Ideal Interpolation, H-Bases and Symmetry

Erick Rodriguez Bazan, Evelyne Hubert

Ideal Interpolation, H-Bases and Symmetry

Erick Rodriguez Bazan
Université Côte d'Azur, France
Inria Méditerranée, France
erick-david.rodriguez-bazan@inria.fr

Evelyne Hubert
Université Côte d'Azur, France
Inria Méditerranée, France
evelyne.hubert@inria.fr

ABSTRACT

Multivariate Lagrange and Hermite interpolation are examples of ideal interpolation. More generally an ideal interpolation problem is defined by a set of linear forms, on the polynomial ring, whose kernels intersect into an ideal.

For an ideal interpolation problem with symmetry, we address the simultaneous computation of a symmetry adapted basis of the least interpolation space and the symmetry adapted H-basis of the ideal. Beside its manifest presence in the output, symmetry is exploited computationally at all stages of the algorithm.

CCS CONCEPTS

• **Computing methodologies → Symbolic and algebraic algorithms**;

KEYWORDS

Interpolation; Symmetry; Representation Theory; Group Action; H-basis; Macaulay matrix; Vandermonde matrix

1 INTRODUCTION

Preserving and exploiting symmetry in algebraic computations is a challenge that has been addressed within a few topics and, mostly, for specific groups of symmetry; For instance interpolation and symmetric group [23], cubature [4, 14], global optimisation [17, 32], equivariant dynamical systems [15, 20] and solving systems of polynomial equations [12, 13, 16, 19, 21, 31, 38]. In [33] we addressed multivariate interpolation and in this article we go further with ideal interpolation. We provide an algorithm to compute simultaneously a symmetry adapted basis of the least interpolation space and a symmetry adapted H-basis of the associated ideal. In addition to being manifest in the output, symmetry is exploited all along the algorithm to reduce the size of the matrices involved, and avoid sizable redundancies. Based on QR-decomposition (as opposed to LU-decomposition previously) the algorithm also lends itself to numerical computations.

Multivariate Lagrange, and Hermite, interpolation are examples of the encompassing notion of ideal interpolation, introduced in [2]. They are defined by linear forms consisting of evaluation at some nodes, and possibly composed with differential operators, without *gaps*. More generally a space of linear forms Λ on the polynomial ring $\mathbb{K}[x] = \mathbb{K}[x_1, \ldots, x_n]$ is an ideal interpolation scheme if

$$\mathcal{I} = \bigcap_{\lambda\in\Lambda} \ker \lambda = \{p \in \mathbb{K}[x] : \lambda(p) = 0, \text{ for all } \lambda \text{ in } \Lambda\} \qquad (1)$$

is an ideal in $\mathbb{K}[x]$. In the case of Lagrange interpolation, $\mathcal{I}$ is the ideal of the nodes and is thus a radical ideal.

If Λ is invariant under the action of a group G, then so is $\mathcal{I}$. In [33] we addressed the computation of an interpolation space for Λ *i.e.,* a subspace of the polynomial ring that has a unique interpolant for each instantiated interpolation problem, that is both invariant and of minimal degree. An interpolation space for Λ identifies with the quotient space $\mathbb{K}[x]/\mathcal{I}$. Hence a number of operations related to $\mathcal{I}$ can already be performed with a basis of an interpolation space for Λ: decide of membership to $\mathcal{I}$, determine normal forms of polynomials modulo $\mathcal{I}$ and compute matrices of multiplication maps in $\mathbb{K}[x]/\mathcal{I}$. Yet it has also proved relevant to compute Gröbner bases or H-bases of $\mathcal{I}$.

Initiated in [26], for a set Λ of point evaluations, computing a Gröbner basis of $\mathcal{I}$ found applications in the design of experiments [29, 30]. As pointed out in [25], one can furthermore interpret the FGLM algorithm [10] as an instance of this problem. The linear forms are the coefficients, in the normal forms, of the reduced monomials. The alternative approach in [11] can be understood similarly.

The resulting algorithm then pertains to the Berlekamp-Massey-Sakata algorithm and is related the multivariate version of Prony's problem to compute Gröbner bases, border bases, or H-bases [1, 28, 35, 36]

All ,the above mentioned algorithms and complexity analyses heavily depend on a term order and basis of monomials. These are notoriously not suited for preserving symmetry. Our ambition in this paper is to showcase how symmetry can be embedded in the representation of both the interpolation space and the representation of the ideal. This is a marker for the more canonical representations.

The *least interpolation space*, defined in [6], and revisited in [33] is a canonically defined interpolation space. It serves here as the canonical representation of the quotient of the polynomial algebra by the ideal. It has great properties, even beyond symmetry, that cannot be achieved by a space spanned by monomials. In [33] we freed the computation of the least interpolation space from its reliance on the monomial basis by introducing *dual bases*. We pursue this approach here for the representation of the ideal by H-bases [24, 27]. Where Gröbner bases single out leading terms with a term order, H-bases work with leading forms and the orthogonality with respect to the apolar product. The least interpolation space then reveals itself as the orthogonal complement of the ideal of leading forms.

As a result, computing a H-basis of the interpolation ideal is achieved with linear algebra in subspaces of homogeneous polynomials of growing degrees. Yet we shall first redefine the concepts at play in an intrinsic manner, contrary to the computation centered approach in [27, 34]. The precise algorithm we shall offer to compute H-bases somehow fits in the loose sketch proposed in [5]. Yet we are now in a position to incorporate symmetry in a natural way, refining the algorithm to exploit it; A totally original contribution.

Symmetry is preserved and exploited thanks to the block diagonal structure of the matrices at play in the algorithms. This block diagonalisation, with predicted repetitions in the blocks, happens when the underlying maps are discovered to be equivariant and expressed in the related *symmetry adapted bases*. The case of the Vandermonde matrix was settled in [33]. In this paper, we also need the matrix of the prolongation map, knowned in the monomial basis as the Macaulay matrix. Figuring out the equivariance of this map is one of the original key results of this paper.

The paper is organized as follows. In Section 2 we define ideal interpolation and explain the identification of an interpolation space with the quotient algebra. In Section 3 we review H-bases and discuss how they can be computed in the ideal interpolation setting. In Section 4 we provide an algorithm to compute simultaneously a basis of the least interpolation space and an orthogonal H-basis of the ideal. In Section 5 we show how the Macaulay matrix can be block diagonalized in the presence of symmetry. This is then applied in Section 6 to obtain an algorithm to compute simultaneously a symmetry adapted basis of the least interpolation space and a symmetry adapted H-basis of the ideal. All along the paper, the definitions and notations comply with those in [33].

2 IDEAL INTERPOLATION

In this section, we consider the ideal interpolation problem and explain the identification of an interpolation space with the quotient algebra. We recall that the least interpolation space is the orthogonal complement of the ideal of the leading forms, $\mathcal{I}^0$.

$\mathbb{K}$ denotes either $\mathbb{C}$ or $\mathbb{R}$. $\mathbb{K}[x] = \mathbb{K}[x_1, \ldots, x_n]$ denotes the ring of polynomials in the variables $x_1, \ldots, x_n$ with coefficients in $\mathbb{K}$; $\mathbb{K}[x]_{\leq d}$ and $\mathbb{K}[x]_d$ the $\mathbb{K}$−vector spaces of polynomials of degree at most d and the space of homogeneous polynomials of degree d respectively. The *dual* of $\mathbb{K}[x]$, the set of $\mathbb{K}$−linear forms on $\mathbb{K}[x]$, is denoted by $\mathbb{K}[x]^*$. A typical example of a linear form on $\mathbb{K}[x]$ is the evaluation e_ξ at a point ξ of $\mathbb{K}^n$: $e_\xi(p) = p(\xi)$.

$\mathbb{K}[x]^*$ can be identified with the ring of formal power series $\mathbb{K}[[\partial]] = \mathbb{K}[[\partial_1, \ldots, \partial_r]]$, with the understanding that $\partial^\beta(x^\alpha) = \alpha!$ or 0 according to whether $\alpha = \beta$ or not. Concomitantly $\mathbb{K}[x]$ is equipped with the apolar product that is defined, for $p = \sum_\alpha p_\alpha x^\alpha$ and $q = \sum_\alpha q_\alpha x^\alpha$, by $\langle p, q\rangle := \overline{p}(\partial)q = \sum_\alpha \alpha!\overline{p}_\alpha q_\alpha \in \mathbb{K}$.

If $\mathcal{P}$ is a (homogeneous) basis of $\mathbb{K}[x]$ we denote $\mathcal{P}^\dagger$ its dual with respect to this scalar product. For $\lambda \in \mathbb{K}[x]^*$ we can write $\lambda = \sum_{p\in\mathcal{P}} \lambda(p)p^\dagger(\partial)$.

An *interpolation problem* is a pair (Λ, ϕ) where Λ is a finite dimensional linear subspace of $\mathbb{K}[x]^*$ and $\phi : \Lambda \longrightarrow \mathbb{K}$ is a $\mathbb{K}$-linear map. An interpolant, *i.e.,* a solution to the interpolation problem, is a polynomial p such that $\lambda(p) = \phi(\lambda)$ for any $\lambda \in \Lambda$. An *interpolation space for* Λ is a polynomial subspace P of $\mathbb{K}[x]$ such that there is a unique interpolant for any map ϕ.

The *least interpolation space* $\Lambda_\downarrow$ was introduced in [7], and revisited in [33]. The least term $\lambda_\downarrow \in \mathbb{K}[x]$ of a power series $\lambda \in \mathbb{K}[[\partial]]$ is the unique homogeneous polynomial for which $\lambda - \lambda_\downarrow(\partial)$ vanishes to highest possible order at the origin. Given a linear space of linear forms Λ, we define $\Lambda_\downarrow$ as the linear span of all $\lambda_\downarrow$ with $\lambda \in \Lambda$.

