Journal of Algebraic Combinatorics, 22, 471–491, 2005


# On the Diaconis-Shahshahani Method in Random Matrix Theory

MICHAEL STOLZ michael.stolz@ruhr-uni-bochum.de
*Ruhr-Universität Bochum, Fakultät für Mathematik, NA 4/30, D-44780 Bochum, Germany*

*Received December 2, 2004; Revised April 25, 2005; Accepted May 19, 2005*

**Abstract.** If $\Gamma$ is a random variable with values in a compact matrix group $K$, then the traces $\mathrm{Tr}(\Gamma^j)$ $(j \in \mathbb{N})$ are real or complex valued random variables. As a crucial step in their approach to random matrix eigenvalues, Diaconis and Shahshahani computed the joint moments of any fixed number of these traces if $\Gamma$ is distributed according to Haar measure and if $K$ is one of $\mathrm{U}_n$, $\mathrm{O}_n$ or $\mathrm{Sp}_n$, where $n$ is large enough. In the orthogonal and symplectic cases, their proof is based on work of Ram on the characters of Brauer algebras.

The present paper contains an alternative proof of these moment formulae. It invokes classical invariant theory (specifically, the tensor forms of the First Fundamental Theorems in the sense of Weyl) to reduce the computation of matrix integrals to a counting problem, which can be solved by elementary means.

**Keywords:** random matrices, matrix integrals, classical invariant theory, tensor representations, Schur-Weyl duality

## 1. Introduction

In the 1980s and early 1990s, Diaconis, Mallows and Shahshahani devised a method for studying the eigenvalues of random elements of the compact classical groups which are chosen according to Haar measure. The paper [3] of Diaconis and Shahshahani is probably the best-known reference, whereas the paper [2] of Diaconis and Evans contains the state of the art, including many applications. In a nutshell, the method is Fourier analysis built upon an explicit solution to the following problem: Fix $n \in \mathbb{N}$ and let $K = K_n$ be one of $\mathrm{U}_n$, $\mathrm{O}_n$, $\mathrm{Sp}_n$ ($n$ even in the last case). Consider a random variable $\Gamma = \Gamma_n$ with values in $K$, whose distribution is Haar measure. Compute the joint moments of the real random vector

$$(\mathrm{Tr}(\Gamma), \mathrm{Tr}(\Gamma^2), \ldots, \mathrm{Tr}(\Gamma^r)), \tag{1.1}$$

i.e., matrix integrals of the form

$$\int (\mathrm{Tr}(g))^{a_1} (\mathrm{Tr}(g^2))^{a_2} \ldots (\mathrm{Tr}(g^r))^{a_r} \omega_K(dg) \tag{1.2}$$

($r \in \mathbb{N},\ a \in \mathbb{N}_0^r,\ \omega_K$ Haar measure), in the cases $K = \mathrm{O}_n$ and $K = \mathrm{Sp}_n$, and the joint moments of the complex random vector

$$(\mathrm{Tr}(\Gamma), \ldots, \mathrm{Tr}(\Gamma^r), \overline{\mathrm{Tr}(\Gamma)}, \ldots, \overline{\mathrm{Tr}(\Gamma^r)}) \tag{1.3}$$

in the case $K = \mathrm{U}_n$. It turns out that this is in fact possible if $n$ is large enough, and that these moments equal the corresponding moments of suitable multivariate normal distributions. The proof which is given in [3] for the moment formula in the case $K = \mathrm{U}_n$ uses nothing more than basic character theory of groups together with a well-known explicit decomposition of power sum symmetric functions, which is often referred to as Schur-Weyl duality. On the other hand, the treatment of the cases $K = \mathrm{O}_n$ and $K = \mathrm{Sp}_n$ makes use of less familiar material, namely, Ram's work [9, 10] on the characters of Brauer algebras.

Nowadays there exist alternative methods to prove these moment formulae. Hughes and Rudnick [7] have chosen an approach via the combinatorics of cumulants and Weyl's integration formula. Pastur and Vasilchuk [8] have used ideas from statistical mechanics to obtain an entirely different proof. The present paper proposes yet another method, which is based on classical invariant theory. This theory has undergone some refinement since Weyl's classic [12], and there exist accessible expository texts such as the monograph [4]. It will emerge from our discussion that the fundamentals of this theory (which include an abstract version of Schur-Weyl duality) suffice to prove the moment formulae for all three groups in a uniform way. Invariant theory serves to reduce the computation of integrals directly to an easy counting problem, and there is no need to deal with special functions explicitly.

The paper is organized as follows: Section 2 serves to fix notation, to review a fragment of Lie theory (Theorem 2.5) and to present a version of Schur-Weyl duality, which will be termed Double Centralizer Theorem, in a way that clearly brings out the connection with invariant theory (Theorem 2.2 and Addendum 2.3). The central piece of the paper is Section 3, and there the orthogonal case is the paradigmatic one. The presentation of the symplectic and unitary cases builds upon the previous discussion of the paradigm and explains how the difficulties which are specific for the other groups can be overcome.

## 2. Preliminaries

For a subgroup $H$ of a group $G$ write $G{:}H := \{Hg :\ g \in G\}$ for the set of right cosets with respect to $H$. A $G$-space $(M, G)$ is a set $M$ together with a right action $M \times G \to M :\ (\mu, g) \mapsto \mu g$. For $\mu \in M$ set $G_\mu := \{g \in G :\ \mu g = \mu\}$ and $\mu^G := \{\mu g : g \in G\}$. Then $(\mu^G, G)$ and $((G : G_\mu), G)$ are isomorphic for any $\mu \in M$.

If $M = \{1, \ldots, k\}$ ($k \in \mathbb{N}$), write $\mathrm{S}_k$ for the symmetric group $\mathrm{Sym}(M)$. For each $s \in \mathrm{Sym}(M)$ define $[s] := \{j \in M :\ js \neq j\}$ and call it the *support* of $s$. If $s$ is of the form

$$s = \prod_{j=1}^{r} \prod_{i=1}^{a_j} \zeta_i^j,$$

where $\zeta_i^j$ is the $i$-th $j$-cycle (in some fixed order), we write type($s$) for the partition

$$\lambda = (\underbrace{r, r, \ldots, r}_{a_r}, \underbrace{r-1, r-1, \ldots, r-1}_{a_{r-1}}, \ldots, \underbrace{1, 1, \ldots, 1}_{a_1}),$$

which is in turn abbreviated to $\lambda = (1^{a_1} 2^{a_2} \ldots r^{a_r})$. $l(\lambda) := a_r + a_{r-1} + \cdots + a_1$ is called the *length* of $\lambda$.

If $M$ is a finite set, $k := \#M < \infty$, write $\mathcal{M}_r(M)$ for the set of all *$r$-matchings* in $M$, where an $r$-matching is a partition of $M$ into $r$ two-element and $k - 2r$ one-element subsets. A *matching* in $M$ is an $r$-matching for a suitable $r$. If $k = 2r$, then an $r$-matching is also called a *two-partition* of $M$, and one writes $\mathcal{M}(M) := \mathcal{M}_r(M)$. Abbreviate $\mathcal{M}_r(k) = \mathcal{M}_r(\{1, \ldots, k\})$ and $\mathcal{M}(k) = \mathcal{M}(\{1, \ldots, 2k\})$. Note that $\mathcal{M}(k) = \mathcal{M}_k(2k)$. The natural action of $\mathrm{Sym}(M)$ on $M$ induces transitive actions on $\mathcal{M}(M)$ and $\mathcal{M}_r(M)$ in the obvious way.

**Lemma 2.1** *Let $k, r \in \mathbb{N}$, $r \leq \lfloor \frac{k}{2} \rfloor$.*

$$\#\mathcal{M}_r(k) = \frac{k!}{2^r\, r!\, (k-2r)!} = \binom{k}{2r}(2r-1)!!, \tag{2.1}$$

$$\#\mathcal{M}(k) = (2k-1)!!. \tag{2.2}$$

*Here we use for $k \in \mathbb{N}$ the shorthand* $(2k-1)!! := (2k-1)(2k-3)\ldots 5 \cdot 3 \cdot 1$.

Let $V$ be a finite-dimensional complex vector space and write $V^{\otimes k}$ for its $k$-fold tensor power. Suppose that $\mathfrak{b} = (b_j)_{j=1,\ldots,n}$ is a $\mathbb{C}$-basis of $V$. Write $\mathcal{F}(k, n)$ for the set of all maps from $\{1, \ldots, k\}$ to $\{1, \ldots, n\}$. It is well known that the family

$$\mathfrak{b}^{\otimes k} := \left\{ \otimes_{i=1}^k b_{i\varphi} : \varphi \in \mathcal{F}(k, n) \right\}$$

is a $\mathbb{C}-$basis of $V^{\otimes k}$ ( [5], Ch I §6). For $s \in \mathrm{S}_k$, $\otimes_{i=1}^k b_{i\varphi} \in \mathfrak{b}^{\otimes k}$ set

$$\left(\otimes_{i=1}^k b_{i\varphi}\right) s := \otimes_{i=1}^k b_{(is^{-1})\varphi} \tag{2.3}$$

and proceed by linear continuation. This defines an action of $\mathrm{S}_k$ on $V^{\otimes k}$, which in turn determines a homomorphism $\sigma_k : \mathrm{S}_k \to \mathrm{GL}(V^{\otimes k})$, hence a linear representation $(V^{\otimes k}, \sigma_k)$.

Given a representation $(V, \rho)$ of $G$, we define on $V^* = \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$ the contragredient representation $\rho^*$ via

$$v^* \rho^*(g) := \rho(g^{-1}) v^* : \; V \overset{\rho(g^{-1})}{\to} V \overset{v^*}{\to} \mathbb{C}. \tag{2.4}$$

Given representations $(V_i, \rho_i)$ of $G_i$ $(i = 1, \ldots, k)$, define a representation $\rho_1 \otimes \cdots \otimes \rho_k$ of $G_1 \times \cdots \times G_k$ on $V_1 \otimes \cdots \otimes V_k$ by setting

$$\left(\otimes_{i=1}^k v_i\right)(\otimes_{i=1}^k \rho_i)((g_1, \ldots, g_k)) := \otimes_{i=1}^k v_i(\rho_i(g_i)) \tag{2.5}$$

and then proceeding by linear continuation. If one applies this procedure to $k$ copies of the same representation $(V, \rho)$ of $G$ and restricts the resulting tensor product representation to the diagonal, then one obtains a representation $\rho_k = \rho^{\otimes k}$ of $G$.

