Graph parameters and invariants of the orthogonal group

Regts, G.

Citation for published version (APA):
Regts, G. (2013). Graph parameters and invariants of the orthogonal group.
Chapter 4

Invariant theory

Throughout this thesis we will use the language of, and some important results from, invariant theory. We will give a short introduction to invariant theory in this chapter. It is by all means not a complete introduction. We refer to [35, 25] for more details; see [50] for some advanced topics and we refer to [36] for background on algebra. This introduction is partly based on the manuscript by Kraft and Procesi [35].

4.1 Representations and invariants

Basic definitions

Let $G$ be a group and let $W$ be a vector space. We say that $G$ acts linearly (sometimes we omit linearly) on $W$ if there exists a homomorphism of groups $\rho : G \to \text{GL}(W)$, where $\text{GL}(W)$ denotes the group of invertible linear maps from $W$ to $W$. The pair $(W, \rho)$ is called a representation of $G$; $W$ is sometimes called a $G$-module.\footnote{More specifically, $W$ is a left module of the group algebra of $G$. A left module $W$ of a ring $A$ is an abelian group with an action of $A$ on $W$ satisfying $(a + b)w = aw + bw$, $a(v + w) = av + aw$ and $(ab)w = a(bw)$ for all $v, w \in W$ and $a, b \in A$.} We will usually just write $gw$ instead of $\rho(g)w$ for $w \in W$ and $g \in G$. Let $V, W$ be two $G$-modules. A linear map $\phi : V \to W$ is called $G$-equivariant if $\phi(gv) = g\phi(v)$ for all $g \in G$ and $v \in V$.

A subspace $W'$ of a $G$-module $W$ is called $G$-stable if $gw' \in W'$ for all $w' \in W'$. A $G$-module $W$ is called completely reducible if for each $G$-stable subspace $W' \subset W$ there exists a $G$-stable subspace $U$ such that $W' \oplus U = W$. By Maschke’s Theorem (cf. [36] XVIII, §1 or [57] Section 1.5]), if $G$ is a finite group
and if $W$ is a finite-dimensional $G$-module, then $W$ is completely reducible. By $W^G$ we denote the subspace of $G$-invariants, i.e.,

$$W^G := \{ w \in W \mid gw = w \text{ for all } g \in G \}.$$  \hspace{1cm} (4.1)

**Hilbert’s theorem**

Suppose that $G$ acts on an $n$-dimensional vectorspace $W$. Let $W^*$, denote the space of linear functions $f : W \to \mathbb{F}$ and let $O(W)$ denote the space of regular functions on $W$ (the algebra generated by $W^*$). The action of $G$ on $W$ induces an action on $O(W)$ via $(gf)(w) := f(g^{-1}w)$ for $g \in G$, $f \in O(W)$ and $w \in W$. Note that $O(W)$ has natural grading coming from the homogenous functions. This grading is respected by the group action. So $O(W)$ splits into an infinite sum of finite dimensional $G$-modules.

The next theorem is due to Hilbert.

**Theorem 4.1.** Let $W$ be a $G$-module and assume that the representation of $G$ on $O(W)$ is completely reducible. Then the invariant ring $O(W)^G$ is finitely generated.

We will not prove this result here; see [35] or [9] for a proof. We want however to highlight an important idea from the proof.

**The Reynolds operator**

Let $W$ be a $G$-module and suppose that $O(W)$ is completely reducible. Let $\rho_G : O(W) \to O(W)^G$ denote the $G$-equivariant linear projection onto $O(W)^G$. This map is usually called the Reynolds operator of $G$. (More generally, if $V$ is any completely reducible $G$-module, then the projection onto $V^G$ is called the Reynolds operator.) Then $\rho_G$ satisfies

$$\rho_G(pq) = p\rho_G(q) \quad \text{for } p \in O(W)^G \text{ and } q \in O(W).$$  \hspace{1cm} (4.2)

To see this, let $Q \subset O(W)$ denote a $G$-stable complement to $O(W)^G$. It is convenient to first prove the following:

$$\text{for } p \in O(W)^G \text{ and } q \in Q, \ pq \in Q.$$  \hspace{1cm} (4.3)