If $\mathcal{L} = \{\lambda_1, \lambda_2, \ldots, \lambda_r\}$ is a basis of Λ and $\mathcal{P} = \{p_1, p_2, \ldots, p_r\} \subset \mathbb{K}[x]$, then $\mathcal{P}$ is a basis for an interpolation space of Λ if and only if the *Vandermonde matrix*

$$W_{\mathcal{L}}^{\mathcal{P}} := \left[\lambda_i\left(p_j\right)\right]_{\substack{1\leq i\leq r\\1\leq j\leq r}} \qquad (2)$$

is invertible. This latter is to be interpreted as the matrix in the bases $\mathcal{P}$ and the dual of $\mathcal{L}$ of the restriction of the Vandermonde operator $w : \mathbb{K}[x] \to \Lambda^*$ such that $w(p)(\lambda) = \lambda(p)$. This is the adjoint of embedding $\Lambda \hookrightarrow \mathbb{K}[x]^*$ and hence is surjective.

All along this paper we shall assume that

$$\mathcal{I} = \ker w = \cap_{\lambda\in\Lambda} \ker \lambda$$

is an ideal. When for instance $\Lambda = \langle e_{\xi_1}, \ldots, e_{\xi_r}\rangle_K$ then $\mathcal{I}$ is the ideal of the points $\{\xi_1, \ldots, \xi_r\} \subset \mathbb{K}[x]$. One sees in general that $\dim \mathbb{K}[x]/\mathcal{I} = \dim \Lambda^* = \dim \Lambda =: r$.

With $Q = \{q_1, \ldots, q_r\} \subset \mathbb{K}[x]$, we can identify $\mathbb{K}[x]/\mathcal{I}$ with $\langle Q\rangle_\mathbb{K}$ if $\langle Q\rangle_\mathbb{K} \oplus \mathcal{I} = \mathbb{K}[x]$. With a slight shortcut, we say that Q is a basis for $\mathbb{K}[x]/\mathcal{I}$.

Proposition 2.1. *$Q = \{q_1, \ldots, q_r\} \subset \mathbb{K}[x]$ spans an interpolation space for Λ iff it is a basis for the quotient $\mathbb{K}[x]/\mathcal{I}$.*

Proof. If $Q = \{q_1, \ldots, q_r\}$ is a basis of $\mathbb{K}[x]/\mathcal{I}$ then for any $p \in \mathbb{K}[x]$ there is a $q \in \langle q_1, \ldots, q_r\rangle_\mathbb{K}$ such that $p \equiv q \mod \mathcal{I}$. Hence $\lambda(p) = \lambda(q)$ for any $\lambda \in \Lambda$ and thus $\langle Q\rangle_\mathbb{K}$ is an interpolation space for Λ. Conversely if $\langle q_1, \ldots, q_r\rangle_\mathbb{K}$ is an interpolation space for Λ then $\{q_1, \ldots, q_r\}$ are linearly independent modulo $\mathcal{I}$ and therefore a basis for $\mathbb{K}[x]/\mathcal{I}$. Indeed if $q = a_1q_1 + \ldots + a_rq_r \in \mathcal{I}$ then any interpolation problem has multiple solutions in $\langle Q\rangle_\mathbb{K}$, i.e, if p is the solution of (Λ, ϕ) so is $p + q$, contradicting the interpolation uniqueness on $\langle Q\rangle_\mathbb{K}$. □

For $p \in \mathbb{K}[x]$ we can find its natural projection on $\mathbb{K}[x]/\mathcal{I}$ by taking the unique $q \in \langle Q\rangle_\mathbb{K}$ that satisfies $\lambda(q) = \lambda(p)$ for all $\lambda \in \Lambda$. From a computational point of view, q is obtained by solving the Vandermonde system, i.e.,

$$q = (q_1, \ldots, q_r)\left(W_{\mathcal{L}}^{Q}\right)^{-1}\begin{pmatrix}\lambda_1(p)\\ \vdots \\ \lambda_r(p)\end{pmatrix} \text{ with } \mathcal{L} = \{\lambda_1, \ldots, \lambda_r\} \text{ a basis of } \Lambda.$$

Similarly, the matrix of the multiplication map, in the basis Q, is

$$\begin{array}{rccc} \mathfrak{m}_p : & \mathbb{K}[x]/\mathcal{I} & \to & \mathbb{K}[x]/\mathcal{I}, \\ & [q] & \mapsto & [pq] \end{array}$$

is obtained as $[\mathfrak{m}_p]_Q = \left(W_{\mathcal{L}}^{Q}\right)^{-1} W_{\mathcal{L}\circ m_p}^{Q}$ where $\mathcal{L} \circ m_p = \{\lambda_1 \circ m_p, \ldots, \lambda_r \circ m_p\}$.

When working with Gröbner bases, one fixes a term order and focuses on leading terms of polynomials and the initial ideal of $\mathcal{I}$. The basis of choice for $\mathbb{K}[x]/\mathcal{I}$ consists of the monomials that do not belong to the initial ideal. An H-basis of $\mathcal{I}$ is somehow the complement of the least interpolation space $\Lambda_\downarrow$ and hence can be made to reflect the possible invariance of Λ and $\mathcal{I}$. Instead of leading terms, the focus is then on the leading homogeneous forms.

Hereafter we denote by p^0 the leading homogeneous form of p, i.e., the unique homogeneous polynomial such that $\deg\left(p - p^0\right) < \deg(p)$. Given a set of polynomials P we denote $P^0 = \left\{p^0 \mid p \in P\right\}$.

Proposition 2.2. *Let Q be an interpolation space of minimal degree for Λ. Then $Q \oplus \mathcal{I}^0 = \mathbb{K}[x]$.*

Proof. We proceed by induction on the degree, i.e, we assume that any polynomial p in $\mathbb{K}[x]_{\leq d}$ can be written as $p = q + l$ where $q \in Q$ and $l \in \mathcal{I}^0$. Note that the hypothesis holds trivially when d is equal to zero.

Now let $p \in \mathbb{K}[x]_{\leq d+1}$. Since $\mathbb{K}[x] = \langle Q \rangle_{\mathbb{K}} \oplus \mathcal{I}$ there exists $q \in Q$ and $l \in \mathcal{I}$ such that $p = q + l$. Since Q is of minimal degree, q and l are in $\mathbb{K}[x]_{\leq d+1}$. Writing $l = l^0 + l_1$ he have $p = q + l^0 + l_1$ with $l_1 \in \mathbb{K}[x]_{\leq d}$ then by induction $l_1 = q_1 + l_2$ with $q_1 \in Q$ and $l_2 \in \mathcal{I}^0$ and therefore $p = q + q_1 + l^0 + l_2 \in Q \oplus I^0$. □

As a consequence we retrieve the result of [7, Theorem 4.8].

Corollary 2.3. *Considering orthogonality with respect to the apolar product it holds that* $\Lambda_{\downarrow} \overset{\perp}{\oplus} \mathcal{I}^0 = \mathbb{K}[x]$.

Proof. Follows from the fact that $\lambda(p) = 0 \Rightarrow \langle \lambda_{\downarrow}, p^0 \rangle = 0$. □

3 H-BASES

H-bases were introduced by [24]. The use of H-basis in interpolation has been further studied in [27, 34]. In this section we review the definitions and present the sketch of an algorithm to compute the H-basis of $\mathcal{I} = \bigcap_{\lambda \in \Lambda} \ker \lambda$.

Definition 3.1. A finite set $\mathcal{H} := \{h_1, \ldots, h_m\} \subset \mathbb{K}[x]$ is an H-basis of the ideal $\mathcal{I} := \langle h_1, \ldots, h_m \rangle$ if, for all $p \in \mathcal{I}$ there are $g_1, \ldots g_m$ such that,

$$p = \sum_{i=1}^{m} h_i g_i \text{ and } \deg(h_i) + \deg(g_i) \leq \deg(p), i = 1, \ldots, m.$$

Theorem 3.2. *[27] Let $\mathcal{H} := \{h_1, \ldots, h_m\}$ and $\mathcal{I} := \langle \mathcal{H} \rangle$. Then the following conditions are equivalent:*

(1) *$\mathcal{H}$ is an H-basis of $\mathcal{I}$.*
(2) $\mathcal{I}^0 := \left\langle \left\{ h^0 \mid h \in \mathcal{I} \right\} \right\rangle = \left\langle h_1^0, \ldots, h_m^0 \right\rangle$.

Hilbert Basis Theorem says that $\mathcal{I}^0$ has a finite basis, hence any ideal in $\mathbb{K}[x]$ has a finite H-basis. We shall now introduce the concepts of minimal, orthogonal and reduced H-basis. The notion of orthogonality is considered w.r.t the apolar product. Our definitions somewhat differ from [27] as we dissociate them from the computational aspect. We need to introduce first the following vector space of homogeneous polynomials.

Definition 3.3. Given a set $\mathcal{H} = \{h_1, \ldots, h_m\}$ of homogeneous polynomials in $\mathbb{K}[x]$ and a degree d, we define the subspace $\mathrm{V}_d(\mathcal{H})$ as

$$\mathrm{V}_d(\mathcal{H}) = \left\{ \sum_{i=1}^{s} g_i h_i \mid g_i \in \mathbb{K}[x]_{d-\deg(h_i)} \right\} \subset \mathbb{K}[x]_d.$$

$\mathrm{V}_d(\mathcal{H})$ is the image of the linear map ψ_d:

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

We denote by $\mathrm{M}_{\mathcal{M}_d, \mathcal{P}_d}(\mathcal{H})$ the matrix of ψ_d in the bases $\mathcal{M}_d$ and $\mathcal{P}_d$ of $\mathbb{K}[x]_{d-d_1} \times \ldots \times \mathbb{K}[x]_{d-d_m}$ and $\mathbb{K}[x]_d$ respectively. It is referred to as the Macaulay matrix for $\mathcal{H}$. We can write $\mathrm{V}_d(\mathcal{H})$ as

$$\mathrm{V}_d(\mathcal{H}) = \left\{ \sum_{i=0}^{|\mathcal{P}_d|} a_i p_i \mid (a_1, \ldots, a_{|\mathcal{P}_d|}) \in \mathcal{R}\left(\mathrm{M}_{\mathcal{M}_d, \mathcal{P}_d}(\mathcal{H})\right) \right\},$$

where $\mathcal{R}\left(\mathrm{M}_{\mathcal{M}_d, \mathcal{P}_d}(\mathcal{H})\right)$ denotes the column space of $\mathrm{M}_{\mathcal{M}_d, \mathcal{P}_d}(\mathcal{H})$.

