathcal{H}_d) = \mathbb{C}[\mathrm{x}]_d$.

Previously. The structure of our algorithm bears some comparison to King's algorithm [Kin13] to compute a generating set of invariants (and only invariants). Both algorithms, for each degree d, look for invariants that cannot be obtained from the invariants of degree $d-1$. In King's algorithm this is decided upon the membership to the ideal generated by invariants of degree $d-1$, which requires the computation of its Gröbner basis. We compute the orthogonal complement of $\Psi_d^{(1)}(\mathcal{H}_{d-1})$ in $\mathbb{C}[\mathrm{x}]_d^{(1)}$. The termination criterion of King's algorithm is based on a degree bound that is updated when the ideal under construction becomes zero dimensional. It is quite different from the termination criterion we put forth. Our algorithm terminates when $\Psi_d(\mathcal{H}_d) = \mathbb{C}[\mathrm{x}]_d$.

Prior approaches to compute generating invariants of finite groups [DK15] proceed by first determining a set of primary invariants, and then a set of secondary invariants. Molien's series is then key: it provides the degrees of the secondary invariants, and hints for the degrees of the primary invariants. These are then computed applying the Reynolds operator.

The computation of generating θ-equivariants in [Gat96, Algorithm 3.16] is in the same spirit as the computation secondary invariants. They introduce the representation $\tau : \mathfrak{G} \to \mathrm{Aut}(\mathbb{C}[\mathrm{x}]^m), \tau(g)(\mathrm{p}) = \theta(g) \cdot \mathrm{p} \circ \varrho(g^{-1})$ and use the fact that the related Reynolds operator is a projection on the $\mathbb{C}[\mathrm{x}]_\theta^{\mathfrak{G}}$ vector space. Note that the linear algebra operations at degree d are then made in a vector space of dimension m times the dimension of $\mathbb{C}[\mathrm{x}]_d$.

As explained in Section 2.2, any equivariant can be written as linear combinations of basic equivariants. Our algorithm computes generating sets of these with linear algebra in the vector spaces $\mathbb{C}[\mathrm{x}]_d$ of homogeneous polynomials, and not vectors of them. Furthermore we actually only compute the generators for the $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-modules $\mathbb{C}[\mathrm{x}]^{(\ell,1)}$, from which the generators of any $\mathbb{C}[\mathrm{x}]_{\mathfrak{r}^{(\ell)}}^{\mathfrak{G}}$ can be deduced.

Sylvester map revisited. For a row vector of polynomials $\mathrm{h} = \begin{bmatrix} h_1 & \dots & h_m \end{bmatrix} \in \mathbb{C}[\mathrm{x}]^m$, with h_i of degree d_i, the Sylvester map to degree d already introduced in Section 3.3 is

$$\begin{array}{rccc} \psi_{d\,\mathrm{h}}: & \mathbb{C}[\mathrm{x}]_{d-d_1} \times \ldots \times \mathbb{C}[\mathrm{x}]_{d-d_m} & \to & \mathbb{C}[\mathrm{x}]_d \\ & (g_1, \ldots, g_m) & \mapsto & \sum_{i=1}^m g_i h_i \end{array}.$$

For $1 \le \ell \le \mathfrak{n}$, and $1 \le k \le \mathfrak{n}_\ell$ we shall consider the following restriction of this map:

$$\begin{array}{rccc} \psi_{d\,\mathrm{h}}^{(\ell,k)}: & \mathbb{C}[\mathrm{x}]_{d-d_1}^{(\ell,k)} \times \ldots \times \mathbb{C}[\mathrm{x}]_{d-d_m}^{(\ell,k)} & \to & \mathbb{C}[\mathrm{x}]_d \\ & (g_1, \ldots, g_m) & \to & \sum_{i=1}^m g_i h_i \end{array}.$$

For the set $\mathcal{H} = \{h_1, \ldots, h_m\}$ we shall denote by $\Psi_d(\mathcal{H})$ and $\Psi_d^{(\ell,k)}(\mathcal{H})$ the respective images of $\psi_{d\,\mathrm{h}}$ and $\psi_{d\,\mathrm{h}}^{(\ell,k)}$. Note that

$$\Psi_d(\mathcal{H}) = \sum_{\ell=1}^{\mathfrak{n}} \sum_{k=1}^{\mathfrak{n}_\ell} \Psi_d^{(\ell,k)}(\mathcal{H}). \tag{5}$$

