A generating function approach to the enumeration of matrices in classical groups over finite fields

Jason Fulman, Peter M. Neumann, and Cheryl E. Praeger

Author address:

Department of Math, University of Pittsburgh, Pittsburgh, PA 15260, USA
E-mail address: fulman@math.pitt.edu

The Queen's College, Oxford OX1 4AW, England
E-mail address: peter.neumann@queens.oxford.ac.uk

Department of Mathematics and Statistics, University of Western Australia, Crawley, WA 6009, Australia
E-mail address: praeger@maths.uwa.edu.au

Contents

Abstract

Generating function techniques are used to study the probability that an element of a classical group defined over a finite field is separable, cyclic, semisimple or regular. The limits of these probabilities as the dimension tends to infinity are calculated in all cases, and exponential convergence to the limit is proved. These results complement and extend earlier results of the authors, G. E. Wall, and Guralnick & Lübeck.

Received by the editor September 8, 2003, and in revised form May 18, 2004.

1991 *Mathematics Subject Classification.* Primary 05E15; Secondary 20G40.

Key words and phrases. Generating function, finite classical group, cyclic matrix, regular element, semisimple element.

Much of this research took place while the authors were participants in the Research in Pairs Programme in Oberwolfach in 1998. We thank the Oberwolfach institute for their hospitality, generosity, and support. The first-named author gratefully acknowledges the support of a National Science Foundation Postdoctoral Fellowship and NSA Grant MDA 904-03-1-0049.

CHAPTER 1

Introduction, Tables, and Preliminaries

1.1. Introduction

An $n \times n$ matrix X over a field F is said to be *separable* if its characteristic polynomial $c_X(t)$ is separable (in the sense that it has no repeated roots in the algebraic closure of F), *semisimple* if its minimal polynomial $m_X(t)$ is separable, *cyclic* if $c_X(t)$ is equal to the minimal polynomial $m_X(t)$, and *regular* if its centraliser in the corresponding algebraic group over the algebraic closure of F has dimension equal to the Lie rank of the group. The term cyclic recognises that X is cyclic in this sense if and only if the vector space of $1 \times n$ row vectors over F is cyclic as a right $F\langle X\rangle$-module. In most (but not quite all) classical groups an element is cyclic if and only if it is regular; an element is separable if and only if it is regular and semisimple; and over a finite field an element is semisimple if and only if it is a p'-element, where p is the characteristic of the field.

Throughout this paper we treat matrix groups over the finite field $\mathbb{F}_q$, thinking of q as fixed but allowing the dimension to grow large. Our aim is to give accurate estimates for the probability that an element of a classical group over $\mathbb{F}_q$ is of one of the above kinds. In almost all cases these probabilities are of the form $1 - aq^{-1} + b(n)q^{-2}$ or $1 - aq^{-3} + b(n)q^{-4}$ (depending on the codimension of the variety of matrices that do not have the relevant property), where a is a constant depending on the group and the property, and $b(n)$ depends on the dimension n of the group but is bounded above and below independently of n provided that n is large enough to avoid trivialities ($n > 1$ usually suffices). Thus these probabilities tend to 1 as $q \to \infty$ uniformly in n. Such estimates are not only of intrinsic interest: they have turned out to be useful for the design and analysis of algorithms in computational group theory [**16**], [**19**]; further applications are to the study of monodromy groups of curves [**7**], [**8**], [**10**], and to random generation of simple groups [**9**].

The paper is in three chapters. The first consists of

- Section 1.1 (this section), containing an overview of the results,
- Section 1.2, containing summary tables,
- Section 1.3, in which preliminaries are collected.

Most of the latter is devoted to a discussion of the polynomials that arise as characteristic polynomials of matrices in classical groups. The second chapter consists of

- Section 2.1, on the unitary groups,
- Section 2.2, on the symplectic groups,
- Section 2.3, on the orthogonal groups,

which are devoted to extending the methods of Wall [**23**] to treat the probabilities of separable and cyclic matrices in the named groups. The third chapter consists of

- Section 3.1, on semisimple matrices,
- Section 3.2, on regular matrices in orthogonal groups.