We shall use the notation P_d^0 for the set of the degree d elements of P^0. In other words $P_d^0 = P^0 \cap \mathbb{K}[x]_d$.

Definition 3.4. We say that an H-basis $\mathcal{H}$ is minimal if, for any $d \in \mathbb{N}$, $\mathcal{H}_d^0$ is linearly independent and

$$V_d\left(\mathcal{I}_{d-1}^0\right) \oplus \left\langle \mathcal{H}_d^0 \right\rangle_{\mathbb{K}} = \mathcal{I}_d^0. \tag{3}$$

Furthermore $\mathcal{H}$ is said to be orthogonal if $\left\langle \mathcal{H}_d^0 \right\rangle_{\mathbb{K}}$ is the orthogonal complement of $V_d\left(\mathcal{I}_{d-1}^0\right)$ in $\mathcal{I}_d^0$.

Note that if h_i and h_j are two elements with $\deg h_i > \deg h_j$ of an orthogonal H-basis we have

$$\left\langle h_i^0, p h_j^0 \right\rangle = 0 \text{ for all } p \in \mathbb{K}[x]_{\deg h_i - \deg h_j}.$$

Definition 3.5. Let $\mathcal{H} = \{h_1, \ldots, h_m\}$ be an orthogonal H-basis of an ideal $\mathcal{I}$. The *reduced* H-basis of $\mathcal{H}$ is defined by

$$\widetilde{\mathcal{H}} = \left\{ h_1^0 - \widetilde{h_1^0}, \ldots, h_m^0 - \widetilde{h_m^0} \right\} \tag{4}$$

where, for $p \in \mathbb{K}[x]$, $\tilde{p}$ is the projection of p on the orthogonal complement of $\mathcal{I}^0$ parallel to $\mathcal{I}$.

[27, Lemma 6.2] show how $\tilde{p}$ can be computed given $\mathcal{H}$.

Schematic computation of H-bases. In the next section we elaborate on an algorithm to compute concomitantly the least interpolation space and an H-basis for the ideal associated to a set of linear forms Λ. As a way of introduction we reproduce the sketch of an algorithm as proposed by [5] to compute an H-basis until degree D. It is based on the asumption that we have access to a basis of $\mathcal{I}_d := \mathcal{I} \cap \mathbb{K}[x]_{\leq d}$ for any d.

Algorithm 1 [5] H-basis construction

Input: - a degree D.
- basis for $\mathcal{I}_d$ for $1 \leq d \leq D$.
Output : - an H-basis until degree D

1: $\mathcal{H} \leftarrow \{\}$;
2: **for** $d = 0$ `to` D **do**
3: $C_d \leftarrow$ a basis of $\mathrm{V}_d(\mathcal{H}^0)$;
4: $\mathcal{B}_d \leftarrow$ a basis for the complement of $\mathrm{V}_d(\mathcal{H})$ in $\mathcal{I}_d^0$;
5: $\widehat{\mathcal{B}}_d \leftarrow$ projection of $\mathcal{B}_d$ in $\mathcal{I}_d$
6: $\mathcal{H} \leftarrow \mathcal{H} \bigcup \widehat{\mathcal{B}}_d$;
7: **return** $\mathcal{H}$;

The correctness of Algorithm 1 is shown by induction. Assume that $\mathcal{H}_{d-1}$ consists of the polynomials in an H-basis of $\mathcal{I}$ up to degree $d-1$. Consider $p \in \mathcal{I}$ with $\deg(p) = d$. By Step 4 in Algorithm 1 we have

$$p^0 = \sum_{h_i \in \mathcal{H}} h_i^0 g_i + \sum_{b_i \in \mathcal{B}_d} a_i b_i \tag{5}$$

with $g_i \in \mathbb{K}[x]_{d-\deg(h_i)}$ and $a_i \in \mathbb{K}$. From (5) we have that $p \in \mathcal{I}$ and $\sum_{h_i \in \mathcal{H}} h_i g_i + \sum_{b_i \in \mathcal{B}_{d+1}} a_i \hat{b}_i \in \mathcal{I}$ have the same leading form. Thus

$$p - \sum_{h_i \in \mathcal{H}_{d-1}} h_i g_i - \sum_{b_i \in \mathcal{B}_d} a_i \hat{b}_i \in \mathcal{I}_{d-1}$$

therefore using the induction hypothesis we get that

$$p = \sum_{h_i \in \mathcal{H}_{d-1}} h_i g_i + \sum_{b_i \in \mathcal{B}_{d+1}} a_i \hat{b}_i + \sum_{h_i \in \mathcal{H}_{d-1}} h_i q_i$$

with $q_i \in \mathbb{K}[\mathrm{x}]_{\leq d-1-\deg(h_i)}$ and therefore $\mathcal{H}$ is an H-basis.

Algorithm 1 can be applied in the ideal interpolation scheme. In this setting a basis of $\mathcal{I}_d$ can be computed for any d using Linear Algebra techniques due to the following relation.

$$\mathcal{I}_d = \left\{ \sum_{i=1}^{|\mathcal{P}_{\leq d}|} a_i p_i \mid \left(a_1, \ldots, a_{|\mathcal{P}_{\leq d}|}\right)^t \in \ker\left(\mathrm{W}_{\mathcal{L}}^{\mathcal{P}_{\leq d}}\right) \text{ and } p_i \in \mathcal{P}_{\leq d} \right\},$$

for any basis $\mathcal{P}_{\leq d}$ of $\mathbb{K}[\mathrm{x}]_{\leq d}$.

In the next section we will give an efficient and detailed version of Algorithm 1 in the ideal interpolation case. We will integrate the computations of an H-basis for $\mathcal{I} = \cap_{\lambda\in\Lambda} \ker \lambda$ and a basis for $\Lambda_{\downarrow}$.

When the ideal is given by a set of generators it is also possible to compute an H-basis with linear algebra if you know a bound on the degree of the syzygies of the generators. A numerical approach, using singular value decomposition, was introduced in [22]. Alternatively an extension of Buchberger's algorithm is presented in [27]. It relies, at each step, on the computation of a basis for the module of syzygies of a set of homogeneous polynomials.

4 SIMULTANEOUS COMPUTATION OF THE H-BASIS AND LEAST INTERPOLATION SPACE

In this section we present an algorithm to compute both a (orthogonal) basis of $\Lambda_{\downarrow}$ and an orthogonal H-basis $\mathcal{H}$ of the ideal $\mathcal{I} = \cap_{\lambda\in\Lambda} \ker \lambda$. We proceed degree by degree. At each iteration of the algorithm we compute a basis of $\Lambda_{\downarrow} \cap \mathbb{K}[\mathrm{x}]_d$ and the set $\mathcal{H}^0_d = \mathcal{H}^0 \cap \mathbb{K}[\mathrm{x}]_d$. Recall from Corollary 2.3, Theorem 3.2, and Definition 3.4 that

$$\mathbb{K}[\mathrm{x}] = \Lambda_{\downarrow} \overset{\perp}{\oplus} \mathcal{I}^0, \quad \mathcal{I}^0 = \langle \mathcal{H}^0 \rangle, \quad \text{and} \quad \mathcal{I}^0_d = V_d\left(\mathcal{I}^0_{d-1}\right) \overset{\perp}{\oplus} \langle \mathcal{H}^0_d \rangle_{\mathbb{K}}.$$

$\mathcal{I}$ is the kernel of the Vandermonde operator while $\Lambda_{\downarrow}$ can be inferred from a rank revealing form of the Vandermonde matrix. With orthogonality prevailing in the objects we compute it is natural that the QR-decomposition plays a central role in our algorithm.

For a $m\times n$ matrix M, the QR-decomposition is M = QR where Q is a $m\times m$ orthogonal matrix and R is a $m\times n$ upper triangular matrix. If r is the rank of M the first r columns of Q form an orthogonal basis of the column space of M and the remaining $m-r$ columns of Q form an orthogonal basis of the kernel of M^T [18, Theorem 5.2.1]. We thus often denote the QR-decomposition of a matrix M as

$$[\mathrm{Q}_1 \mid \mathrm{Q}_2] \cdot \begin{bmatrix} \mathrm{R} \\ 0 \end{bmatrix} = \mathrm{M}$$

where $\mathrm{Q}_1 \in \mathbb{K}^{m\times r}$, $\mathrm{Q}_2 \in \mathbb{K}^{m\times(m-r)}$ and $\mathrm{R} \in \mathbb{K}^{r\times n}$. Algorithms to compute the QR-decomposition can be found for instance in [18].

In the Lagrange interpolation case, Fassino and Möller [8] already used the QR-decomposition to propose a variant of the BM-algorithm [26] so as to compute a monomial basis of an interpolation space, the complement of the initial ideal for a chosen term order. They furthermore study the gain in numerical stability for perturbed data. We shall use QR-decomposition to further obtain a homogeneous basis of $\Lambda_{\downarrow}$ and an orthogonal H-basis of the ideal.

Due to Corollary 2.3 the reduction $\tilde{p}$ of p that appeared in Definition 3.5 is the unique interpolant of p in $\Lambda_{\downarrow}$.