To see this, define $\phi : Q \to O(W)$ by $q \mapsto pq$. Then $\phi$ is $G$-equivariant. Indeed, since $p$ is $G$-invariant, $g(pq) = gp \cdot gq = p \cdot gq$. Suppose now that $pq \notin Q$ for some $q \in Q$. Since the Reynolds operator is also $G$-equivariant we may assume that $\phi(q) = p'$ for some nonzero $p' \in O(W)^G$. Moreover, by restricting $\phi$, we may assume that $\phi(Q) = \mathbb{F}p'$. Now note that $\text{Ker } \phi$ is $G$-stable and moreover that $G$ acts on $Q/\text{Ker } \phi$. Then $\phi$ induces an $G$-equivariant isomorphism $\phi : Q/\text{Ker } \phi \to \mathbb{F}p'$. But this implies that $G$ acts trivially on $Q/\text{Ker } \phi$. Hence $q \in O(W)^G + \text{Ker } \phi$. A contradiction. This proves (4.3).
To prove (4.2), write $q = q_1 + q_2$ with $q_1 \in \mathcal{O}(W)^G$ and $q_2 \in Q$. Note that $q_1 = \rho_G(q)$. Then $\rho_G(pq) = \rho_G(pq_1) + \rho_G(pq_2) = pq_1$ by (4.3).

The proof of (4.2) revealed a special case of Schur’s lemma which will be convenient to record.

**Lemma 4.2.** Suppose $G$ acts on a space $W$ and suppose that $W$ admits a direct sum decomposition $W = W^G \oplus W'$, with $W'$ stable under $G$. Let $\phi : W \rightarrow \mathbb{F}$ be a linear map such that $\phi(gw) = \phi(w)$ for all $g \in G$ and $w \in W$. Then $\phi(W') = 0$.

### Classical invariant theory

By Theorem 4.1 we know that there exists finitely many $f_1, \ldots, f_m \in \mathcal{O}(W)$ that generate $\mathcal{O}(W)^G$. In classical invariant theory one is interested in finding an explicit set of generators for $\mathcal{O}(W)^G$ and determining relations between them. In the next section we will state some results about this for the orthogonal group acting on $W = \mathbb{F}^{k \times n}$.

The results in Chapter 5 can be viewed from the perspective of classical invariant theory: describing generators for a certain algebra of (polynomial) functions invariant under the action of the orthogonal group and describing relations between them.

### 4.2 FFT and SFT for the orthogonal group

In this section we consider the natural action of the orthogonal $O_k$ on $\mathbb{F}^{k \times n}$. The theorem describing generators of $\mathcal{O}(\mathbb{F}^{k \times n})$ is called the First Fundamental Theorem (FFT) for the orthogonal group and the theorem describing the relations between these generators is called the Second Fundamental Theorem (SFT) for the orthogonal group. In this section we will state these theorems. We will however start with the natural action of $O_k$ on $V^\otimes n$, where $V := \mathbb{F}^k$, and describe a generating set for the $O_k$-invariants. This is usually referred to as the Tensor FFT for $O_k$.

Let $\mathcal{M}_m$ be the set of perfect matchings on $[2m]$, i.e., $M \in \mathcal{M}_m$ is the disjoint union of $2m$ edges. Define for $M \in \mathcal{M}_m$ the tensor $t_M \in V^\otimes 2m$ by

$$t_M := \sum_{\phi : [2m] \rightarrow [k], \; \phi(u) = \phi(v)} e_{\phi(1)} \otimes \cdots \otimes e_{\phi(2m)}.$$

(4.4)

**Theorem 4.3** (Tensor FFT for $O_k$). If $n$ is odd, then $(V^\otimes)^{O_k} = 0$ and if $n = 2m$ for some $m$, then

$$(V^\otimes 2m)^{O_k} = \text{span}\{t_M \mid M \in \mathcal{M}_m\}.$$  

(4.5)
Invariant theory

For a proof of Theorem 4.3 see [25, Section 5.2], (the proof there is given for $F = C$, but it is valid for arbitrary algebraically closed fields of characteristic zero and hence it is also valid for $F$ as $O_k(F)$ is Zariski dense in the orthogonal group over the algebraic closure of $F$ (cf. [35, §10 Exercise 5])). We will prove it in Section 4.4 using a different approach.

