Contemporary Mathematics
Volume 155, 1994

Formal Determination of Polynomial Consequences of Real Orthogonal Matrices

M. J. GONZÁLEZ-LOPEZ AND T. RECIO

1. Motivation

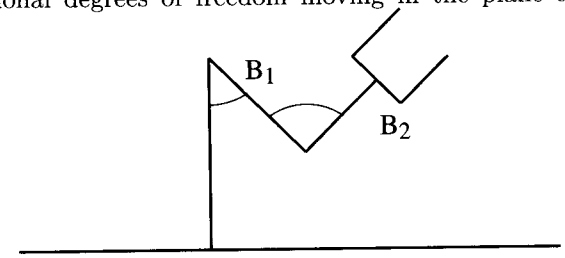
Geometric problems (as motion planning in robotics) dealing with position of rigid bodies in physical n-space (for instance in real two or three dimensional euclidean space) are often approached by attaching a reference system to the body and considering the algebraic set in $\mathbb{R}^{n^2+n}$ of all possible positions of this reference system with respect to a fixed external reference. The points of this algebraic set represent direct motions, i.e. pairs composed by a real $n \times n$ orthogonal matrix (rotation) and an n-array (translation), and in this way the algebraic statement (and algorithmic solution) of a variety of geometric problems involves systems of polynomial equations in the rotational and translational variables. A representative example of these problems is the computation of the inverse geometric model of a robot manipulator, which consists in determining the placement and orientation of the arms of the robot knowing the end effector placement and orientation. Buchberger [**B**] has studied this problem assuming as input a system of algebraic equalities that describes the relations satisfied by all the variables of the model (for instance, parameterizing rotational and translational variables for each body in the robot), so that finding a solution to the inverse model problem consists in obtaining the arm-variables of the system as a function of the end effector coordinates. Roughly, triangularization of the system by means of a Grobner basis with respect to some pure lexicographical order in which the end effector variables are smaller than the remaining ones is regarded by Buchberger as to facilitate the searching of the inverse model.

1991 *Mathematics Subject Classification.* Primary: 13P10 14P05 68Q40 Secondary: 14L35 13A50.

Partially supported by CICyT PB 89/0379/C02/01, TIC 88/0197 and Esprit/Bra 6846 (Posso).

This paper is submitted in final form and no version of it will be submitted for publication elsewhere

EXAMPLE. Let's consider the very simple robot manipulator with two bodies and two rotational degrees of freedom moving in the plane as in the figure.



We denote by $P_i := (v_i, A_i)$ the position of the body B_i, $i = 1, 2$, where

$$v_i := (a_i, b_i) \in \mathbb{R}^2,\ A_i := \begin{pmatrix} x_i & y_i \\ z_i & t_i \end{pmatrix} \in SO(2).$$

The geometric constraints that express conditions on $P_i's$ to represent the position of a body in the plane and relations between positions of the two bodies are given through the system of algebraic equalities:

$$A_i A_i^t = I,\ \det(A_i) = 1,\ i = 1, 2,$$

$$(1 \quad 0 \quad 0) \cdot \begin{pmatrix} 1 & a_1 & b_1 \\ 0 & x_1 & y_1 \\ 0 & z_1 & t_1 \end{pmatrix} = (1 \quad 0 \quad 0),$$

$$(1 \quad 1 \quad 0) \cdot \begin{pmatrix} 1 & a_1 & b_1 \\ 0 & x_1 & y_1 \\ 0 & z_1 & t_1 \end{pmatrix} = (1 \quad 0 \quad 0) \cdot \begin{pmatrix} 1 & a_2 & b_2 \\ 0 & x_2 & y_2 \\ 0 & z_2 & t_2 \end{pmatrix}$$

where $(1 \quad 0 \quad 0)$ and $(1 \quad 1 \quad 0)$ represent, in homogeneous coordinates, the extreme points of the bodies. A Grobner basis of the ideal generated by these polynomials, with respect to the pure lexicographical order in which $x_1 > y_1 > z_1 > t_1 > a_1 > b_1 > x_2 > y_2 > z_2 > t_2 > a_2 > b_2$ provides the equivalent (triangularized) system:

$$x_1 = a_2,\ y_1 = b_2,\ z_1 = -b_2,\ t_1 = a_2,\ a_1 = 0,\ b_1 = 0,$$
$$a_2^2 + b_2^2 = 1,\ z_2^2 + t_2^2 = 1,\ y_2 = -z_2,\ x_2 = t_2$$

where we obtain, in particular, the coordinates in P_1 as a function of the coordinates in P_2.

Let us remark that equations describing that a matrix is orthogonal ($AA^t = I$) or proper orthogonal ($AA^t = I$ and $\det(A) = 1$) appear for every body of the robot under consideration. More generally, an algebraic description of the orthogonal group $O(n)$ or of the special orthogonal group $SO(n)$ by equations describing these groups as subgroups of the set $\mathcal{M}(n, \mathbb{R})$ of matrices $n \times n$ with real coefficients appears in many algorithms in robotics other than the inverse geometric model: namely, in the computation of the direct geometric model, in the computation of the degrees of freedom of a robot system, in the checking of

irredundancy, etc. Thus we quite naturally yield to the study of these algebraic descriptions, and, in particular, to the question of finding a "well behaved" polynomial description for the mentioned groups. For instance, we will like to obtain a description such that:

1) all and only all matrices in the group satisfy the polynomial equations;
2) any polynomial consequence of the matrix group (see definition below) is in the ideal generated by the polynomials in the description;
3) we can exhibit an algorithm to test whether a polynomial is a consequence or not of the matrix group;
4) there is a geometric or matricial interpretation of the polynomial equations in the description.

DEFINITION. Let G be a subgroup of $\mathcal{M}(n,\mathbb{R})$. A polynomial consequence for G is a polynomial $P(\underline{x}) \in \mathbb{R}[\underline{x}]$, $\underline{x} = (x_{1,1},\ldots,x_{1,n},\ldots,x_{n,1},\ldots,x_{n,n})$, such that:

$$P(a_{1,1},\ldots,a_{1,n},\ldots,a_{n,1},\ldots,a_{n,n}) = 0, \quad \text{for all} \begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \ldots & a_{n,n} \end{pmatrix} \in G.$$

Examples of (almost trivial) polynomial consequences for $O(n)$ are:

- $P_i(\underline{x}) = x_{i,1}^2 + \cdots + x_{i,n}^2 - 1,\ i = 1,\ldots,n;$
- $Q_i(\underline{x}) = x_{1,i}^2 + \cdots + x_{n,i}^2 - 1,\ i = 1,\ldots,n;$
- $P_{i,j}(\underline{x}) = x_{i,1}x_{j,1} + \cdots + x_{i,n}x_{j,n},\ i,j = 1,\ldots,n;$
- $Q_{i,j}(\underline{x}) = x_{1,i}x_{1,j} + \cdots + x_{n,i}x_{n,j},\ i,j = 1,\ldots,n;$
- $\begin{vmatrix} x_{1,1} & \ldots & x_{1,n} \\ \vdots & & \vdots \\ x_{n,1} & \ldots & x_{n,n} \end{vmatrix}^2 - 1;$
- $H_{i,j}(\underline{x}) = x_{i,j}^2 - \tilde{x}_{i,j}^2,$

where

$$\tilde{x}_{i,j} := (-1)^{i+j} \begin{vmatrix} x_{1,1} & \ldots & x_{1,j-1} & x_{1,j+1} & \ldots & x_{1,n} \\ \vdots & & & & & \vdots \\ x_{i-1,1} & \ldots & x_{i-1,j-1} & x_{i-1,j+1} & \ldots & x_{i-1,n} \\ x_{i+1,1} & \ldots & x_{i+1,j-1} & x_{i+1,j+1} & \ldots & x_{i+1,n} \\ \vdots & & & & & \vdots \\ x_{n,1} & \ldots & x_{n,j-1} & x_{n,j+1} & \ldots & x_{n,n} \end{vmatrix}, i,j = 1,\ldots,n.$$

Again, a specific polynomial consequence for $SO(n)$ is:

$$H_{i,j}(\underline{x}) = x_{i,j} - \tilde{x}_{i,j},\ i,j = 1,\ldots,n.$$

From the point of view of algebraic geometry, properties 1 and 2 above mean just that the polynomial description gives a basis of the ideal of the algebraic

variety of all matrices in the group (identifying matrices and points in $\mathbb{R}^{n^2}$). Property 3, computationally oriented, says just that the sought polynomial basis of the ideal solves the ideal membership problem . As is well known, the Grobner basis of an ideal also has this property, but there could be other bases, not necessarily Grobner, for solving the same problem. Polynomial descriptions having these four properties could be of use in the algorithmic approach to some of the problems in robotics we have mentioned at the beginning, as it is clear that the lack of property 2 will imply, for instance in the example of the inverse model, the consideration of multiple-redundant solutions. On the other hand having property 3 could ease the computation of the Grobner basis or the triangularization of the given system (see §5 below). One could claim that it could be better to this purpose to have computed directly a Grobner basis of the ideal of matrices in the group, but it turns out that we have been unable to find a geometric or matricial interpretation of the elements of the Grobner basis of this ideal for many conceivable orders, while the basis we have found has a quite natural interpretation (property 4). In this way we can write explicitly a basis, depending on any n, with the four properties for any orthogonal or proper orthogonal group; while in the case of Grobner basis we have not been able to do so for general n. Moreover for the case $n = 2$, $n = 3$ the basis we have found happens to be also Grobner basis for the proper orthogonal ideal with respect to several orderings.

2. Main results

Coming to this point let us state formally the main results of this paper.

NOTATION. Let $\mathbb{K}$ be the field of real numbers $\mathbb{R}$ or the field of complex numbers $\mathbb{C}$. We identify a $n \times n$ matrix $A = (a_{i,j})$ with entries in $\mathbb{K}$, with the array $a = (a_{1,1}, \ldots, a_{1,n}, \ldots, a_{n,1}, \ldots, a_{n,n})$ in $\mathbb{K}^{n^2}$. If $\mathbb{K}[\underline{x}] = \mathbb{K}[x_{1,1}, \ldots, x_{1,n}, \ldots, x_{n,1}, \ldots, x_{n,n}]$ is the polynomial ring in n^2 variables with coefficients in $\mathbb{K}$ and $f(\underline{x}) \in \mathbb{K}[\underline{x}]$, we denote by $f(A) := f(a) \in \mathbb{K}$. Let $A(\underline{x}) = (x_{i,j})$ be a matrix whose entries are the variables in $\mathbb{K}[\underline{x}]$. We consider the polynomials:

(i) $\det(\underline{x}) := \det(A(\underline{x}))$.

(ii) $D^*_{i,j}(\underline{x}) := \sum_{k=1}^{n} x_{k,i}.x_{k,j} - \delta_{i,j}$; $\quad i,j \in 1,\ldots,n,\ i \leq j$.

(iii) $D_{i,j}(\underline{x}) := \sum_{k=1}^{n} x_{i,k}.x_{j,k} - \delta_{i,j}$; $\quad i,j \in 1,\ldots,n,\ i \leq j$.