Definition 4.1. Given a space of linear forms Λ, we denote by $\Lambda_{\geq d}$ the subspace of Λ given by

$$\Lambda_{\geq d} = \left\{\lambda \in \Lambda \mid \lambda_{\downarrow} \in \mathbb{K}[\mathrm{x}]_{\geqslant d}\right\} \cup \{0\}.$$

Hereafter we organize the elements of the bases of $\mathbb{K}[\mathrm{x}]$, Λ, or their subspaces, as row vectors. In particular $\mathcal{P}$ and $\mathcal{P}^\dagger$ are dual homogeneous bases for $\mathbb{K}[\mathrm{x}]$ according to the apolar product. Their degree part $\mathcal{P}_d$ and $\mathcal{P}^\dagger_d$ are dual bases of $\mathbb{K}[\mathrm{x}]_d$.

A basis $\mathcal{L}_{\geq d}$ of $\Lambda_{\geq d}$ can be computed inductively thanks to the following observation.

Proposition 4.2. *Assume $\mathcal{L}_{\geq d}$ is a basis of $\Lambda_{\geq d}$. Consider the QR-decomposition*

$$\mathrm{W}^{\mathcal{P}_d}_{\mathcal{L}_{\geq d}} = [\mathrm{Q}_1 \mid \mathrm{Q}_2] \cdot \begin{bmatrix} \mathrm{R}_d \\ 0 \end{bmatrix}$$

and the related change of basis $[\mathcal{L}_d \mid \mathcal{L}_{\geq d+1}] = \mathcal{L}_{\geq d} \cdot [\mathrm{Q}_1 \mid \mathrm{Q}_2]$. Then

- *$\mathcal{L}_{\geq d+1}$ is a basis of $\Lambda_{\geq d+1}$;*
- *$\mathrm{R}_d = \mathrm{W}^{\mathcal{P}_d}_{\mathcal{L}_d}$ has full row rank;*
- *The components of $\mathcal{L}_{d\downarrow} = \mathcal{P}^\dagger_d \cdot R^T_d$ form a basis of $\Lambda_{\downarrow} \cap \mathbb{K}[\mathrm{x}]_d$.*

We shall furthermore denote by $\mathcal{L}_{\leq d} = \bigcup_{i=0}^d \mathcal{L}_i$ the thus constructed basis of a complement of $\Lambda_{\geq d+1}$ in Λ.

Proof. It all follows from the fact that a change of basis $\mathcal{L}' = \mathcal{L}Q$ of Λ implies that $\mathrm{W}^{\mathcal{P}}_{\mathcal{L}'} = Q^T \mathrm{W}^{\mathcal{P}}_{\mathcal{L}}$. In the present case $Q = [\mathrm{Q}_1 \mid \mathrm{Q}_2]$ is orthogonal and hence $Q^T = Q^{-1}$.

The last point simply follows from the fact that, for $\lambda \in \Lambda$, $\lambda = \sum_{p\in\mathcal{P}} \lambda(p) p^\dagger(\partial)$. Hence if $T = \mathrm{W}^{\mathcal{P}}_{\mathcal{L}}$ then the j-th component of $\mathcal{L}$ is $\sum_i t_{ji} p^\dagger(\partial)$. □

This construction gives us a basis of $\Lambda_{\downarrow} \cap \mathbb{K}[\mathrm{x}]_d$ in addition to a basis of $\Lambda_{\geq d+1}$ to pursue the computation at the next degree. Before going there, we need to compute a basis $\mathcal{H}^0_d$ for the complement of $V_d(\mathcal{H}^0_{<d})$ in $\mathcal{I}^0_d$. For that we shall use an additional QR-decomposition as explained in Proposition 4.5, after two preparatory lemmas.

Lemma 4.3. *Let $d \geq 0$ and let $\mathcal{P}_d$ be a basis of $\mathbb{K}[\mathrm{x}]_d$ then:*

$$\mathcal{I}^0_d = \left\{ \sum_{i=1}^{|\mathcal{P}_d|} a_i p_i \mid \left(a_1, \ldots, a_{|\mathcal{P}_d|}\right)^t \in \ker\left(\mathrm{W}^{\mathcal{P}_d}_{\mathcal{L}_d}\right) \text{ and } p_i \in \mathcal{P}_d \right\}.$$

Proof. Recall that $\mathcal{I}$ is the kernel of the Vandermonde operator, and $\mathrm{W}^{\mathcal{P}}_{\mathcal{L}}$ is the matrix of this latter. The Vandermonde submatrix $\mathrm{W}^{\mathcal{P}_{\leq d}}_{\mathcal{L}_{\leq d}}$ can be written as follows

$$\mathrm{W}^{\mathcal{P}_{\leq d}}_{\mathcal{L}_{\leq d}} = \mathrm{W}^{\mathcal{P}_{\leq d}}_{[\mathcal{L}_{\leq d-1} \mid \mathcal{L}_d]} = \begin{pmatrix} \mathrm{W}^{\mathcal{P}_{\leq d-1}}_{\mathcal{L}_{\leq d-1}} & \mathrm{W}^{\mathcal{P}_d}_{\mathcal{L}_{\leq d-1}} \\ 0 & \mathrm{W}^{\mathcal{P}_d}_{\mathcal{L}_d} \end{pmatrix} \tag{6}$$

where $\mathrm{W}^{\mathcal{P}_{\leq d-1}}_{\mathcal{L}_{\leq d-1}}$ has full row rank.

Assume first that p is a polynomial in $\mathcal{I}^0_d$. Then there is $q \in \mathcal{I}$ of degree d such that $q^0 = p$. Let $\mathrm{q} = \begin{pmatrix} \mathrm{q}_{\leq d-1} \\ \mathrm{q}_d \end{pmatrix}$ and $\mathrm{p} = \mathrm{q}_d$ be the coefficients of q and p respectively in the basis $\mathcal{P}$. As $q \in \mathcal{I}_d$ we have that

$$\mathrm{W}_{\mathcal{L}_{\le d}}^{\mathcal{P}_{\le d}} \cdot \mathrm{q} = \begin{pmatrix} \mathrm{W}_{\mathcal{L}_{\le d-1}}^{\mathcal{P}_{\le (d-1)}} \cdot \mathrm{q}_{\le d-1} + \mathrm{W}_{\mathcal{L}_{\le d-1}}^{\mathcal{P}_d} \cdot \mathrm{q}_d \\ \mathrm{W}_{\mathcal{L}_d}^{\mathcal{P}_d} \cdot \mathrm{q}_d \end{pmatrix} = 0$$

and therefore $\mathrm{p} = \mathrm{q}_d$ is in kernel of $\mathrm{W}_{\mathcal{L}_d}^{\mathcal{P}_d}$. Now let v a vector in the kernel of $\mathrm{W}_{\mathcal{L}_d}^{\mathcal{P}_d}$. A vector u such that $\begin{pmatrix} \mathrm{u} \\ \mathrm{v} \end{pmatrix} \in \mathbb{K}^{\binom{n+d}{d}}$ and $\mathrm{W}_{\mathcal{L}_{\le d}}^{\mathcal{P}_{\le d}} \cdot \begin{pmatrix} \mathrm{u} \\ \mathrm{v} \end{pmatrix} = 0$ can be found as the solution of the following equation.

$$\mathrm{W}_{\mathcal{L}_{\le d-1}}^{\mathcal{P}_{\le (d-1)}} \mathrm{u} = \mathrm{W}_{\mathcal{L}_d}^{\mathcal{P}_d} \mathrm{v} - \mathrm{W}_{\mathcal{L}_{\le d-1}}^{\mathcal{P}_d} \mathrm{v}. \tag{7}$$

As $\mathrm{W}_{\mathcal{L}_{\le d-1}}^{\mathcal{P}_{\le (d-1)}}$ has full row rank, Equation 7 always has a solution. Then $\mathcal{P}_{\le d} \cdot \begin{pmatrix} \mathrm{u} \\ \mathrm{v} \end{pmatrix} \in \mathcal{I}$ and therefore $\mathcal{P}_d \cdot \mathrm{v} \in \mathcal{I}_d^0$. □

Lemma 4.4. *Consider the row vector* q *of coefficients of a polynomial q of $\mathbb{K}[\mathrm{x}]_d$ in the basis $\mathcal{P}_d$. The polynomial q is in the orthogonal complement of $\mathrm{V}_d(\mathcal{H})$ in $\mathbb{K}[\mathrm{x}]_d$ if and only if the row vector* q *is in the left kernel of $\mathrm{M}_{\mathcal{M}_d, \mathcal{P}_d^\dagger}(\mathcal{H})$.*

Proof. The columns of $\mathrm{M}_{\mathcal{M}_d, \mathcal{P}_d^\dagger}$ are the vectors of coefficients, in the basis $\mathcal{P}_d^\dagger$, of polynomials that span $\mathrm{V}_d(\mathcal{H})$. The membership of q in the left kernel of $\mathrm{M}_{\mathcal{M}_d, \mathcal{P}_d^\dagger}(\mathcal{H})$ translates as the apolar product of q with these vectors to be zero. And conversely. □

Proposition 4.5. *Consider the QR-decomposition*

$$\begin{bmatrix} \left(\mathrm{W}_{\mathcal{L}_d}^{\mathcal{P}_d}\right)^T & \mathrm{M}_{\mathcal{M}_d, \mathcal{P}_d^\dagger}(\mathcal{H}) \end{bmatrix} = [\mathrm{Q}_1 \mid \mathrm{Q}_2] \cdot \begin{bmatrix} \mathrm{R} \\ 0 \end{bmatrix}$$

The components of the row vector $\mathcal{P}_d \cdot Q_2$ span the orthogonal complement of $\mathrm{V}_d(\mathcal{H})$ in $\mathcal{I}_d^0$.

Proof. The columns in Q_2 span $\ker \mathrm{W}_{\mathcal{L}_d}^{\mathcal{P}_d} \cap \ker \left(\mathrm{M}_{\mathcal{M}_d, \mathcal{P}_d^\dagger}\right)^t$. The result thus follows from Lemmas 4.3 and 4.4. □

We are now able to show the correctness and termination of Algorithm 2.

