Random Matrices

and

Invariant Theory

Michael Stolz

University of Tübingen

Compute the joint moments of

$$\left(\mathrm{Tr}(\Gamma), \ \mathrm{Tr}(\Gamma^2), \ldots, \mathrm{Tr}(\Gamma^r) \right)$$

for a Haar-distributed random element Γ of O_n, Sp_n,

or of

$$\left(\mathrm{Tr}(\Gamma), \ldots, \mathrm{Tr}(\Gamma^r), \overline{\mathrm{Tr}(\Gamma)}, \ldots, \overline{\mathrm{Tr}(\Gamma^r)} \right)$$

for a Haar-distributed random element Γ of U_n.

Moment formulae were obtained in joint work of Diaconis, Mallows, and Shahshahani, starting in the 1980s.
First published proof in Diaconis-Shahshahani '94.

The proof (Diaconis - Shahshahani '94) exploits in the unitary case an explicit decomposition of power sum symmetric polynomials ("Schur - Weyl duality") and elementary character theory of groups.

The corresponding results about random orthogonal and symplectic matrices use advanced results from combinatorial representation theory (Ram '95, '97) ("character theory of Brauer algebras").

One would like to have a new proof which

- is elementary and accessible in that it avoids any specialized calculi (as they are in use in combinatorial representation theory)

- emphasizes the underlying structural features and avoids the explicit use of special functions.

$\Gamma_n : (\Omega, \mathfrak{A}, P) \longrightarrow (O_n, \mathfrak{B}(O_n))$

with distribution ω_{O_n} (normalized Haar measure)

$r \in \mathbb{N}$, $a = (a_1, \dots, a_r) \in \mathbb{N}_0^r$,

$Z_1, \dots, Z_r$ iid $N(0,1)$

Theorem

If $2n \geq \sum_{j=1}^{r} j a_j$,

then

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

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

$\Gamma_n : (\Omega, \mathcal{A}, P) \longrightarrow (O_n, \mathcal{B}(O_n))$ $(Sp_n, \mathcal{B}(Sp_n))$

with distribution ω_{O_n} $_{Sp_n}$ (normalized Haar measure)

$r \in \mathbb{N}$, $a = (a_1, \dots, a_r) \in \mathbb{N}_0^r$,

$Z_1, \dots, Z_r$ iid $N(0,1)$

Theorem

If $2n \geqslant \sum_{j=1}^{r} j a_j$,
$n \geqslant$

then

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

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

Fixed data:

$n \in \mathbb{N}$ $(n = 2m)$

$K \in \{O_n, Sp_n\}$, $G \in \{O(n,\mathbb{C}), Sp(n,\mathbb{C})\}$

$V = \mathbb{C}^n$

$r \in \mathbb{N}$, $a = (a_1, \dots, a_r) \in \mathbb{N}_0^r$

$$k := \sum_{j=1}^{r} j\, a_j$$

Structure of proof:

① For $g \in G$, interpret $\prod_{j=1}^{r} (\mathrm{Tr}\, g^j)^{a_j}$

as the trace of a suitable

operator on $V^{\otimes k}$.

② Simplify using representation theory of semisimple algebras.

③ Invoke invariant theory to yield a reduction to a combinatorial problem.

④ Do the combinatorics.

ρ : natural representation of G on V

$\rho_k := \rho^{\otimes k}$ representation on $V^{\otimes k}$

$$\left(\bigotimes_{i=1}^{k} v_i\right)\rho_k(g) := \bigotimes_{i=1}^{k}\left(v_i\,\rho(g)\right)$$

σ_k : representation of S_k on $V^{\otimes k}$

$$\left(\bigotimes_{i=1}^{k} v_i\right)\sigma_k(s) := \bigotimes_{i=1}^{k} v_{is^{-1}}$$

$$\left(\bigotimes_{i=1}^{k} v_i\right)(\rho_k\times\sigma_k)(g,s) := \left(\left(\bigotimes_{i=1}^{k} v_i\right)\sigma_k(s)\right)\rho_k(g)$$

Key observation : For $g\in GL(n,\mathbb{C})$ [diagonalizable] :