(iv) Let $\pi = (i_1, \ldots, i_a, I_1, \ldots, I_b)$ and $\omega = (k_1, \ldots, k_a, K_1, \ldots, K_b)$ be even permutations of $(1, \ldots, n)$, $b \leq a \leq n-1$ and $a + b = n$; we denote:

$$D(\pi, \omega; a, b) := \begin{vmatrix} x_{i_1,k_1} & \ldots & x_{i_1,k_a} \\ \vdots & & \vdots \\ x_{i_a,k_1} & \ldots & x_{i_a,k_a} \end{vmatrix} - \begin{vmatrix} x_{I_1,K_1} & \ldots & x_{I_1,K_b} \\ \vdots & & \vdots \\ x_{I_b,K_1} & \ldots & x_{I_b,K_b} \end{vmatrix}.$$

And the ideals in $\mathbb{K}[\underline{x}]$:

$$\mathbf{so} := \langle \det(\underline{x}) - 1, \{D_{i,j}(\underline{x})/i, j \in \{1, \ldots, n\}, i \leq j\}\rangle,$$

$$\mathbf{o} := \langle \{D_{i,j}(\underline{x})/i, j \in \{1, \ldots, n\}, i \leq j\}\rangle.$$

THEOREM 1. (See Theorem 3.3 in §3.) *The ideal* $\mathbf{o}$ *in* $\mathbb{R}[\underline{x}]$ *is real (i.e. it is the ideal of the real algebraic set* $V(\mathbf{o}, \mathbb{R})$*; there is an equivalent purely algebraic description by the Dubois-Risler Nullstellensatz* [**D**][**R**]*). Analogoulsly the ideal* $\mathbf{so}$ *in* $\mathbb{R}[\underline{x}]$ *is real and prime.*

THEOREM 2. (See Theorems 4.4.1 and 4.4.2 in §4.) *Any real polynomial of degree* d *vanishing over all real orthogonal matrices is a combination of*

$$\{D_{i,j},\ D^*_{i,j}/i, j \in \{1, \ldots, n\}, i \leq j\}$$

with polynomial coefficients of degree at most $d-2$*. Analogously, any real polynomial of degree* d *vanishing over all proper real orthogonal matrices is a combination of*

$$\{D_{i,j},\ D^*_{i,j}/i, j \in \{1, \ldots, n\}, i \leq j\}$$
$$\cup$$
$$\{D(\pi, \omega; a, b)/\omega, \pi \text{ even permutations of } (1, \ldots, n)\ , b \leq a \leq n-1, a+b = n\}$$

by means of coefficients which are polynomials of degree at most $d-2$*,* $d-2$ *and* $d-a$ *respectively.*

THEOREM 3. (See technical results 3.1.2 and 3.1.4 in §3.) *One can exhibit the polynomials in* $\{D^*_{i,j}/i, j \in \{1, \ldots, n\}, i \leq j\}$ *as a polynomial combination of those in* $\{D_{i,j}/i, j \in \{1, \ldots, n\}, i \leq j\}$*. Also* $\{D(\pi, \omega; a, b)/\omega, \pi$ even permutations of $(1, \ldots, n)\ , b \leq a \leq n-1, a+b = n\}$ *as a polynomial combination of* $\{D_{i,j}/i, j \in \{1, \ldots, n\}, i \leq j\}$ *and* $\det(\underline{x}) - 1$.

THEOREM 4. (see Corollary 4.4.3 in §4.) *One can determine algorithmically in a priori bounded number of steps whether any real polynomial* p *of degree* d *is a polynomial consequence of the group of real orthogonal (real proper orthogonal) matrices and if it is so, to construct the combination of polynomials that gives the membership to the ideal.*

It follows from the results above that $\{D_{i,j}, D^*_{i,j}\}$ (respectively $\{D_{i,j},\ D^*_{i,j},\ D(\pi, \omega; a, b)\}$) are the "well behaved" basis of $\mathbf{o}$ (respectively $\mathbf{so}$) that we were looking for, verifying properties 1 to 4 of §1. For reasons that will be clear in a moment we propose to name such basis the **Weyl basis** of the corresponding ideal. From the purely mathematical point of view, the interest of finding a basis with these properties is already present in the reputed invariant-theoretic book of H. Weyl, *The Classical Groups* [**W**]. In fact one can follow his fascinating winding way towards this basis during the first one hundred pages of the book. The modern approach to invariant theory seems to overpass the need for such a

basis, as we have not found references to its existance or to its construction in more recent but also classical books ([**D-C**], [**F**], [**N**], [**S**], [**BO**]).

In fact we can say that our main results in the paper are just a reformulation of some theorems of Weyl (namely his Theorems 5.2.C, 5.3.B, 5.4.B, 5.4.C, 5.4.D). We have moreover also followed some of his proofs. The (if any) originality of the paper has to be therefore carefully explained. First, we have made a shorter and direct proof to the reality of the orthogonal or the proper orthogonal ideal, which is intrinsically tangled in Weyl's proof with the algorithmic property 3 of the basis. Second, we prove this algorithmic property without using (as it is done in his book) a cumbersome detour to Cayley's parameterization and to "formalized" main theorems for invariants (here "formalized" is used in a technical sense, as in Weyl's Chapter II, §11, meaning roughly invariants for generic orthogonal matrices). Third, we have formalized (in the sense of being less literary than the wonderful prose of Weyl) many of the concepts used in Weyl's proof and which are scattered throughout one hundred pages of his book, as he introduces them for a variety of purposes. We have also tried to make a self-contained proof, referring only to modern texts for some auxiliary results needed (in particular, a variation of Wedderburn's theorem from representation theory). Finally, our proof is a final check to Weyl's proof—as he does not detail the case of proper orthogonal matrices, leaving to the reader the task of adaptation from the non-proper orthogonal case proof—but in the case of non-proper orthogonal matrices Weyl's proof has a gap ([**W**] p. 143, Theorem 5.3.A, Supplement, Theorem 5.3.B and Corollary), as recognized by him in the Errata to the second edition, which includes a brief sketch about how to correct the mistake. We want to acknowledge our thanks to professor E. Becker who first mentioned the relation between our originally naively posed problem in robotics and the result of Weyl; to the late professor P. Menal, who helped us with the aspects in representation theory a few weeks before his sudden tragic death; and to professors T. Mora, C. Traverso and M. Coste for their help regarding the relations with Grobner basis.

3. Technical results and reality questions

In this paragraph we prove one of the main results (§3.3), namely that the ideals $\mathbf{o}.\mathbb{R}[\underline{x}]$ and $\mathbf{so}.\mathbb{R}[\underline{x}]$ are real and moreover that $\mathbf{so}.\mathbb{R}[\underline{x}]$ is prime (see notation in §2). In §3.1 we introduce some technical results, obtaining different basis for these ideals that will be used later. The proof of the reality and primality first considers the complex zeroes of the ideals, checking that the local rings of $\mathbf{o}.\mathbb{C}[\underline{x}]$ and $\mathbf{so}.\mathbb{C}[\underline{x}]$ at any complex zero are regular. This follows from the computation of Jacobians. Then it is a standard algebraic result to conclude that $\mathbf{o}.\mathbb{C}[\underline{x}]$ and $\mathbf{so}.\mathbb{C}[\underline{x}]$ are radical ideals. Next we prove (§3.2) that $V(\mathbf{so}, \mathbb{C})$ is connected by using a parameterization with skew-symmetric matrices via the exponential mapping. Thus, as $V(\mathbf{so}, \mathbb{C})$ is non-singular and connected, we conclude that $\mathbf{so}.\mathbb{C}[\underline{x}]$ is prime and therefore $\mathbf{so}.\mathbb{R}[\underline{x}]$ is prime. Again computation

of local dimension allows us to prove that $\mathbf{so}.\mathbb{R}[\underline{x}]$ is real. For $\mathbf{o}.\mathbb{R}[\underline{x}]$ the result follows from its representation as intersection of two copies of $\mathbf{so}.\mathbb{R}[\underline{x}]$.

3.1. Let us denote, following the notation in §2:

$$\begin{aligned}
\mathbf{so} &:= \langle \det(\underline{x}) - 1, \{D_{i,j}(\underline{x})/i, j \in \{1,\dots,n\}, i \le j\}\rangle,\\
\mathbf{so}' &:= \langle \det(\underline{x}) - 1, \{D^*_{i,j}(\underline{x})/i, j \in \{1,\dots,n\}, i \le j\}\rangle,\\
\mathbf{o} &:= \langle \{D_{i,j}(\underline{x})/i, j \in \{1,\dots,n\}, i \le j\}\rangle,\\
\mathbf{o} &:= \langle \{D^*_{i,j}(\underline{x})/i, j \in \{1,\dots,n\}, i \le j\}\rangle.
\end{aligned}$$

Let $\mathbb{K}$ be the field of real numbers $\mathbb{R}$ or the field of complex numbers $\mathbb{C}$. If $\mathbf{q}$ is an ideal in $\mathbb{K}[\underline{x}]$, let $V(\mathbf{q}, \mathbb{K}) := \{a \in \mathbb{K}^{n^2}/p(a) = 0, p(\underline{x}) \in \mathbf{q}\}$. If $B(\underline{x})$ and $C(\underline{x})$ are matrices $n \times n$ with entries in $K[\underline{x}]$ we write $B(\underline{x}) = C(\underline{x})(mod\ \mathbf{q})$ if all the entries of $B(\underline{x}) - C(\underline{x})$ belong to $\mathbf{q}$. We shall use the following properties:

- if $B(\underline{x}) = C(\underline{x})(mod\ \mathbf{q})$, then $\det(B(\underline{x})) = \det(C(\underline{x}))(mod\ \mathbf{q})$;
- if $H(\underline{x})$ is another matrix, and $B(\underline{x}) = C(\underline{x})(mod\ \mathbf{q})$, then $H(\underline{x})B(\underline{x}) = H(\underline{x})C(\underline{x})(mod\ \mathbf{q})$ and $B(\underline{x})H(\underline{x}) = C(\underline{x})H(\underline{x})(mod\ \mathbf{q})$.

The following results are clear from a geometric point of view (i.e. they are trivial to check for any orthogonal or proper orthogonal matrix, according to the case) but we are interested at the ideal (formal) level. The claims are valid over $\mathbb{K}$, real or complex.

3.1.1. $\det(\underline{x})^2 - 1 \in \mathbf{o} \cap \mathbf{o}'$.

Note that polynomials $\{D_{i,j}(\underline{x})/i, j \in \{1,\dots,n\}, i \le j\}$ are the entries of the (symmetric) matrix $A(\underline{x})A(\underline{x})^t - I$. Thus $A(\underline{x})A(\underline{x})^t = I(mod\ \mathbf{o})$, implies $\det(A(\underline{x})A(\underline{x})^t) = \det(I)(mod\ \mathbf{o})$, and $\det(\underline{x})^2 = \det(A(\underline{x})A(\underline{x})^t) = 1(mod\ \mathbf{o})$.

Likewise we obtain $\det(\underline{x})^2 = 1(mod\ \mathbf{o}')$ using instead the entries of $A(\underline{x})^t A(\underline{x}) - I$.

3.1.2. $\mathbf{o} = \mathbf{o}'$ and $\mathbf{so} = \mathbf{so}'$.

Let $adj(A(\underline{x}))$ be the adjoint matrix of $A(\underline{x})$. We have the following list of formal implications:

$$\begin{gathered}
adj(A(\underline{x}))A(\underline{x})^t = \det(\underline{x})I\\
A(\underline{x})^t A(\underline{x}) = I\ (mod\ \mathbf{o}')\\
adj(A(\underline{x}))A(\underline{x})^t A(\underline{x}) = adj(A(\underline{x}))\ (mod\ \mathbf{o}')\\
\det(\underline{x})A(\underline{x}) = adj(A(\underline{x}))\ (mod\ \mathbf{o}')\\
\det(\underline{x})A(\underline{x})A(\underline{x})^t = adj(A(\underline{x}))A(\underline{x})^t\ (mod\ \mathbf{o}')\\
\det(\underline{x})A(\underline{x})A(\underline{x})^t = \det(\underline{x})I\ (mod\ \mathbf{o}')\\
\det(\underline{x})^2 A(\underline{x})A(\underline{x})^t = \det(\underline{x})^2 I\ (mod\ \mathbf{o}')\\
A(\underline{x})A(\underline{x})^t = I\ (mod\ \mathbf{o}'),
\end{gathered}$$

so that finally $\{D_{i,j}(\underline{x})/i, j \in \{1,\dots,n\}, i \le j\} \subset \mathbf{o}'$. Similarly $\{D^*_{i,j}(\underline{x})/i, j \in \{1,\dots,n\}, i \le j\} \subset \mathbf{o}$. So $\mathbf{o} = \mathbf{o}'$ and obviously $\mathbf{so} = \mathbf{so}'$.