It is well known that a representation of a group $G$ can be regarded as a representation of its group algebra $\mathbb{C}G$, and vice versa. A representation of $\mathbb{C}G$ on the complex vector space $V$ gives rise to a $\mathbb{C}G$-module structure on $V$, and vice versa. If $\mathcal{A}$ is a $\mathbb{C}$-algebra and $V_1,\ V_2$ are $\mathbb{C}$-vector spaces with an additional structure as $\mathcal{A}$-modules, write $\mathrm{Hom}_{\mathcal{A}}(V_1, V_2) := \{\varphi \in \mathrm{Hom}_{\mathbb{C}}(V_1, V_2) : \ (va)\varphi = (v\varphi)a \quad \forall v \in V, a \in \mathcal{A}\}$. If $\mathcal{A} \subseteq \mathrm{End}_{\mathbb{C}}(V)$, then $\mathrm{End}_{\mathcal{A}}(V) = \mathrm{C}_{\mathrm{End}_{\mathbb{C}}(V)}(\mathcal{A}) = \{b \in \mathrm{End}_{\mathbb{C}}(V) : \ ab = ba \ \forall a \in \mathcal{A}\}$.

If $\rho$ is a completely reducible representation of $G$, then the image of $\mathbb{C}G$ under $\rho$ is a semisimple subalgebra of $\mathrm{End}_{\mathbb{C}}(V)$ (see [4], Thm. 3.3.4), i.e., isomorphic to a direct product of full matrix algebras. Therefore the following result is applicable:

**Theorem 2.2** (Double Centralizer Theorem, DCT) *Let $V$ be a finite dimensional $\mathbb{C}$-vector space, $\mathcal{A}$ a semisimple subalgebra of $\mathrm{End}_{\mathbb{C}}(V)$, $\mathcal{B} := \mathrm{End}_{\mathcal{A}}(V)$. Fix a family $V_\mu$ $(\mu \in M)$ of mutually nonisomorphic irreducible $\mathcal{A}$-submodules of $V$ such that all isomorphism classes of irreducible $\mathcal{A}$-modules which occur in $V$ have a representative among the $V_\mu$. Set $U_\mu := \mathrm{Hom}_{\mathcal{A}}(V_\mu, V)$ for all $\mu \in M$. Then the $U_\mu$ are mutually nonisomorphic irreducible $\mathcal{B}$-modules with respect to the action $(\varphi, b) \mapsto \varphi b$ (where on the right-hand side stands the composition $V_\mu \overset{\varphi}{\to} V \overset{b}{\to} V$), and the following isomorphism of $\mathcal{A}$- and of $\mathcal{B}$-modules holds*:

$$V \cong \bigoplus_{\mu \in M} V_\mu \otimes U_\mu.$$

**Proof 1:** [4], Thm. 3.3.7. □

Now consider the special case that $\mathcal{A}$ is the image of a group algebra $\mathbb{C}G$ under a representation $\rho$ (which we drop in what follows in order to simplify notation). Set

$$[V]^G := \{v \in V : \ vg = v \quad \forall g \in G\}.$$

Since $G$ acts linearly, $[V]^G$ is a vector space. Its elements are called the *$G$-invariants* in $V$ (with respect to $\rho$). $[V]^G$ is $\mathcal{B}$-invariant ($b \in \mathcal{B}$ acting as an endomorphism of $V$), because for $v \in [V]^G,\ b \in \mathcal{B},\ g \in G : (vb)g = (vg)b = vb$. If $v \in [V]^G,\ a = \sum_{g \in G} \alpha_g g \in \mathcal{A}$, then $va = \sum_{g \in G} \alpha_g (vg) = (\sum_{g \in G} \alpha_g)v \in \mathbb{C}v$. (By the definition of group algebras we are in fact dealing with a finite sum.) This means that $\mathbb{C}v$ is a one-dimensional $\mathcal{A}$-invariant subspace of $V$, hence an irreducible $\mathcal{A}$-module.

At a critical juncture in our application of Theorem 2.2 in Section 3 we will need an answer to the following question: What does $U_\mu$ look like when $V_\mu = \mathbb{C}v_0$ for some $v_0 \in [V]^G$? We give our answer in the form of an addendum to the DCT.

**Addendum 2.3** *If $\mathcal{A} = \rho(\mathbb{C}G),\ v_0 \in [V]^G,\ V_\mu = \mathbb{C}v_0$, then $U_\mu$ is isomorphic to $[V]^G$ as a $\mathcal{B}$-module.*

**Proof 2:** For $w \in [V]^G$ define $\varphi_w \in \mathrm{Hom}_{\mathbb{C}}(V_\mu, V)$ by setting $(cv_0)\varphi_w := cw$ for all $c \in \mathbb{C}$. It is easily verified that $\varphi_w \in \mathrm{Hom}_{\mathcal{A}}(V_\mu, V) = U_\mu$ and that the map $w \mapsto \varphi_w$ is a $\mathbb{C}$-linear bijection. As to the module operation, let $w \in [V]^G,\ b \in \mathcal{B}$. Then $\varphi_{wb} = \varphi_w b : V_\mu \xrightarrow{\varphi_w} V \xrightarrow{b} V$, because for any $c \in \mathbb{C}$, $(cv_0)(\varphi_w b) = (cw)b = c(wb) = c(v_0\varphi_{wb}) = (cv_0)\varphi_{wb}$. □

For $n \in \mathbb{N}$ let $\mathrm{I}_n$ denote the identity matrix in $\mathbb{C}^{n\times n}$, and for $n$ even set

$$\mathrm{J}_n := \begin{pmatrix} 0 & \mathrm{I}_{\frac{n}{2}} \\ -\mathrm{I}_{\frac{n}{2}} & 0 \end{pmatrix} \in \mathbb{C}^{n\times n}. \tag{2.6}$$

Let $I \subseteq \mathbb{N}$ and consider families $(V_n, \beta_n, G_n, K_n)_{n\in I}$, where $V_n$ is an $n$-dimensional $\mathbb{C}$-vector space, which we will for simplicity identify with $\mathbb{C}^n$, $\beta_n : V_n \times V_n \to \mathbb{C}$ a $\mathbb{C}$-bilinear form, $G_n := \{g \in \mathrm{GL}(V_n) :\ \beta_n(vg, wg) = \beta_n(v, w)\ \forall v, w \in V_n\}$, $K_n := G_n \cap \mathrm{U}_n$, where $\mathrm{U}_n$ is the unitary group. Consider the following cases:

**(1)** $I = \mathbb{N}$, and for all $n \in I$ $\beta_n \equiv 0$. Here $G_n = \mathrm{GL}(n, \mathbb{C})$, $K_n = \mathrm{U}_n$.
**(2)** $I = \mathbb{N}$, and for all $n \in I$ $\beta_n$ is the nondegenerate symmetric form $(x, y) \mapsto x'\mathrm{I}_n y$. Here $G_n = \mathrm{O}(n, \mathbb{C})$, $K_n = \mathrm{O}_n$.
**(3)** $I = \{2m :\ m \in \mathbb{N}\}$, and for all $n \in I$ $\beta_n$ is the nondegenerate skew-symmetric form $(x, y) \mapsto x'\mathrm{J}_n y$. Here $G_n = \mathrm{Sp}(n, \mathbb{C})$, $K_n = \mathrm{Sp}_n$.

The relation in which the $K_n$ stand to the $G_n$ is but an instance of a general theory which links compact to complex Lie groups (see [6], Ch. XVII). Nevertheless, a pedestrian verification of the following important aspect of this correspondence is possible.

**Lemma 2.4** *In all three cases* (**1**), (**2**), (**3**) *for all* $n \in \mathbb{N}$

$$\mathfrak{L}(G_n) = \mathfrak{L}(K_n) \otimes_{\mathbb{R}} \mathbb{C},$$

*i.e. the Lie algebra of* $G_n$ *is the complexification* (*as a vector space*) *of the Lie algebra of* $K_n$.

**Theorem 2.5** *Let* $G$ *and* $K$ *be connected closed matrix groups,* $K \leq G$. *Assume further that* $K$ *is compact and that* $\mathfrak{L}(G) = \mathfrak{L}(K) \otimes_{\mathbb{R}} \mathbb{C}$. *Let* $(V, \rho)$ *be a holomorphic representation of* $G$. *Then*

(i) $(V, \rho)$ *is completely reducible.*
(ii) $(V, \rho)$ *is irreducible if, and only if,* $(V, \rho_K)$ *is irreducible, where* $\rho_K$ *is the restriction of* $\rho$ *to* $K$.

**Proof 3:** [11], Lemma 4.11.13, together with the proof of Thm. 4.11.14. □

Since we wish to apply Theorem 2.5 to $G = \mathrm{O}(n, \mathbb{C})$, which has two connected components, we give an addendum, which follows by a minor modification of the proof of Maschke's theorem roughly as in the proof of [4], Prop. 2.4.2.

**Addendum 2.6** *Theorem* 2.5 *remains true when the assumption that G and K be connected is weakened to the requirement that* $G_1$, *i.e. the connected component of the unit element, have finite index in G.*

Before this section comes to a close, let us prepare the ground for our subsequent applications of invariant theory by defining in the cases (**2**) and (**3**) two special bases $(f_i)_{i=1,\dots,n}$, $(f^i)_{i=1,\dots,n}$ of $V_n$ such that $\beta_n(f_i, f^j) = \delta_{ij}$ for all $i, j = 1, \dots, n$. In case (**2**), for all $i = 1, \dots, n$ set $f_i := e_i =: f^i$, where $(e_i)_{i=1,\dots,n}$ is the standard basis of $V_n = \mathbb{C}^n$. In case (**3**), $n = 2m$, there exists a *symplectic basis* $b_1, c_1, b_2, c_2, \dots, b_m, c_m$ such that for all $i, j = 1, \dots, m$:

$$\beta_n(b_i, b_j) = \beta_n(c_i, c_j) = 0, \tag{2.7}$$

$$\beta_n(b_i, c_i) = 1,\ \beta_n(b_i, c_j) = 0\ (i \neq j). \tag{2.8}$$

We then set for all $i = 1, \dots, m$

$$f_{2i-1} := b_i, \quad f_{2i} := c_i, \quad f^{2i-1} := c_i, \quad f^{2i} := -b_i. \tag{2.9}$$

## 3. Moment identities

### *3.1. The general setup*

Fix $n \in \mathbb{N}$, and let $K_n$ be one of $\mathrm{U}_n,\ \mathrm{O}_n,\ \mathrm{Sp}_n$. Consider a random variable $\Gamma_n$ whose distribution is the normalized Haar measure $\omega_{K_n}$ on $K_n$. In addition, fix $r, q \in \mathbb{N},\ a = (a_1, \dots, a_r) \in \mathbb{N}_0^r,\ b = (b_1, \dots, b_q) \in \mathbb{N}_0^q$. Set

$$k_a := \sum_{j=1}^{r} j a_j \tag{3.1}$$

and define $k_b$ analogously. It is our object to compute the $a$-moment

$$\mathrm{E}\left( \prod_{j=1}^{r} \left(\mathrm{Tr}\left(\Gamma_n^j\right)\right)^{a_j} \right)$$

of the random vector $(\mathrm{Tr}(\Gamma_n), \mathrm{Tr}(\Gamma_n^2), \dots, \mathrm{Tr}(\Gamma_n^r))$ in the cases $K_n = \mathrm{O}_n$ and $K_n = \mathrm{Sp}_n$, and in the case $K_n = \mathrm{U}_n$ the $(a_1, \dots, a_r,\ b_1, \dots, b_q)$-moment of the random vector $(\mathrm{Tr}(\Gamma_n), \dots, \mathrm{Tr}(\Gamma_n^r), \overline{\mathrm{Tr}(\Gamma_n)}, \dots, \overline{\mathrm{Tr}(\Gamma_n^q)})$. We will usually drop the subscript $n$.