Proposition 6.1 *Assume* $\mathcal{H} \subset \mathbb{C}[\mathrm{x}]^{(1)}_{\leq d}$. *Then* $\Psi^{(\ell,k)}_d(\mathcal{H}) \subset \mathbb{C}[\mathrm{x}]^{(\ell,k)}_d$. *If* $\mathcal{R}^{(\ell,1)}_d = \{q_1,\dots,q_m\}$ *is a basis of the orthogonal complement of* $\Psi^{(\ell,1)}_d(\mathcal{H})$ *in* $\mathbb{C}[\mathrm{x}]^{(\ell,1)}_d$ *then*

$$\mathcal{R}^{(\ell,k)}_d := \pi^{(\ell)}_{k1}\left(\mathcal{R}^{(\ell,1)}_d\right) = \left\{\pi^{(\ell)}_{k1}(q_1),\dots,\pi^{(\ell)}_{k1}(q_m)\right\}$$

is a basis of the orthogonal complement of $\Psi^{(\ell,k)}_d(\mathcal{H})$ *in* $\mathbb{C}[\mathrm{x}]^{(\ell,k)}_d$. *Furthermore* $\bigcup_{\ell=1}^{\mathfrak{n}}\bigcup_{k=1}^{\mathfrak{n}_\ell}\mathcal{R}^{(\ell,k)}_d$ *is a symmetry adapted basis of the orthogonal complement of* $\Psi_d(\mathcal{H})$.

In the algorithm we shall exploit that we have a symmetry adapted basis $\mathcal{Q}_{d-1}$ of the orthogonal complement of $\Psi_{d-1}(\mathcal{H}_d)$ to compute $\Psi^{(\ell,1)}_d(\mathcal{H}_d)$. This is due to the following exchange property.

Lemma 6.2 *For* $2 \leq \ell \leq \mathfrak{n}$, *consider* $\mathcal{H} \subset \mathbb{C}[\mathrm{x}]^{(1)}_{\leq d} \setminus \mathbb{C}$ *and* $\mathcal{Q} \subset \mathbb{C}[\mathrm{x}]^{(\ell,k)}_{\leq d-1}$. *Assume that both*

- $\Psi^{(1)}_e(\mathcal{Q}) = \mathbb{C}[\mathrm{x}]^{(\ell,k)}_e$ *for all* $1 \leq e \leq d-1$, *and*
- $\Psi^{(1)}_e(\mathcal{H}) = \mathbb{C}[\mathrm{x}]^{(1)}_e$ *for all* $1 \leq e \leq d$.

Then $\Psi^{(\ell,k)}_d(\mathcal{H}) = \Psi^{(1)}_d(\mathcal{Q})$.

PROOF: Note first that both $\Psi^{(\ell,k)}_d(\mathcal{H})$ and $\Psi^{(1)}_d(\mathcal{Q})$ are contained in $\mathbb{C}[\mathrm{x}]^{(\ell,k)}_d$ since $\mathbb{C}[\mathrm{x}]^{(\ell,k)}$ is a $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-module.
A polynomial $q \in \Psi^{(\ell,k)}_d(\mathcal{H})$ can be written $q = \sum_{h_i\in\mathcal{H}} h_i p_i$ with $p_i \in \mathbb{C}[\mathrm{x}]^{(\ell,k)}_{d-\deg(h_i)}$. Since $\Psi^{(1)}_{d-\deg(h_i)}(\mathcal{Q}) = \mathbb{C}[\mathrm{x}]^{(\ell,k)}_{d-\deg(h_i)}$, we can write $p_i = \sum_{q_j\in Q} r_{ij}q_j$ with $r_{ij} \in \mathbb{C}[\mathrm{x}]^{(1)}_{d-\deg(h_iq_j)}$. Hence

$$q = \sum_{h_i\in\mathcal{H}} h_i \sum_{q_j\in\mathcal{Q}} r_{ij}q_j = \sum_{q_j\in Q} q_j \sum_{h_i\in\mathcal{H}} r_{ij}h_i \in \Psi^{(1)}_d(\mathcal{Q}),$$

so that $\Psi^{(\ell,k)}_d(\mathcal{H}) \subset \Psi^{(1)}_d(\mathcal{Q})$. Analogously any $q \in \Psi^{(1)}_d(\mathcal{Q})$ can be written $q = \sum_{q_j\in\mathcal{Q}} r_jq_j$ with $r_i \in \mathbb{C}[\mathrm{x}]^{(1)}_{d-\deg q_j}$. By hypothesis $r_i = \sum_{h_i\in\mathcal{H}} p_{ij}h_i$ with $p_{ij} \in \mathbb{C}[\mathrm{x}]^{(1)}_{d-\deg q_jh_i}$ and thus

$$q = \sum_{q_j\in\mathcal{Q}}\left(\sum_{h_i\in\mathcal{H}} h_ir_{ij}\right)q_j = \sum_{h_i\in\mathcal{H}} h_i \sum_{q_j\in\mathcal{Q}} r_{ij}q_j \in \Psi^{(\ell,k)}_d(\mathcal{H}).$$

Therefore $\Psi^{(\ell,k)}_d(\mathcal{H}) = \Psi^{(1)}_d(\mathcal{Q})$. □

Algorithm 6.3 ***Fundamental Invariants and Equivariants***

Input: $\mathcal{P} = \bigcup_{\ell=1}^{\mathfrak{n}}\bigcup_{d=1}^{|\mathfrak{G}|}\mathcal{P}^{(\ell,1)}_d$ *a symmetry adapted basis of* $\mathbb{C}[\mathrm{x}]_{|\mathfrak{G}|}$.