Correctness. In the spirit of Algorithm 1, Algorithm 2 proceeds degree by degree. At the iteration for degree d we first compute a basis for $\Lambda_{\ge d+1}$ by splitting $\mathcal{L}_{\ge d}$ into $\mathcal{L}_{\ge d+1}$ and $\mathcal{L}_d$. As explained in Proposition 4.2, this is obtained through the QR-decomposition of $\mathrm{W}_{\mathcal{L}_{\ge d}}^{\mathcal{P}_d}$. From this decomposition we also obtain a basis for $\Lambda_\downarrow \cap \mathbb{K}[\mathrm{x}]_d$ as well as $\mathrm{W}_{\mathcal{L}_d}^{\mathcal{P}_d}$. We then go after $\mathcal{H}_d^0$, which spans the orthogonal complement of $\mathrm{V}_d(\mathcal{H}_{\le d-1}^0)$ in $\mathcal{I}_d^0$. The elements of $\mathcal{H}_d^0$ are computed via intersection of $\ker \mathrm{W}_{\mathcal{L}_d}^{\mathcal{P}_d}$ and $\ker \left(\mathrm{M}_{\mathcal{M}_d, \mathcal{P}_d^\dagger}\right)^t$ as showed in Proposition 4.5. Algorithm 2 stops when we reach a degree δ such that $\mathcal{L}_{\ge \delta}$ is empty. Notice that for $d \ge \delta$ the matrix $\mathrm{W}_{\mathcal{L}_d}^{\mathcal{P}_d}$ is an empty matrix and therefore its kernel is the full space $\mathbb{K}[\mathrm{x}]_d$. Then as a consequence of Lemma 4.3, for all $d > \delta$ we have that $V_d(\mathcal{I}_{d-1}^0) = \mathcal{I}_d^0$ hence $\langle \mathcal{H}_d^0 \rangle$ is an empty set. The latter implies that when the algorithm stops we have computed the full H-basis $\mathcal{H}^0$ for $\mathcal{I}^0$.

We then obtain an H-basis of $\mathcal{I}$ by finding the projections, onto $\Lambda_\downarrow$ and parallel to $\mathcal{I}$, of the elements of $\mathcal{H}^0$. These are the polynomials of $\Lambda_\downarrow$ interpolating the elements of $\mathcal{H}^0$ according to Λ.

Algorithm 2

Input: - $\mathcal{L}$ a basis of Λ ($r = |\mathcal{L}| = \dim(\Lambda)$)
- $\mathcal{P}$ a basis of $\mathbb{K}[\mathrm{x}]_{\le r}$
- $\mathcal{P}^\dagger$ the dual basis of $\mathcal{P}$ w.r.t the apolar product.

Output: - $\mathcal{H}$ a reduced H-basis for $\mathcal{I} := \ker \Lambda$
- $\mathcal{P}_\Lambda$ a basis of the least interpolation space of Λ.

1: $\mathcal{H}^0 \leftarrow \{\}$, $\mathcal{P}_\Lambda \leftarrow \{\}$
2: $d \leftarrow 0$
3: $\mathcal{L}_{\le 0} \leftarrow \{\}$, $\mathcal{L}_{\ge 0} \leftarrow \mathcal{L}$
4: **while** $\mathcal{L}_{\ge d} \ne \{\}$ **do**
5: $\quad \mathrm{Q} \cdot \begin{bmatrix} \mathrm{R}_d \\ 0 \end{bmatrix} = \mathrm{W}_{\mathcal{L}_{\ge d}}^{\mathcal{P}_d}$ ▷ QR-decomposition of $\mathrm{W}_{\mathcal{L}_{\ge d}}^{\mathcal{P}_d}$
6: $\quad \mathcal{P}_\Lambda \leftarrow \mathcal{P}_\Lambda \bigcup \mathcal{P}_d^\dagger \cdot \mathrm{R}_d^T$
7: $\quad [\mathcal{L}_d \mid \mathcal{L}_{\ge d+1}] \leftarrow \mathcal{L}_{\ge d} \cdot \mathrm{Q}^T$ ▷ Note that $\mathrm{R}_d = \mathrm{W}_{\mathcal{L}_d}^{\mathcal{P}_d}$
8: $\quad \mathcal{L}_{\le d+1} \leftarrow \mathcal{L}_{\le d} \cup \mathcal{L}_d$
9: $\quad [\mathrm{Q}_1 \mid \mathrm{Q}_2] \cdot \mathrm{R} = \begin{bmatrix} \mathrm{R}_d^T & \mathrm{M}_{\mathcal{M}_d, \mathcal{P}_d^\dagger}(\mathcal{H}) \end{bmatrix}$
10: $\quad \mathcal{H}^0 \leftarrow \mathcal{H}^0 \bigcup \mathcal{P}_d \cdot \mathrm{Q}_2$
11: $\quad d \leftarrow d + 1$
12: **for all** $p \in \mathcal{H}^0$ **do**
13: $\quad \mathcal{H} \leftarrow \mathcal{H} \bigcup \left\{ p - \mathcal{P}_\Lambda \left(\mathrm{W}_{\mathcal{L}_{\le d}}^{\mathcal{P}_\Lambda} \right)^{-1} (\mathcal{L}_{\le d})^T \right\}$
14: **return** $(\mathcal{H}, \mathcal{P}_\Lambda)$

Termination. Considering $r := \dim(\Lambda)$ we have that $\mathcal{L}_{\ge r}$ is an empty set, this implies that in the worst case our algorithm stops after r iterations.

Complexity. The most expensive computational step in Algorithms 2 is the computation of the kernel of $\left[\left(\mathrm{W}_{\mathcal{L}_d}^{\mathcal{P}_d}\right)^T \ \mathrm{M}_{\mathcal{M}_d, \mathcal{P}_d^\dagger}(\mathcal{H}) \right]$, with number of columns and rows given by

$$\begin{aligned} \mathrm{row}(d) &= \binom{d+n-1}{n-1} = \frac{d^{n-1}}{(n-1)!} + O\left(d^{n-1}\right) \\ \mathrm{col}(d) &= \sum_{i=1}^{|\mathcal{H}|} \binom{d-d_i+n-1}{n-1} + |\mathcal{L}_d| = \frac{|\mathcal{H}| d^{n-1}}{(n-1)!} + O\left(d^{n-1}\right) \end{aligned} \tag{8}$$

where $d_1, \ldots, d_{|\mathcal{H}|}$ are the degrees of the elements of the computed H-basis until degree d. Then the computational complexity of Algorithm 2 relies on the method used for the kernel computation of $VM(d)$, which in our case is the QR-decomposition.

We are giving a frame for the simultaneous computation of an H-basis and the Least interpolation space, but there is still room for improving the performance of Algorithm 2. The structure of the Macaulay matrix might be taken into account to alleviate the linear algebra operations as for instance in [1]. We can also consider different variants of Algorithm 2. In Proposition 4.6 we show that orthogonal bases for $\mathbb{K}[\mathrm{x}]_d \cap \Lambda_\downarrow$ and $\mathcal{I}_d^0$ can be simultaneously computed by applying QR-decomposition in the Vandermonde matrix $(\mathrm{W}_{\mathcal{L}_{\ge d}}^{\mathcal{P}_d})^T$. Therefore we can split Step 9 in two steps. First we do a QR-decomposition $(\mathrm{W}_{\mathcal{L}_{\geq d}}^{\mathcal{P}_d})^T$ to obtain orthogonal bases of $\mathbb{K}[\mathrm{x}]_d \cap \Lambda_\downarrow$ and $\mathcal{I}_d^0$. Once that we have in hand a basis of $\mathcal{I}_d^0$ we obtain the elements of $\mathcal{H}_d$ as its complement in the column space of $\mathrm{M}_{\mathcal{M}_d,\mathcal{P}_d^\dagger}(\mathcal{H})$.

Proposition 4.6. *Let* $[\mathrm{Q}_1 \mid \mathrm{Q}_2] \cdot \begin{bmatrix} \mathrm{R}_d \\ 0 \end{bmatrix} = \left(\mathrm{W}_{\mathcal{L}_{\geq d}}^{\mathcal{P}_d}\right)^T$ *be a QR-decomposition of* $\left(\mathrm{W}_{\mathcal{L}_{\geq d}}^{\mathcal{P}_d}\right)^T$. *Let r be the rank of* $\left(\mathrm{W}_{\mathcal{L}_{\geq d}}^{\mathcal{P}_d}\right)^T$. *Let* $\{q_1 \ldots q_r\}$ *and* $\{q_{r+1} \ldots q_m\}$ *be the columns of* Q_1 *and* Q_2 *respectively. Then the following holds:*

(1) $\mathcal{P}_{\Lambda,d} = \left\{\mathcal{P}_d^\dagger \cdot q_1, \ldots, \mathcal{P}_d^\dagger \cdot q_r\right\}$ *is a basis of* $\mathbb{K}[\mathrm{x}]_d \bigcap \Lambda_\downarrow$.
(2) $\mathcal{N} = \{\mathcal{P}_d \cdot q_{r+1}, \ldots, \mathcal{P}_d \cdot q_m\}$ *is a basis of* $\mathcal{I}_d^0$.
(3) *If* $p \in \mathcal{P}_{\Lambda,d}$ *and* $q \in \mathcal{N}$ *then* $\langle p, q\rangle = 0$, *i.e.,* $\mathbb{K}[\mathrm{x}] = (\Lambda_\downarrow \cap \mathbb{K}[\mathrm{x}]_d) \overset{\perp}{\oplus} \mathcal{I}_d^0$.

In the case where $\mathcal{P}$ is orthonormal with respect to the apolar product, i.e. $\mathcal{P} = \mathcal{P}^\dagger$, then $\mathcal{P}_{\Lambda,d}$ and $\mathcal{N}$ are also orthonormal bases.