**Theorem 4.4** (FFT for $O_k$). The $O_k$-invariants in $O(F^{k \times n})$ are generated by the polynomials $\sum_{l=1}^{k} x_{l,i}x_{l,j}$ for $i, j = 1, \ldots, n$.

Theorem 4.4 can easily be derived from the Tensor FFT (cf. [25, Section 5.4]). For a direct proof see [35, Section 10.3].

Now for the relations between the generators of $O(F^{k \times n})$. Let $SF^{n \times n}$ denote the space of symmetric $n \times n$ matrices in $F^{n \times n}$. Define

$$\tau : O(SF^{n \times n}) \to O(F^{k \times n}) \quad \text{by} \quad z \mapsto (M \mapsto z(M^T M)). \quad (4.6)$$

Then Theorem 4.4 says that $\tau(O(SF^{n \times n})) = O(F^{k \times n})O_k$.

**Theorem 4.5** (SFT for $O_k$). The kernel of $\tau$ is the ideal generated by the $(k + 1) \times (k + 1)$ minors of $SF^{n \times n}$.

For a proof of Theorem 4.5 see [25, Section 11.2]. The proof there is for $F = C$, but it is valid for any algebraically closed field of characteristic zero; it is quite technical. We now sketch an outline for a different proof. Assume first that $F$ is algebraically closed. Define $t : F^{k \times n} \to SF^{n \times n}$ by $M \mapsto M^T M$, for $M \in F^{k \times n}$. Then $\text{Ker} \, \tau \subseteq O(SF^{n \times n})$ is the ideal defined by those polynomials that vanish on the image of $t$. The image of the map $t$ is equal to the space of all symmetric matrices of rank at most $k$ (cf. [25, Lemma 5.2.4]). As the image of $t$ is determined by the vanishing of the $(k + 1) \times (k + 1)$ minors, it follows by the Nullstellensatz (see below) that if these minors generate a radical ideal, then this ideal equals the kernel of $\tau$. Unfortunately, it is not easy to prove that the minors generate a radical ideal. It can be proved using Gröbner bases; Conca [14] proved that the minors form a Gröbner basis. Combined with the fact each monomial in a minor is square free, this implies that they generate a radical ideal. (See [16] for an introduction to Gröbner bases.)

To see that the SFT is also valid for non-algebraically closed fields $F$, note that $F^{k \times n}$ is Zariski dense in $F^{k \times n}$, implying that the same holds for the image of $t$. So the vanishing ideals of $t(F^{k \times n})$ and $t(F^{k \times n})$ are the same (when viewed as ideals of $O(SF^{n \times n})$). As the minors are defined over $F$, it follows that the SFT also holds over $F$. 

28
4.3 Existence and uniqueness of closed orbits

Finite groups and also the orthogonal group are examples of linear algebraic groups. Using the algebraic structure, one can obtain some useful results such as the existence and uniqueness of closed orbits. We will state this result here; we will however only do this for affine algebraic groups. For more details on linear algebraic groups we refer to [4, 30]. Throughout this section we will work with algebraically closed fields. So $F = \mathbb{F}$ throughout this section.

Zariski topology and the Nullstellensatz

Let $V := \mathbb{F}^n$. A set $A \subseteq V$ is called Zariski closed if it is the zero set of finitely many polynomials, i.e., if there exists polynomials $f_1, \ldots, f_m$ such that $A = \mathcal{V}(\{f_1, \ldots, f_m\}) := \{v \in V \mid f_i(v) = 0 \mid i = 1, \ldots, m\}$. Clearly, we can replace the set $\{f_1, \ldots, f_m\}$ by the ideal they generate. With this definition, $V$ becomes a topological space. The Zariski closure of a set $A \subset V$ is defined by all the zeros of all the polynomials vanishing on $A$. A Zariski closed set is sometimes called an affine variety. Define for an ideal $I \subseteq R = \mathbb{F}[x_1, \ldots, x_n]$ its radical by $\sqrt{I} := \{f \mid f^k \in I \text{ for some } k \in \mathbb{N}\}$. We will now state a fundamental result in algebraic geometry.

**Theorem 4.6** (Hilbert’s Nullstellensatz). Let $F = \mathbb{F}$ and let $I$ be an ideal in $R$. Then $\{f \mid f(v) = 0 \text{ for all } v \in \mathcal{V}(I)\} = \sqrt{I}$. In particular, if $I \neq R$, then there exists $v \in \mathbb{F}^n$ such that $f(v) = 0$ for all $f \in I$.