### 3.2. *The trace lemma*

Let $\rho$ be the defining representation of $\mathrm{GL}(V)$ on $V$. For $k \in \mathbb{N}$ write $\rho_k$ for $\rho^{\otimes k} : \mathrm{GL}(V) \to \mathrm{GL}(V^{\otimes k})$, the $k$-fold tensor power of $\rho$. Recall from (2.3) the representation $\sigma_k$ of $\mathrm{S}_k$ on $V^{\otimes k}$. Obviously the images of $\rho_k$ and $\sigma_k$ centralize each other. We thus can define a representation

$$\rho_k \times \sigma_k : \mathrm{GL}(V) \times \mathrm{S}_k \to \mathrm{GL}(V^{\otimes k}) \tag{3.2}$$

by setting

$$\big(\otimes_{i=1}^k v_i\big)(\rho_k \times \sigma_k)((g,s)) := \big(\otimes_{i=1}^k v_i \rho(g)\big)\sigma_k(s), \tag{3.3}$$

and proceeding by linear continuation. For $g \in \mathrm{GL}(V)$ write $c_i(g)$ $(i = 1, \ldots, n)$ for the (not necessarily distinct) complex roots of its characteristic polynomial (in any order). If $p \in \mathbb{C}[X_1, \ldots, X_n]$ is a symmetric polynomial, then $p(c_1(g), \ldots, c_n(g))$ is defined unambiguously and will be abbreviated to $p(g)$. For $\nu \in \mathbb{N}$ define $p_\nu := \sum_{i=1}^n X_i^\nu \in \mathbb{C}[X_1, \ldots, X_n]$, and for any partition $\lambda$ set $p_\lambda := p_{\lambda_1} p_{\lambda_2} \ldots p_{\lambda_{l(\lambda)}}$.

We now specialize $k$ to $k_a$ as in (3.1), consider $(\rho_k \times \sigma_k)(g, s)$ as a linear operator on $V^{\otimes k}$ and compute its trace.

**Lemma 3.1** (Trace Lemma) *For any $g \in \mathrm{GL}(V)$,*

$$\prod_{j=1}^r (\mathrm{Tr}(g^j))^{a_j} = \mathrm{Tr}((\rho_k \times \sigma_k)((g,s))), \tag{3.4}$$

*where $s \in \mathrm{S}_k$ is of type $(1^{a_1} 2^{a_2} \ldots r^{a_r})$.*

The *proof* consists in the following two lemmata, the first of which is stated without proof in [9], Thm. 4.6(a). The second one seems to be the starting point for the approach of Diaconis and Shahshahani.

**Lemma 3.2** *For any $g \in \mathrm{GL}(V)$, $s \in \mathrm{S}_k$, we have*

$$\mathrm{Tr}((\rho_k \times \sigma_k)((g,s))) = p_{\mathrm{type}(s)}(g).$$

**Proof 4:** In the first step suppose that $g$ is diagonalizable. Consider a basis $(v_i)_{i=1,\ldots,n}$ of $V$ consisting of eigenvectors of $g$, and let $(c_i)_{i=1,\ldots,n}$ denote the corresponding eigenvalues. Then $\{\otimes_{j=1}^k v_{j\varphi} : \varphi \in \mathcal{F}(k,n)\}$ is a basis of $V^{\otimes k}$. Evidently, $(\rho_k \times \sigma_k)((g,s))$ maps any basis tensor to a scalar multiple of another basis tensor. This means that in order to compute the trace of $(\rho_k \times \sigma_k)((g,s))$, we have to consider the fixed points of the action of $s$. Now $\otimes_{j=1}^k v_{j\varphi}$ is fixed by $s$ if, and only if, $\varphi$ is constant on the supports of the cycles of $s$. Writing $\lambda = (\lambda_j)_{j=1,\ldots,l(\lambda)} = \mathrm{type}(s)$, this observation yields

$$\mathrm{Tr}((\rho_k \times \sigma_k)((g,s))) = \sum_{\psi \in \mathcal{F}(l(\lambda),n)} \prod_{j=1}^{l(\lambda)} c_{j\psi}^{\lambda_j}.$$

On the other hand,

$$p_\lambda(g) = \prod_{j=1}^{l(\lambda)} p_{\lambda_j}(g) = \prod_{j=1}^{l(\lambda)} \sum_{i=1}^{n} c_i^{\lambda_j},$$

which is the same.

The general case follows from the well-known fact that the set of all complex matrices whose characteristic polynomial has pairwise distinct roots is dense in $\mathbb{C}^{n\times n}$. □

**Lemma 3.3** *For any* $g \in \mathrm{GL}(V)$

$$\prod_{j=1}^{r} (\mathrm{Tr}(g^j))^{a_j} = p_\lambda(g),$$

*where* $\lambda$ *is the partition* $(1^{a_1} 2^{a_2} \dots r^{a_r})$.

**Proof 5:** If $g$ is diagonalizable, then it is immediate that $\mathrm{Tr}(g^j) = \sum_{i=1}^{n} (c_i(g))^j$. Hence

$$\prod_{j=1}^{r} (\mathrm{Tr}(g^j))^{a_j} = \prod_{j=1}^{r} \left( \sum_{i=1}^{n} (c_i(g))^j \right)^{a_j} = \prod_{j=1}^{r} (p_j(g))^{a_j}.$$

On the other hand, when one groups in $p_\lambda(g) = \prod_{v=1}^{l(\lambda)} p_{\lambda_v}(g)$ the factors with the same $\lambda_v$ together, by the very definition of the partition $\lambda$ one again arrives at $\prod_{j=1}^{r} (p_j(g))^{a_j}$. A density argument yields the conclusion. □

### *3.3. The orthogonal case*

We consider the case $(G, K) = (\mathrm{O}(n, \mathbb{C}), \mathrm{O}_n)$. Let $Z_1, \dots, Z_r$ be iid standard normal random variables. Set $k = k_a$.

**Theorem 3.4** *If*

$$2n \geq k, \tag{3.5}$$

*then*

$$\mathrm{E}\left( \prod_{j=1}^{r} (\mathrm{Tr}(\Gamma^j))^{a_j} \right) = \mathrm{E}\left( \prod_{j=1}^{r} (\sqrt{j} Z_j + \eta_j)^{a_j} \right), \tag{3.6}$$

*where*

$$\eta_j := \begin{cases} 1, & \text{if } j \text{ is even}, \\ 0, & \text{if } j \text{ is odd}. \end{cases}$$

**Remark 3.5** If $k$ is odd, then (3.6) holds regardless of whether condition (3.5) is met or not, both sides being equal to zero in this case.

The *proof* of Theorem 3.4 is the content of this subsection. Obviously the representation $\rho_k$ of $\mathrm{GL}(V)$ can be regarded as a representation of $G$ by restriction. We now apply the DCT to $V^{\otimes k}$ in the place of $V$, and take $\mathcal{A} := \rho_k(\mathbb{C}G)$. Note that $\sigma_k(\mathbb{C}\mathrm{S}_k) \subseteq \mathcal{B} := \mathrm{End}_{\mathcal{A}}(V^{\otimes k})$. The semisimplicity of $\mathcal{A}$ is guaranteed by Theorem 2.5, Addendum 2.6 and the remark before the DCT. Using the Trace Lemma 3.1 we get

$$\prod_{j=1}^{r}(\mathrm{Tr}(g^j))^{a_j} = \mathrm{Tr}((\rho_k \times \sigma_k)((g,s))) = \sum_{\mu\in M} \mathrm{Tr}(\rho_k(g)|_{V_\mu})\mathrm{Tr}(\sigma_k(s)|_{U_\mu}),$$

where $V_\mu, U_\mu$ ($\mu \in M$) are defined as in the DCT, and $s \in \mathrm{S}_k$ is of type $(1^{a_1}2^{a_2}\dots r^{a_r})$. On the right the symbol $\rho_k(g)|_{V_\mu}$ is to indicate that $\rho_k(g) \in \mathrm{End}_{\mathbb{C}}(V^{\otimes k})$ is considered as an endomorphism of the invariant subspace $V_\mu$, and analogously for $\sigma_k(s)|_{U_\mu}$. Integration over $K$ yields

$$\mathrm{E}\left(\prod_{j=1}^{r}(\mathrm{Tr}(\Gamma^j))^{a_j}\right) = \sum_{\mu\in M} \mathrm{Tr}(\sigma_k(s)|_{U_\mu}) \int \mathrm{Tr}(\rho_k(g)|_{V_\mu})\omega_K(dg). \tag{3.7}$$

Now for all $\mu \in M$ the map $\chi_\mu : G \to \mathbb{C} : g \mapsto \mathrm{Tr}(\rho_k(g)|_{V_\mu})$ is an irreducible character of $G$, and by Theorem 2.5 its restriction to $K$ is an irreducible character of $K$. If there exists $\mu_0 \in M$ such that $V_{\mu_0}$ is a trivial irreducible $G$-module (hence of the form $\mathbb{C}v_0$ for some $v_0 \in [V^{\otimes k}]^G$), then by the orthogonality of irreducible characters we see that (3.7) reduces to

$$\mathrm{Tr}\big(\sigma_k(s)\big|_{U_{\mu_0}}\big). \tag{3.8}$$

Otherwise the expectation in (3.7) equals 0. Now we invoke our Addendum 2.3 to the DCT. It says that $U_{\mu_0}$ is—up to an isomorphism of $\mathcal{B}$-modules—nothing else than the space $[V^{\otimes k}]^G$ of $G$-invariant tensors (with respect to $\rho_k$). So, in order to compute (3.8), we can apply the invariant theory of the complex orthogonal group. To simplify notation, we drop the representation $\rho_k$. The first obvious question is whether there are any nontrivial $G$-invariants. Since $-\mathrm{I} \in G$, it is clear that the answer is negative if $k$ is odd. So we assume that $k = 2l$ is even. Recall that $\mathfrak{f} := (f_i)_{i=1,\dots,n}$ is an orthonormal basis with respect to $\beta$. Set

$$\theta_l := \sum_{\varphi\in\mathcal{F}(l,n)} f_{1\varphi} \otimes f_{1\varphi} \otimes \cdots \otimes f_{l\varphi} \otimes f_{l\varphi}. \tag{3.9}$$

and

$$\theta_l^{\mathrm{S}_{2l}} := \{\theta_l\sigma_{2l}(s) : \ s \in \mathrm{S}_{2l}\}.$$

In the sequel we will drop the representation $\sigma_{2l}$.