An explanation of context and a discussion of some open problems are included in this introductory section.

Background. Before amplifying our aims and ambitions, we recall some earlier work (Fulman [**5**], [**6**]; Guralnick & Lübeck [**12**]; Neumann & Praeger [**17**], [**18**]; Wall [**23**]) about separable and cyclic matrices. Let $\mathrm{M}(n,q)$ denote the set of all $n \times n$ matrices over $\mathbb{F}_q$. Denote by $s_{\mathrm{M}}(n,q)$, $s_{\mathrm{GL}}(n,q)$ the proportion of separable elements in $\mathrm{M}(n,q)$, $\mathrm{GL}(n,q)$ respectively, and by $c_{\mathrm{M}}(n,q)$, $c_{\mathrm{GL}}(n,q)$ the corresponding proportions of cyclic matrices. The main results of [**17**] are the bounds

$$1 - \frac{1}{(q^2-1)(q-1)} < c_{\mathrm{M}}(n,q) < 1 - \frac{1}{q^2(q+1)}\,,$$
$$1 - \frac{q^2}{(q^2-1)(q-1)} - \tfrac{1}{2}q^{-2} - \tfrac{2}{3}q^{-3} < s_{\mathrm{M}}(n,q) < 1 - q^{-1} + q^{-2} + q^{-3},$$

which hold for $n \geqslant 2$. Let $s_{\mathrm{M}}(\infty,q)$, $s_{\mathrm{GL}}(\infty,q)$, $c_{\mathrm{M}}(\infty,q)$, $c_{\mathrm{GL}}(\infty,q)$ be the limits of the proportions defined above as $n \to \infty$. Using generating function techniques, it was proved independently in [**6**] and [**23**] that these limits exist and that

$$s_{\mathrm{M}}(\infty,q) = \prod_{r\geqslant 1}(1-q^{-r})\,, \qquad c_{\mathrm{M}}(\infty,q) = (1-q^{-5})\prod_{r\geqslant 3}(1-q^{-r})\,,$$

and

$$s_{\mathrm{GL}}(\infty,q) = 1 - q^{-1}\,, \qquad c_{\mathrm{GL}}(\infty,q) = \frac{1-q^{-5}}{1+q^{-3}}\,.$$

In [**23**] the following explicit estimate for speed of convergence was obtained:

$$|c_{\mathrm{GL}}(n,q) - c_{\mathrm{GL}}(\infty,q)| \leqslant \frac{1}{q^n(q-1)}\,,$$

and it was shown that in fact the convergence rate is very nearly q^{-2n} in the sense that $|c_{\mathrm{GL}}(n,q) - c_{\mathrm{GL}}(\infty,q)| = o(r^{-n})$ for any r in the range $1 < r < q^2$.

In what follows we consider the situation in other classical groups. We use n to denote the dimension of the group, while for the symplectic and orthogonal groups it is also convenient to use the parameter m specified in Table 1 (see p. 7). Thus the classical groups other than GL are:

the unitary group $\mathrm{U}(n,q)$ (as a subgroup of $\mathrm{GL}(n,q^2)$);
the symplectic group $\mathrm{Sp}(2m,q)$;
the orthogonal group $\mathrm{O}(2m+1,q)$;
the orthogonal groups $\mathrm{O}^+(2m,q)$ and $\mathrm{O}^-(2m,q)$.