Proof. Let D such that $\mathcal{L}_{\geq D} = \{\}$ and let $\mathcal{L}_{\leq D} = \bigcup_{d\leq D} \mathcal{L}_d$ be a basis of Λ. Then the matrix $\mathrm{W}_{\mathcal{L}_{\leq D}}^{\mathcal{P}_{\leq D}}$ is block upper triangular with non singular diagonal blocks. Consider $\{a_1, \ldots a_\ell\} \in \mathbb{K}^{|\mathcal{P}_{\leq D}|}$ the rows of $\mathrm{W}_{\mathcal{L}_{\leq D}}^{\mathcal{P}_{\leq D}}$. By Proposition [33, Proposition 2.3] we have that $\mathcal{P}_\Lambda \left\{\left(\mathcal{P}_{\leq D}^\dagger \cdot a_1^t\right)_\downarrow, \ldots, \left(\mathcal{P}_{\leq D}^\dagger \cdot a_\ell^t\right)_\downarrow\right\}$ is a basis of $\Lambda_\downarrow$, we can rewrite $\mathcal{P}_\Lambda$ as $\bigcup_{d=1}^{D} \left\{\mathcal{P}_d^\dagger \cdot b_1^t, \ldots, \mathcal{P}_d^\dagger \cdot b_{\ell_d}^t\right\}$ where $\left\{b_1, \ldots, b_{\ell_d}\right\}$ is a basis of the row space of $\left(\mathrm{W}_{\mathcal{L}_d}^{\mathcal{P}_d}\right)$. Since $\mathcal{P}_\Lambda$ is a graded basis then $\left\{\mathcal{P}_d^\dagger \cdot b_1^t, \ldots, \mathcal{P}_d^\dagger \cdot b_{\ell_d}^t\right\}$ is a basis $\mathbb{K}[\mathrm{x}]_d \cap \Lambda_\downarrow$.

Part (2) in the proposition is a direct consequence of Lemma 4.3 and the fact that the columns of Q_2 form a basis of the kernel of $\mathrm{W}_{\mathcal{L}_{\geq d}}^{\mathcal{P}_d}$. Let now $q \in \mathcal{P}_{\Lambda,d}$ and $p \in \mathcal{N}$. Then,

$$\langle p, q\rangle = \left\langle \sum_{p_i\in\mathcal{P}_d} a_i p_i, \sum_{q_i\in\mathcal{P}_d^\dagger} b_i q_i \right\rangle = \sum_{i=1} a_i b_i = 0.$$

Last equality stems from a and b being different rows in Q. □

5 SYMMETRY REDUCTION

The symmetries we deal with are given by the linear action of a finite group G on $\mathbb{K}^n$. It is thus given by a representation ϑ of G on $\mathbb{K}^n$. It induces a representation ρ of G on $\mathbb{K}[\mathrm{x}]$ given by

$$\rho(g)p(x) = p(\vartheta(g^{-1})x). \tag{9}$$

It also induces a linear representation on the space of linear forms, the dual representation of ρ :

$$\rho^*(g)\lambda(p) = \lambda(\rho(g^{-1})p),\ p \in \mathbb{K}[\mathrm{x}] \text{ and } \lambda \in \mathbb{K}[\mathrm{x}]^*. \tag{10}$$

We shall deal with an invariant subspace Λ of $\mathbb{K}[\mathrm{x}]^*$. Hence the restriction of ρ^* to Λ is a linear representation of G in Λ.

In the above Algorithm 2, to compute an H-basis of $\mathcal{I} = \ker w$, we use the Vandermonde and Macaulay matrices. We showed in [33, Section 4.2] how the Vandermonde matrix can be block diagonalized using appropriate symmetry adapted bases of $\mathbb{K}[\mathrm{x}]$ and Λ. We show here how to obtain such a block diagonalization on the Macaulay matrix when the space spanned by $\mathcal{H}$ is invariant under the induced action of a group G on $\mathbb{K}[\mathrm{x}]$. The key relies on exhibiting the equivariance of the prolongation map $\Psi_{d,\mathrm{h}}$ defined in Section 3.

With notations compliant with [33], for any representation θ of a group G on a $\mathbb{K}$-vector space V, a *symmetry adapted basis* $\mathcal{P}$ of V is characterized by the fact that the matrix of the representation θ in $\mathcal{P}$ is

$$[\theta(g)]_{\mathcal{P}} = \mathrm{diag}\left(\mathrm{R}_1(g) \otimes \mathrm{I}_{c_1},\ \ldots,\ \mathrm{R}_N(g) \otimes \mathrm{I}_{c_N}\right).$$

where $\mathrm{R}_j = \left(r_{kl}^j\right)_{1\leq k,l\leq n_j}$ is the matrix representation of the irreducible representation ρ_j of G and c_j is the multiplicity of ρ_j in θ. Hence $\mathcal{P} = \cup_{j=1}^N \mathcal{P}^j$ where $\mathcal{P}^j$ spans the isotypic component V_j associated to ρ_j. Introducing the map $\pi_{j,kl} = \frac{n_j}{|G|} \sum_{g\in G} r_{kl}^j(g^{-1})\theta(g)$ we can say that $\mathcal{P}^j$ is *determined* by $p_1^j, \ldots, p_{c_j}^j$ to mean that $p_1^j, \ldots, p_{c_j}^j$ is a basis of $\pi_{j,11}(V)$ and

$$\mathcal{P}^j = \{p_1^j, \ldots, p_{c_j}^j, \ldots, \pi_{j,n_j1}(p_1^j), \ldots, \pi_{j,n_j1}(p_{c_j}^j)\}. \tag{11}$$

When dealing with $\mathbb{K} = \mathbb{R}$, the statements we write are for the case where all the irreducible representations of G are absolutely irreducible, and thus the matrices $R_j(g)$ all have real entries. This is the case of all reflection groups. Yet these statements can be modified to also work with irreducible representations of complex type, which occur, for instance, for the cyclic group C_m with $m > 2$.

Consider now a set $\mathcal{H} = \{h_1, \ldots, h_l\}$ of homogeneous polynomials of $\mathbb{K}[\mathrm{x}]$. We denote $d_1, \ldots, d_\ell$ their respective degrees and $\mathrm{h} = [h_1, \ldots, h_\ell]$ the row vector of $\mathbb{K}[x]^\ell$. Associated to h, and a degree d, is the map introduced in Section 3

$$\begin{array}{rccc} \psi_{d,\mathrm{h}}: & \mathbb{K}[\mathrm{x}]_{d-d_1} \times \ldots \times \mathbb{K}[\mathrm{x}]_{d-d_\ell} & \to & \mathbb{K}[\mathrm{x}]_d \\ & \mathrm{f} = [f_1, \ldots, f_\ell]^t & \to & \mathrm{h} \cdot \mathrm{f}. \end{array} \tag{12}$$

We assume that $\mathcal{H}$ forms a basis of an invariant subspace of $\mathbb{K}[\mathrm{x}]$ and we call θ the restriction of the representation ρ to this subspace, while Θ is the matrix representation in the basis $\mathcal{H}$: $\Theta(g) = [\theta(g)]_{\mathcal{H}}$. Then $[\rho(g)(h_1), \ldots, \rho(g)(h_\ell)] = \mathrm{h} \circ \vartheta(g^{-1}) = \mathrm{h} \cdot \Theta(g)$. Note that, since the representation ρ on $\mathbb{K}[\mathrm{x}]$ preserves degree, $\deg h_i \neq \deg h_j \quad \Rightarrow \quad \Theta_{ij}(g) = 0,\ \forall g \in G$.

Proposition 5.1. *Consider* $\mathrm{h} = [h_1, \ldots, h_\ell] \in \mathbb{K}[x]_{d_1} \times \ldots \times \mathbb{K}[x]_{d_l}$ *and assume 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 for the representation* τ *on* $\mathbb{K}[\mathrm{x}]_{d-d_1} \times \ldots \times \mathbb{K}[\mathrm{x}]_{d-d_\ell}$ *defined by* $\tau(g)(\mathrm{f}) = \Theta(g) \cdot \mathrm{f} \circ \vartheta(g^{-1})$.

Proof. $(\rho(g) \circ \psi_{d,\mathrm{h}})(\mathrm{f}) = \rho(g)(\mathrm{h} \cdot \mathrm{f}) = \mathrm{h} \circ \vartheta(g^{-1}) \cdot \mathrm{f} \circ \vartheta(g^{-1}) = \mathrm{h} \cdot \Theta(g) \cdot \mathrm{f} \circ \vartheta(g^{-1}) = (\psi_{\mathrm{h}} \circ \tau(g))\,(\mathrm{f})$. □

By application of [9, Theorem 2.5], the matrix of $\psi_{d,\mathrm{h}}$ is block diagonal in symmetry adapted bases of $\mathbb{K}[\mathrm{x}]_{d-d_1} \times \ldots \times \mathbb{K}[\mathrm{x}]_{d-d_\ell}$ and $\mathbb{K}[\mathrm{x}]_d$. Yet, in the algorithm to compute symmetry adapted H-basis, the set $\mathcal{H}$ increases with d at each iteration and τ changes accordingly. We proceed to discuss how to hasten the computation of a symmetry adapted basis of the evolving space $\mathbb{K}[\mathrm{x}]_{d-d_1} \times \ldots \times \mathbb{K}[\mathrm{x}]_{d-d_\ell}$.

The set $\mathcal{H} = \mathcal{H}^1 \cup \ldots \mathcal{H}^N$ that we shall build, degree by degree, is actually a symmetry adapted basis. In particular, for $1 \leq i \leq N$, $\mathcal{H}^i$ spans the isotypic component associated to the irreducible representation ρ_i. If the multiplicity of the latter, in the span of $\mathcal{H}$, is

ℓ_i then the cardinality of $\mathcal{H}^i$ is $\ell_i\, n_i$. The matrices of the representation θ in this basis are $\Theta(g) = \operatorname{diag}(R_i(g) \otimes I_{\ell_i} | i = 1 \ldots N)$.