**Theorem 3.6** (First Fundamental Theorem, FFT) $[V^{\otimes p}]^G = \{0\}$ *if $p$ is odd, and for $l \in \mathbb{N}$ one has*

$$[V^{\otimes 2l}]^G = \mathrm{span}_{\mathbb{C}}\big(\theta_l^{\mathrm{S}_{2l}}\big).$$

**Proof 6:** [4], Thm. 4.3.3. □

Hence, to evaluate (3.8), we have to compute the trace of $s \in \mathrm{S}_{2l}$ on $\mathrm{span}_{\mathbb{C}}(\theta_l^{\mathrm{S}_{2l}})$. We will facilitate this computation by giving another description of the action of $\mathrm{S}_{2l}$ on $\theta_l^{\mathrm{S}_{2l}}$. Recall that $\mathcal{M}(l)$ denotes the set of all two-partitions of $\{1, \ldots, 2l\}$. A family $(\{m_\nu, n_\nu\})_{\nu=1,\ldots,l}$ such that $\{\{m_\nu, n_\nu\} : \nu = 1, \ldots, l\} \in \mathcal{M}(l)$ is called a *labelled two-partition* of $\{1, \ldots, 2l\}$. Write $\mathcal{M}^{\mathfrak{l}}(l)$ for the set of all labelled two-partitions of $\{1, \ldots, 2l\}$. For $\mathfrak{m}^{\mathfrak{l}},\ \mathfrak{n}^{\mathfrak{l}} \in \mathcal{M}^{\mathfrak{l}}(l)$ write $\mathfrak{m}^{\mathfrak{l}} \equiv \mathfrak{n}^{\mathfrak{l}}$ if $\mathfrak{m}^{\mathfrak{l}}$ equals $\mathfrak{n}^{\mathfrak{l}}$ up to a permutation of the index set $\{1, \ldots, l\}$. Then $\mathcal{M}(l)$ can be regarded as the system of equivalence classes in $\mathcal{M}^{\mathfrak{l}}(l)$ with respect to $\equiv$.

For $\mathfrak{m}^{\mathfrak{l}} = (\{m_\nu, n_\nu\}) \in \mathcal{M}^{\mathfrak{l}}(l),\ \varphi \in \mathcal{F}(l, n)$ let $[\mathfrak{m}^{\mathfrak{l}}, \varphi]$ denote the tensor $\otimes_{i=1}^{2l} v_i$ with the property that $v_i = f_{\nu\varphi}$ if $i \in \{m_\nu, n_\nu\}$. Let $\mathrm{S}_{2l}$ act on $\mathcal{M}^{\mathfrak{l}}(l)$ as follows: $\mathfrak{m}^{\mathfrak{l}} = (\{m_\nu, n_\nu\})_{\nu=1,\ldots,l}$ is mapped to $\mathfrak{m}^{\mathfrak{l}}s := (\{m_\nu s, n_\nu s\})_{\nu=1,\ldots,l}$. From the definitions, recalling that $\mathrm{S}_{2l}$ acts on $V^{\otimes 2l}$ via $\sigma_{2l}$, we see:

**Lemma 3.7** *For $\mathfrak{m}^{\mathfrak{l}} \in \mathcal{M}^{\mathfrak{l}}(l),\ \varphi \in \mathcal{F}(l, n),\ s \in \mathrm{S}_{2l}$,*

$$[\mathfrak{m}^{\mathfrak{l}}, \varphi]s = [\mathfrak{m}^{\mathfrak{l}}s, \varphi].$$

Let $\mathfrak{m}_0^{\mathfrak{l}} := (\{1, 2\}, \{3, 4\}, \ldots, \{2l-1, 2l\})$. Then we have the following

**Corollary 3.8** *For all $s \in \mathrm{S}_{2l}$*

$$\theta_l s = \sum_{\varphi \in \mathcal{F}(l,n)} \big[\mathfrak{m}_0^{\mathfrak{l}}s, \varphi\big].$$

**Remark 3.9** Since for $\pi \in \mathrm{S}_l$ the mapping $\varphi \mapsto \pi\varphi$ induces a permutation of $\mathcal{F}(l, n)$, the sum $\sum_{\varphi \in \mathcal{F}(l,n)} [\mathfrak{m}^{\mathfrak{l}}, \varphi]$ is independent of the labelling in $\mathfrak{m}^{\mathfrak{l}}$, hence depends only on $\equiv(\mathfrak{m}^{\mathfrak{l}})$.

The $[\mathfrak{m}_0^{\mathfrak{l}}, \varphi]$ $(\varphi \in \mathcal{F}(l, n))$, i.e., the summands of $\theta_l$, are pairwise distinct elements of the basis $\mathfrak{f}^{\otimes 2l}$ of $V^{\otimes 2l}$, and $\mathrm{S}_{2l}$ maps them again to elements of $\mathfrak{f}^{\otimes 2l}$. By the very definition of a basis this implies that $\theta_l s = \theta_l$ if, and only if, $s$ permutes the summands of $\theta_l$. Now assume $n \geq l$ (which is the same as $2n \geq k$, hence our assumption (3.5)). Then there exists some $\varphi_0 \in \mathcal{F}(l, n)$ which is injective. Write $\mathcal{S}$ for the stabilizer of $\equiv(\mathfrak{m}_0^{\mathfrak{l}}) =: \mathfrak{m}_0$ with respect to the induced action of $\mathrm{S}_{2l}$ on $\mathcal{M}(l)$. Then for $[\mathfrak{m}_0^{\mathfrak{l}}, \varphi_0]s = [\mathfrak{m}_0^{\mathfrak{l}}s, \varphi_0]$ to be a summand of $\theta_l$ it is necessary that $s \in \mathcal{S}$. Together with Corollary 3.8 and Remark 3.9 this implies

**Lemma 3.10** *If $n \geq l$, then $\theta_l s = \theta_l$ if, and only if, $s \in \mathcal{S}$.*

**Corollary 3.11** *If $n \geq l$*

$$(\mathcal{M}(l),\ \mathrm{S}_{2l}) \cong \left(\mathrm{S}_{2l} : \mathcal{S},\ \mathrm{S}_{2l}\right) \cong \left(\theta_l^{\mathrm{S}_{2l}},\ \mathrm{S}_{2l}\right).$$

Corollary 3.11 implies that the number of fixed points of $s \in \mathrm{S}_{2l}$ in its action on $\theta_l^{\mathrm{S}_{2l}}$ is the same as in its action on $\mathcal{M}(l)$. Now, if we can show that $\theta_l^{\mathrm{S}_{2l}}$ is not only a spanning set, but also a basis of $[V^{\otimes 2l}]^G$, the trace we are interested in will be this number of fixed points. Note that the family $(\theta_l s)_{s\in \mathrm{S}_{2l}}$ contains repetitions. We can introduce an injective parametrization of the orbit as follows: For $\mathfrak{m} \in \mathcal{M}(l)$ choose $s_{\mathfrak{m}} \in \mathrm{S}_{2l}$ such that $\mathfrak{m}_0 s_{\mathfrak{m}} = \mathfrak{m}$. Then $(s_{\mathfrak{m}})_{\mathfrak{m}\in\mathcal{M}(l)}$ is a system of representatives for the coset space $\mathrm{S}_{2l} : \mathcal{S}$, and we have that $\theta_l^{\mathrm{S}_{2l}} = (\theta_l s_{\mathfrak{m}})_{\mathfrak{m}\in\mathcal{M}(l)}$.

**Lemma 3.12** *If $n \geq l$, then $\{\theta_l s_{\mathfrak{m}} : \mathfrak{m} \in \mathcal{M}(l)\}$ is $\mathbb{C}$-linearly independent.*

**Proof 7:** For all $\mathfrak{m} \in \mathcal{M}(l)$ $\theta_l s_{\mathfrak{m}}$ is a sum of suitable distinct elements of the basis $\mathfrak{f}^{\otimes 2l}$. Let $\varphi_0 \in \mathcal{F}(l, n)$ be injective. Then for each $\mathfrak{m} \in \mathcal{M}(l)$ $\equiv(\mathfrak{m}_0^{\natural} s_{\mathfrak{m}}) = \mathfrak{m}$, and $[\mathfrak{m}_0^{\natural} s_{\mathfrak{m}}, \varphi_0] = [\mathfrak{m}_0^{\natural}, \varphi_0] s_{\mathfrak{m}}$ is a summand of $\theta_l s_{\mathfrak{m}}$, but not of $\theta_l s_{\mathfrak{n}}$ ($\mathfrak{n} \neq \mathfrak{m}$). This proves the lemma. □

Summing up, we have established the following

**Theorem 3.13** *If $k = k_a = \sum_{j=1}^{r} j a_j$ is odd, then*

$$\mathrm{E}\left(\prod_{j=1}^{r} \left(\mathrm{Tr}(\Gamma^j)\right)^{a_j}\right) = 0.$$

*If $k = 2l$ is even and $2n \geq k$, then this expectation equals the number of fixed points with respect to the induced action on $\mathcal{M}(l)$ of any $s \in \mathrm{S}_{2l}$ with cycle type $(1^{a_1} 2^{a_2} \ldots r^{a_r})$.*

Theorem 3.13 has transformed our original problem into a purely combinatorial task, which we are going to take up right now.