$s\in S_k$, $\mathrm{type}(s) = (1^{a_1}\,2^{a_2}\,\dots\,r^{a_r})$

$$\left(= (\underbrace{r\,r\,r\dots r}_{a_r}\ \underbrace{(r-1)(r-1)\dots(r-1)}_{a_{r-1}}\ \dots\ \underbrace{1\,1\,1\,1}_{a_1})\right)$$

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

Sketch of proof:

$v_i \ (i=1,\dots,n)$ basis of V consisting of eigenvectors of g

$\updownarrow$

c_i corresponding eigenvalues

$V^{\otimes k}$ has a basis

$$B := \left\{ \bigotimes_{j=1}^{k} v_{f(j)} \;\middle|\; f : \{1,\dots,k\} \to \{1,\dots,n\} \right\}$$

Observe: $\forall\, b \in B \ \exists\, b' \in B$

$$b((\rho_k \times \sigma_k)(g,s)) \in \mathbb{C}\, b'$$

Hence, b "contributes" to $\mathrm{Tr}(\dots)$

iff $bs = b$

Now $\bigotimes_{j=1}^{k} v_{f(j)}$ is fixed by s

iff f is constant on the cycles of s.

Claim:

$$\int_K \mathrm{Tr}\left(\left(\rho_k \times \sigma_k\right)(g,s)\right)\, \omega_K(dg)$$

$$= \mathrm{Tr}\left(\sigma_k(s)\Big|_{\text{restricted to a module with nice properties}}\right)$$

Basic ingredients of the proof:

- $\mathrm{Lie}(G) = \mathrm{Lie}(K) \otimes_{\mathbb{R}} \mathbb{C}$

$\rightsquigarrow$ Correspondence between the irreducible representations of G and K

- $\rho_k(\mathbb{C}G)$ is a semisimple subalgebra of $\mathrm{End}(V^{\otimes k})$

- $\sigma_k(\mathbb{C}S_k) \subseteq C_{\mathrm{End}(V^{\otimes k})}(\rho_k(\mathbb{C}G))$

centralizer

The abstract setting:

W finite dimensional $\mathbb{C}$-vector space

$\mathfrak{A} \subseteq \mathrm{End}(W)$ semisimple, $\mathrm{id}_V \in \mathfrak{A}$

(i.e. direct product of full matrix algebras)

$$\mathfrak{B} := C_{\mathrm{End}(W)}(\mathfrak{A}) := \{ b \in \mathrm{End}(W) : ab = ba \ \forall a \in \mathfrak{A}$$

Double Centralizer Theorem (Schur, Weyl ?)

$\exists$ finite set M,

irred. $\mathfrak{A}$-modules V_μ ($\mu \in M$), $V_\mu \not\cong V_{\mu'}$ ($\mu \neq \mu'$)

" $\mathfrak{B}$ " U_μ " $U_\mu \not\cong U_{\mu'}$ ($\mu \neq \mu'$)

Such that

$$\boxed{W \cong \bigoplus_{\mu \in M} V_\mu \otimes U_\mu}$$

Isomorphism of $\mathfrak{A}$-modules and of $\mathfrak{B}$-modules

Application

$$W = V^{\otimes k}, \quad \mathfrak{A} = \rho_k(\mathbb{C}G),$$

$$\Rightarrow \sigma_k(\mathbb{C}S_k) \subseteq \mathfrak{B}$$

$$\int_K \mathrm{Tr}\big((\rho_k \times \sigma_k)(g,s)\big)\, \omega_K(dg)$$

$$= \sum_{\mu \in M} \int_K \mathrm{Tr}\big(\rho_k(g)\big|_{V_\mu}\big)\, \mathrm{Tr}\big(\sigma_k(s)\big|_{U_\mu}\big)\, \omega_K(dg)$$

$$= \sum_{\mu \in M} \mathrm{Tr}\big(\sigma_k(s)\big|_{U_\mu}\big) \int_K \mathrm{Tr}\big(\rho_k(g)\big|_{V_\mu}\big)\, \omega_K(dg)$$

$$= \mathrm{Tr}\big(\sigma_k(s)\big|_{U_{\mu_0}}\big), \qquad (*)$$

where μ_0 is uniquely determined by the requirement that V_{μ_0} be the trivial G-module

orthogonality of the nontrivial irred. characters of K to 1_K
(keep in mind that $\mathrm{Lie}(G) = \mathrm{Lie}(K) \otimes_{\mathbb{R}} \mathbb{C}$.)