Output: $\mathcal{H} \subset \mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$ *and* $\mathcal{Q} = \bigcup_{\ell=1}^{\mathfrak{n}}\mathcal{Q}^{(\ell)}$

- $\mathcal{H}$ *is a minimal generating set of homogeneous invariants*
- $Q^{(\ell)} = \left\{\left[q^{(\ell)}_{i1},\dots,q^{(\ell)}_{i\mathfrak{n}_\ell}\right] \mid 1 \leq i \leq m_\ell\right\}$ *is a generating set for* $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}_{\mathfrak{r}^{(\ell)}}$ *as a* $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$*-module*

$\mathcal{Q}_0^{(1,1)} \leftarrow \{1\}$

$\mathcal{H}_0, \mathcal{Q}_0^{(2,1)}, \ldots, \mathcal{Q}_0^{(\mathfrak{n},1)} \leftarrow \varnothing$

$d \leftarrow 0$

$a \leftarrow 1$ *(the number of degree d elements in $\bigcup_{\ell=1}^{\mathfrak{n}} \mathcal{Q}_d^{(\ell,1)}$)*

while *$a > 0$ and $d < |\mathfrak{G}|$* ***do***

  $d \leftarrow d + 1$

  $\mathcal{K}_d \leftarrow$ *a basis of the orthogonal complement of* $\Psi_d^{(1)}(\mathcal{H}_{d-1})$ *in* $\mathbb{C}[\mathrm{x}]_d^{(1)}$

  $\mathcal{H}_d \leftarrow \mathcal{H}_{d-1} \cup \mathcal{K}_d$

  $a \leftarrow 0$

  for *$\ell = 2$ to $\mathfrak{n}$* ***do***

    $\mathcal{R}_d^{(\ell,1)} \leftarrow$ *a basis of the orthogonal complement of* $\Psi_d^{(\ell,1)}(\mathcal{H}_d)$ *in* $\mathbb{C}[\mathrm{x}]_d^{(\ell,1)}$

    $\mathcal{Q}_d^{(\ell,1)} \leftarrow \mathcal{Q}_{d-1}^{(\ell,1)} \cup \mathcal{R}_d^{(\ell,1)}$

    $a \leftarrow a + |\mathcal{K}|$

  end-do

end-do

return $\mathcal{H}_d$ *and* $\bigcup_{\ell=1}^{\mathfrak{n}} \left\{ \left[\pi_{11}^{(\ell)}(q), \ldots, \pi_{\mathfrak{n}_\ell 1}^{(\ell)}(q) \right] \mid q \in Q_d^{(\ell,1)} \right\}$

PROOF: Thanks to Proposition 6.1 and Lemma 6.2, the following three properties are true at the end of each iteration of the *while* loop:

A(d) **:** $\Psi_e^{(1)}(\mathcal{H}_d) = \mathbb{C}[\mathrm{x}]_e^{\mathfrak{G}}$ for all $1 \le e \le d$.

B(d) **:** $\Psi_e^{(1)}\left(\mathcal{Q}_d^{(\ell,1)}\right) = \mathbb{C}[\mathrm{x}]_e^{(\ell,1)}$ for all $1 \le e \le d$.

C(d) **:** $\bigcup_{\ell=1}^{\mathfrak{n}} \left\{ \left[\pi_{11}^{(\ell)}(q), \ldots, \pi_{1\mathfrak{n}_\ell}^{(\ell)}(q) \right] \mid q \in Q_d^{(\ell,1)} \right\}$ is a basis of the orthogonal complement of $\bigoplus_{e=1}^{d} \Psi_e(\mathcal{H}_d)$ in $\mathbb{C}[\mathrm{x}]_{\le d}$

We now prove that when $d = |\mathfrak{G}|$ or $a = 0$ we have that $\mathcal{H}_d$ is a generating set of $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$ and $\mathcal{Q}_d^{(\ell,1)}$ is a generating set of $\mathbb{C}[\mathrm{x}]^{(\ell,1)}$ as a $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-module.