**Theorem 3.14** *Let $l \in \mathbb{N}$, $k = 2l$, $s \in \mathrm{S}_k$ with cycle type $(1^{a_1} 2^{a_2} \ldots r^{a_r})$. Then, with respect to the induced action of $\mathrm{S}_k$ on $\mathcal{M}(l) = \mathcal{M}(\{1, \ldots, 2l\})$, the number of fixed points of $s$ is*

$$\prod_{j=1}^{r} f_a(j),$$

*where*

$$f_a(j) := \begin{cases} 1 & \text{if } a_j = 0, \\ 0 & \text{if } ja_j \text{ is odd}, a_j \geq 1, \\ j^{\frac{a_j}{2}}(a_j - 1)!! & \text{if } j \text{ is odd and } a_j \text{ is even}, a_j \geq 2, \\ 1 + \sum_{d=1}^{\lfloor \frac{a_j}{2} \rfloor} j^d \binom{a_j}{2d} (2d-1)!! & \text{if } j \text{ is even}, a_j \geq 1. \end{cases} \tag{3.10}$$

*Here for* $m \in \mathbb{N}$ $(2m-1)!! = (2m-1)(2m-3)\ldots 3 \cdot 1$. *The empty sum is zero.*

The *proof* of this theorem becomes more transparent when one makes explicit a series of more or less trivial lemmata. Fix $s \in S_{2l}$ of the form

$$s = \prod_{j=1}^{r} \prod_{i=1}^{a_j} \zeta_i^j.$$

Now let $A \subseteq \{1, \ldots, 2l\}$, $\mathfrak{m} = \{\{m_\nu, n_\nu\} : \nu = 1, \ldots, l\} \in \mathcal{M}(l)$. We say that $\mathfrak{m}$ *can be restricted to* $A$, if there exists a subset $I_A \subseteq \{1, \ldots, l\}$ such that $A = \bigcup_{\nu \in I_A} \{m_\nu, n_\nu\}$.

**Lemma 3.15** *Let* $\mathfrak{m} \in \mathcal{M}(l)$ *be* $s$*-invariant,* $j \in \{1, \ldots, r\}$ *with* $a_j \geq 1$, $i \in \{1, \ldots, a_j\}$. *Then exactly one of the following cases occurs*:

(*a*) $\mathfrak{m}$ *can be restricted to* $[\zeta_i^j]$.

(*b*) $a_j \geq 2$, *and there exists a unique* $h \in \{1, \ldots, a_j\}$, $h \neq i$, *such that* $\mathfrak{m}$ *can be restricted neither to* $[\zeta_i^j]$ *nor to* $[\zeta_h^j]$, *but to* $[\zeta_i^j] \cup [\zeta_h^j]$.

*In case* (*a*) *the restriction of* $\mathfrak{m}$ *to* $[\zeta_i^j]$ *is* $\zeta_i^j$*-invariant, and in case* (*b*) *the restriction of* $\mathfrak{m}$ *to* $[\zeta_i^j] \cup [\zeta_h^j]$ *is* $\zeta_i^j \zeta_h^j$*-invariant.*

**Proof 8:** Suppose that (a) does not hold. Then there exists $\{p, q\} \in \mathfrak{m}$ with $p \in [\zeta_i^j]$, $q \notin [\zeta_i^j]$. Now there exist unique $i'$, $j'$ such that $q \in [\zeta_{i'}^{j'}]$. We claim that $j = j'$. Assume $j \neq j'$ and let $\nu = \min(j, j')$. Then $\#(\{ps^\nu, qs^\nu\} \cap \{p, q\}) = \#(\{p(\zeta_i^j)^\nu, q(\zeta_{i'}^{j'})^\nu\} \cap \{p, q\}) = 1$, contradicting $\mathfrak{m}s = \mathfrak{m}$. Write $h$ instead of $i'$. Since $p \notin [\zeta_h^j]$, $\mathfrak{m}$ cannot be restricted to $[\zeta_h^j]$, either. On the other hand, as $(\zeta_i^j)^j = 1_{S_{2l}} = (\zeta_h^j)^j$,

$$\left\{\left\{p\left(\zeta_i^j\right)^\mu, q\left(\zeta_h^j\right)^\mu\right\} : \mu \in \mathbb{N}\right\} = \left\{\left\{p\left(\zeta_i^j\right)^\mu, q\left(\zeta_h^j\right)^\mu\right\} : \mu = 1, \ldots, j\right\}$$

is the restriction of $\mathfrak{m}$ to $[\zeta_i^j] \cup [\zeta_h^j]$. The statements about invariance are obvious. □

For $A \subseteq \{1, \ldots, 2l\}$ consider the following hypotheses:

**(1)** There exist $j \in \{1, \ldots, r\}$ with $a_j \geq 1$, $i \in \{1, \ldots, a_j\}$ such that $A = [\zeta_i^j]$.

**(2)** There exist $j \in \{1, \ldots, r\}$ with $a_j \geq 2$, $i, h \in \{1, \ldots, a_j\}$, $i \neq h$, such that $A = [\zeta_i^j] \cup [\zeta_h^j]$.

Now suppose that $\mathcal{P}$ is a partition of $\{1, \ldots, 2l\}$ such that each $A \in \mathcal{P}$ satisfies (**1**) or (**2**). Then it is obvious that any family $(\mathfrak{m}_A)_{A\in\mathcal{P}}$ where $\mathfrak{m}_A \in \mathcal{M}(A)$ is $\zeta_i^j$- (resp. $\zeta_i^j\zeta_h^j$-) invariant gives rise to an $s$-invariant element of $\mathcal{M}(l)$.

**Lemma 3.16** *Let $A \subseteq \{1, \ldots, 2l\}$.*

(i) *If $A$ satisfies hypothesis (**1**), then $\mathcal{M}(A) = \emptyset$ if $j$ is odd, and $\mathcal{M}(A)$ contains exactly one $\zeta_i^j$-invariant element if $j$ is even.*

(ii) *If $A$ satisfies hypothesis (**2**), then $\mathcal{M}(A)$ contains exactly $j$ elements which are $\zeta_i^j\zeta_h^j$-invariant and which can be restricted neither to $[\zeta_i^j]$ nor to $[\zeta_h^j]$.*

**Proof 9:**

(i) If $j = \#[\zeta_i^j]$ is odd, then $[\zeta_i^j]$ admits no two-partition. If $j = 2\iota$ is even, write $\zeta_i^j = (p_1 p_2 \ldots p_{2\iota})$ and let $\mathfrak{m} \in \mathcal{M}([\zeta_i^j])$ be $\zeta_i^j$-invariant. Suppose $\{p_1, p_{1+\nu}\} \in \mathfrak{m}$. Then $\{p_1(\zeta_i^j)^\nu, p_{1+\nu}(\zeta_i^j)^\nu\} = \{p_{1+\nu}, p_{1+2\nu}\}$ if $1 \le \nu \le \iota - 1$, or $= \{p_{1+\nu}, p_{1+2(\nu-\iota)}\}$ if $\iota \le \nu \le 2\iota - 1$. By invariance only $\nu = \iota$ is possible. On the other hand, $\{\{p_\nu, p_{\nu+\iota}\} : \nu = 1, \ldots, \iota\}$ is $\zeta_i^j$-invariant.

(ii) Write $\zeta_i^j = (p_1 p_2 \ldots p_j)$, $\zeta_h^j = (q_1 q_2 \ldots q_j)$, and consider an $\zeta_i^j\zeta_h^j$-invariant $\mathfrak{m} \in \mathcal{M}([\zeta_i^j] \cup [\zeta_h^j])$. If $\mathfrak{m}$ can be restricted neither to $[\zeta_i^j]$ nor to $[\zeta_h^j]$, there are $\mu_1,\ \mu_2 \in \{1, \ldots, j\}$ such that $\{p_{\mu_1}, q_{\mu_2}\} \in \mathfrak{m}$. $\zeta_i^j\zeta_h^j$-invariance implies that

$$\mathfrak{m} = \left\{\left\{p_{\mu_1}\left(\zeta_i^j\right)^\nu,\ q_{\mu_2}\left(\zeta_h^j\right)^\nu\right\} : \nu = 1, \ldots, j\right\}.$$

On the other hand, for all $p \in [\zeta_i^j]$, $q \in [\zeta_h^j]$,

$$\mathfrak{m}(p, q) := \left\{\left\{p\left(\zeta_i^j\right)^\nu,\ q\left(\zeta_h^j\right)^\nu\right\} :\ \nu = 1, \ldots, j\right\}$$

is $\zeta_i^j\zeta_h^j$-invariant. Now, for all $\nu = 1, \ldots, j$ we have that $\mathfrak{m}(p, q) = \mathfrak{m}(p(\zeta_i^j)^\nu, q(\zeta_h^j)^\nu)$, hence $\{\mathfrak{m}(p_1, q_\nu) :\ \nu = 1, \ldots, j\} = \{\mathfrak{m}(p, q) :\ p \in [\zeta_i^j], q \in [\zeta_h^j]\}$. □

**Proof 10** (Proof of Theorem 3.14)**:** We have seen so far that all $s$-invariant two-partitions can be obtained by gluing together invariant two-partitions of the supports of the individual cycles or of the union of the supports of two cycles. There is a degree of freedom in the way one groups some of the cycles into pairs, but since only cycles of equal length can be paired, it is possible to consider each cycle length $j = 1, \ldots, r$ separately. If $a_j \ge 1$, write $f_a(j)$ for the number of $\prod_{i=1}^{a_j} \zeta_i^j$-invariant two-partitions of $\bigcup_{i=1}^{a_j}[\zeta_i^j]$. If $j$ is odd, then there exist invariant partitions only if all cycles come in pairs, hence only if $a_j$ is even. In this case, there are as many pairings of $j$-cycles as there are two-partitions of $\{1, \ldots, a_j\}$. Once a pairing is fixed, each of the $\frac{a_j}{2}$ pairs, say $(\zeta_i^j,\ \zeta_h^j)$, gives rise to $j$ $\zeta_i^j\zeta_h^j$-invariant partitions of $[\zeta_i^j] \cup [\zeta_h^j]$. If $j$ is even, each $j$-cycle can remain single or be paired with another $j$-cycle,

so there are as many possible configurations as there are matchings in the set $\{1, \ldots, a_j\}$. Lemma 2.1 now yields our claim. □

An easy computation shows that (3.6) follows from Theorems 3.13 and 3.14.