3.1.3. Let $\Delta_{i,j}$ be the (i,j)-entry of the matrix $adj(A(\underline{x}))$. Then we have $x_{i,j} - \Delta_{i,j} \in \mathbf{so}$, $i,j \in \{1,\ldots,n\}$. In fact we have the following implications:

$$A(\underline{x})^t A(\underline{x}) = I(mod\ \mathbf{so})$$
$$adj(A(\underline{x}))A(\underline{x})^t A(\underline{x}) = adj(A(\underline{x}))(mod\ \mathbf{so})$$
$$\det(\underline{x})A(\underline{x}) = adj(A(\underline{x}))(mod\ \mathbf{so})$$
$$A(\underline{x}) = adj(A(\underline{x}))(mod\ \mathbf{so})$$
$$x_{i,j} - \Delta_{i,j} \in \mathbf{so},\ i,j \in \{1,\ldots,n\}.$$

3.1.4. With notation as in §2, let

$$W := \{D(\pi,\omega;a,b)/\omega, \pi \text{ even permutations of } (1,\ldots,n) \quad b \le a \le n-1, a+b=n\}.$$

Then $W \subset \mathbf{so}$.

PROOF. Let A be a $n \times n$ matrix with complex entries and let $C := adj(A)$. Then:

$$\begin{pmatrix} c_{i_1,k_1} & \ldots & c_{i_1,k_a} & c_{i_1,K_1} & \ldots & c_{i_1,K_b} \\ \vdots & & \vdots & \vdots & & \vdots \\ c_{i_a,k_1} & \ldots & c_{i_a,k_a} & c_{i_a,K_1} & \ldots & c_{i_a,K_b} \\ 0 & \ldots & 0 & 1 & \ldots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \ldots & 0 & 0 & \ldots & 1 \end{pmatrix} \cdot$$

$$\begin{pmatrix} a_{i_1,k_1} & \ldots & a_{i_a,k_1} & a_{I_1,k_1} & \ldots & a_{I_b,k_1} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i_1,k_a} & \ldots & a_{i_a,k_a} & a_{I_1,k_a} & \ldots & a_{I_b,k_a} \\ a_{i_1,K_1} & \ldots & a_{i_a,K_1} & a_{I_1,K_1} & \ldots & a_{I_b,K_1} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i_1,K_b} & \ldots & a_{i_a,K_b} & a_{I_1,K_b} & \ldots & a_{I_b,K_b} \end{pmatrix} =$$

$$\begin{pmatrix} \det(A) & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \ldots & \det(A) & 0 & \ldots & 0 \\ a_{i_1,K_1} & \ldots & a_{i_a,K_1} & a_{I_1,K_1} & \ldots & a_{I_b,K_1} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i_1,K_b} & \ldots & a_{i_a,K_b} & a_{I_1,K_b} & \ldots & a_{I_b,K_b} \end{pmatrix}.$$

Thus we have:

$$\begin{vmatrix} c_{i_1,k_1} & \ldots & c_{i_1,k_a} \\ \vdots & & \vdots \\ c_{i_a,k_1} & \ldots & c_{i_a,k_a} \end{vmatrix} \det(A) = \det(A)^a \begin{vmatrix} a_{I_1,K_1} & \ldots & a_{I_1,K_b} \\ \vdots & & \vdots \\ a_{I_b,K_1} & \ldots & a_{I_b,K_b} \end{vmatrix}.$$

As this identity is proved for all matrices we conclude that it is also formally true, which means that polynomials:

$$p(\pi,\omega;a,b) := \begin{vmatrix} adj(A(\underline{x}))_{i_1,k_1} & \dots & adj(A(\underline{x}))_{i_1,k_a} \\ \vdots & & \vdots \\ adj(A(\underline{x}))_{i_a,k_1} & \dots & adj(A(\underline{x}))_{i_a,k_a} \end{vmatrix}$$

$$\det(A(\underline{x})) - \det(A(\underline{x}))^a \begin{vmatrix} x_{I_1,K_1} & \dots & x_{I_1,K_b} \\ \vdots & & \vdots \\ x_{I_b,K_1} & \dots & x_{I_b,K_b} \end{vmatrix}$$

are identically null, thus they belong to **so**. Since $\det(A(\underline{x})) = 1(mod\ \mathbf{so})$ and $adj(A(\underline{x})) = x_{i,j}(mod\ \mathbf{so})$ for all i,j, we conclude that polynomials $D(\pi,\omega;a,b)$ belong to **so**. □

THEOREM 3.2. *$V(\mathbf{so},\mathbb{C})$ is a connected algebraic variety.*

PROOF. We will denote by $SS(\mathbb{R})$ the set of skew-symmetric $n \times n$ matrices $(A + A^t = 0)$ with entries in $\mathbb{R}$. This set can be identified with $\mathbb{R}^{\frac{n(n-1)}{2}}$ and it is therefore connected in the set $\mathcal{M}(n,\mathbb{R})$ of $n \times n$ matrices with entries in $\mathbb{R}$ endowed with topology given by the euclidean norm. Our theorem will follow from the construction of a continuous surjective map:

$$h\colon SS(\mathbb{R}) \times V(\mathbf{so},\mathbb{R}) \longrightarrow V(\mathbf{so},\mathbb{C})$$

as it is well known that $V(\mathbf{so},\mathbb{R})$ is also connected. We define this map by $h(S,R) := R\exp(iS)$. Then it is easy to check that h is well defined using some properties of the exp mapping with respect to the trace and the determinant. Moreover h is clearly continuous. To prove surjectivity let $B \in V(\mathbf{so},\mathbb{C})$; then B^*B (where B^* is the conjugate transpose matrix of B) is hermitian, positive-definite and orthogonal, and therefore using a result of Gantmacher (cf. [**G**, vol. II, Chap. 11, Lemma 1, §1]) there exists $S' \in SS(\mathbb{R})$ such that $B^*B = \exp(iS')$. Let $S := \frac{1}{2}S' \in SS(\mathbb{R})$ and $R := B\exp(-iS)$. It is clear that $B = R\exp(iS)$. To conclude it is enough to prove that $R \in V(\mathbf{so},\mathbb{R})$. Since $\exp(-iS) \in V(\mathbf{so},\mathbb{C})$, we have that $R \in V(\mathbf{so},\mathbb{C})$. Besides R has real entries because it is also unitary; in fact:

$$R^*R = (B\exp(-iS))^*B\exp(-iS) = (\exp(-iS))^*B^*B\exp(-iS) =$$
$$= \exp(-iS)\exp(iS')\exp(-iS) = \exp(-iS)\exp(2iS)\exp(-iS) =$$
$$= \exp(-iS)\exp((2iS) + (-iS)) = \exp(-iS)\exp(iS) = I. \quad \square$$

THEOREM 3.3. *The ideal **so** is real and prime in $\mathbb{R}[\underline{x}]$. The ideal **o** is real and radical in $\mathbb{R}[\underline{x}]$.*

PROOF. Let $a \in V(\mathbf{o},\mathbb{K})$ for $\mathbb{K}$ either the real or complex numbers, and denote $J(\mathbf{o})(a)$ the jacobian matrix evaluated in the point a. Then some easy computation yields $rank(J(\mathbf{o})(a)) = \frac{n(n+1)}{2}$. Analogously for $a \in V(\mathbf{so},\mathbb{K})$, we

have $rank(J(\mathbf{so})(a)) = \frac{n(n+1)}{2}$. Next we remark that ideals **so** and **o** are equal in $I\!K[\underline{x}]_{\mathbf{m}_a}$, where $\mathbf{m}_a = \{p(\underline{x}) \in I\!K[\underline{x}]/p(a) = 0\}$, using 3.1.1. As **o** is generated by $\frac{n(n+1)}{2}$ polynomials it follows that $I\!K[\underline{x}]_{\mathbf{m}_a}/(\mathbf{o}.I\!K[\underline{x}]_{\mathbf{m}_a})$ is a regular local ring of dimension $\frac{n(n-1)}{2}$ and therefore also $I\!K[\underline{x}]_{\mathbf{m}_a}/(\mathbf{so}.I\!K[\underline{x}]_{\mathbf{m}_a})$ is a regular local ring of dimension $\frac{n(n-1)}{2}$. Now recall that if $\mathbf{b} = \langle h_1(\underline{x}), \ldots, h_r(\underline{x})\rangle$ is an ideal in $\mathbb{C}[\underline{x}]$, $a \in \mathbb{C}^n$; $\delta_a : \mathbb{C}[\underline{x}] \longrightarrow \mathbb{C}[\underline{x}]_{\mathbf{m}_a}$ the canonical inclusion, and $V(\mathbf{b}, \mathbb{C})$ the set of zeros in $\mathbb{C}^n$ of $\mathbf{b}$, then

$$\mathbf{b} = \bigcap_{a \in V(\mathbf{b},\mathbb{C})} \delta_a^{-1}(\mathbf{b}.\mathbb{C}[\underline{x}]_{\mathbf{m}_a}).$$

It follows that $\mathbf{so}.\mathbb{C}[\underline{x}]$ and $\mathbf{o}.\mathbb{C}[\underline{x}]$ are radical ideals and therefore also $\mathbf{so}.\mathbb{R}[\underline{x}]$ and $\mathbf{o}.\mathbb{R}[\underline{x}]$. We conclude that $V(\mathbf{so}, \mathbb{C})$ is an irreducible algebraic variety as it is non singular and connected (3.2). Therefore $\mathbf{so}.\mathbb{C}[\underline{x}]$ is prime and the same follows for $\mathbf{so}.\mathbb{R}[\underline{x}]$. As the dimension of $\mathbf{so}.\mathbb{R}[\underline{x}]$ is equal to $\frac{n(n-1)}{2}$ and agrees with the topological dimension of $V(\mathbf{so}, \mathbb{R})$ we conclude that $\mathbf{so}.\mathbb{R}[\underline{x}]$ is real. The reality of $\mathbf{o}.\mathbb{R}[\underline{x}]$ follows, again using 3.1.1, from $\mathbf{o}.\mathbb{R}[\underline{x}] = \mathbf{so}.\mathbb{R}[\underline{x}] \cap \mathbf{so}^-.\mathbb{R}[\underline{x}]$, where $\mathbf{so}^-$ is defined by

$$\mathbf{so}^- := \langle \det(\underline{x}) + 1, \{D_{i,j}(\underline{x})/i, j \in \{1, \ldots, n\}, i \leq j\}\rangle . \quad \square$$

4. Weyl basis

In this paragraph we obtain basis for the orthogonal and proper orthogonal ideals verifying the properties 1 to 4 of §1. First we introduce some notions from invariant and representation theory, namely the concept of enveloping algebra and the double centralizer property (4.1.1) for semi-simple rings. The idea of Weyl is, very roughly speaking, that using Kronecker products we are able to linearize polynomial consequences of orthogonal (or proper orthogonal) matrices. Next some linear conditions satisfied for all orthogonal (or proper orthogonal) matrices (again we recall that no precision is intended in this explanation) are introduced (4.3.1) so that the main point (4.3.2) is to prove that, conversely, any matrix satisfying such conditions is orthogonal (or proper orthogonal). Here we use the criterion given by the double centralizer property and therefore checking orthogonality is reduced to checking commutativity of such matrices with all commutators of orthogonal matrices. But this commutativity implies the invariancy of functions of the entries of the matrices with respect to the group considered (4.2.3). Therefore using the first main theorem (4.1.2 and 4.1.3) of the invariant theory for the group we have an easier way of checking the double commutativity. Finally the ideal membership problem is reduced to the same problem for an ideal generated by linear polynomials and we are done. Our proof, for the reasons explained in §2, is done for the special orthogonal group, but of course the simpler case for the orthogonal group follows along the same

lines and it is therefore omitted. In what follows [**W**] will be the standard reference, but we have also included references to more modern texts for the basic concepts.