The results of [**17**] are extended in [**18**] to these groups. It is proved there that if G is a classical subgroup of $\mathrm{GL}(n,q)$ (or, in the case of the unitary groups $\mathrm{U}(n,q)$,

a subgroup of $\mathrm{GL}(n,q^2)\big)$ and $\nu(G) := \mathrm{Prob}\,[X \in G \text{ is non-cyclic}]$, then

$$\nu(G) \leqslant \begin{cases} q^{-3}+O(q^{-4}) & \text{if } \mathrm{SL}(n,q) \leqslant G \leqslant \mathrm{GL}(n,q), \\ q^{-3}+O(q^{-4}) & \text{if } \mathrm{SU}(n,q) \leqslant G \leqslant \mathrm{GU}(n,q), \\ (\tau(G)+1)q^{-3}+O(q^{-4}) & \text{if } \mathrm{Sp}(2m,q) \leqslant G \leqslant \mathrm{GSp}(2m,q), \\ \frac{1}{2}\tau(G)q^{-1}+O(q^{-2}) & \text{if } \Omega(n,q) \leqslant G \leqslant \mathrm{GO}(n,q), \end{cases}$$

where the constants implicit in the O notation depend on the type of the group G but not on n, and the numbers $\tau(G)$ take values 1 or 2 in the symplectic case, 1, 2 or 4 in the orthogonal case. Here $\mathrm{GU}(n,q)$, $\mathrm{GSp}(n,q)$, and $\mathrm{GO}(n,q)$ denote the "general classical groups", that is, the subgroup of the general linear group consisting of all matrices which leave the relevant form invariant modulo scalars. Similar results for separable elements have been proved by Guralnick and Lübeck [**12**]. They prove that if $r'(G) := \mathrm{Prob}\,[X \in G \text{ is non-separable}]$ then

$$r'(G) \leqslant \begin{cases} (q-1)^{-1}+2(q-1)^{-2} & \text{if } G \sim \mathrm{SL}(n,q) \\ (q-1)^{-1}+4(q-1)^{-2} & \text{if } G \sim \mathrm{SU}(n,q) \\ (\tau(G)+1)(q-1)^{-1}+(q-1)^{-2} & \text{if } G \sim \mathrm{Sp}(2m,q) \\ (q-1)^{-1}+2(q-1)^{-2} & \text{if } G \sim \mathrm{O}^{\pm}(2m,q) \\ 2(q-1)^{-1}+2(q-1)^{-2} & \text{if } G \sim \mathrm{O}(2m+1,q),\ q \text{ odd} \end{cases}$$

where $\tau(G)$ is the same as for cyclic matrices, and $G \sim \mathrm{X}(n,q)$ means that G is an almost simple classical group of type X, and, in each case, the bounds may be a little different for a few small values of n.

In the present paper we extend the methods of Fulman and Wall for separable and cyclic matrices to the classical groups other than GL; we also extend them for all the classical groups (including GL) to two other important types of matrices, namely semisimple and regular elements. These extensions turn out to be rather delicate and non-trivial, especially for the orthogonal groups and for semisimple elements. In each case, if p_n is the relevant probability for $n \times n$ matrices, our aims are

(i) to prove the existence of the limit p_∞ of p_n as $n \to \infty$, and to find an expression for it as a function of the field size q;
(ii) where p_∞ is given by a complicated infinite product, to find effective upper and lower bounds as simple functions of q;
(iii) to find explicit estimates for the convergence rate of p_n to the limit, that is for the difference $|p_n - p_\infty|$.

With respect to aims (ii) and (iii) we are guided by the ambition to derive estimates which are sufficiently accurate that they may be used to yield good estimates for the probabilities p_n themselves.

Because the methods of Wall and Fulman are based on careful study of generating functions for the probabilities p_n, we have as a subsidiary aim

(iv) to understand the generating functions in some detail and, in particular, to find extensions of them from the unit disc in the complex plane (their

natural domain of definition) to larger discs in which the functions have a pole at $z = 1$, and perhaps a few other poles, but are otherwise analytic.

These larger discs will usually have radius q or q^2. Their boundaries will, in fact, be natural boundaries for the functions (in the sense that there is no analytic extension to any larger domain than the open disc), but we do not prove such facts.