Note that Property A(d) implies that any $p \in \mathbb{C}[\mathrm{x}]_{\le d}^{\mathfrak{G}}$ can be written as a polynomial in the elements of $\mathcal{H}_d$. Hence, if $d = |\mathfrak{G}|$, Noether's bound, $\mathcal{H}_d$ is a generating set of invariants [Stu07, Theorem 2.1.4]. By [Sta79, Theorem 3.1], $\mathbb{C}[\mathrm{x}]_{|\mathfrak{G}|}^{(\ell)}$ generates $\mathbb{C}[\mathrm{x}]^{(\ell)}$ as a $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-module. Thus Property B$(d)$, together with the properties of the maps $\pi_{k1}^{(\ell)}$, implies that $\mathcal{Q}_d^{(\ell,1)}$ is a generating set for $\mathbb{C}[\mathrm{x}]_{|\mathfrak{G}|}^{(\ell,1)}$ as a $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-module. So by Proposition 2.3, $\bigcup_{\ell=1}^{\mathfrak{n}} \left\{ \left[\pi_{11}^{(\ell)}(q), \ldots, \pi_{\mathfrak{n}_\ell 1}^{(\ell)}(q) \right] \mid q \in Q_d^{(\ell,1)} \right\}$ is a generating set for $\mathbb{C}[\mathrm{x}]_{\mathfrak{r}^\ell}^{\mathfrak{G}}$ as a $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-module.

At the end of an iteration $a = 0$ means that $\Psi_d^{(\ell,k)}(\mathcal{H}_d) = \mathbb{C}[\mathrm{x}]_d^{(\ell,k)}$, for all $1 \le k \le \mathfrak{n}_\ell$, and thus $\Psi_d(\mathcal{H}_d) = \mathbb{C}[\mathrm{x}]_d$. It follows that $\Psi_e(\mathcal{H}_d) = \mathbb{C}[\mathrm{x}]_e$ for all $e \ge d$. Hence

$$\mathbb{C}[\mathrm{x}] = \langle \mathcal{H} \rangle \bigoplus \left(\bigoplus_{\ell=1}^{\mathfrak{n}} \bigoplus_{k=1}^{\mathfrak{n}_\ell} \bigoplus_{q \in \mathcal{Q}_d^{(\ell,1)}} \mathbb{C}\, \pi_{k1}^{(\ell)}(q) \right).$$

Any homogeneous invariant of positive degree thus belongs to $\langle\mathcal{H}\rangle$. By the classical argument used in Hilbert's finiteness theorem [Stu07, Theorem 2.1.3], $\mathcal{H}_d$ is a generating set of homogeneous invariants. It is a minimal such set by construction. Then, by Nakayama's lemma for graded algebra [DK15, Lemma 3.7.1] and the fact that the different $\mathbb{C}[\mathrm{x}]^{(\ell,k)}$ are in direct sum we have

$$\mathbb{C}[\mathrm{x}] = \bigoplus_{\ell=1}^{\mathfrak{n}} \bigoplus_{k=1}^{\mathfrak{n}_\ell} \left(\sum_{q\in\mathcal{Q}_d^{(\ell,1)}} \mathbb{C}[\mathrm{x}]^{\mathfrak{G}} \, \pi_{k1}^{(\ell)}(q) \right).$$

It follows that $\mathbb{C}[\mathrm{x}]^{(\ell,k)} = \sum_{q\in\mathcal{Q}_d^{(\ell,1)}} \mathbb{C}[\mathrm{x}]^{\mathfrak{G}} \, \pi_{k1}^{(\ell)}(q)$. $\square$

In the algorithm we have made use of Noether's bound to mark termination. Yet we could have use $a = 0$ as unique stopping criterion : it is indeed enough to know that $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$ is finitely generated as an algebra and $\mathbb{C}[\mathrm{x}]^{(\ell)}$ is finitely generated as a $\mathbb{C}[\mathrm{x}]^{\mathfrak{G}}$-module.

Example 6.4 *Consider the representation of $\mathfrak{D}_6$ given by*

$$\varrho(s_1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \text{ and } \varrho(s_2) = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} & 0 \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