Life would be easy if we had

$$\mathfrak{L} = \sigma_k(\mathbb{C}S_k) .$$

But ....

Solution 1 (D-S):

Use the theory of Brauer algebras.

Solution 2: Identify U_{μ_0} and compute the trace directly.

Why is solution 2 viable?

Because the DCT contains extra information:

$$\mathcal{U}_\mu = \mathrm{Hom}_{\mathfrak{A}}(V_\mu, \underbrace{W}_{V^{\otimes k}})$$

Observation: If V_{μ_0} is the trivial irred. $\rho_k(\mathbb{C}G)$-module, then

$\exists\, v_0 \in [V^{\otimes k}]^G := \{ v \in V^{\otimes k} : vg = v \ \forall g \in G \}$

s. th. $\quad V_{\mu_0} = \mathbb{C} v_0$

Note that if $\varphi \in \mathrm{Hom}_{\mathfrak{A}}(V_{\mu_0}, V^{\otimes k})$,

then $\quad v_0 \varphi \in [V^{\otimes k}]^G$

Consequence: $\mathcal{U}_{\mu_0}$ can be identified with $[V^{\otimes k}]^G$, the space of tensor invariants of G (acting via ρ_k).

Description of $[V^{\otimes k}]^G$

Observe: $-\mathrm{id} \in G \Rightarrow [V^{\otimes k}]^G = \{0\}$
if k is odd

Assume $k = 2\ell$ even.

Fact: $\vartheta_\ell \in [V^{\otimes 2\ell}]^G$

(σ_k, ρ_k commute)

$$\Rightarrow \vartheta_\ell^{S_{2\ell}} := \{\vartheta_\ell \sigma_{2\ell}(s) : s \in S_{2\ell}\} \subseteq [V^{\otimes 2\ell}]^G$$

FFT:

$$[V^{\otimes 2\ell}]^G = \mathrm{span}_{\mathbb{C}}(\vartheta_\ell^{S_{2\ell}})$$

Description of $[V^{\otimes k}]^G$

Observe: $-\mathrm{id} \in G \Rightarrow [V^{\otimes k}]^G = \{0\}$
if k is odd

Assume $k = 2l$ even.

$G = O(n, \mathbb{C})$. $(f_i)_{i=1,\dots,n}$ standard basis of $V = \mathbb{C}^n$

$$\vartheta_l := \sum_{\substack{\varphi : \{1,\dots,l\} \\ \to \{1,\dots,n\}}} f_{1\varphi} \otimes f_{1\varphi} \otimes \dots \otimes f_{l\varphi} \otimes f_{l\varphi}$$

Fact: $\vartheta_l \in [V^{\otimes 2l}]^G$

(σ_k, ρ_k commute)

$$\Rightarrow \vartheta_l^{S_{2l}} := \{\vartheta_l \sigma_{2l}(s) : s \in S_{2l}\} \subseteq [V^{\otimes 2l}]^G$$

<u>FFT</u>:

$$[V^{\otimes 2l}]^G = \mathrm{span}_{\mathbb{C}}(\vartheta_l^{S_{2l}})$$

Description of $[V^{\otimes k}]^G$

Observe: $-\mathrm{id} \in G \Rightarrow [V^{\otimes k}]^G = \{0\}$
if k is odd

Assume $k = 2\ell$ even.

$G = Sp(n, \mathbb{C})$, $n = 2m$,

$\beta_n : (x, y) \mapsto x' \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix} y$

$(f_i)_{i=1\ldots n}$, $(f^i)_{i=1\ldots n}$ dual basis pair with resp. to β.

$$\vartheta_\ell := \sum_{\substack{\varphi : \{1 \ldots \ell\} \\ \to \{1 \ldots n\}}} f_{1\varphi} \otimes f^{1\varphi} \otimes \ldots \otimes f_{\ell\varphi} \otimes f^{\ell\varphi}$$

Fact: $\vartheta_\ell \in [V^{\otimes 2\ell}]^G$

(σ_k, ρ_k commute)

$$\Rightarrow \vartheta_\ell^{S_{2\ell}} := \{\vartheta_\ell \, \sigma_{2\ell}(s) : s \in S_{2\ell}\} \subseteq [V^{\otimes 2\ell}]^G$$