Separable matrices and cyclic matrices. To complement the work of Wall and Fulman we treat separable and cyclic matrices first. We treat them together because it turns out—somewhat surprisingly—that the relevant probabilities are closely related. We use $s_G(n,q)$ to denote the probability that an element of the classical group $G(n,q)$ is separable, and $c_G(n,q)$ to denote the probability that it is cyclic. Our first objective is to compute the limits $s_G(\infty,q)$ and $c_G(\infty,q)$, as $n \to \infty$, and the rates of convergence to these limits, where G is one of U, Sp, O, O^+, O^-. That these limits exist is not *a priori* obvious, but emerges very naturally from the methods of Fulman and Wall. For the symplectic and orthogonal groups the limiting probabilities depend on whether the characteristic is 2 or not.

In contrast to the case of $\mathrm{M}(n,q)$ and $\mathrm{GL}(n,q)$, we have been unable to find simple expressions for $s_G(\infty,q)$ and $c_G(\infty,q)$. Nevertheless, as will emerge, we do have formulae for them—see Theorems 2.1.3, 2.1.9, 2.2.3, 2.2.9, 2.3.4 and 2.3.11, or Tables 2 and 6 (our tables include the results for GL for comparison). Although these formulae are expressed as infinite products of complicated expressions, they can be used to give good estimates—see Theorems 2.1.4, 2.1.12, 2.2.6, 2.2.14, 2.3.5 and the last paragraph of §2.3, or Tables 4 and 8. From the form of the infinite products it is quite easy to see that they can be expanded to yield expressions for the limiting probabilities as power series in q^{-1}. Wall treats the series for the general linear group in some detail in [**23**, §7]. The papers by Lehrer [**13**] and Lehrer & Segal [**14**] give topological and cohomological interpretations of the coefficients of these power series. In particular, in [**13**] Lehrer gives interesting connections between $s_G(n,q)$ and representation theory of the Weyl group of G. The first ten terms of the power series are summarized in Tables 3 and 7.

The method allows one to estimate the rate of convergence to the limiting values. It is exponential in the following sense.

Let $G(n,q)$ be a finite classical group of dimension n over $\mathbb{F}_q$, and let m be related to n as in Table 1. Then for any $\varepsilon > 0$ there exists m_0 such that, for all $m \geqslant m_0$,

$$|s_G(n,q) - s_G(\infty,q)| < (q-\varepsilon)^{-m}$$

and

$$|c_G(n,q) - c_G(\infty,q)| < (q^2-\varepsilon)^{-m}.$$

This is a compendium of the last assertions of Theorems 2.1.3, 2.1.9, 2.2.3, 2.2.9, 2.3.4, and 2.3.11. Although it gives the "correct" rate of convergence in very crude terms, it is too inexplicit to be of much practical use. Exploiting Wall's method of comparison of power series we can deduce bounds of the form

$$|s_G(n,q) - s_G(\infty,q)| < k_{s,G}\, p_{s,G}(m)\, q^{-m}$$

and

$$|c_G(n,q) - c_G(\infty,q)| < k_{c,G}\, p_{c,G}(m)\, q^{-2m}$$

where $k_{s,G}$, $k_{c,G}$ are certain constants and $p_{s,G}$, $p_{c,G}$ are certain functions closely related to the partition function (see Theorems 2.1.6, 2.1.11, 2.2.5, 2.2.13, 2.3.6, 2.3.8, 2.3.12, and 2.3.13). These lead to weaker but quite explicit bounds which are also given in those theorems and listed in Tables 5 and 9.

Semisimple matrices. For a classical group G define $ss_G(n,q)$ to be the proportion of semisimple matrices in G. As has been mentioned above, in [**12**] Guralnick and Lübeck derived upper bounds for $1 - s_G(n,q)$, which are very useful for large q, in order to have such bounds for $1 - ss_G(n,q)$. Their theorems carry little or no information when q is small, however. Using our generating function methods we are able to find good estimates for $ss_G(n,q)$ also for small values of q.