This action was examined in [Stu07, Example 2.2.6] and we already considered it in Example 4.7. $\mathfrak{D}_6$ has six absolutely irreducible representations, four of dimension 1 and two of dimension 2 [Ser77, Section 5.3]. Applying Algorithm 6.3 we obtain the following fundamental invariants

$$\mathcal{H} = \left\{x^2+y^2,\, z^2, x^6+15x^2y^2(y^2-x^2)-y^6,\, xyz\left(3x^4-10x^2y^2+3y^4\right)\right\},$$

and equivariants

$$Q^{(2)} = \left\{[z], \left[xy\left(3x^4-10x^2y^2+3y^4\right)\right]\right\}, \quad Q^{(3)} = \left\{\left[x\left(x^2-3y^2\right)\right], \left[yz\left(3x^2-y^2\right)\right]\right\}$$

$$Q^{(4)} = \left\{\left[y\left(3x^2-y^2\right)\right], \left[xz\left(x^2-3y^2\right)\right]\right\},$$

$$Q^{(5)} = \left\{[x,y], [yz,-xz], \left[x\left(x^4-10x^2y^2+5y^4\right), y\left(y^4-10y^2x^2+5x^4\right)\right],\right.$$
$$\left.\left[yz\left(y^4-10x^2y^2+5x^4\right), xz\left(x^4-10y^2x^2+5y^4\right)\right]\right\},$$

$$Q^{(6)} = \left\{\left[x^2-y^2, 2xy\right], \left[2xyz, z(y^2-x^2)\right], \left[x^4-6x^2y^2+y^4, xy\left(x^2-y^2\right)\right],\right.$$
$$\left.\left[xyz\left(x^2-y^2\right), z\left(x^4-6x^2y^2+y^4\right)\right]\right\}.$$

Example 6.5 *Consider the three-dimensional representation of the cyclic group $\mathfrak{C}_4$ of order 4 over $\mathbb{C}[x,y,z]$ given by the matrices*

$$\left\{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}\right\}.$$

This action was examined in [Stu07, Example 2.3.7]. $\mathfrak{C}_4$ is an Abelian group with four irreducible representations of dimension 1, two of which can be realized over the reals and the other two are conjugate to each other [Ser77, Section 5.1]. Applying Algorithm 6.3 we get the following generating invariants

$$\mathcal{H} = \left\{x^2+y^2,\, z^2,\, xyz,\, z(x^2-y^2),\, x^4+y^4,\, xy\left(x^2-y^2\right)\right\}$$

and equivariants

$$\begin{aligned} Q^{(2)} &= \left\{z,\, xy,\, x^2 - y^2\right\}, \\ Q^{(3)} &= \left\{x - iy,\, z\,(x + iy)\,,\, 3x^2y + y^3 + i(x^3 + 3xy^2)\right\}, \\ Q^{(4)} &= \left\{x + iy,\, z\,(x - iy)\,,\, 3x^2y + y^3 - i(x^3 + 3xy^2)\right\}. \end{aligned}$$

In the above, the elements of $Q^{(3)}$ and $Q^{(4)}$ are conjugate of each other. They can be combined as a generating set of equivariants for the underlying real irreducible representation of dimension 2.

Example 6.6 *We consider the 3 dimensional representation of $\mathfrak{S}_4$, a group already encountered in Example 4.8, given by*

$$\varrho(s_1) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \varrho(s_2) = \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \varrho(s_3) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}.$$

Applying Algorithm 6.3 we obtain the following fundamental invariants

$$\mathcal{H} = \left\{ \begin{array}{c} x^2 + y^2 + z^2, \quad x^4 + y^4 + z^4 - \frac{3}{5}\left(x^2 + y^2 + z^2\right)^2, \\ x^6 + y^6 + z^6 + \frac{30}{77}\left(x^2 + y^2 + z^2\right)^2 - \frac{15}{11}\left(x^2 + y^2 + z^2\right)\left(x^4 + y^4 + z^4\right), \\ xyz(z^2 - y^2)(x^2 - z^2)(y^2 - x^2) \end{array} \right\},$$

and equivariants

$$\mathcal{Q}^{(2)} = \left\{[xyz]\,, \left[(y^2 - z^2)(z^2 - x^2)(x^2 - y^2)\right]\right\},$$

$$\mathcal{Q}^{(3)} = \left\{ \begin{array}{c} \left[2\,x^2 - y^2 - z^2, \sqrt{3}\left(y^2 - z^2\right)\right], \\ \left[6\,x^2(y^2 + z^2) - 12\,y^2z^2 - 2\,x^4 + y^4 + z^4, \sqrt{3}\left(6\,x^2 - y^2 - z^2\right)\left(y^2 - z^2\right)\right], \\ \left[\sqrt{3}xyz\left(y^2 - z^2\right), -xyz\left(2\,x^2 - y^2 - z^2\right)\right], \\ \left[\sqrt{3}xyz\left(10\,x^2 - 3\,y^2 - 3\,z^2\right)\left(y^2 - z^2\right), xyz\left(6\,x^4 - 3\,y^4 - 3\,z^4 - 10\,x^2(y^2 + z^2) + 20\,y^2z^2\right)\right] \end{array} \right\},$$