See [36 IX, §1] for a proof of the Nullstellensatz.

Orbits of affine algebraic groups

An affine algebraic group is an affine variety $G \subset \mathbb{F}^n$ with a group structure such that the group operations are given by polynomial maps in the coordinates of $\mathbb{F}^n$. The orthogonal group $O_k$ is an example of an affine variety; $O_k$ is determined by $g^t g = I$ for $g \in \mathbb{F}^{k \times k}$. Clearly, the group operation and taking the inverse are polynomial maps in the coordinates of $\mathbb{F}^{k \times k}$.

A representation $(W, \rho)$ of an affine algebraic group $G \subset \mathbb{F}^n$ is called polynomial if the map $\rho : G \to \text{GL}(W)$ is given by polynomial maps in the coordinates of $\mathbb{F}^n$. All representations we will encounter in this thesis are polynomial. An affine algebraic group is called reductive if each finite dimensional polynomial representation is completely reducible. It is a well-known fact that the orthogonal group is reductive (cf. [25 Theorem 3.3.12]). We will see a proof of this fact in the next section.

Suppose $(W, \rho)$ is a finite dimensional polynomial representation of a reductive affine algebraic group $G$. Recall from Theorem [4.1] that $\mathbb{F}[W]^G$ is finitely
generated. Let \( f_1, \ldots, f_m \) be generators of \( \mathbb{F}[W]^G \). Define \( \pi : W \to \mathbb{F}^m \) by
\[
\pi(w)_j = f_j(w) \quad \text{for } j = 1, \ldots, m.
\] (4.7)

The map \( \pi \) is called the quotient map. (The quotient map of course depends on the choice of generators, but it can be shown that \( \pi(W) \) is an affine variety and that for different choices of generators these varieties are isomorphic; \( \pi(W) \) is usually denoted by \( W//G \).) Note that for each \( v \in \pi(W) \), \( \pi^{-1}(v) \) is Zariski closed. Furthermore, it is \( G \)-stable; so it is union of \( G \)-orbits. (A \( G \)-orbit is a set \( Gw := \{gw \mid g \in G \} \) for some \( w \in W \).) Then there is a unique Zariski-closed \( G \)-orbit (which is the orbit of minimal Krull-dimension) contained in \( \pi^{-1}(v) \) which is contained in the Zariski closure of each orbit in \( \pi^{-1}(v) \). (We will often just say closed orbit instead of Zariski-closed orbit.) We will record it as a theorem.

**Theorem 4.7.** Let \( \mathbb{F} = \overline{\mathbb{F}} \) and let \( \pi : W \to \mathbb{F}^m \) be the quotient map. Then for each \( v \in \pi(W) \), the fiber \( \pi^{-1}(v) \) contains a unique Zariski-closed \( G \)-orbit \( C \). Moreover, if \( C' \) is another \( G \)-orbit contained in \( \pi^{-1}(v) \), then \( C \subseteq C' \).

To prove existence in Theorem 4.7 one can proceed as follows: let \( w \in \pi^{-1}(v) \). If \( Gw \) is not closed, then \( Gw \) is open in its closure \( \overline{Gw} \) and so \( \overline{Gw} \setminus Gw \) is the union of \( G \)-orbits of strictly lower Krull-dimension. Hence an orbit of minimal Krull-dimension must be closed. See [30, Section 8.3] for details. See [9] or [34, II.3.2-3] for a proof of both existence and uniqueness.

### 4.4 Proof of the Tensor FFT

The proof of Theorem 4.3 in [25] is quite technical. Here we will prove it using a different approach, but we will not include all details. We consider the case \( \mathbb{F} = \mathbb{C} \). (The proof is valid for arbitrary algebraically closed fields of characteristic zero as we will point out later.) First we need some preparations.