4.1. Let K be a field. If U is a set of $n \times n$ matrices with entries in K we define its linear closure $[U]$ in K as the set of all finite linear combinations

$$a_1 A_1 + \cdots + a_r A_r$$

of matrices A_i in U by means of coefficients a_i in K. If U is a (multiplicative) group, then addition of two matrices, multiplication of a matrix by an element in K and multiplication of two matrices are three operations closed in $[U]$, so that this set is an (matrix) algebra in K which is called the **enveloping algebra** of the group U (cf. also [**SH**, vol. I, 3.5.1]). The **commutator** of U is the set:

$$C(U) := \{B \in \mathcal{M}(n, K)/AB = BA \text{ for all } A \in U\}.$$

Clearly we see that $C(U)$ is a K-algebra and $C(U) = C([U])$. Let V be a n-dimensional K-vector space, $W \subset V$ a subspace and $U \subset \mathcal{M}(n, K)$ a group of matrices acting on V by means of:

$$\begin{array}{rccc} A\colon & V & \longrightarrow & V, \quad A \in U \\ & \underline{x} & \longmapsto & \underline{x}A\,. \end{array}$$

If $A \in \mathcal{M}(n, K)$ we say that W is A-**invariant** if $wA \in W$ for all $w \in W$; and W is $U-$invariant if it is A-invariant for all $A \in U$. Note that W is U-invariant if and only if W is $[U]$-invariant. The group U is **fully reducible** if we can write $V = V_1 \oplus \cdots \oplus V_k$, where V_i is an U-invariant subspace for all $i = 1, \ldots, k$. (cf. also [**C-R**, §10], as completely reducible).

The following theorem (**the double centralizer property**) is an extension of the theorem of Wedderburn on simple rings to semi-simple rings.

THEOREM 4.1.1. (Cf. [**C-R**, §59] or [**SH**, p. 124]). *The enveloping algebra of a fully reducible matrix set U is the commutator algebra of the commutator algebra of U, i.e. $C(C(U)) = [U]$.*

For the applications of this theorem let us remark that clearly any set of orthogonal transformations over a real field K is fully reducible and in particular the groups $O(n)$ and $SO(n)$ are fully reducible.

DEFINITION 4.1.2. Let $f(x^{(1)}, \ldots, x^{(k)})$ a function on V^k. We say that f is invariant on W associated to k vectors, with respect to U, if $f(x^{(1)}, \ldots, x^{(k)}) = f(x^{(1)}A, \ldots, x^{(k)}A)$ for all A in U and all x_i in W.

THEOREM 4.1.3. (First main theorem on invariants of the orthogonal group.) *If f is a function invariant on $\mathbb{R}^n$ associated to k vectors with respect to $O(n)$, then there exists a polynomial p (in k^2 variables) such that:*

$$f(x^{(1)}, \ldots, x^{(k)}) = p(\langle x^{(1)}, x^{(1)}\rangle, \langle x^{(1)}, x^{(2)}\rangle, \ldots, \langle x^{(1)}, x^{(k)}\rangle, \ldots, \langle x^{(k)}, x^{(1)}\rangle, \ldots, \langle x^{(k)}, x^{(k)}\rangle)$$

for all $x^{(i)} \in \mathbb{R}^n, i = 1, \ldots, k$, *where* $\langle -, - \rangle$ *denotes the canonical scalar product in* $\mathbb{R}^n$.

THEOREM 4.1.4. (First main theorem on invariants of the special orthogonal group.) *If* f *is a function invariant on* $\mathbb{R}^n$ *associated to* k *vectors with respect to* $SO(n)$, *then* f *is in the* $\mathbb{R}$*-algebra generated by functions of the form:*

(i) $[x^{(i_1)}, \ldots, x^{(i_n)}]$,

(ii) $g(x^{(1)}, \ldots, x^{(k)})$,

where

$$[x^{(i_1)}, \ldots, x^{(i_n)}] := \begin{vmatrix} x_1^{(i_1)} & \ldots & x_n^{(i_1)} \\ \vdots & & \vdots \\ x_1^{(i_n)} & \ldots & x_n^{(i_n)} \end{vmatrix},$$

$$i_j \in \{1, \ldots, k\}, j = 1, \ldots, n, \text{ (bracket factor)},$$

and g *is a polynomial combination of the scalar products* $\langle x^{(i)}, x^{(j)} \rangle$, $i, j \in \{1, \ldots, k\}$.

DEFINITION 4.2. Let $A \in \mathcal{M}(n \times m, K)$, $B \in \mathcal{M}(n' \times m', K)$. The Kronecker product of A and B is the $nn' \times mm'$ matrix:

$$A \otimes B := \begin{pmatrix} a_{1,1}B & \ldots & a_{1,n}B \\ \vdots & & \vdots \\ a_{m,1}B & \ldots & a_{m,n}B \end{pmatrix}.$$

Thus if r is a natural number and $A \in \mathcal{M}(n, K)$ the r-Kronecker power of A is the $n^r \times n^r$ matrix:

$$\Pi_r(A) := A \otimes \overset{(r)}{\ldots} \cdots \otimes A =$$

$$\begin{pmatrix} a(1,1,\ldots,1;1,1,\ldots,1) & a(1,1,\ldots,1;1,1,\ldots,2) \cdots a(1,1,\ldots,1;n,n,\ldots,n) \\ a(1,1,\ldots,2;1,1,\ldots,1) & a(1,1,\ldots,2;1,1,\ldots,2) \cdots a(1,1,\ldots,2;n,n,\ldots,n) \\ \vdots & \vdots \\ a(n,n,\ldots,n;1,1,\ldots,1) & a(n,n,\ldots,n;1,1,\ldots,2) \cdots a(n,n,\ldots,n;n,n,\ldots,n) \end{pmatrix}$$

where $a(i_1, \ldots, i_r; k_1, \ldots, k_r) := a(i_1, k_1)a(i_2, k_2) \ldots a(i_r, k_r)$.

4.2.1. Some basic properties of $\Pi_r(A)$ are:

(1) $\Pi_r(A)$ is bisymmetric, i.e., if η is a permutation of $(1, \ldots, r)$, then

$$a(i_1, \ldots, i_r; k_1, \ldots, k_r) = a(i_{\eta(1)}, \ldots, i_{\eta(r)}; k_{\eta(1)}, \ldots, k_{\eta(r)})$$

for all indices i_j, k_m.

(2) $\Pi_r(AB) = \Pi_r(A)\Pi_r(B)$, thus if U is a matrix group then the set

$$\Pi_r(U) := \{\Pi_r(A)/A \in U\}$$

is also a matrix group.

(3) If A is an orthogonal matrix then $\Pi_r(A)$ is also orthogonal.

(4) If $\det(A) = 1$ then $\det(\Pi_r(A)) = 1$.

We shall proceed further considering the set $R^{(r)}$ of matrices of the form:

$$A^{(r)} := \begin{pmatrix} A_r & & & 0 \\ & A_{r-1} & & \\ & & \ddots & \\ 0 & & & A_0 \end{pmatrix}$$

where A_v is a $n^v \times n^v$ bisymmetric matrix and we denote its entries by $a(i_1, \ldots, i_v; k_1, \ldots, k_v) \in K$, $i_j, k_s \in \{1, \ldots, n\}$, $v = 1, \ldots, r$, and $A_0 := a(-,-) \in K$. Remark that $R^{(r)} \subset \mathcal{M}(m, K)$, where $m = 1 + n + n^2 + \cdots + n^r = \frac{n^{r+1}-1}{n-1}$.

4.2.2. Some properties of $R^{(r)}$ are:

(1) $R^{(r)}$ is a matrix algebra. In fact the product $A(r)B(r)$ is a bisymmetric matrix that has the form:

$$\begin{pmatrix} A_rB_r & & & 0 \\ & A_{r-1}B_{r-1} & & \\ & & \ddots & \\ 0 & & & A_0B_0 \end{pmatrix}.$$

(2) A subset of $R^{(r)}$ is the set of matrices of the form:

$$\Pi^{(r)}(A) := \begin{pmatrix} \Pi_r(A) & & & 0 \\ & \Pi_{(r-1)}(A) & & \\ & & \ddots & \\ 0 & & & \Pi_0(A) \end{pmatrix},$$

where $A \in SO(n)$ and $\Pi_0(A) := 1$.

It is easy to verify that $\Pi^{(r)}(AB) = \Pi^{(r)}(A)\Pi^{(r)}(B)$, so the set $\Pi^{(r)}(SO(n)) := \{\Pi^{(r)}(A)/A \in SO(n)\}$ is a group; besides $\Pi^{(r)}(A)\Pi^{(r)}(A)^t = I$, so $\Pi^{(r)}(SO(n))$ is a set of orthogonal matrices and consequently fully reducible.

We are interested in describing the enveloping algebra of $\Pi^{(r)}(SO(n))$, which agrees with $C(C(\Pi^{(r)}(SO(n))))$, after Theorem 4.1.1. Note first that if we denote:

$$B = \begin{pmatrix} B_{r,r} & B_{r,r-1} & \cdots & B_{r,0} \\ \vdots & \vdots & & \vdots \\ B_{0,r} & B_{0,r-1} & \cdots & B_{0,0} \end{pmatrix}$$

where $B_{u,v}$ are matrices of dimension $n^u \times n^v$ and coefficients $b(i_1, \ldots, i_u; j_1, \ldots, j_v)$, with $i_k, j_l \in \{1, \ldots, n\}$, then:

$$C(\Pi^{(r)}(SO(n))) = \{B \in M(m, K)/B\Pi^{(r)}(A) = \Pi^{(r)}(A)B, \text{ for all } A \in SO(n)\}.$$

PROPOSITION 4.2.3. *If $B \in C(\Pi^{(r)}(SO(n)))$, and for each $u, v \in \{0, \ldots, r\}$, we consider the multilinear form asociated to $u+v$ vectors:*

$$\begin{array}{rccc} f_{u,v}: & (\mathbb{R}^n)^{u+v} & \longrightarrow & \mathbb{R} \\ & (x^{(1)}, \ldots, x^{(u)}; & \longmapsto & \sum_{i_j, k_l \in \{1,\ldots,n\}} b(i_1, \ldots, i_u; k_1, \ldots, k_v) \\ & y^{(1)}, \ldots, y^{(v)}) & & x^{(1)}_{i_1} \ldots x^{(u)}_{i_u} y^{(1)}_{k_1} \ldots y^{(v)}_{k_v} \end{array}$$

defined by means of the (u,v)-entry $B_{u,v}$ of B, then $f_{u,v}$ is invariant asociated to $u+v$ vectors with respect to the group $SO(n)$.

PROOF. First note that

$$f_{u,v}(x^{(1)}, \ldots, x^{(u)}; y^{(1)}, \ldots, y^{(v)}) = (x^{(1)} \otimes \cdots \otimes x^{(u)}) B_{u,v}((y^{(1)})^t \otimes \cdots \otimes (y^{(v)})^t).$$

Let $A \in SO(n)$; since $B \in C(\Pi^{(r)}(SO(n)))$ it is easy to check that $B_{u,v} = \Pi_u(A) B_{u,v} (\Pi_v(A))^t$ for all $u, v \in \{0, \ldots, r\}$ and for all $A \in SO(n)$. Then we have the following identities:

$$\begin{aligned} & f_{u,v}(x^{(1)}A, \ldots, x^{(u)}A, y^{(1)}A, \ldots, y^{(v)}A) = \\ & = (x^{(1)}A \otimes \cdots \otimes x^{(u)}A) B_{u,v}((y(1)A)^t \otimes \cdots \otimes (y(v)A)^t) = \\ & = (x^{(1)} \otimes \cdots \otimes x^{(u)}) \Pi_u(A) B_{u,v} (\Pi_v(A))^t ((y(1))^t \otimes \cdots \otimes (y(v))^t) = \\ & = (x^{(1)} \otimes \cdots \otimes x^{(u)}) B_{u,v}((y^{(1)})^t \otimes \cdots \otimes (y^{(v)})^t) = \\ & = f_{u,v}(x^{(1)}, \ldots, x^{(u)}; y^{(1)}, \ldots, y^{(v)}). \quad \square \end{aligned}$$

COROLLARY 4.2.4. *With the notation above, if $B \in C(\Pi^{(r)}(SO(n)))$, then $f_{u,v}$ is in the $\mathbb{R}$-algebra generated by functions of the form:*

(1) $[z^{(i_1)}, \ldots, z^{(i_n)}]$,
(2) $g(z^{(1)}, \ldots, z^{(k)})$,

where $[z^{(i_1)}, \ldots, z^{(i_n)}]$, is the bracket factor, g is a polynomial combination of the scalar products $\langle z^{(i)}, z^{(j)} \rangle$, $i, j \in \{1, \ldots, k\}$, and the $z^{(i)}$ are choosen among the $x^{(l)}$ or $y^{(j)}$ variables. Moreover f can be written in such a way that there is no repeated variable in every monomial.