*3.4. The symplectic case*

We consider the case $(G, K) = (\mathrm{Sp}(n, \mathbb{C}), \mathrm{Sp}_n)$ ($n = 2m$ even). Let $Z_1, \ldots, Z_r$ be iid standard normal random variables. Set $k = k_a$.

**Theorem 3.17** *If*

$$n \geq k, \tag{3.11}$$

*then*

$$\mathrm{E}\left(\prod_{j=1}^{r}(\mathrm{Tr}(\Gamma^j))^{a_j}\right) = \mathrm{E}\left(\prod_{j=1}^{r}(\sqrt{j}Z_j - \eta_j)^{a_j}\right), \tag{3.12}$$

*where $\eta_j$ is as in the orthogonal case.*

**Remark 3.18** If $k$ is odd, then (3.12) holds regardless of whether condition (3.11) is met or not, both sides being equal to zero in this case.

The *proof* of Theorem 3.17 is the content of this subsection. As in the orthogonal case we see that, if the trivial irreducible $G$-module occurs in $V^{\otimes k}$,

$$\mathrm{E}\left(\prod_{j=1}^{r}(\mathrm{Tr}(\Gamma^j))^{a_j}\right) = \mathrm{Tr}\big(\sigma_k(s)\big|_{[V^{\otimes k}]^G}\big), \tag{3.13}$$

where $s \in \mathrm{S}_k$ has type $(1^{a_1}2^{a_2}\ldots r^{a_r})$. Now let $(f_i)_{i=1,\ldots,n}$, $(f^i)_{i=1,\ldots,n}$ be a dual basis pair for $V$. Set

$$\theta_l := \sum_{\varphi\in\mathcal{F}(l,n)} f_{1\varphi} \otimes f^{1\varphi} \otimes \cdots \otimes f_{l\varphi} \otimes f^{l\varphi}.$$

With this definition, the FFT looks like in the orthogonal case.

**Theorem 3.19** $[V^{\otimes p}]^G = \{0\}$ *if $p$ is odd, and for $l \in \mathbb{N}$ one has*

$$[V^{\otimes 2l}]^G = \mathrm{span}_{\mathbb{C}}\big(\theta_l^{\mathrm{S}_{2l}}\big).$$

**Proof 11:** [4], Thm. 4.3.3. □

What makes the symplectic case more delicate than the orthogonal one is precisely that the definition of $\theta_l$ involves two bases, not one. This means that the proof of the crucial Lemma 3.10 cannot be carried over to the symplectic case in a straightforward manner. This problem can be overcome by choosing for $(f_i)_{i=1,\dots,n}, (f^i)_{i=1,\dots,n}$ the special dual basis pair which was constructed in (2.9) starting from a symplectic basis $\mathfrak{b} = (b_1, c_1, b_2, c_2, \dots, b_m, c_m)$ $(m = \frac{n}{2})$. Then the action of $\mathrm{S}_{2l}$ on $\theta_l^{\mathrm{S}_{2l}}$ can be described with respect to $\mathfrak{b}^{\otimes 2l}$, and this makes it possible to mimic the overall strategy of the above treatment of the orthogonal case. But resorting to $\mathfrak{b}$ comes at the price that one has to develop a technology to deal with the minus sign which shows up in (2.9).

To begin with, consider an example. Assume as in (3.11) that $n \geq k$, hence $m \geq l$. Then $\theta_l$ contains the summand

$$F := f_1 \otimes f^1 \otimes f_3 \otimes f^3 \otimes \cdots \otimes f_{2l-3} \otimes f^{2l-3} \otimes f_{2l-1} \otimes f^{2l-1} \tag{3.14}$$

$$= b_1 \otimes c_1 \otimes b_2 \otimes c_2 \otimes \cdots \otimes b_l \otimes c_l. \tag{3.15}$$

This means that for $\theta_l s = \theta_l$ to hold it is necessary that $s$ stabilize the two-partition $\{\{1, 2\}, \{3, 4\}, \dots, \{2l - 1, 2l\}\}$. But this is not a sufficient condition because the transposition $\tau = (12)$ maps $F$ to

$$F\tau = c_1 \otimes b_1 \otimes b_2 \otimes c_2 \otimes \cdots \otimes b_l \otimes c_l \tag{3.16}$$

$$= -f_2 \otimes f^2 \otimes f_3 \otimes f^3 \otimes \cdots \otimes f_{2l-3} \otimes f^{2l-3} \otimes f_{2l-1} \otimes f^{2l-1}. \tag{3.17}$$

Let us analyze this situation more carefully. To this end we introduce the following terminology. Define an *ordered two-partition* of $\{1, \dots, 2l\}$ to be a family $((m_\nu, n_\nu))_{\nu=1,\dots,l}$ of ordered pairs such that $\{\{m_\nu, n_\nu\} : \nu = 1, \dots, l\} \in \mathcal{M}(l)$, and write $\mathcal{M}^{\mathrm{o}}(l)$ for the system of ordered two-partitions of $\{1, \dots, 2l\}$. Note that a two-partition can be regarded as an equivalence class in $\mathcal{M}^{\mathrm{o}}(l)$ with respect to the equivalence relation $\equiv$ which is defined for $\mathfrak{m}^{\mathrm{o}} = ((m_\nu, n_\nu))_{\nu=1,\dots,l}$, $\mathfrak{p}^{\mathrm{o}} = ((p_\nu, q_\nu))_{\nu=1,\dots,l}$ by

$$\mathfrak{m}^{\mathrm{o}} \equiv \mathfrak{p}^{\mathrm{o}} \ :\Leftrightarrow\ \exists \pi \in \mathrm{S}_l \ \forall \nu = 1, \dots, l :$$
$$(m_\nu = p_{\nu\pi} \text{ and } n_\nu = q_{\nu\pi}) \text{ or } (m_\nu = q_{\nu\pi} \text{ and } n_\nu = p_{\nu\pi}).$$

For $\mathfrak{m}^{\mathrm{o}} = ((m_\nu, n_\nu))_{\nu=1,\dots,l} \in \mathcal{M}^{\mathrm{o}}(l)$ define the *sign*

$$\operatorname{sgn}(\mathfrak{m}^{\mathrm{o}}) := \prod_{\nu=1}^{l} \frac{n_\nu - m_\nu}{|n_\nu - m_\nu|}.$$

Define the equivalence relation $\sim$ in $\mathcal{M}^{\mathrm{o}}(l)$ via

$$\mathfrak{m}^{\mathrm{o}} \sim \mathfrak{p}^{\mathrm{o}} \ :\Leftrightarrow\ \mathfrak{m}^{\mathrm{o}} \equiv \mathfrak{p}^{\mathrm{o}} \quad \text{and} \quad \operatorname{sgn}(\mathfrak{m}^{\mathrm{o}}) = \operatorname{sgn}(\mathfrak{p}^{\mathrm{o}}).$$

An equivalence class in $\mathcal{M}^{\mathrm{o}}(l)$ with respect to $\sim$ will be called a *signed two-partition*. Write $\mathcal{M}^{\mathrm{s}}(l)$ for the system of signed two-partitions. It is easily verified that the definition

$(\sim(\mathfrak{m}^{\mathfrak{o}}))s := \sim(\mathfrak{m}^{\mathfrak{o}}s)$ where

$$\mathfrak{m}^{\mathfrak{o}}s := ((m_\nu s, n_\nu s))_{\nu=1,\dots,l} \tag{3.18}$$

yields a well defined action of $S_{2l}$ on $\mathcal{M}^{\mathfrak{s}}(l)$. Note that the analogous definition $(\equiv(\mathfrak{m}^{\mathfrak{o}}))s := \equiv(\mathfrak{m}^{\mathfrak{o}}s)$ amounts to nothing else than the usual action of $S_{2l}$ on $\mathcal{M}(l)$.

Let $\mathfrak{m}^{\mathfrak{o}} = ((m_\nu, n_\nu))_{\nu=1,\dots,l} \in \mathcal{M}^{\mathfrak{o}}(l),\ \varphi \in \mathcal{F}(l,n)$. Write $[\mathfrak{m}^{\mathfrak{o}}, \varphi]$ for the tensor $\otimes_{i=1}^{2l} v_i$ which is defined as follows: If $i = m_\nu$, then $v_i := f_{\nu\varphi}$, if $i = n_\nu$ then $v_i := f^{\nu\varphi}$. By the definition of $[\mathfrak{m}^{\mathfrak{o}}, \varphi]$ and of the action $\sigma_{2l}$ we have

**Lemma 3.20** *For all* $\mathfrak{m}^{\mathfrak{o}} \in \mathcal{M}^{\mathfrak{o}}(l),\ \varphi \in \mathcal{F}(l,n),\ s \in S_{2l}$,

$$[\mathfrak{m}^{\mathfrak{o}}, \varphi]s = [\mathfrak{m}^{\mathfrak{o}}s, \varphi],$$

*where* $\mathfrak{m}^{\mathfrak{o}}s$ *is defined as in* (3.18).

**Corollary 3.21** *For all* $s \in S_{2l}$

$$\theta_l s = \sum_{\varphi\in\mathcal{F}(l,n)} \left[\mathfrak{m}_0^{\mathfrak{o}}s, \varphi\right],$$

*where*

$$\mathfrak{m}_0^{\mathfrak{o}} := \left(\left(m_\nu^0, n_\nu^0\right)\right)_{\nu=1,\dots,l} := ((1,2),(3,4),\dots,(2l-1,2l)). \tag{3.19}$$

Generalizing the above counterexample (3.16), (3.17), one observes that for $i = 1,\dots,m$

$$f^{2i-1} \otimes f_{2i-1} = -f_{2i} \otimes f^{2i} \quad \text{and} \quad f^{2i} \otimes f_{2i} = -f_{2i-1} \otimes f^{2i-1}. \tag{3.20}$$

For $\nu = 1,\dots,l$ define a map $T_\nu : \mathcal{F}(l,n) \to \mathcal{F}(l,n)$ which assigns to $\varphi$ the map $\psi$ which coincides with $\varphi$ on $\{1,\dots,l\}\backslash\{\nu\}$, and which is defined for $\nu$ as follows: $\nu\psi := \nu\varphi + 1$ if $\nu\varphi$ is odd and $\nu\psi := \nu\varphi - 1$ if $\nu\varphi$ is even. Note that indeed $\psi \in \mathcal{F}(l,n)$ because $n$ is even, and that $T_\nu \circ T_\nu = \mathrm{id}$. If $\mathfrak{m}^{\mathfrak{o}} = ((m_\nu, n_\nu))_{\nu=1,\dots,l} \in \mathcal{M}^{\mathfrak{o}}(l)$ and $\tau$ is a transposition which leaves $\equiv(\mathfrak{m}^{\mathfrak{o}})$ invariant, i.e. $\tau = (m_\nu n_\nu)$ for some $\nu = 1,\dots,l$, then (3.20) says that

$$[\mathfrak{m}^{\mathfrak{o}}\tau, \varphi] = -[\mathfrak{m}^{\mathfrak{o}}, T_\nu(\varphi)].$$