Assume $\mathcal{H}^i$ is determined by $h_{i,1}, \ldots, h_{i,\ell_i}$, of respective degrees $d_{i,1}, \ldots, d_{i,\ell_i}$. In other words, for $1 \le l \le \ell_i$,

$$\mathrm{h}_{i,l} = \left[h_{i,l}, \pi_{i,21}(h_{i,l}), \ldots, \pi_{i,n_i 1}(h_{i,l})\right]$$

is such that $\mathrm{h}_{i,l} \circ \vartheta(g^{-1}) = \mathrm{h}_{i,l} \cdot R_i(g)$. Hence the related product subspace $\mathbb{K}[\mathrm{x}]^{n_i}_{d-d_{i,l}}$ is invariant under τ. The symmetry adapted bases for all these subspaces can be combined into a symmetry adapted basis for the whole product space $\left(\mathbb{K}[\mathrm{x}]_{d_{1,1}} \times \mathbb{K}[\mathrm{x}]_{d_{1,\ell_1}}\right)^{n_1} \times \ldots \times \left(\mathbb{K}[\mathrm{x}]_{d_{N,1}} \times \mathbb{K}[\mathrm{x}]_{d_{1,\ell_N}}\right)^{n_N}$. Note that the components $\mathbb{K}[\mathrm{x}]^{n_i}_e$ with representation $\tau_{i,e}$ defined by $\tau_{i,e}(g)(\mathrm{f}) = R_i(g) \cdot f \circ \vartheta(g^{-1})$ are bound to reappear several times in the overall algorithm of next section. Hence the symmetry adapted bases for the evolving τ can be computed dynamically.

6 CONSTRUCTING SYMMETRY ADAPTED H-BASIS

In this section we show, when the space Λ is invariant, an orthogonal equivariant H-basis $\mathcal{H}$ can be computed. In this setting, we exploit the symmetries of Λ to build $\mathcal{H}$. A robust and symmetry adapted version of Algorithm 2 is presented. The block diagonal structure of the Vandermonde and Macaulay matrices allow to reduce the size of the matrices to deal with. The H-basis obtained as the output of Algorithm 3 inherits the symmetries of Λ.

Proposition 6.1. *Let $\mathcal{I} = \cap_{\lambda \in \Lambda} \ker \lambda$ and $d \in \mathbb{N}$. If Λ is invariant, then so are $\mathcal{I}$, $\mathcal{I}^0$, $\mathcal{I}^0_d$, $V_d\left(\mathcal{I}^0_{<d}\right)$. Also, if $\mathcal{H}$ is an orthogonal H-basis of $\mathcal{I}$, then $\langle \mathcal{H}^0_d \rangle_{\mathbb{K}}$ is invariant.*

Proof. Let $p \in \mathcal{I}$ and $g \in G$, since Λ is closed under the action of G, $\lambda(\rho(g)(p)) = \rho^*(g) \circ \lambda(p) = 0$ for all $\lambda \in \Lambda$ therefore $\rho(g)(p) \in \mathcal{I}$ implying the invariance of $\mathcal{I}$. Considering d the degree of p we can write p as $p = p^0 + p_1$, with $p_1 \in \mathbb{K}[\mathrm{x}]_{<d}$. Then we have that $\rho(g)p = \rho(g)p^0 + \rho(g)p_1 \in \mathcal{I}$, as ρ is degree preserving then $\rho(g)p^0 \in I^0_d$ and the invariance of $\mathcal{I}^0$ follows. Now for every $q = \sum_{h_i \in \mathcal{I}^0_{d-1}} q_i h_i \in V_d\left(\mathcal{I}^0_{\le d}\right)$, it holds that $\rho(g)q = \sum_{h_i \in \mathcal{I}^0_{d-1}} \rho(g) q_i \rho(g) h_i \subset V_d\left(\mathcal{I}^0_{\le d}\right)$, thus $V_d\left(\mathcal{I}^0_{\le d}\right)$ is an invariant subspace. Finally recalling (3) we conclude that $\langle \mathcal{H}^0_d \rangle_{\mathbb{K}}$ is also G-invariant for being the orthogonal complement of a $G-$invariant subspace. ◻

Algorithm 3 is a symmetry adapted version of Algorithm 2. In any iteration we compute $\mathcal{H}^0_d$ as a symmetry adapted basis of the orthogonal complement of $V_d(\mathcal{H}^0_{<d})$ in $\mathcal{I}^0$.

This structure is obtained degree by degree. Assuming that the elements of $\mathcal{H}^0_{<d}$ form a symmetry adapted basis it follows from [33, Section 4.2] and Proposition 5.1 that the matrices $\mathrm{W}^{\mathcal{P}_d}_{\mathcal{L}}$ and $\mathrm{M}_{\mathcal{M}_d, \mathcal{P}_d}(\mathcal{H}^0_{<d})$ are block diagonal. Computations over the symmetry blocks leads to the symmetry adapted structure of $\mathcal{H}^0_d$. For any degree d we only need to consider the matrices $\mathrm{W}^{\mathcal{P}^{i,1}_d}_{\mathcal{L}^{i,1}_{\ge d}}$ and $\mathrm{M}^i_d(\mathcal{H}^0_{<d})$, i.e., only one block per irreducible representation.

Once we have in hand $\mathcal{H}^0 = \left[h^1_{11}, \ldots, h^1_{1n_1}, \ldots, h^N_{c_N n_N}\right]^T$ and a symmetry adapted basis for $\Lambda_\downarrow$, we compute $\mathcal{H}$ by interpolation. Since $\mathcal{H}^0 \in \mathbb{K}[\mathrm{x}]^\theta_\vartheta$, by [33, Proposition 3.5], its interpolant in $\Lambda_\downarrow$ is also $\vartheta - \theta$ equivariant. Therefore

$$\mathcal{H} = \left[h^1_{11} - \widetilde{h^1_{11}}, \ldots, h^1_{1n_1} - \widetilde{h^1_{1n_1}}, \ldots, h^N_{c_N n_N} - \widetilde{h^N_{c_N n_N}}\right]^T \in \mathbb{K}[\mathrm{x}]^\theta_\vartheta.$$

The set $\mathcal{H}$ of its component is thus a symmetry adapted basis. The correctness and termination of Algorithm 3 follow from the same arguments exposed for Algorithm 2. Note that both Macaulay and Vandermonde matrices split in $\sum_{i=1}^N n_i$ blocks. Assuming that the blocks are equally distributed and thanks to [37, Proposition 5] we can approximate the dimensions of the blocks by $\frac{\mathrm{M}^i(\mathcal{H}^0)}{\mathrm{M}(\mathcal{H}^0)} \approx \frac{\mathrm{W}^{\mathcal{P}^i}_{\mathcal{L}^i}}{\mathrm{W}^{\mathcal{P}}_{\mathcal{L}}} \approx \frac{1}{|G|}$. Therefore depending on the size of G the dimensions of the matrices to deal with in Algorithm 3 can be considerably reduced.

Algorithm 3

Input: - $\mathcal{L}$ a s.a.b of Λ ($r = |\mathcal{L}| = \dim(\Lambda)$, $r_i = \left|\mathcal{L}^{i,1}\right|$)
- $\mathcal{P}$ an orthonormal graded s.a.b of $\mathbb{K}[\mathrm{x}]_{\le r}$
- $\mathcal{M}_i$ a graded s.a.b of $\mathbb{K}[\mathrm{x}]^{n_i}_{\le r}$, $1 \le i \le N$

Output: - $\mathcal{H}$ an orthogonal equivariant H-basis for $\mathcal{I} := \ker \Lambda$
- $\mathcal{P}_\Lambda$ a s.a.b of the least interpolation space for Λ.

$\mathcal{H}^0 \leftarrow \{\}$, $\mathcal{P}_\Lambda \leftarrow \{\}$
$d \leftarrow 0$
$\mathcal{L}_{\le 0} \leftarrow \{\}$, $\mathcal{L}_{\ge 0} \leftarrow \mathcal{L}$
while $\mathcal{L}_{\ge d} \ne \{\}$ **do**
  for $i = 1$ **to** N such that $\mathcal{L}^{i,1}_{\ge d} \ne \emptyset$ **do**
    $\mathrm{Q} \cdot \begin{bmatrix} \mathrm{R}_{d,i} \\ 0 \end{bmatrix} = \mathrm{W}^{\mathcal{P}^{i,1}_d}_{\mathcal{L}^{i,1}_{\ge d}}$ ▹ QR-decomposition of $\mathrm{W}^{\mathcal{P}^{i,1}_d}_{\mathcal{L}^{i,1}_{\ge d}}$
    $\left[\mathcal{L}^{i,1}_d \mid \mathcal{L}^{i,1}_{\ge d+1}\right] \leftarrow \mathcal{L}^{i,1}_{\ge d} \cdot \mathrm{Q}^T$
    $\mathcal{L}^{i,1}_{\le d+1} \leftarrow \mathcal{L}^{i,1}_{\le d} \cup \mathcal{L}^{i,1}_d$
    $[\mathrm{Q}_1 \mid \mathrm{Q}_2] \cdot \mathrm{R} = \begin{bmatrix} \mathrm{R}^T_{d,i} & \mathrm{M}^i_d(\mathcal{H}^0) \end{bmatrix}$
    for $\alpha = 1$ **to** n_i **do**
      $\mathcal{P}^i_\Lambda \leftarrow \mathcal{P}^i_\Lambda \cup \mathcal{P}^{i,\alpha}_d \cdot \mathrm{R}^T_{d,i}$
      $\mathcal{H}^0_i \leftarrow \mathcal{H}^0_i \bigcup \mathcal{P}^{i,\alpha}_d \cdot \mathrm{Q}_2$
  $d \leftarrow d + 1$
for $i = 1$ **to** N **do**
  for all $p \in \mathcal{H}^0_i$ **do**
    $\mathcal{H} \leftarrow \mathcal{H} \bigcup \left\{ p - \mathcal{P}^{i,1}_\Lambda \left(\mathrm{W}^{\mathcal{P}^{i,1}_\Lambda}_{\mathcal{L}^{i,1}_{\le d}}\right)^{-1} \left(\mathcal{L}^{i,1}_{\le d}\right)^T \right\}$
return $(\mathcal{H}, \mathcal{P}_\Lambda)$