Write \( W := V^\otimes m \). Then we have a representation \( \rho : \text{GL}(V) \to \text{GL}(W) \) defined by
\[
v_1 \otimes \cdots \otimes v_m \mapsto g v_1 \otimes \cdots \otimes g v_m
\] (4.8)
for \( g \in \text{GL}(V) \) and \( v_1, \ldots, v_m \in V \). We moreover have a representation \( \tau : S_m \to \text{GL}(W) \) defined by
\[
v_1 \otimes \cdots \otimes v_m \mapsto v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(m)}
\] (4.9)
for \( \sigma \in S_n \) and \( v_1, \ldots, v_m \in V \). (The group \( S_m \) is the symmetric group; it consists of all permutations of the set \([m]\).)
For a subset $S \subseteq \text{End}(W)$ we define its commutant by
\[
\text{Comm}(S) := \{ x \in \text{End}(W) \mid xs = sx \text{ for all } s \in S \}. \quad (4.10)
\]
Let $\mathcal{A}$ be the span of the $\rho(g) \in \text{End}(W)$ for $g \in \text{GL}(V)$ and let $\mathcal{S}$ be the span of the $\tau(\sigma)$ for $\sigma \in S_n$. Schur (cf. [25 Section 4.2.4]) proved that these algebras are each others commutant.

**Theorem 4.8** (Schur). $\text{Comm}(S) = \mathcal{A}$ and $\text{Comm}(\mathcal{A}) = \mathcal{S}$.

See [25 Section 4.2.4] or [35 Section 3.1] for a proof. The proofs are based on the so-called Double Commutant Theorem:

**Theorem 4.9** (Double Commutant Theorem). Let $W$ be a finite dimensional vector space and let $A$ be a subalgebra of $\text{End}(W)$ containing $I_W$. Set $B := \text{Comm}(A)$. If $W$ is a completely reducible $A$-module, then $\text{Comm}(B) = A$. Moreover, $W$ is a completely reducible $B$-module.

See [35 Section 3.2] for a proof of the Double Commutant Theorem; see [25 Section 4.1.5] for a proof of the first statement only. We will use Theorem 4.8 combined with the Double Commutant Theorem to prove Theorem 4.3.

**Theorem 4.3** (Tensor FFT for $O_k$). If $n$ is odd, then $(V^{\otimes n})^{O_k} = 0$ and if $n = 2m$ for some $m$, then
\[
(V^{\otimes n})^{O_k} = \text{span}\{t_M \mid M \in \mathcal{M}_m\}. \quad (4.11)
\]

**Proof.** Since $-I \in O_k$ if follows that if $n$ is odd, the only invariant is 0. Now suppose $n = 2m$ for some $m$. We may assume that $m \geq 2$, as the case $m = 1$ directly follows from the general case.

First identify $V$ with $V^*$ as $O_k$-modules through the bilinear form. Let $W := V^{\otimes m}$ and make $\text{End}(W)$ a $\text{GL}(V)$-module by setting $gx := \rho(g)x\rho(g^{-1})$ for $g \in \text{GL}(V)$ and $x \in \text{End}(V)$. We then have a canonical isomorphism $\text{End}(W) \cong V^{\otimes m} \otimes (V^*)^{\otimes m}$ as $\text{GL}(V)$-modules. So $\text{GL}(V)$-invariant tensors in $V^{\otimes m} \otimes (V^*)^{\otimes m}$ correspond uniquely to elements of $\text{Comm}(A)$. Similarly, $O_k$-invariant tensors in $V^{\otimes 2m}$ correspond uniquely to elements of the commutant of the space spanned by the $\rho(g)$ for $g \in O_k$.

For $\phi : \{2m\} \to [k]$ we think of $e_{\phi(1)} \cdots e_{\phi(m)}$ as living in $V^{\otimes m}$ and $e_{\phi(m+1)} \cdots, e_{\phi(2m)}$ as living in $(V^*)^{\otimes m}$. For a perfect matching $M$ on $2m$ points we can therefore naturally view $t_M$ as an element of $\text{End}(W)$. Thinking of $M \in \mathcal{M}_m$ as a $2m$-fragment, $\mathcal{C}M_m \subset \mathcal{F}_{2m}$ becomes an algebra if we replace each $\circ$ in $M_1 \cdot M_2$ (the gluing product of the $2m$-fragments) by $k$. Recall that the identity element is the matching connecting $i$ to $m + i$ for $i \in [m]$. This algebra was introduced by Brauer [8] and is called the Brauer algebra. Let $B_m \subset \text{End}(W)$ be
the span of the $t_M$ for $M \in \mathcal{M}_m$. Note that the linear map sending $M$ to $t_M$ is a surjective homomorphism of algebras from $\mathbb{C}M_m$ to $B_m$.