Together with Lemma 3.20 and the obvious analog of Remark 3.9, this yields

**Lemma 3.22** *For any* $s \in S_{2l}$ *with* $(\equiv(\mathfrak{m}^{\mathfrak{o}}))s = \equiv(\mathfrak{m}^{\mathfrak{o}})$ *we have*

$$\left(\sum_{\varphi\in\mathcal{F}(l,m)} [\mathfrak{m}^{\mathfrak{o}}, \varphi]\right)s = \sum_{\varphi\in\mathcal{F}(l,m)} [\mathfrak{m}^{\mathfrak{o}}s, \varphi] = \begin{cases} \displaystyle\sum_{\varphi\in\mathcal{F}(l,m)} [\mathfrak{m}^{\mathfrak{o}}, \varphi] & \text{if } (\sim(\mathfrak{m}^{\mathfrak{o}}))s = \sim(\mathfrak{m}^{\mathfrak{o}}), \\ \displaystyle -\sum_{\varphi\in\mathcal{F}(l,m)} [\mathfrak{m}^{\mathfrak{o}}, \varphi] & \text{otherwise.} \end{cases}$$

Recall that one of the many equivalent definitions of the sign of a permutation $s \in \mathrm{S}_{2l}$ is as follows:

$$\operatorname{sgn}(s) = \prod_{1 \le i < j \le 2l} \frac{js - is}{j - i}.$$

From this it is not difficult to obtain the following

**Lemma 3.23** *For $\mathfrak{m}^{\circ} \in \mathcal{M}^{\circ}(l)$, $s \in \mathrm{S}_{2l}$, the following statements are equivalent*:
(i) $(\sim(\mathfrak{m}^{\circ}))s = \sim(\mathfrak{m}^{\circ})$.
(ii) $(\equiv(\mathfrak{m}^{\circ}))s = \equiv(\mathfrak{m}^{\circ})$ *and* $\operatorname{sgn}(s) = 1$.

Denote by $\mathcal{S}$ the stabilizer of $\sim(\mathfrak{m}_0^{\circ})$ in $\mathrm{S}_{2l}$. By Lemma 3.23 $\mathcal{S}$ is contained in the alternating group $\mathrm{A}_{2l}$. More precisely it is the stabilizer of $\equiv(\mathfrak{m}_0^{\circ})$ in $\mathrm{A}_{2l}$. By (3.15) and the subsequent discussion on the one hand, and Lemma 3.22 and the other, it is evident that $\mathcal{S}$ coincides with the stabilizer of $\theta_l$ in $\mathrm{A}_{2l}$ if $n \ge k$. Since $\mathrm{A}_{2l}$ acts transitively on $\mathcal{M}(l)$, then, $(\mathcal{M}(l), \mathrm{A}_{2l})$ and $(\theta_l^{\mathrm{A}_{2l}}, \mathrm{A}_{2l})$ are isomorphic.

If $\tau = (12)$, then $\mathrm{S}_{2l} = \mathrm{A}_{2l} \cup \tau\mathrm{A}_{2l}$. Again by Lemma 3.22 we have $\theta_l^{\tau} = -\theta_l$, hence $\operatorname{span}_{\mathbb{C}}(\theta_l^{\mathrm{A}_{2l}}) = \operatorname{span}_{\mathbb{C}}(\theta_l^{\mathrm{S}_{2l}}) = [V^{\otimes 2l}]^G$. Let $(a_{\mathfrak{m}})_{\mathfrak{m} \in \mathcal{M}(l)}$ be a set of representatives for the coset space $(\mathrm{A}_{2l} : \mathcal{S})$ such that $\mathfrak{m}_0 a_{\mathfrak{m}} = \mathfrak{m}$ for all $\mathfrak{m} \in \mathcal{M}(l)$.

**Lemma 3.24** *If $n \ge k = 2l$, then*

$$\{\theta_l a_{\mathfrak{m}} : \mathfrak{m} \in \mathcal{M}(l)\} \tag{3.21}$$

*is a basis of $[V^{\otimes 2l}]^G$.*

**Proof 12:** Only the linear independence remains to be shown. For all $\mathfrak{m} \in \mathcal{M}(l)$, $\theta_l a_{\mathfrak{m}}$ is a sum of suitable distinct elements of the basis $\mathfrak{b}^{\otimes 2l}$. Let $\varphi_0 \in \mathcal{F}(l, n)$ be such that $[\mathfrak{m}_0^{\circ}, \varphi_0] = F$ from (3.14). Then for each $\mathfrak{m} \in \mathcal{M}(l)$, $\equiv(\mathfrak{m}_0^{\circ} a_{\mathfrak{m}}) = \mathfrak{m}$, and $[\mathfrak{m}_0^{\circ} a_{\mathfrak{m}}, \varphi_0] = [\mathfrak{m}_0^{\circ}, \varphi_0] a_{\mathfrak{m}}$ is a summand of $\theta_l a_{\mathfrak{m}}$, but not of $\theta_l a_{\mathfrak{n}}$ ($\mathfrak{n} \ne \mathfrak{m}$). □

**Lemma 3.25** *Assume $n \ge k$, and let $s \in \mathrm{S}_{2l}$, $\mathfrak{m} \in \mathcal{M}(l)$. Then the following statements are equivalent*:

(i) *When $(\theta_l a_{\mathfrak{m}})s$ is expressed as a linear combination in the basis* (3.21), *then $\theta_l a_{\mathfrak{m}}$ has nonzero coefficient.*
(ii) $(\theta_l a_{\mathfrak{m}})s = \operatorname{sgn}(s)\, \theta_l a_{\mathfrak{m}}$.
(iii) $\mathfrak{m}s = \mathfrak{m}$.

**Proof 13:** Lemmata 3.22, 3.23 and 3.24. □

**Theorem 3.26** *If $n \ge k$, then for all $s \in \mathrm{S}_{2l}$*

$$\operatorname{Tr}\big(\sigma_{2l}(s)|_{[V^{\otimes 2l}]^G}\big) = \operatorname{sgn}(s) \cdot \#\{\mathfrak{m} \in \mathcal{M}(l) : \mathfrak{m}s = \mathfrak{m}\}.$$

**Proof 14:** Lemmata 3.24 and 3.25. □

Now $s \in S_{2l}$ is odd if, and only if, it has an odd number of cycles of even length ($\geq 2$). Suppose type$(s) = (1^{a_1} 2^{a_2} \dots r^{a_r})$. In order to get a handy version of our main result, we observe:

**Lemma 3.27**

$$\sum_{\substack{j=1 \\ j \text{ even}}}^{r} a_j \equiv \sum_{j=1}^{r} (j-1) a_j \pmod 2.$$

Putting Theorems 3.14 and 3.26 and Lemma 3.27 together, we finally obtain

**Theorem 3.28** *If $k = \sum_{j=1}^{r} j a_j$ is odd, then*

$$\mathrm{E}\left( \prod_{j=1}^{r} (\mathrm{Tr}(\Gamma^j))^{a_j} \right) = 0.$$

*If $k = 2l$ is even and $n \geq k$, then this expectation equals*

$$\prod_{j=1}^{r} (-1)^{(j-1)a_j} f_a(j),$$

*where $f_a$ is defined as in* (3.10) *above in the orthogonal case.*

An easy computation shows that (3.12) follows from Theorem 3.28.

### *3.5. The unitary case*

We consider the case $(G, K) = (\mathrm{GL}(n, \mathbb{C}), \mathrm{U}_n)$.

**Theorem 3.29** *If $k_a \neq k_b$, then*

$$\alpha_{(a,b)} := \mathrm{E}\left( \prod_{j=1}^{r} (\mathrm{Tr}(\Gamma^j))^{a_j} \prod_{j=1}^{q} \overline{(\mathrm{Tr}(\Gamma^j))^{b_j}} \right) = 0, \tag{3.22}$$

*and if $k_a = k_b$ and $n \geq k_a$, then*

$$\alpha_{(a,b)} = \delta_{ab} \prod_{j=1}^{r} j^{a_j} a_j! \tag{3.23}$$

The interpretation of the right-hand side as a moment of a normal random vector requires some preparation which will be deferred to the end of this subsection.

Since in the unitary case the conjugates come into play, we will have to prove an extension of the Trace Lemma 3.1. Let $\gamma$ be the standard scalar product on $V = \mathbb{C}^n$, semilinear in the first argument and linear in the second argument. To any orthonormal basis $(v_i)_{i=1,\dots,n}$ of $V$ with respect to $\gamma$ we assign a dual basis $(v_i^*)_{i=1,\dots,n}$ of $V^*$ by defining $v_i^* := (x \mapsto \gamma(v_i, x))$ for $i = 1, \dots, n$. Recall that $\rho$ denotes the defining representation of $G$ on $V$, and that $\rho^*$ is the contragredient representation on $V^*$ (see (2.4)). Write $\rho_{k_b}^*$ for $(\rho^*)^{\otimes k_b}$. The image of the tensor product representation $\rho_{k_a} \otimes \rho_{k_b}^*$ of $G$ on $V^{\otimes k_a} \otimes (V^*)^{\otimes k_b}$ centralizes the image of the tensor product representation $\sigma_{k_a} \otimes \sigma_{k_b}$ of $\mathrm{S}_{k_a} \times \mathrm{S}_{k_b}$ on $V^{\otimes k_a} \otimes (V^*)^{\otimes k_b}$.