PROOF. After theorem 4.1.4, it is obvious that $f_{u,v}$ belongs to the $\mathbb{R}$-algebra generated by the functions stated in (i) and (ii). Besides $f_{u,v}$ has degree 1 in every variable $x^{(i)}_j$, so that functions generating it cannot have repeated variables. (Remark also that bracket factors with repeated variables $z^{(i)}$ are identically zero.) $\square$

Explaining a little more on the form of functions $f_{u,v}$ we remark that it is a linear combination of functions of the form:

$$\begin{aligned} (i)\ f^{\sigma\eta ab}_{u,v}(x^{(1)}, \ldots, x^{(u)}; y^{(1)}, \ldots, y^{(v)}) := & \langle x^{(\sigma(1))}, x^{(\sigma(2))} \rangle \cdot \ldots \cdot \langle x^{(\sigma(2a-1))}, \\ & x^{(\sigma(2a))} \rangle \cdot \langle y^{(\eta(1))}, y^{(\eta(2))} \rangle \cdot \ldots \cdot \langle y^{(\eta(2b-1))}, y^{(\eta(2b))} \rangle \cdot \\ & \cdot \langle x^{(\sigma(2a+1))}, y^{(\eta(2b+1))} \rangle \cdot \ldots \cdot \langle x^{(\sigma(u))}, y^{(\eta(v))} \rangle. \end{aligned}$$

$$(ii)\ g_{u,v}^{\sigma\eta\omega\alpha}{}_{cda'b'}(x^{(1)},\dots,x^{(u)};y^{(1)},\dots,y^{(v)}) := [x^{(\sigma(1))},\dots,x^{(\sigma(c))},y^{(\eta(1))},$$
$$\dots,y^{(\eta(d))}]\cdot f_{u-c,v-d}^{\omega\alpha a'b'}(x^{(\sigma(c+1))},\dots,x^{(\sigma(u))};y^{(\eta(d+1))},\dots,y^{(\eta(v))})$$

where σ and η are permutations of $(1,\dots,u)$ and $(1,\dots,v)$ respectively, $u-2a = v-2b$, $u-c-2a' = v-d-2b'$, $c+d=n$ and, finally, ω and α are permutations of $(\sigma(c+1),\dots,\sigma(u))$ and $(\eta(d+1),\dots,\eta(v))$ respectively. Remark that powers of bracket factors do not appear because of the relation:

$$[x^{(1)},\dots,x^{(n)}]\cdot[y^{(1)},\dots,y^{(n)}] = \begin{vmatrix} \langle x^{(1)},y^{(1)}\rangle & \dots & \langle x^{(1)},y^{(n)}\rangle \\ \vdots & & \vdots \\ \langle x^{(n)},y^{(1)}\rangle & \dots & \langle x^{(n)},y^{(n)}\rangle \end{vmatrix}.$$

Let's denote by $\delta_{u,v}^{\sigma\eta ab}(i_{1,\dots,u};k_{1,\dots,v})$ the function:

$$\delta(i_{\sigma(1)},i_{\sigma(2)})\cdot\dots\cdot\delta(i_{\sigma(2a-1)},i_{\sigma(2a)})\cdot\delta(k_{\eta(1)},k_{\eta(2)})\cdot\dots\cdot$$
$$\delta(k_{\eta(2b-1)},k_{\eta(2b)})\cdot\delta(i_{\sigma(2a+1)},k_{\eta(2b+1)})\cdot\dots\cdot\delta(i_{\sigma(u)},k_{\eta(v)})$$

and by $\gamma_{u,v}^{\sigma\eta cd}(i_{1,\dots,u};k_{1,\dots,v})$ the function:

$$\#\gamma(i_{\sigma(1)},i_{\sigma(2)})\cdot\dots\cdot\gamma(i_{\sigma(1)},i_{\sigma(c)})\cdot\gamma(i_{\sigma(1)},k_{\eta(1)})\cdot\dots\cdot\gamma(i_{\sigma(1)},k_{\eta(d)})\cdot$$
$$\cdot\gamma(i_{\sigma(2)},i_{\sigma(3)})\cdot\dots\cdot\gamma(i_{\sigma(2)},i_{\sigma(c)})\cdot\gamma(i_{\sigma(2)},k_{\eta(1)})\cdot\dots\cdot\gamma(i_{\sigma(2)},k_{\eta(d)})\cdot$$
$$\vdots$$
$$\cdot\gamma(i_{\sigma(c)},k_{\eta(1)})\cdot\dots\cdot\gamma(i_{\sigma(c)},k_{\eta(d)})\cdot$$
$$\cdot\gamma(k_{\eta(1)},k_{\eta(2)})\cdot\dots\cdot\gamma(k_{\eta(1)},k_{\eta(d)})\cdot$$
$$\dots$$
$$\cdot\gamma(k_{\eta(d-1)},k_{\eta(d)})$$

where $\gamma(i,j) := 1-\delta(i,j)$ and $\#$ takes value 1 or -1 according to the parity of the permutations σ and η ; in fact when the function $\gamma_{u,v}^{\sigma\eta cd}(i_{1,\dots,u};k_{1,\dots,v})$ is different from 0 the n-uple $(\sigma(1),\dots,\sigma(c),\eta(1),\dots,\eta(d))$ is a permutation of $(1,\dots,n)$; if it is even then $\# := 1$ and $\# := -1$ in other case. Remark that both $\delta_{u,v}$ and $\gamma_{u,v}$ are $\{0,1,-1\}$ valued functions.

COROLLARY 4.2.5. *With the notation above, if $B \in C(\Pi^{(r)}(SO(n)))$ then we have, for all indices i_j and k_l that:*

$$b(i_1,\dots,i_u;k_1,\dots,k_v) =$$

$$= \sum_{\sigma,\eta,a,b}\lambda_{\sigma\eta ab}\cdot\delta_{u,v}^{\sigma\eta ab}(i_{1,\dots,u};k_{1,\dots,v}) +$$
$$+\sum_{\substack{\sigma,\eta,\omega,\alpha\\ c,d,a,b}}\beta_{cdab}^{\sigma\eta\omega\alpha}\cdot\gamma_{u,v}^{\sigma\eta cd}(i_{1,\dots,u};k_{1,\dots,v})\cdot\delta_{u-c,v-d}^{\omega\alpha ab}(i_{\sigma(c+1),\dots,\sigma(u)};k_{\eta(d+1),\dots,\eta(v)})$$

where $\lambda_{\sigma\eta ab}$ *and* $\beta^{\sigma\eta\omega\alpha}_{cdab}$ *are constants.*

PROOF. As we have seen, it is possible to write:

$$f_{u,v} = \sum_{\sigma,\eta,a,b} \lambda_{\sigma\eta ab} \cdot f^{\sigma\eta ab}_{u,v} + \sum_{\substack{\sigma,\eta,\omega,\alpha \\ c,d,a,b}} \beta^{\sigma\eta\omega\alpha}_{cdab} \cdot g^{\sigma\eta\omega\alpha\ cdab}_{u,v}.$$

In particular we can write:

$$\sum_{\sigma,\eta,a,b} \lambda_{\sigma\eta ab} \cdot f^{\sigma\eta ab}_{u,v} = \sum_{i_j,k_l} \Big[\sum_{\sigma,\eta,a,b} \lambda_{\sigma\eta ab} \cdot \delta^{\sigma\eta ab}_{u,v}(i_{1,\ldots,u}; k_{1,\ldots,v}) \Big] x^{(1)}_{i_1} \ldots x^{(u)}_{i_u} y^{(1)}_{k_1} \ldots y^{(v)}_{k_v}$$

and analogously:

$$\sum_{\substack{\sigma,\eta,\omega,\alpha \\ c,d,a,b}} \beta^{\sigma\eta\omega\alpha}_{cdab} \cdot g^{\sigma\eta\omega\alpha\ cdab}_{u,v} =$$

$$= \sum_{i_j,k_l} \Big[\sum_{\sigma,\eta,a,b} \beta^{\sigma\eta\omega\alpha}_{cdab} \cdot \gamma^{\sigma\eta ab}_{u,v}(i_{1,\ldots,u}; k_{1,\ldots,v}) +$$

$$+ \sum_{\substack{\sigma,\eta,\omega,\alpha \\ c,d,a,b}} \beta^{\sigma\eta\omega\alpha}_{cdab} \cdot \gamma^{\sigma\eta cd}_{u,v}(i_{1,\ldots,u}; k_{1,\ldots,v}) \cdot \delta^{\omega\alpha ab}_{u-c,v-d}(i_{\sigma(c+1),\ldots,\sigma(u)}; k_{\eta(d+1),\ldots,\eta(v)}) \Big]$$

$$x^{(1)}_{i_1} \ldots x^{(u)}_{i_u} y^{(1)}_{k_1} \ldots y^{(v)}_{k_v}.$$

So, identifying in the first expression the coefficients corresponding to the monomial $x^{(1)}_{i_1} \ldots x^{(u)}_{i_u} y^{(1)}_{k_1} \ldots y^{(v)}_{k_v}$, we obtain the desired equality. □

4.3. After this preparation we are ready to prove the main point, namely the description of the set of "linearized orthogonal matrices" (i.e. $[\Pi^{(r)}(SO(n))]$) by means of a set $U^{(r)}$ of linear equations in the entries of the matrices in $R^{(r)}$. As explained at the beginning of this paragraph, we shall use theorem 4.1.1 to test equality between $U^{(r)}$ and $[\Pi^{(r)}(SO(n))]$. Naturally we shall profit from the special form of writing the elements in $C(\Pi^{(r)}(SO(n)))$ given by corollary 4.2.5.

DEFINITION 4.3.1. Consider the sets of matrices:[1]

$$U^{(r)} := \Big\{ A^{(r)} \in R^{(r)} / \sum_{k=1}^{n} a(i_1, \ldots, i_v; k, k, k_3, \ldots, k_v) = \delta(i_1, i_2) a(i_3, \ldots, i_v; k_3, \ldots, k_v),$$
$$\sum_{i=1}^{n} a(i, i, i_3, \ldots, i_v; k_1, \ldots, k_v) = \delta(k_1, k_2) a(i_3, \ldots, i_v; k_3, \ldots, k_v),$$
$$v \in \{2, \ldots, r\}; i_j, k_j \in \{1, \ldots, n\} \Big\}.$$

[1]The set $U^{(r)}$ alone is the one needed for the proof of the orthogonal case.