Example 6.2. The subgroup of the orthogonal group $\mathbb{R}^3$ that leaves the regular the cube invariant is commonly called O_h. It has order 48 and 10 inequivalent irreducible representations whose dimensions are (1, 1, 1, 1, 2, 2, 3, 3, 3, 3). Consider $\Xi \subset \mathbb{R}^3$ the invariant set of 26 points illustrated on Figure 1a. They are grouped in three orbits O_1, O_2 and O_3 of O_h. The points in O_1 are the vertices of a cube with the center at the origin and with edge length $\sqrt{3}$. The points in O_2 and in O_3 are the centers of the faces and middle of the edges of a cube with the center at the origin and edge length 1. Consider $\Lambda = \operatorname{span}\left(\left\{e_\xi \mid \xi \in \Xi\right\} \bigcup \left\{e_\xi \circ D_{\vec{\xi}} \mid \xi \in O_2\right\}\right)$. Λ is an invariant subspace and $\mathcal{I} = \bigcap_{\lambda \in \Lambda} \ker \lambda$ is an ideal. An orthogonal equivariant H-basis $\mathcal{H}$ of $\mathcal{I}$ is given by

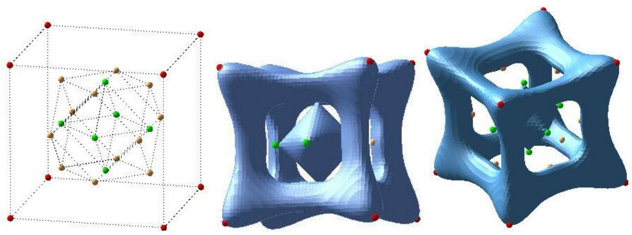
$$h_1^1 = \left[-\tfrac{36}{37} + \tfrac{109}{37}\left(x^2+y^2+z^2\right) - \tfrac{110}{37}\left(x^4+y^4+z^4\right) - \tfrac{36}{37}\left(x^2y^2+x^2z^2+y^2z^2\right) + x^6+y^6+z^6\right]$$

$$h_1^7 = \left[yz^3 - y^3z,\, xz^3 - x^3z,\, xy^3 - x^3y\right]$$

$$h_2^7 = \Big[x\,(y^4 - y^2 + z^4 - z^2 - 3(x^4 - 2x^2 + 1)),\, y\,(z^4 - z^2 + x^4 - x^2 - 3(y^4 - 2y^2 + 1)),$$
$$z\left(\tfrac{4}{3}x^2y^2 - 3(z^4 - 2z^2 + 1)\right)\Big]$$

$$h_1^9 = \Big[yz\,(-2 - \tfrac{4}{3}x^2 + y^2 + z^2),\, xz\,(-2 + x^2 - \tfrac{4}{3}y^2 + z^2),\, xy\,(-2 + x^2 + y^2 - \tfrac{4}{3}z^2)$$

From the structure of $\mathcal{H}$ it follows that h_{11}^1 is the minimal degree invariant polynomial (up to a constant multiple) of $\mathcal{I}$. In Figure 1b we show the zero surface of h_{11}^1 which is O_h invariant.



(a) Points in Ξ divided in orbits **(b) Variety of the minimal degree invariant polynomial h_{11}^1 of $\mathcal{I}$**

Figure 1: Lowest degree invariant algebraic surface through an invariant set of the points Ξ

Example 6.3. Lets consider the cyclic group C_3, and its action over R^3. It has order 3 and 3 inequivalent irreducible representations of dimension 1, one absolutely irreducible representation and a pair of conjugate irreducible representations of complex type. We analyze the cyclic n−th roots system [3], which has been widely used as a benchmark. The cyclic 3−th roots system is defined by:

$$C(3) : x + y + z, \quad xy + yz + zx, \quad xyz - 1.$$

The associated ideal $\mathcal{I} = \langle C(3) \rangle$ of $C(3)$ is invariant under C_3. The reduced Gröbner basis $\mathcal{G}$ of $\mathcal{I}$ w.r.t the graded reverse lexicographic order and its corresponding normal set $\mathcal{N}$ are given by $\mathcal{G} := \left\{x + y + z, y^2 + yz + z^2, z^3 - 1\right\}$ and $\mathcal{N} := \left\{1, z, y, z^2, yz, yz^2\right\}$. Applying Algorithm 3 to the linear forms given by the coefficients of the normal forms w.r.t $\mathcal{N}$, we obtain a symmetry adapted H-basis $\mathcal{H} = \left\{x + y + z, x^2 + y^2 + z^2, x^3 + y^3 + z^3 - 3\right\}$ as well as a symmetry preserving and robust representation of the quotient $\mathcal{P} = \{1, (y - z)(x - z)(x - y), x - z, y - z, (x - y)(x - 2z + y), (y - z)(2x - y - z)\}$.

REFERENCES

[1] J. Berthomieu, B. Boyer, and J.-C. Faugère. 2017. Linear algebra for computing Gröbner bases of linear recursive multidimensional sequences. *Journal of Symbolic Computation* 83 (2017), 36 – 67.

[2] G. Birkhoff. 1979. The algebra of multivariate interpolation. *Constructive approaches to mathematical models* (1979), 345–363.

[3] G. Björck. 1990. Functions of modulus 1 on Z n whose Fourier transforms have constant modulus, and "cyclic n-roots". In *Recent Advances in Fourier Analysis and its Applications*. Springer, 131–140.

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

[5] C. De Boor. 1994. Gauss elimination by segments and multivariate polynomial interpolation. In *Approximation and Computation: A Festschrift in Honor of Walter Gautschi*. Springer, 1–22.

[6] C. De Boor and A. Ron. 1990. On multivariate polynomial interpolation. *Constructive Approximation* 6, 3 (1990).

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

[8] C. Fassino and H.M. Möller. 2016. Multivariate polynomial interpolation with perturbed data. *Numerical Algorithms* 71, 2 (2016), 273–292.

[9] A. Fässler and E. Stiefel. 1992. *Group theoretical methods and their applications.*

[10] J.-C Faugere, P. Gianni, D. Lazard, and T. Mora. 1993. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation* 16, 4 (1993), 329–344.

[11] J.-C. Faugère and C. Mou. 2017. Sparse FGLM algorithms. *Journal of Symbolic Computation* 80, 3 (2017), 538 – 569.

[12] J.-C. Faugere and J. Svartz. 2013. Grobner bases of ideals invariant under a commutative group: the non-modular case. In *Proc. ISSAC 2013*. ACM, 347–354.

[13] K. Gatermann. 1990. Symbolic solution of polynomial equation systems with symmetry. In *ISSAC'90 Tokyo, Japan*. ACM-Press, 112–119.

[14] K. Gatermann. 1992. Linear representations of finite groups and the ideal theoretical construction of G-invariant cubature formulas. In *Numerical integration (Bergen, 1991)*. NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., Vol. 357. Kluwer Acad. Publ., Dordrecht, 25–35.

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

[16] K. Gatermann and F. Guyard. 1999. Gröbner bases, invariant theory and equivariant dynamics. *J. Symbolic Comput.* 28, 1-2 (1999), 275–302.

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

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

[19] E. Hubert and G. Labahn. 2012. Rational invariants of scalings from Hermite normal forms. In *Proc. ISSAC 2012*. ACM, 219–226.

[20] E. Hubert and G. Labahn. 2013. Scaling invariants and symmetry reduction of dynamical systems. *Found. Comput. Math.* 13, 4 (2013), 479–516.

[21] E. Hubert and G. Labahn. 2016. Computation of the Invariants of Finite Abelian Groups. *Mathematics of Computations* 85, 302 (2016), 3029–3050.

[22] M. Javanbakht and T. Sauer. 2019. Numerical computation of H-bases. *BIT Numerical Mathematics* 59, 2 (2019), 417–442.

[23] T. Krick, A. Szanto, and M. Valdettaro. 2017. Symmetric interpolation, Exchange Lemma and Sylvester sums. *Comm. Algebra* 45, 8 (2017), 3231–3250.

[24] F.S. Macaulay. 1916. The algebraic theory of modular systems. *Cambridge Tracts in Mathematics and Mathematical Physics* 19 (1916).

[25] M.G. Marinari, H.M. Möller, and T. Mora. 1991. Gröbner bases of ideals given by dual bases. In *ISSAC'91*. ACM, 55–63.

[26] H.M. Möller and B. Buchberger. 1982. The construction of multivariate polynomials with preassigned zeros. In *European Computer Algebra Conference*.

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

[28] B. Mourrain. 2017. Fast algorithm for border bases of Artinian Gorenstein algebras. In *ISSAC'17 Kaiserslautern, Germany*. ACM Press, 333–340.

[29] G. Pistone, E. Riccomagno, and H.P. Wynn. 2000. *Algebraic statistics: Computational commutative algebra in statistics.* Chapman and Hall/CRC.

[30] G. Pistone and H.P. Wynn. 1996. Generalised confounding with Gröbner bases. *Biometrika* 83, 3 (1996), 653–666.

[31] C. Riener and M. Safey El Din. 2018. Real root finding for equivariant semi-algebraic systems. In *Proc. ISSAC 2018*. ACM, 335–342.

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

[33] E. Rodriguez Bazan and E. Hubert. 2019. Symmetry Preserving Interpolation. In *ISSAC'19*. https://hal.inria.fr/hal-01994016

[34] T. Sauer. 2001. Gröbner bases, H−bases and interpolation. *Trans. Amer. Math. Soc.* 353, 6 (2001), 2293–2308.

[35] T. Sauer. 2017. Prony's method in several variables. *Numer. Math.* 136, 2 (2017).

[36] T. Sauer. 2018. Prony's method in several variables: symbolic solutions by universal interpolation. *J. Symbolic Comput.* 84 (2018), 95–112.

[37] J. P. Serre. 1977. *Linear representations of finite groups.* Springer.

[38] J. Verschelde and K. Gatermann. 1995. Symmetric Newton polytopes for solving sparse polynomial systems. *Adv. in Appl. Math.* 16, 1 (1995), 95–127.