FFT:

$$[V^{\otimes 2\ell}]^G = \mathrm{span}_{\mathbb{C}} (\vartheta_\ell^{S_{2\ell}})$$

Reduction to combinatorics :

the orthogonal case

$\mathcal{M}(\ell) :=$ { Partitions of $\{1, \dots, 2\ell\}$ into two-element subsets }

$m_0 := \{\{1,2\}, \{3,4\}, \dots, \{2\ell-1, 2\ell\}\}$

Observe: Let $s \in S_{2\ell}$. Then

$$\vartheta_\ell \, \sigma_{2\ell}(s) = \vartheta_\ell \iff m_0 s = m_0$$

Cor.: $(\mathcal{M}(\ell), S_{2\ell}) \cong (\vartheta_\ell^{S_{2\ell}}, S_{2\ell})$

Lemma: $n \geq \ell$ (i.e. $2n \geq k$)

$\Rightarrow$ The orbit $\vartheta_\ell^{S_{2\ell}}$ is a basis of $[V^{\otimes 2\ell}]^G$

$$\boxed{\begin{array}{l}\text{Cor: If } n \geq \ell \text{, then for } s \in S_{2\ell} \\[1em] \quad \operatorname{Tr}\left(s|_{[V^{\otimes 2\ell}]^G}\right) = \#\text{ fixed points of } s \text{ in } \mathcal{M}(\ell)\end{array}}$$

Reduction to combinatorics:

the symplectic case

Problem: The above strategy is not directly applicable, because two different bases are involved in the definition of ϑ_ℓ.

Solution: Define both bases starting with the same symplectic basis of V

i.e. $b_1, c_1, b_2, c_2, \ldots, b_m, c_m$

$$\beta(b_i, b_j) = \beta(c_i, c_j) = 0$$

$$\beta(b_i, c_i) = 1, \quad \beta(b_i, c_j) = 0 \quad (i \neq j)$$

Set $f_{2i-1} := b_i, \quad f_{2i} := c_i$

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

Problem: ϑ_ℓ contains the summand

$$\mathcal{F} := f_1 \otimes f^1 \otimes f_3 \otimes f^3 \otimes \dots \otimes f_{2\ell-1} \otimes f^{2\ell-1}$$

$$= b_1 \otimes c_1 \otimes b_2 \otimes c_2 \otimes \dots \otimes b_\ell \otimes c_\ell ,$$

and $\mathcal{F}(12) = c_1 \otimes b_1 \otimes b_2 \otimes c_2 \otimes \dots \otimes b_\ell \otimes c_\ell$

$$= - f_2 \otimes f^2 \otimes f_3 \otimes f^3 \otimes \dots \otimes f_{2\ell-1} \otimes f^{2\ell-1}$$

$\therefore$ $\vartheta_\ell s = \vartheta_\ell$

$\Updownarrow$

$m_0 s = m_0$

and s preserves a suitably defined sign of this two-partition

Finally one obtains

If $n \geq k$, then for $s \in S_{2\ell}$

$$\mathrm{Tr}\left(s\big|_{[V^{\otimes 2\ell}]^G} \right) = \mathrm{sgn}(s) \cdot \#\text{ fixed points of } s \text{ in } \mathcal{M}(\ell).$$

Theorem:

If $s \in S_{2\ell}$, $\mathrm{type}(s) = (1^{a_1} 2^{a_2} \ldots r^{a_r})$,

then

fixed points of s in $\mathcal{M}(\ell)$

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

where for $j \in \mathbb{N}$, $a \in \mathbb{N}_0^r$,

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

$[(2m-1)!! = (2m-1)(2m-3) \cdots 3 \cdot 1]$

Typical situations

$(1\ 2\ 3)(4\ 5\ 6)$

fixes $\{\{1,4\},\{2,5\},\{3,6\}\}$,

$\{\{1,5\},\{2,6\},\{3,4\}\}$,

$\{\{1,6\},\{2,4\},\{3,5\}\}$

$(1\ 2\ 3\ 4\ 5\ 6)$

fixes $\{\{1,4\},\{2,5\},\{3,6\}\}$

Observe: Given a permutation in cycle representation, typically there are several ways to group cycles of equal length into pairs (or leave them single).

Example:

$(1\ 2)(3\ 4)(5\ 6)(7\ 8\ 9)(10\ 11\ 12)$