$$\mathcal{Q}^{(4)} = \left\{ \begin{array}{c} [yz, xz, xy]\,, \qquad \left[x\left(y^2 - z^2\right), y\left(z^2 - x^2\right), z\left(x^2 - y^2\right)\right], \\ \left[yz\left(y^2 + z^2 - 6\,x^2\right), xz\left(z^2 + x^2 - 6\,y^2\right), xy\left(x^2 + y^2 - 6\,z^2\right)\right], \\ \left[x\left(z^2 - y^2\right)\left(2\,x^2 - y^2 - z^2\right), y\left(x^2 - z^2\right)\left(2\,y^2 - z^2 - x^2\right), z\left(y^2 - z^2\right)\left(2\,z^2 - x^2 - y^2\right)\right], \\ \left[zy\left(30\,x^4 - 3\,y^4 - 3\,z^4 - 30\,x^2(y^2 + z^2) + 20\,y^2z^2\right), xz\left(30\,y^4 - 3\,z^4 - 3\,x^4 - 30\,y^2(z^2 + x^2) + 20\,x^2z^2\right), \right. \\ \left. yx\left(30\,z^4 - 3\,x^4 - 3\,y^4 - 30\,z^2(x^2 + y^2) + 20\,x^2y^2\right)\right], \\ \left[x\left(y^2 - z^2\right)\left(3\,x^4 - 5\,x^2(z^2 + y^2) + 15\,z^2y^2\right), y\left(z^2 - x^2\right)\left(3\,y^4 - 5\,y^2(x^2 + z^2) - 15\,x^2z^2\right), \right. \\ \left. z\left(x^2 - y^2\right)\left(3\,z^4 - 5\,z^2(y^2 + x^2) + 15\,y^2x^2\right)\right], \end{array} \right\},$$

$$\mathcal{Q}^{(5)} = \left\{ \begin{array}{c} [x,y,z], \quad \left[x\left(3\,y^2+3\,z^2-2\,x^2\right), y\left(3\,z^2+3\,x^2-2\,y^2\right), z\left(3\,x^2+3\,y^2-2\,z^2\right)\right], \\ \left[yz(y^2-z^2), zx(z^2-x^2), xy(x^2-y^2)\right], \\ \left[x\left(2\,x^4-5\,y^4-5\,z^4-10\,x^2(y^2+z^2)+60\,y^2z^2\right), y\left(2\,y^4-5\,x^4-5\,z^4-10\,y^2(x^2+z^2)+60\,x^2z^2\right),\right. \\ \left. z\left(2\,z^4-5\,x^4-5\,y^4-10\,z^2(x^2+y^2)+60\,x^2y^2\right)\right], \\ \left[yz\left(z^2-y^2\right)\left(10\,x^2-y^2-z^2\right), xz\left(x^2-z^2\right)\left(10\,y^2-x^2-z^2\right), xy\left(y^2-z^2\right)\left(10\,z^2-x^2-y^2\right)\right], \\ \left[yz\left(y^2-z^2\right)\left(5\,x^4-3\,x^2(y^2+z^2)+y^2z^2\right), xz\left(z^2-x^2\right)\left(5\,y^4-3\,y^2(x^2+z^2)+x^2z^2\right),\right. \\ \left. yx\left(x^2-y^2\right)\left(5\,z^4-3\,z^2(x^2+y^2)+x^2y^2\right)\right] \end{array} \right\}.$$

We observe that the minimal number of fundamental invariants is 4 and hence we are not dealing here with a reflection group. One can furthermore observe that, except for $\mathcal{Q}^{(1)} = \{[1]\}$, each $\mathcal{Q}^{(\ell)}$ has $\mathfrak{n}_\ell$ equivariants.

One might want to compute a Hironaka decomposition of the equivariant modules, and of polynomial ring by direct sum of these. For that one can pick the primary invariants to be the first three fundamental invariants, or $\mathcal{P} = \left\{x^2+y^2+z^2, \quad x^4+y^4+z^4, x^6+y^6+z^6\right\}$. The product of their degrees is 48, while the group has order 24. Hence a set of secondary invariants has cardinality 2. Applying the strategy of Section 5, one indeed obtains the secondary invariants $\mathcal{Q}^{(1)} = \left\{[1], \left[xyz(z^2-y^2)(x^2-z^2)(y^2-x^2)\right]\right\}$ while the rest of the symmetry adapted basis of $\mathbb{C}[\mathrm{x}]/\langle\mathcal{P}\rangle$ is the same as above. A similar result holds for Example 6.4

7 Conclusion and prospects

We presented three constructions for fundamental invariants and equivariants for the representation of a finite group $\mathfrak{G}$ over $\mathbb{C}$. These are the first algorithms to compute fundamental equivariants simultaneously to invariants.