**Lemma 3.30** *Let $g \in K = \mathrm{U}_n$, $s \in \mathrm{S}_{k_a}$, $t \in \mathrm{S}_{k_b}$, $\lambda^s := \mathrm{type}(s) = (1^{a_1} 2^{a_2} \dots r^{a_r})$, $\lambda^t := \mathrm{type}(t) = (1^{b_1} 2^{b_2} \dots q^{b_q})$. Then*

$$\mathrm{Tr}\big(\big((\rho_{k_a} \otimes \rho_{k_b}^*) \times (\sigma_{k_a} \otimes \sigma_{k_b})\big)\big((g, (s, t))\big)\big) = \prod_{j=1}^{r} (\mathrm{Tr}(g^j))^{a_j} \prod_{j=1}^{q} \overline{(\mathrm{Tr}(g^j))^{b_j}}.$$

**Proof 15:** Recall the notation of the proof of the Trace Lemma and observe that $x\rho(g^{-1})v_i^* = (xg^{-1})v_i^* = \gamma(v_i, xg^{-1}) = \gamma(v_i g, x) = \gamma(c_i v_i, x) = \overline{c_i}\ \gamma(v_i, x) = \overline{c_i}(x v_i^*) = x(\overline{c_i} v_i^*)$, hence $v_i^* \rho^*(g) = \overline{c_i} v_i^*$. So we can argue exactly as in 3.1. □

As to the proof of the moment formula, our standard application of the DCT shows that we have to compute the trace of $(s, t) \in \mathrm{S}_{k_a} \times \mathrm{S}_{k_b}$ on the space of $G$-invariants in $V^{\otimes k_a} \otimes (V^*)^{\otimes k_b}$. Now for any $0 \neq c \in \mathbb{C}$ the scalar matrix $c\mathrm{I}$ is in $G$. By the definition of the contragredient representation, for any $v \in V^{\otimes k_a} \otimes (V^*)^{\otimes k_b}$ we have $v((\rho_{k_a} \otimes \rho_{k_b}^*)(c\ \mathrm{I})) = c^{k_a - k_b} v$. Therefore there are no $G$-invariants unless $k_a = k_b$. Now assume that $k_a = k_b$ and set $k := k_a$. Let $(e_i)_{i=1,\dots,n}$ be the standard basis of $V = \mathbb{C}^n$. For $\pi \in \mathrm{S}_k$ set

$$C_\pi := \sum_{\varphi \in \mathcal{F}(k,n)} \big(\otimes_{i=1}^k e_{i\pi^{-1}\varphi}\big) \otimes \big(\otimes_{i=1}^k e_{i\varphi}^*\big).$$

We are now in a position to state the FFT for $G$.

**Theorem 3.31**

$$[V^{\otimes k} \otimes (V^*)^{\otimes k}]^G = \mathrm{span}_{\mathbb{C}}\{C_\pi : \pi \in \mathrm{S}_k\}.$$

**Proof 16:** [4], Thm. 4.3.1. □

**Lemma 3.32** *If $n \geq k$, then $\{C_\pi : \pi \in \mathrm{S}_k\}$ is $\mathbb{C}$-linearly independent.*

**Proof 17:** Since $n \geq k$ there exists some $\varphi_0 \in \mathcal{F}(k, n)$ which is injective. Then the summand $(\otimes_{i=1}^k e_{i\pi^{-1}\varphi_0}) \otimes (\otimes_{i=1}^k e_{i\varphi_0}^*)$ occurs only in $C_\pi$. This suffices to justify our claim, because $\{(\otimes_{i=1}^k e_{i\varphi}) \otimes (\otimes_{i=1}^k e_{i\psi}^*) : \varphi, \psi \in \mathcal{F}(k, n)\}$ is a basis of $V^{\otimes k} \otimes (V^*)^{\otimes k}$. □

For $s \in \mathrm{S}_k$, $\mathrm{C}_{\mathrm{S}_k}(s)$ denotes the centralizer of $s$ in $\mathrm{S}_k$.

**Lemma 3.33** *If $n \geq k$, then for any $(s,t) \in \mathrm{S}_k \times \mathrm{S}_k$ with* $\mathrm{type}(s) = (1^{a_1}2^{a_2}\dots r^{a_r})$, $\mathrm{type}(t) = (1^{b_1}2^{b_2}\dots q^{b_q})$, *the trace of $(\sigma_k \otimes \sigma_k)((s,t))$ on $\mathrm{span}_{\mathbb{C}}\{C_\pi : \pi \in \mathrm{S}_k\}$ equals $\delta_{ab}\,\#(\mathrm{C}_{\mathrm{S}_k}(s))$.*

**Remark 3.34** Note that if $a = b$, then $\#(\mathrm{C}_{\mathrm{S}_k}(s)) = \#(\mathrm{C}_{\mathrm{S}_k}(t))$, because in this case the centralizers are conjugate.

**Proof 18** (Proof of Lemma 3.33)**:** If $(s_\lambda)_{\lambda\in\mathrm{Par}(k)}$ is a system of representatives for the conjugacy classes in $\mathrm{S}_k$, then $(s_\lambda, s_\mu)_{\lambda,\mu\in\mathrm{Par}(k)}$ is such a system for $\mathrm{S}_k \times \mathrm{S}_k$. Since we are computing a trace we may assume that $(s,t)$ is one such representative. $(\varphi \mapsto t\varphi)$ being a bijection of $\mathcal{F}(k,n)$, we have

$$\begin{aligned} C_\pi((\sigma_k \otimes \sigma_k)((s,t))) &= \sum_{\varphi\in\mathcal{F}(k,n)} \left(\otimes_{i=1}^k e_{is^{-1}\pi^{-1}\varphi}\right) \otimes \left(\otimes_{i=1}^k e^*_{it^{-1}\varphi}\right) \\ &= \sum_{\varphi\in\mathcal{F}(k,n)} \left(\otimes_{i=1}^k e_{is^{-1}\pi^{-1}t\varphi}\right) \otimes \left(\otimes_{i=1}^k e^*_{i\varphi}\right) = C_{t^{-1}\pi s}. \end{aligned}$$

Therefore $(s,t)$ permutes the $C_\pi$, and Lemma 3.32 implies that the trace we are interested in equals the number of fixed points. Now fix $\varphi_0 \in \mathrm{S}_k$ and regard it as an element of $\mathcal{F}(k,n)$. If $C_{t^{-1}\pi s} = C_\pi$, then $s^{-1}\pi^{-1}t\varphi_0 = \pi^{-1}\varphi_0$, hence $s^{-1}\pi^{-1}t = \pi^{-1}$, and therefore $t = \pi s\pi^{-1}$. This implies that $\mathrm{type}(s) = \mathrm{type}(t)$, i.e. $a = b$, and $s = t$ by the above special choice for $(s,t)$. Then $\pi s = s\pi$, hence $\pi \in \mathrm{C}_{\mathrm{S}_k}(s)$.

On the other hand, if $\pi \in \mathrm{C}_{\mathrm{S}_k}(s)$, $a = b$, then

$$\begin{aligned} C_\pi((\sigma_k \otimes \sigma_k)(s,t)) = C_\pi((\sigma_k \otimes \sigma_k)(s,s)) &= \sum_{\varphi\in\mathcal{F}(k,n)} \left(\otimes_{i=1}^k e_{is^{-1}\pi^{-1}\varphi}\right) \otimes \left(\otimes_{i=1}^k e^*_{is^{-1}\varphi}\right) \\ = \sum_{\varphi\in\mathcal{F}(k,n)} \left(\otimes_{i=1}^k e_{i\pi^{-1}(s^{-1}\varphi)}\right) \otimes \left(\otimes_{i=1}^k e^*_{i(s^{-1}\varphi)}\right) &= \sum_{\varphi\in\mathcal{F}(k,n)} \left(\otimes_{i=1}^k e_{i\pi^{-1}\varphi}\right) \otimes (\otimes_{i=1}^k e^*_{i\varphi}) \\ = C_\pi. \end{aligned}$$

The remaining assertion is obvious. □

For an interpretation of the moment formula (3.23), let $Z$ be an $\mathbb{R}^2$-valued random vector with distribution $\mathrm{N}(0, \frac{1}{2}\mathrm{I}_2)$. By a standard result on rotationally invariant distributions (see [1], Prop. 4.10) $Z$ has the same distribution as a product $RU$ of independent random variables $R$ and $U$, where $U$ has the uniform distribution on the unit circle and $R$ has the same distribution as the euclidean norm $\|Z\|_2$ of $Z$. In the present case it is in fact an exponential distribution with parameter 1, and one has $\mathrm{E}((R^2)^k) = k!$ for all $k \in \mathbb{N}_0$. Now regard $Z$ as a complex random variable and call it a *standard complex normal* random variable. Write $U = e^{iT}$, where $T$ is uniformly distributed on $[0, 2\pi]$. Let $a, b \in \mathbb{N}_0$. Then

$\mathrm{E}(Z^a \overline{Z}^b) = \mathrm{E}(R^{(a+b)})\,\mathrm{E}(e^{i(a-b)T}) = \delta_{ab}\,\mathrm{E}(R^{2a}) = \delta_{ab}\,a!$ Hence for iid standard complex normal random variables $Z_j$ ($j \in \mathbb{N}$) one has

$$\alpha_{(a,b)} = \delta_{rq} \prod_{j=1}^{r} \delta_{a_j b_j}\, j^{\frac{a_j+b_j}{2}} a_j! = \mathrm{E}\left( \prod_{j=1}^{r} (\sqrt{j} Z_j)^{a_j} \prod_{j=1}^{q} \overline{(\sqrt{j} Z_j)^{b_j}} \right).$$

## References


1. M. Bilodeau and D. Brenner, *Theory of Multivariate Statistics*, Springer, New York, 1999.
2. P. Diaconis and S.N. Evans, "Linear functionals of eigenvalues of random matrices," *Trans. Amer. Math. Soc.* **353** (2001), 2615–2633.
3. P. Diaconis and M. Shahshahani, "On the eigenvalues of random matrices," *J. Appl. Probab.* **31A** (1994), 49–62.
4. R. Goodman and N.R. Wallach, *Representations and Invariants of the Classical Groups*, Cambridge UP, New York, 1998.
5. W.H. Greub, *Multilinear Algebra*, Springer, Berlin, 1967.
6. G. Hochschild, *The Structure of Lie Groups*, Holden Day, San Francisco, 1965.
7. C.P. Hughes and Z. Rudnick, "Mock-Gaussian behaviour for linear statistics of classical compact groups," *J. Phys. A* **36** (2003), 2919–2932.
8. L. Pastur and V. Vasilchuk, "On the moments of traces of matrices of classical groups," *Commun. Math. Phys.* **252** (2004), 149–166.
9. A. Ram, "Characters of Brauer's centralizer algebras," *Pacific J. Math.* **169** (1995), 173–200.
10. A. Ram, "Second orthogonality relation for characters of Brauer algebras," *European J. Combin.* **18** (1997), 685–706.
11. V.S. Varadarajan, *Lie Groups, Lie Algebras, and their Representations*, Springer, New York, 1984.
12. H. Weyl, *The Classical Groups. Their Invariants and Representations*, 2nd ed., Princeton UP, Princeton, 1953.