We will denote by π_a a permutation of $(1,\dots,a)$, and $|\pi_a|$ takes value 1 if π_a is even and -1 if it is odd.

$$\begin{aligned}T^{(r)}:=\Big\{&A^{(r)}\in R^{(r)}/\\ &\sum_{\pi_a}|\pi_a|a(i_1,\dots,i_a,i_{a+1},\dots,i_v;k_{\pi_a(1)},\dots,k_{\pi_a(a)},k_{a+1},\dots,k_v)\\ &=\sum_{\omega_b}|\omega_b|a(I_1,\dots,I_b,i_{a+1},\dots,i_v;K_{\omega_b(1)},\dots,K_{\omega_b(b)},k_{a+1},\dots,k_v),\\ &(i_1,\dots,i_a,I_1,\dots,I_b)\text{ and }(k_1,\dots,k_a,K_1,\dots,K_b)\\ &\text{even permutations of }(1,\dots,n),i_{a+1},\dots,i_v,k_{a+1},\dots,k_v\\ &\qquad\in\{1,\dots,n\},a+b=n,a\geq b,1\leq v\leq r\Big\}.\end{aligned}$$

Finally let us call $\underline{U}^{(r)}:=U^{(r)}\cap T^{(r)}$.

It is an easy exercise to prove that all these sets are $\mathbb{K}$-algebras.

THEOREM 4.3.2. (Cf. [**W**].) *For any natural number r,*

$$\underline{U}^{(r)}:=[\Pi^{(r)}(SO(n))].$$

PROOF. For the inclusion $[\Pi^{(r)}(SO(n))]\subset\underline{U}^{(r)}$, since $\underline{U}^{(r)}$ is a $\mathbb{K}$-algebra, it suffices to prove $\Pi^{(r)}(SO(n))\subset\underline{U}^{(r)}$. Let $\Pi^{(r)}(A)\in\Pi^{(r)}(SO(n))$, $A\in SO(n)$; as we have seen, $\Pi^{(r)}(A)\in R^{(r)}$ and it verifies:

$$\begin{aligned}\sum_{k=1}^{n}a(i_1,\dots,i_v;k,k,k_3,\dots,k_v)&=\Big[\sum_{k=1}^{n}a(i_1,k)a(i_2,k)\Big]x(i_3,k_3)\dots x(i_v,k_v)\\ &=\delta(i_1,i_2)a(i_3,\dots,i_v;k_3,\dots,k_v).\end{aligned}$$

The same reasoning concludes the other condition needed in order to prove $\Pi^{(r)}(A)\in U^{(r)}$.

On the other hand, technical result 3.1.4 allows us to establish the central identity among the following, to obtain that $\Pi^{(r)}(A)\in T^{(r)}$.

$$\begin{aligned}&\sum_{\pi_a}|\pi_a|a(i_1,\dots,i_a,i_{a+1},\dots,i_v;k_{\pi_a(1)},\dots,k_{\pi_a(a)},k_{a+1},\dots,k_v)=\\ &=\Big[\sum_{\pi_a}|\pi_a|a(i_1,k_{\pi_a(1)})\dots,a(i_a,k_{\pi_a(a)})\Big]a(i_{a+1},k_{a+1})\dots,a(i_v,k_v)=\\ &=\begin{vmatrix}a(i_1,k_1)&\dots&a(i_1,k_a)\\ \vdots&&\vdots\\ a(i_a,k_1)&\dots&a(i_a,k_a)\end{vmatrix}a(i_{a+1},k_{a+1})\dots,a(i_v,k_v)=\\ &=\begin{vmatrix}a(I_1,K_1)&\dots&a(I_1,K_b)\\ \vdots&&\vdots\\ a(I_b,K_1)&\dots&a(I_b,K_b)\end{vmatrix}a(i_{a+1},k_{a+1})\dots,a(i_v,k_v)=\\ &=\Big[\sum_{\omega_b}|\omega_b|a(I_1,K_{\omega_b(1)})\dots,a(I_b,K_{\omega_b(b)})\Big]a(i_{a+1},k_{a+1})\dots,a(i_v,k_v)=\\ &=\sum_{\omega_b}|\omega_b|a(I_1,\dots,I_b,i_{a+1},\dots,i_v;K_{\omega_b(1)},\dots,K_{\omega_b(b)},k_{a+1},\dots,k_v).\end{aligned}$$

With respect to the other inclusion, after theorem 4.1.1., it suffices to prove $\underline{U}^{(r)} \in C(C(\Pi^{(r)}(SO(n))))$. Let $A^{(r)} \in \underline{U}^{(r)}$ and $B \in C(\Pi^{(r)}(SO(n)))$. We will prove, as needed, that $B_{u,v}A_v = A_uB_{u,v}$ for all $u, v \in \{0, \ldots, r\}$. Multiplying the $(i_1, \ldots, i_u)$-row of $B_{u,v}$ times the $(k_1, \ldots, k_v)$-column of A_v we obtain:

$$\sum_j b(i_1, \ldots, i_u; j_1, \ldots, j_v) a(j_1, \ldots, j_v; k_1, \ldots, k_v)$$

$$= \sum_j \Big[\sum_{\sigma,\eta,a,b} \lambda_{\sigma\eta ab} \delta_{u,v}^{\sigma\eta ab}(i_{1,\ldots,u}; k_{1,\ldots,v})$$

$$+ \sum_{\substack{\sigma,\eta,\omega,\alpha \\ c,d,a,b}} \beta_{\substack{\sigma\eta\omega\alpha \\ cdab}} \gamma_{u,v}^{\sigma\eta cd}(i_{1,\ldots,u}; k_{1,\ldots,v}) \delta_{u-c,v-d}^{\omega\alpha ab}(i_{\sigma(c+1),\ldots,\sigma(u)}; k_{\eta(d+1),\ldots,\eta(v)}) \Big]$$

$$a(j_1, \ldots, j_v; k_1, \ldots, k_v) = \sum_{\sigma,\eta,a,b} \lambda_{\sigma\eta ab} \beta_{\substack{\sigma\eta\omega\alpha \\ cdab}}$$

$$\Big[\sum_j \delta_{u,v}^{\sigma\eta ab}(i_{1,\ldots,u}; k_{1,\ldots,v}) a(j_1, \ldots, j_v; k_1, \ldots, k_v) \Big]$$

$$+ \sum_{\substack{\sigma,\eta,\omega,\alpha \\ c,d,a,b}} \Big[\sum_j \gamma_{u,v}^{\sigma\eta cd}(i_{1,\ldots,u}; k_{1,\ldots,v}) \delta_{u-c,v-d}^{\omega\alpha ab}$$

$$(i_{\sigma(c+1),\ldots,\sigma(u)}; k_{\eta(d+1),\ldots,\eta(v)}) a(j_1, \ldots, j_v; k_1, \ldots, k_v) \Big].$$

Making the equivalent computation with $A_uB_{u,v}$ we see that it suffices to prove, for $\sigma, \eta, \omega, \alpha, a, b, c, d$ fixed, the two identities:

(I_1)

$$\sum_j \delta_{u,v}^{\sigma\eta ab}(i_{1,\ldots,u}; j_{1,\ldots,v}) a(j_1, \ldots, j_v; k_1, \ldots, k_v)$$

$$= \sum_j \delta_{u,v}^{\sigma\eta ab}(j_{1,\ldots,u}; k_{1,\ldots,v}) a(i_1, \ldots, i_u; j_1, \ldots, j_u).$$

(I_2)

$$\sum_j \gamma_{u,v}^{\sigma\eta cd}(i_{1,\ldots,u}; j_{1,\ldots,v}) \delta_{u-c,v-d}^{\omega\alpha ab}(i_{\sigma(c+1),\ldots,\sigma(u)}; j_{\eta(d+1),\ldots,\eta(v)})$$

$$a(j_1, \ldots, j_v; k_1, \ldots, k_v) = \sum_j \gamma_{u,v}^{\sigma\eta cd}(j_{1,\ldots,u}; k_{1,\ldots,v}) \delta_{u-c,v-d}^{\omega\alpha ab}(j_{\sigma(c+1),\ldots,\sigma(u)};$$

$$k_{\eta(d+1),\ldots,\eta(v)}) a(i_1, \ldots, i_u; j_1, \ldots, j_u).$$

Playing with the expressions in (I_1) and since $A^{(r)} \in U^{(r)}$, we obtain that both sides of the equality are equal to:

$$\delta(i_{\sigma(1)}, i_{\sigma(2)}) \ldots \delta(i_{\sigma(2a-1)}, i_{\sigma(2a)}) \delta(k_{\eta(1)}, k_{\eta(2)}) \ldots \delta(k_{\eta(2b-1)}, k_{\eta(2b)})$$

$$a(i_{\sigma(2a+1)}, \ldots, i_{\sigma(u)}; k_{\eta(2b+1)}, \ldots, k_{\eta(v)}).$$

With respect to (I_2) in order to simplify [sic] the notation, we will suppose that the fixed permutations are identities. Again playing with the indices and after using the definition of $U^{(r)}$ we have that the identity in (I_2) is equivalent to:

$$\sum_j \#a(j_1,\dots,j_d,i_{c+2a+1},\dots,i_u;k_1,\dots,k_d,k_{d+2b+1},\dots,k_v) = \sum_{j'} \#a(i_1,\dots,i_c,i_{c+2a+1},\dots,i_u;j'_1,\dots,j'_c,k_{d+2b+1},\dots,k_v)$$

where $\{i_1,\dots,i_c,j_1,\dots,j_d\}$ and $\{k_1,\dots,k_d,j'_1,\dots,j'_c\}$ are pairwise distinct; thus, and since $c+d=n$, the sums in j and j' are sums in the permutations of $\{1,\dots,n\}-\{i_1,\dots,i_c\}$ and $\{1,\dots,n\}-\{k_1,\dots,k_d\}$ respectively, so that the last identity is one of the stated in the definition of the set $T^{(r)}$. We remark that in this definition the conditions on the permutations $(i_1,\dots,i_a,I_1,\dots,I_b)$ and $(k_1,\dots,k_a,K_1,\dots,K_b)$ to be even is not essential in this proof. □

4.4. Finally we arrive at the description of the Weyl basis for $SO(n)$ and $O(n)$ in terms of the polynomials $\{\{D_{i,j}\}_{i,j},\{D^*_{i,j}\}_{i,j},\{D(\pi,\omega;a,b)\}_{\pi,\omega,a,b}\}$ introduced in §2.

THEOREM 4.4.1. *Let $p(x_{1,1},\dots,x_{1,n},\dots,x_{n,1},\dots,x_{n,n})\in\mathbf{R}[\underline{x}]$ of degree r such that it vanishes on all proper real orthogonal matrices. Then p can be written in the form:*

$$p=\sum_{i,j}L_{i,j}.D_{i,j}+\sum_{i,j}L^*_{i,j}.D^*_{i,j}+\sum_{\pi,\omega,a,b}H_{\pi,\omega,a,b}.D(\pi,\omega;a,b)$$

where $\deg(L_{i,j})\le r-2,\deg(L^*_{i,j})\le r-2$ *and* $\deg(H_{\pi,\omega,a,b})\le r-a$.