**Proposition 4.10.** For $m > 1$, $\text{Comm}(B_m)$, is equal to the span of the $\rho(g)$ for $g \in O_k$.

**Proof.** Consider the matchings whose edges run between $\{1, \ldots, m\}$ and $\{m+1, \ldots, 2m\}$. Note that each such a matching uniquely defines an element $\sigma \in S_m$. It follows that $S \subseteq B_m$. This implies by Theorem 4.8 that $\text{Comm}(B_m)$ is contained in $A$. Now let $g \in \text{GL}(V)$ such that $\rho(g)b\rho(g^{-1}) = b$ for all $b \in B_m$. In other words, $gt_M = t_M$ for all $M \in \mathcal{M}_m$. Consider the matching $M$ defined as

$$M := \begin{array}{ccccccc}
m + 1 & m + 2 & m + 3 & \cdots & 2m \\
1 & 2 & 3 & \cdots & m
\end{array}$$

Write $f_1, \ldots, f_k$ for the basis of $V^*$ (dual to $e_1, \ldots, e_k$). Then we obtain that $g$ should satisfy:

$$\left( \sum_{i=1}^k ge_i \otimes ge_i \right) \otimes \left( \sum_{j=1}^k gf_j \otimes gf_j \right) = \left( \sum_{i=1}^k e_i \otimes e_i \right) \otimes \left( \sum_{j=1}^k f_j \otimes f_j \right).$$

(4.12)

One directly obtains from (4.12) that

$$\sum_{i=1}^k \sum_{j=1}^k g_{l,i}g_{h,j}(g^{-1})^T_{l',j}(g^{-1})^T_{h',i} = \delta_{h,l}\delta_{h',l'} \text{ for all } l, h, l', h' = 1, \ldots, k,$$

(4.13)

where we write $g = (g_{i,j})$ and $g^{-1} = (g^{-1}_{i,j})$ for $g$ and $g^{-1}$ relative to the basis $e_1, \ldots, e_k$. This implies that $gg^T = aI$ for some nonzero $a$. Hence $\rho(g)$ is contained in the span of the $\rho(g')$ for $g' \in O_k$. This finishes the proof. \qed

The next thing we need is that $W$ is a completely reducible $B_m$-module. This follows from the following observation. Define an inner product on $\text{End}(W)$ by $\langle x, y \rangle := \text{tr}(xy^*)$ for $x, y \in \text{End}(W)$. (Here $\text{tr}(x)$ denotes the trace of $x \in \text{End}(W)$ and by $x^*$ we denote the conjugate transpose of $x$.) Now note that for each $x \in B$, $x^* \in B$, since $t_M^T = t_{M'}$, where $M'$ is the matching obtained from $M$ by interchanging vertex $i$ with $m+i$ for $i = 1, \ldots, m$. This implies that $B$ is a semisimple algebra. (See for example [36, XVII, §7 Exercise 1-7, ].) From this we conclude that $W$ is completely reducible. So by the Double Commutant

\[ \text{2That is, } B \text{ is completely reducible as a } B\text{-module.} \]
4.4. Proof of the Tensor FFT

Theorem, we conclude that $B_m$ is equal to $\text{Comm}\{\rho(g) \mid g \in O_k\}$. This finishes the proof. □

Remark. The proof remains valid for arbitrary algebraically closed fields $\mathbb{F}$ of characteristic zero. A field is called real if $-1$ is not a sum of squares. We just need to find a real subfield of index 2 in $\mathbb{F}$ (whose existence is granted by Zorn’s Lemma cf. [36, XI, §2]) and define a ‘complex conjugation’ to be able to define the inner product.

Note that the Double Commutant Theorem also implies that $W = V^\otimes m$ is completely reducible as an $O_k$-module. (In case $m = 1$, $W$ is irreducible.) Together with the observation in [35, Section 5.3] that any polynomial representation of $O_k$ occurs in a sum $\bigoplus_{i=1}^t V^\otimes n_i$, this implies that $O_k$ is reductive.

**Corollary 4.11.** The orthogonal group $O_k$ is reductive.