When the representation of our group is over $\mathbb{R}$, the output can be recombined, or the algorithm modified, to offer the fundamental invariants and equivariants over $\mathbb{R}$ as well. And similarly for other subfields of $\mathbb{C}$, like $\mathbb{Q}$.

In the constructions we could have used *invariant direct complements* instead of *orthogonal complements w.r.t. the apolar product*. The algorithms are thus amenable to fields of positive characteristic in the non modular case, when the characteristic of the field does not divide the order of $\mathfrak{G}$ [Ser77, Chapter 15.5] This is certainly the case of the independent algorithm in Section 6. The case of the other two constructions is discussed next.

The first construction, that applies to reflection groups, relies entirely on [RH22, Algorithm 3]. This algorithm depends heavily on the apolar product, first off in the definition of the least interpolation space, and the basic linear algebra operation therein is the QR-decomposition. It would take an effort to remanufacture the algorithm for positive characteristic. On the other hand, in the second construction, that takes as input primary invariants, we can substitute [RH22, Algorithm 3], by [RH22, Section 5, Algorithm 1]. This latter computes a symmetry adapted basis of an appropriate invariant complement, of minimal degree, with LU-factorization. It is thus effective in positive characteristic.

References

[ATY97] S. Ariki, T. Terasoma, and H.-F. Yamada. Higher Specht polynomials. *Hiroshima Math. J.*, 27(1):177–188, 1997.

[BG85] C. Benson and L. Grove. *Finite reflection groups*, volume 99 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1985.

[CCDP15] P. Cassam-Chenaï, G. Dhont, and F. Patras. A fast algorithm for the construction of integrity bases associated to symmetry-adapted polynomial representations: application to tetrahedral XY_4 molecules. *J. Math. Chem.*, 53(1):58–85, 2015.

[CCP08] P. Cassam-Chenaï and F. Patras. Symmetry-adapted polynomial basis for global potential energy surfaces-applications to XY_4 molecules. *J. Math. Chem.*, 44(4):938–966, 2008.

[CH15] M. Collowald and E. Hubert. A moment matrix approach to computing symmetric cubatures. https://hal.inria.fr/hal-01188290, 2015.

[Che55] C. Chevalley. Invariants of finite groups generated by reflections. *Amer. J. Math.*, 77:778–782, 1955.

[CL00] P. Chossat and R. Lauterbach. *Methods in equivariant bifurcations and dynamical systems*, volume 15 of *Advanced Series in Nonlinear Dynamics*. World Scientific Publishing Co. Inc., River Edge, NJ, 2000.

[CLO05] D. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2005.

[CLO15] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015.

[DBR92] C. De Boor and A. Ron. The least solution for the polynomial interpolation problem. *Mathematische Zeitschrift*, 210(1), 1992.

[DK15] H. Derksen and G. Kemper. *Computational invariant theory*. Springer-Verlag, 2nd edition, 2015.

[DPZ15] G. Dhont, F. Patras, and B. Zhilinskií. The action of the special orthogonal group on planar vectors: integrity bases via a generalization of the symbolic interpretation of Molien functions. *J. Phys. A*, 48(3):035201, 19, 2015.

[FK77] K. Fox and B. Krohn. Computation of cubic harmonics. *J. Computational Phys.*, 25(4):386–408, 1977.

[FR09] J.-C. Faugère and S. Rahmany. Solving systems of polynomial equations with symmetries using SAGBI-Gröbner bases. In *ISSAC 2009—Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation*, pages 151–158. ACM, New York, 2009.

[FS92] A. Fässler and E. Stiefel. *Group theoretical methods and their applications*. Birkhäuser Boston, Inc., Boston, MA, 1992.

[FS13] J.-C. Faugere and J. Svartz. Gröbner bases - a computational approach to grobbner bases of ideals invariant under a commutative group: the non-modular case. In *Proceedings of the 38th international symposium on International symposium on symbolic and algebraic computation*, ISSAC '13, pages 347–354, New York, NY, USA, 2013. ACM.

[Gat90] K. Gatermann. Symbolic solution of polynomial equation systems with symmetry. In M. Nagata Sh. Watanabe, editor, *ISSAC'90 Tokyo, Japan*, pages 112–119. ACM-Press New York, 1990.

[Gat96] K. Gatermann. Semi-invariants, equivariants and algorithms. *Applicable Algebra in Engineering, Communication and Computing*, 7(2):105–124, 1996.

[Gat00] K. Gatermann. *Computer algebra methods for equivariant dynamical systems*, volume 1728 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2000.

[GHP19] P. Görlach, E. Hubert, and T. Papadopoulo. Rational invariants of even ternary forms under the orthogonal group. *Foundations of Computational Mathematics*, 2019.