PROOF. We can write p in bisymmetric form, i.e.:

$$p(\underline{x})=\sum_{v=0}^{r}\Gamma(i_1,\dots,i_v;k_1,\dots,k_v)x_{i_1,k_1}\dots x_{i_v,k_v}$$

where $\Gamma(i_1,\dots,i_v;k_1,\dots,k_v)=\Gamma(i_{\sigma(1)},\dots,i_{\sigma(v)};k_{\sigma(1)},\dots,k_{\sigma(v)})$ for all σ permutations of $(1,\dots,v)$. Consider the function:

$$g=\sum_{v=0}^{r}\sum_{i_j,k_l}\Gamma(i_1,\dots,i_v;k_1,\dots,k_v)x(i_1,\dots,i_v;k_1,\dots,k_v)\,.$$

Remark that g is a linear form in the variables

$$x(-,-),$$
$$x(1,1),x(1,2),\dots,x(n,n),$$
$$\dots,$$
$$x(1,\dots^{(r)}\dots,1;1,\dots^{(r)}\dots,1),x(1,\dots,2;1,\dots,1),\dots,x(n,\dots,n;n,\dots,n)$$

that vanishes on all matrices in $\Pi^{(r)}(SO(n))$, because $\Pi^{(r)}(A) = p(A) = 0$ for all $A \in SO(n)$, so it vanishes also in $[\Pi^{(r)}(SO(n))] = \underline{U}^{(r)}$. Since $\underline{U}^{(r)}$ is the set of zeroes of the linear forms:

$$
\begin{aligned}
H_v(i_{1,\ldots,v}; k_{3,\ldots,v}) &:= \sum_{k=1}^{n} x(i_1, \ldots, i_v; k, k, k_3, \ldots, k_v) - \delta(i_1, i_2) \\
&\quad x(i_3, \ldots, i_v; k_3, \ldots, k_v), \\
F_v(i_{3,\ldots,v}; k_{1,\ldots,v}) &:= \sum_{i=1}^{n} x(i, i, i_3, \ldots, i_v; k_1, \ldots, k_v) - \delta(k_1, k_2) \\
&\quad x(i_3, \ldots, i_v; k_3, \ldots, k_v), \\
T_v(i_{1,\ldots,v}; k_{1,\ldots,v}; \sigma) &:= x(i_1, \ldots, i_v; k_1, \ldots, k_v) - x(i_{\sigma(1)}, \ldots, i_{\sigma(v)}; \\
&\quad k_{\sigma(1)}, \ldots, k_{\sigma(v)}), Q_v(i_{1,\ldots,v}; k_{1,\ldots,v}; I_{1,\ldots,v}; K_{1,\ldots,v}; a, b; \pi_a, \omega_b) \\
&:= \sum_{\pi_a} |\pi_a| a(i_1, \ldots, i_a, i_{a+1}, \ldots, i_v; k_{\pi_a(1)}, \ldots, k_{\pi_a(a)}, \\
&\qquad k_{a+1}, \ldots, k_v) \\
&\quad - \sum_{\omega_b} |\omega_b| a(I_1, \ldots, I_b, i_{a+1}, \ldots, i_v; K_{\omega_b(1)}, \ldots, K_{\omega_b(b)}, \\
&\qquad k_{a+1}, \ldots, k_v)
\end{aligned}
$$

indices and permutations running over above indicated ranges, then g is a linear combination of these forms, i.e.:

$$
\begin{aligned}
&\sum_{v=0}^{r} \Gamma(i_1, \ldots, i_v; k_1, \ldots, k_v) x_{i_1,k_1} \ldots x_{i_v,k_v} \\
&= \sum_{v=2}^{r} \sum_{i,k} h_v(i_{1,\ldots,v}; k_{3,\ldots,v}) H_v(i_{1,\ldots,v}; k_{3,\ldots,v}) \\
&\quad + \sum_{v=2}^{r} \sum_{i,k} f_v(i_{3,\ldots,v}; k_{1,\ldots,v}) F_v(i_{3,\ldots,v}; k_{1,\ldots,v}) \\
&\quad + \sum_{v=1}^{r} \sum_{i,k,\sigma} t_v(i_{1,\ldots,v}; k_{1,\ldots,v}; \sigma) T_v(i_{1,\ldots,v}; k_{1,\ldots,v}; \sigma) \\
&\quad + \sum_{v=1}^{r} \sum_{i,k,I,K,\pi_a,\omega_b} q_v(i_{1,\ldots,v}; k_{1,\ldots,v}; I_{1,\ldots,v}; K_{1,\ldots,v}; a, b; \pi_a, \omega_b) \\
&\qquad Q_v(i_{1,\ldots,v}; k_{1,\ldots,v}; I_{1,\ldots,v}; K_{1,\ldots,v}; a, b; \pi_a, \omega_b)
\end{aligned}
$$

where h_v, f_v, t_v and q_v are constants in the field.

Putting, in particular, $x(i_1, \ldots, i_v; k_1, \ldots, k_v) = x(i_1, k_1) x(i_2, k_2) \ldots x(i_v, k_v)$

and $x(-,-) = 1$, we obtain:

$$p(\underline{x}) =$$
$$= \sum_{v=2}^{r} \sum_{i,k} h_v(i_{1,\ldots,v}; k_{3,\ldots,v})(x(i_3,k_3)\ldots x(i_v,k_v)D_{i_1,i_2}(\underline{x}))+$$
$$+\sum_{v=2}^{r} \sum_{i,k} f_v(i_{1,\ldots,v}; k_{3,\ldots,v})(x(i_3,k_3)\ldots x(i_v,k_v)D^*_{i_1,i_2}(\underline{x}))+$$
$$+\sum_{v=1}^{r} \sum_{i,k,I,K,\pi_a,\omega_b} q_v(i_{1,\ldots,v}; k_{1,\ldots,v}; I_{1,\ldots,v}; K_{1,\ldots,v}; a, b; \pi_a, \omega_b)$$
$$\left(x(i_{a+1},k_{a+1})\ldots x(i_v,k_v)D_{\pi_a,\omega_b;a,b}(\underline{x})\right),$$

which is the desired combination verifying the requirements on the degrees. □

Analogously we have for the orthogonal ideal the following basis:

THEOREM 4.4.2. *Let $p(x_{1,1},\ldots,x_{1,n},\ldots,x_{n,1},\ldots,x_{n,n}) \in \mathbb{R}[\underline{x}]$ of degree r such that it vanishes on all real orthogonal matrices. Then p can be written in the form:*

$$p = \sum_{i,j} L_{i,j}.D_{i,j} + \sum_{i,j} L^*_{i,j}.D^*_{i,j}$$

where $\deg(L_{i,j}) \leq r-2$ *and* $\deg(L^*_{i,j}) \leq r-2$, $i,j \in 1,\ldots,n$.

COROLLARY 4.4.3.

(i) $\mathbf{so}.\mathbb{R}[\underline{x}] = \langle \{D_{i,j}\}_{i,j}, \{D^*_{i,j}\}_{i,j}, \{D(\pi,\omega;a,b)\}_{\pi,\omega,a,b}\rangle.\mathbb{R}[\underline{x}]$, *and this basis solves the ideal membership problem for* $\mathbf{so}.\mathbb{R}[\underline{x}]$.

(ii) $\mathbf{o}.\mathbb{R}[\underline{x}] = \langle \{D_{i,j}\}_{i,j}, \{D^*_{i,j}\}_{i,j}\rangle.\mathbb{R}[\underline{x}]$, *and this basis solves the ideal membership problem for* $\mathbf{o}.\mathbb{R}[\underline{x}]$.

PROOF. The equality between ideals is obvious from the theorems above and the technical results in 3.1. Concerning the ideal membership problem let us remark that given an element $p(\underline{x})$ in $\mathbf{so}.\mathbb{R}[\underline{x}]$ of degree r we can formally express an identity:

$$p = \sum_{i,j} L_{i,j}.D_{i,j} + \sum_{i,j} L^*_{i,j}.D^*_{i,j} + \sum_{\pi,\omega,a,b} H_{\pi,\omega,a,b}.D(\pi,\omega;a,b)$$

where $L_{i,j}L^*_{i,j}$ and $H_{\pi,\omega,a,b}$ are given with indeterminated coefficients as their degrees are bounded by $\deg(L_{i,j}) \leq r-2, \deg(L^*_{i,j}) \leq r-2$ and $\deg(H_{\pi,\omega,a,b}) \leq r-a$. This identity yields a linear system of equations when we identify the coefficients of $p(\underline{x})$ with the linear combinations in the indeterminated coefficients. Solving this linear system gives us either that $p(\underline{x})$ does not belong to $\mathbf{so}.\mathbb{R}[\underline{x}]$ (if no solution exists) or the coefficients of the representation of $p(\underline{x})$ in terms of the Weyl basis. The same applies for the case $\mathbf{o}.\mathbb{R}[\underline{x}]$. □

5. Some examples and computational remarks

5.1 Weyl basis for $O(2)$ and $SO(2)$.

Weyl basis for $O(2)$	Weyl basis for $SO(2)$
$x_{1,1}^2 + x_{2,1}^2 - 1,$	$x_{1,1}^2 + x_{2,1}^2 - 1,$
$x_{1,2}^2 + x_{2,2}^2 - 1,$	$x_{1,2}^2 + x_{2,2}^2 - 1,$
$x_{1,1}x_{1,2} + x_{2,1}x_{2,2},$	$x_{1,1}x_{1,2} + x_{2,1}x_{2,2},$
$x_{1,1}^2 + x_{1,2}^2 - 1,$	$x_{1,1}^2 + x_{1,2}^2 - 1,$
$x_{2,1}^2 + x_{2,2}^2 - 1,$	$x_{2,1}^2 + x_{2,2}^2 - 1,$
$x_{1,1}x_{2,1} + x_{1,2}x_{2,2}$	$x_{1,1}x_{2,1} + x_{1,2}x_{2,2},$
	$x_{1,1} - x_{2,2},$
	$x_{1,2} + x_{2,1}$

5.2 Weyl basis for $O(3)$ and $SO(3)$.

Weyl basis for $O(3)$	Weyl basis for $SO(3)$
$x_{1,1}^2 + x_{2,1}^2 + x_{3,1}^2 - 1,$	$x_{1,1}^2 + x_{2,1}^2 + x_{3,1}^2 - 1,$
$x_{1,2}^2 + x_{2,2}^2 + x_{3,2}^2 - 1,$	$x_{1,2}^2 + x_{2,2}^2 + x_{3,2}^2 - 1,$
$x_{1,3}^2 + x_{2,3}^2 + x_{3,3}^2 - 1,$	$x_{1,3}^2 + x_{2,3}^2 + x_{3,3}^2 - 1,$
$x_{1,1}x_{1,2} + x_{2,1}x_{2,2} + x_{3,1}x_{3,2},$	$x_{1,1}x_{1,2} + x_{2,1}x_{2,2} + x_{3,1}x_{3,2},$
$x_{1,1}x_{1,3} + x_{2,1}x_{2,3} + x_{3,1}x_{3,3},$	$x_{1,1}x_{1,3} + x_{2,1}x_{2,3} + x_{3,1}x_{3,3},$
$x_{1,2}x_{1,3} + x_{2,2}x_{2,3} + x_{3,2}x_{3,3},$	$x_{1,2}x_{1,3} + x_{2,2}x_{2,3} + x_{3,2}x_{3,3},$
$x_{1,1}^2 + x_{1,2}^2 + x_{1,3}^2 - 1,$	$x_{1,1}^2 + x_{1,2}^2 + x_{1,3}^2 - 1,$
$x_{2,1}^2 + x_{2,2}^2 + x_{2,3}^2 - 1,$	$x_{2,1}^2 + x_{2,2}^2 + x_{2,3}^2 - 1,$
$x_{3,1}^2 + x_{3,2}^2 + x_{3,3}^2 - 1,$	$x_{3,1}^2 + x_{3,2}^2 + x_{3,3}^2 - 1,$
$x_{1,1}x_{2,1} + x_{1,2}x_{2,2} + x_{1,3}x_{2,3},$	$x_{1,1}x_{2,1} + x_{1,2}x_{2,2} + x_{1,3}x_{2,3},$
$x_{1,1}x_{3,1} + x_{1,2}x_{3,2} + x_{1,3}x_{3,3},$	$x_{1,1}x_{3,1} + x_{1,2}x_{3,2} + x_{1,3}x_{3,3},$
$x_{2,1}x_{3,1} + x_{2,2}x_{3,2} + x_{2,3}x_{3,3}$	$x_{2,1}x_{3,1} + x_{2,2}x_{3,2} + x_{2,3}x_{3,3},$
	$x_{1,1} - (x_{2,2}x_{3,3} - x_{3,2}x_{2,3}),$
	$x_{1,2} - (-x_{2,1}x_{3,3} + x_{3,1}x_{2,3}),$
	$x_{1,3} - (x_{2,1}x_{3,2} - x_{3,1}x_{2,2}),$
	$x_{2,1} - (x_{3,2}x_{1,3} - x_{1,2}x_{3,3}),$
	$x_{2,2} - (x_{1,1}x_{3,3} - x_{3,1}x_{1,3}),$
	$x_{2,3} - (x_{3,1}x_{1,2} - x_{1,1}x_{3,2}),$
	$x_{3,1} - (x_{1,2}x_{2,3} - x_{2,2}x_{1,3}),$
	$x_{3,2} - (x_{2,1}x_{1,3} - x_{1,1}x_{2,3}),$
	$x_{3,3} - (x_{1,1}x_{2,2} - x_{2,1}x_{1,2})$

5.3. Weyl bases are a particular case of what we have denominated Macaulay basis according to the following definition:

DEFINITION. A finite basis B of an ideal $\mathbf{I}$ in $I\!K[\underline{x}]$ is a Macaulay basis of $\mathbf{I}$ if for every $f \in \mathbf{I}$ there exist $h_1, \ldots, h_k \in B$ and $l_1, \ldots, l_k \in I\!K[\underline{x}]$ such that:

(i) $f = \sum_{j=1}^{k} l_j.h_j$,
(ii) $\deg(l_i) \leq \deg(f) - \deg(h_i) \geq 0$, $i \in \{1, \ldots, k\}$.

It is easy to see the following equivalence:

PROPOSITION. *Let $B = \{g_1, \ldots, g_r\}$ be a basis of $\mathbf{I}$; we denote by $\mathbf{I}^h$ the homogeneous ideal asociated to $\mathbf{I}$ with respect to a new variable x_0 and we write f^h to denote the polynomial f homogeneized with x_0. The following sentences are equivalent:*

(i) *B is a Macaulay basis of $\mathbf{I}$.*
(ii) *$\{g_1^h, \ldots, g_r^h\}$ is a basis of $\mathbf{I}^h$.*

5.4 Remark. Macaulay basis and Grobner basis share properties (both can be used to test ideal membership and also to find a basis of the homogeneized ideal, for instance) but the following example shows that although Grobner bases for degree compatible ordering are also Macaulay bases, there is a strict inclusion between the two concepts:

For $B := \{x + y, xy\} \subset \mathbb{C}[x, y]$ and $\mathbf{I} := \langle B \rangle$, we have that B is not a Grobner basis with respect to any order degree compatible. In fact we have only two possibilities: $x > y$ and $x < y$; and Grobner basis are, respectively $\{x + y, y^2\}$ and $\{x + y, x^2\}$. However B is Macaulay basis because, since $\{x + y, x^2\}$ is a Grobner basis with respect to an order degree compatible and $x^2 = x.(x+y) - xy$, each $f \in \mathbf{I}$ can be written as $f = l_1.(x + y) + l_2.x^2 = (l_1 + l_2.x).(x + y) - l_2.xy$ with $\deg(l_1) \leq \deg(f) - 1 \geq 0$ and $\deg(l_2) \leq \deg(f) - 2 \geq 0$. Thus $\deg(-l_2) \leq \deg(f) - 2 \geq 0$ and $\deg(l_1 + l_2.x) \leq \deg(f) - 1 \geq 0$.

5.5. The searching for a general rule to describe Grobner basis with respect to a suitable order for the orthogonal and proper orthogonal ideals has produced several negative results that we consider could be of interest when compared with Weyl basis. In the following summary we collect information concerning, for $n = 2, 3, 4$, when the Weyl basis is also a Grobner basis with respect to a degree compatible order.

	$n=2$	$n=3$	$n=4$
$SO(n)$	Yes, for all possible orders	Yes, for the many orders checked	No, for the row-order$^{(*)}$
$O(n)$	Yes, for circular orders$^{(**)}$ No, for the remaining orders	No, for the many orders checked	No, for the row-order$^{(*)}$

$^{(*)}$ The row-order for n is the degree compatible order in which

$$x_{1,1} > x_{1,2} > \ldots x_{1,n} > x_{2,1} > x_{2,2} > \cdots > x_{2,n} > \cdots > x_{n,1} > x_{n,2} > \ldots x_{n,n}.$$

$^{(**)}$ A circular order for $n = 2$ is a degree compatible order in which the ordering over the variables is of the kind:

$$x_{1,1} > x_{2,1} > x_{2,2} > x_{1,2}, \text{ or}$$
$$x_{2,1} > x_{2,2} > x_{1,2} > x_{1,1}, \text{ or}$$
$$x_{2,2} > x_{1,2} > x_{1,1} > x_{2,1}, \text{ or}$$
$$x_{1,2} > x_{1,1} > x_{2,1} > x_{2,2}$$

or the corresponding ones replacing in these the symbol $>$ by $<$.

5.6. Finally we include here a Grobner basis for the group $O(3)$ with respect to the row-order to give the reader an idea of the difficult interpretation in geometric or matricial terms of the polynomials in the basis.

$$x_{1,1}^2 - x_{2,2}^2 - x_{2,3}^2 - x_{3,2}^2 - x_{3,3}^2 + 1,$$
$$x_{1,2}^2 + x_{2,2}^2 + x_{3,2}^2 - 1,$$
$$x_{1,3}^2 + x_{2,3}^2 + x_{3,3}^2 - 1,$$
$$x_{1,1}x_{1,2} + x_{2,1}x_{2,2} + x_{3,1}x_{3,2},$$
$$x_{1,1}x_{1,3} + x_{2,1}x_{2,3} + x_{3,1}x_{3,3},$$
$$x_{1,2}x_{1,3} + x_{2,2}x_{2,3} + x_{3,2}x_{3,3},$$
$$x_{1,2}x_{2,3}^2 + x_{1,2}x_{3,3}^2 - x_{1,3}x_{2,2}x_{2,3} - x_{1,3}x_{3,2}x_{3,3} - x_{1,2},$$
$$x_{1,1}x_{2,3}^2 + x_{1,1}x_{3,3}^2 - x_{1,3}x_{2,1}x_{2,3} - x_{1,3}x_{3,1}x_{3,3} - x_{1,1},$$
$$x_{1,2}x_{2,2}x_{2,3} + x_{1,2}x_{3,2}x_{3,3} - x_{1,3}x_{2,2}^2 - x_{1,3}x_{3,2}^2 + x_{1,3},$$
$$x_{1,2}x_{2,1}x_{2,3} + x_{1,2}x_{3,1}x_{3,3} - x_{1,3}x_{2,1}x_{2,2} - x_{1,3}x_{3,1}x_{3,2},$$
$$x_{1,1}x_{2,2}x_{2,3} + x_{1,1}x_{3,2}x_{3,3} - x_{1,3}x_{2,1}x_{2,2} - x_{1,3}x_{3,1}x_{3,2},$$
$$x_{1,1}x_{2,2}^2 - x_{1,1}x_{3,3}^2 - x_{1,2}x_{2,1}x_{2,2} + x_{1,3}x_{3,1}x_{3,3},$$

$$x_{1,2}x_{2,2}x_{3,3}^2 - x_{1,2}x_{2,3}x_{3,2}x_{3,3} - x_{1,3}x_{2,2}x_{3,2}x_{3,3} + x_{1,3}x_{2,3}x_{3,2}^2 - x_{1,2}x_{2,2} - x_{1,3}x_{2,3},$$
$$x_{1,1}x_{2,2}x_{3,3}^2 - x_{1,1}x_{2,3}x_{3,2}x_{3,3} - x_{1,3}x_{2,2}x_{3,1}x_{3,3} + x_{1,3}x_{2,3}x_{3,1}x_{3,2} - x_{1,1}x_{2,2},$$
$$x_{1,2}x_{2,1}x_{3,3}^2 - x_{1,2}x_{2,3}x_{3,1}x_{3,3} - x_{1,3}x_{2,1}x_{3,2}x_{3,3} + x_{1,3}x_{2,3}x_{3,1}x_{3,2} - x_{1,2}x_{2,1},$$
$$x_{2,2}^2x_{3,3}^2 - 2x_{2,2}x_{2,3}x_{3,2}x_{3,3} + x_{2,3}^2x_{3,2}^2 - x_{2,2}^2 - x_{2,3}^2 - x_{3,2}^2 - x_{3,3}^2 + 1,$$
$$x_{2,1}x_{2,2}x_{3,3}^2 - x_{2,1}x_{2,3}x_{3,2}x_{3,3} - x_{2,2}x_{2,3}x_{3,1}x_{3,3} + x_{2,3}^2x_{3,1}x_{3,2} - x_{2,1}x_{2,2} - x_{3,1}x_{3,2},$$
$$x_{2,1}x_{2,2}x_{3,2} + x_{2,1}x_{2,3}x_{3,3} - x_{2,2}^2x_{3,1} - x_{2,3}^2x_{3,1} + x_{3,1},$$
$$x_{1,1}x_{2,2}x_{3,2} + x_{1,1}x_{2,3}x_{3,3} - x_{1,2}x_{2,2}x_{3,1} - x_{1,3}x_{2,3}x_{3,1},$$
$$x_{1,2}x_{2,1}x_{3,2} - x_{1,2}x_{2,2}x_{3,1} + x_{1,3}x_{2,1}x_{3,3} - x_{1,3}x_{2,3}x_{3,1},$$
$$x_{2,1}x_{3,2}^2 + x_{2,1}x_{3,3}^2 - x_{2,2}x_{3,1}x_{3,2} - x_{2,3}x_{3,1}x_{3,3} - x_{2,1},$$
$$x_{1,1}x_{3,2}^2 + x_{1,1}x_{3,3}^2 - x_{1,2}x_{3,1}x_{3,2} - x_{1,3}x_{3,1}x_{3,3} - x_{1,1},$$
$$x_{2,1}x_{3,1} + x_{2,2}x_{3,2} + x_{2,3}x_{3,3},$$
$$x_{2,1}^2 + x_{2,2}^2 + x_{2,3}^2 - 1,$$
$$x_{3,1}^2 + x_{3,2}^2 + x_{3,3}^2 - 1,$$
$$x_{1,1}x_{2,1} + x_{1,2}x_{2,2} + x_{1,3}x_{2,3},$$
$$x_{1,1}x_{3,1} + x_{1,2}x_{3,2} + x_{1,3}x_{3,3}$$

REFERENCES

[B] B. Buchberger., *Applications of Grobner basis in non-linear computational geometry. Trends in computer algebra*, Lecture Notes in Computer Sci., vol. 296 (R. Jansen, ed.), Springer-Verlag, Berlin and New York, 1989.

[BO] A. Borel, *Linear algebraic groups*, Math. Lecture Note Series, W. A. Benjamin, Inc., 1969.

[C-R] C. W. Curtis and I. Reiner., *Representation theory of finite groups and associative algebras*, Pure and Applied Math., vol. XI, Interscience Publishers, 1962.

[D] D. Dubois, *A Nullstellensatz for ordered fields*, Ark. Mat. **8** (1969), 111–114.

[D-C] J. A. Dieudonne and J. B. Carrell, *Invariant theory old and new*, Academic Press, 1971.

[F] J. Fogarty, *Invariant theory*, Math. Lecture Note Series, W. A. Benjamin, Inc., 1969.

[G] F. R. Gantmacher, *Théorie des matrices*, Collection Universitaire des Mathématiques, vol. 2, DUNOD, Paris, 1966.

[N] D. G. Northcott, *Affine sets and affine groups*, London Math. Soc., Lecture Note Series, vol. 39, Cambridge University Press, 1980.

[R] J. J. Risler, *Une caractérisation des variétés algébriques réelles*, C. R. Acad. Sci. Paris **271** (1970), 1171–1173.

[S] T. A. Springer, *Invariant theory*, Lecture Notes in Math., vol. 585 (A. Dold and B. Eckmann, eds.), Springer-Verlag, Berlin and New York, 1977.

[SH] R. Shaw, *Linear algebra and group representation*, Vol. I, Academic Press, 1982.

[W] H. Weyl, *The classical groups*, Second edition, Princeton University Press, 1946.

DPTO. MATEMÁTICAS, ESTADÍSTICA Y COMPUTACIÓN, FACULTAD DE CIENCIAS, UNIVERSIDAD DE CANTABRIA, SANTANDER 39071, SPAIN

E-mail address: g_lopez@ccucvx.unican.es and recio@ccuvx.unican.es