[GP04] K. Gatermann and P. Parrilo. Symmetry groups, semidefinite programs, and sums of squares. *J. Pure Appl. Algebra*, 192(1-3):95–128, 2004.

[GSS88] M. Golubitsky, I. Stewart, and D. G. Schaeffer. *Singularities and groups in bifurcation theory. Vol. II*, volume 69 of *Applied Mathematical Sciences*. Springer-Verlag, New York, 1988.

[GVL96] G. Golub and C. Van Loan. *Matrix Computations (3rd Ed.)*. 1996.

[GY03] J. H. Grace and A. Young. *The Algebra of Invariants*. Cambridge Univ. Press, Cambridge, 1903.

[HL12] E. Hubert and G. Labahn. Rational invariants of scalings from Hermite normal forms. In *ISSAC 2012—Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, pages 219–226. ACM, New York, 2012.

[HL16] E. Hubert and G. Labahn. Computation of the invariants of finite abelian groups. *Mathematics of Computations*, 85(302):3029–3050, 2016.

[Kan01] R. Kane. *Reflection groups and invariant theory*, volume 5 of *CMS Books in Mathematics*. Springer-Verlag, New York, 2001.

[Kem99] G. Kemper. An algorithm to calculate optimal homogeneous systems of parameters. *Journal of Symbolic Computation*, 27(2):171–184, 1999.

[Kin13] S. King. Minimal generating sets of non-modular invariant rings of finite groups. *J. Symbolic Computation*, 48:101–109, 2013.

[LRS16] R. Lercier, C. Ritzenthaler, and J. Sijsling. Explicit Galois obstruction and descent for hyperelliptic curves with tamely cyclic reduced automorphism group. *Math. Comp.*, 85(300):2011–2045, 2016.

[Mac16] F. Macaulay. The algebraic theory of modular systems. *Cambridge Tracts in Mathematics and Mathematical Physics*, 19, 1916.

[Mes91] J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 313–334. Birkhäuser Boston, Boston, MA, 1991.

[MS00] H. Möller and T. Sauer. H-bases for polynomial interpolation and system solving. *Advances in Computational Mathematics*, 12(4):335–362, 2000.

[Mug72] J. Muggli. Cubic harmonics as linear combinations of spherical harmonics. *Z. Angew. Math. Phys.*, 23:311–317, 1972.

[MZ01] L. Michel and B. Zhilinskii. Symmetry, invariants, topology. i symmetry, invariants, topology. basic tools. *Physics report*, 34:11–84, 2001.

[MZF92] J. Mundy, A. Zisserman, and D. Forsyth, editors. *Application of invariance in computer vision*. Lecture Notes in Computer Science. Springer-Verlag, 1992.

[RH19] E. Rodriguez Bazan and E. Hubert. Symmetry preserving interpolation. In *Proceedings of the 2019 on International Symposium on Symbolic and Algebraic Computation*, ISSAC '19, pages 34–41, New York, NY, USA, 2019. Association for Computing Machinery.

[RH20] E. Rodriguez Bazan and E. Hubert. Ideal interpolation, H-bases and symmetry. In *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*, ISSAC '20, pages 402–409, New York, NY, USA, 2020. Association for Computing Machinery.

[RH21] E. Rodriguez Bazan and E. Hubert. Multivariate interpolation: Preserving and exploiting symmetry. *Journal of Symbolic Computation*, 107:1–22, 2021. https://doi.org/10.1016/j.jsc.2021.01.004. A preliminary version of the paper appeared as [RH19].

[RH22] E. Rodriguez Bazan and E. Hubert. Symmetry in multivariate ideal interpolation. 2022. https://hal.inria.fr/hal-0312976. A preliminary version of the paper appeared as [RH20].

[RTAL13] C. Riener, T. Theobald, L. J. Andrén, and J. B. Lasserre. Exploiting symmetries in SDP-relaxations for polynomial optimization. *Math. Oper. Res.*, 38(1):122–141, 2013.

[Ser77] J.-P. Serre. *Linear representations of finite groups*. Springer-Verlag, New York-Heidelberg, 1977.

[Spe35] W. Specht. Die irreduziblen Darstellungen der symmetrischen Gruppe. *Math. Z.*, 39(1):696–711, 1935.

[Sta79] R. Stanley. Invariants of finite groups and their applications to combinatorics. *Bull. Amer. Math. Soc. (N.S.)*, 1(3):475–511, 1979.

[Stu07] B. Sturmfels. *Algorithms in invariant theory*. Texts and Monographs in Symbolic Computation. Springer-Verlag, 2nd edition, 2007.

[TY93] T Terasoma and H. Yamada. Higher Specht polynomials for the symmetric group. *Proc. Japan Acad. Ser. A Math. Sci.*, 69(2):41–44, 1993.