In [**6**], the limit as $n \to \infty$ of the probability that an element of $\mathrm{M}(n,q)$ or $\mathrm{GL}(n,q)$ is semisimple was computed in terms of Rogers–Ramanujan type products. In §3.1 we find analogous products for $ss_G(\infty,q)$ and we give estimates for the rate of convergence to this limit. Although the expressions for the limits are even more complicated than those for the probabilities of separable or of cyclic matrices, they can be used to give explicit bounds and to express the limiting probabilities $ss_G(\infty,q)$ as power series in q^{-1}, the first few terms of which we have computed. Bounds for the rate of convergence have also been computed. The results for semisimple matrices are summarized in Tables 10 to 13.

Regular elements. Recall that an element of a finite classical group G of characteristic p is called *regular* if its centraliser in the corresponding group over an algebraic closure of $\mathbb{F}_p$ has minimal possible dimension, namely the rank of G. A theorem of Steinberg [**20**] states that the non-regular elements form a variety of codimension 3. For this reason (see [**17**]) one should expect that for large n the probability that an element of $G(n,q)$ is regular would be $1 - c\,q^{-3} + O(q^{-4})$ for some constant c.

For the general linear, unitary and symplectic groups it is quite well known that an element is regular if and only if it is cyclic. In orthogonal groups however, the concepts differ. Both are important. Whereas cyclic elements are useful for computational group theory, regular elements play an important role in the representation theory of algebraic groups and of finite groups of Lie type. Examples of non-cyclic regular elements in even-dimensional orthogonal groups appeared in the last section of [**17**]. The distinction between cyclic and regular elements of the finite orthogonal groups has been clarified in [**11**]. By way of contrast with Steinberg's theorem the non-cyclic matrices form a subvariety of codimension 1 in an orthogonal group.

Let $r_{\mathrm{O}^\epsilon}(2m,q)$, $r_{\mathrm{O}}(2m+1,q)$ be the probabilities that elements of $\mathrm{O}^\epsilon(2m,q)$, or of $\mathrm{O}(2m+1,q)$ respectively, are regular, and define

$$r_{\mathrm{O}^\epsilon}(\infty,q) := \lim_{m\to\infty} r_{\mathrm{O}^\epsilon}(2m,q)\,, \quad r_{\mathrm{O}}(\infty,q) := \lim_{m\to\infty} r_{\mathrm{O}}(2m+1,q)\,.$$

In §3.2 we find expressions for these limiting probabilities. They may, as usual, be expanded as power series in q^{-1}, and we give the first few terms in Table 14.

When q is even there is a natural isomorphism $\mathrm{O}(2m+1,q) \cong \mathrm{Sp}(2m,q)$, and this carries regular elements of $\mathrm{O}(2m+1,q)$ bijectively to cyclic elements of $\mathrm{Sp}(2m,q)$. Thus when q is even $r_{\mathrm{O}}(2m+1,q) = c_{\mathrm{Sp}}(2m,q)$ and $r_{\mathrm{O}}(\infty,q) = c_{\mathrm{Sp}}(\infty,q)$.

Open problems. Let $p_G(\infty, q)$ denote any of the limiting probabilities treated in this paper. As was mentioned above, it was proved by Wall [**23**] and by Fulman [**6**] that the numbers $s_{\mathrm{GL}}(\infty, q)$ and $c_{\mathrm{GL}}(\infty, q)$ (limiting probabilities for separable and cyclic matrices respectively in $\mathrm{GL}(n, q)$) are rational functions of q.

PROBLEM 1. *Which others of the numbers $p_G(\infty, q)$ are rational functions of q?*

It is tempting to believe that at least $s_{\mathrm{U}}(\infty, q)$ and $c_{\mathrm{U}}(\infty, q)$ should be rational because the generating functions associated with the unitary groups are very closely related to those for the general linear groups (see Theorem 2.1.13), but we have been unable to settle the matter even in this case.

In all cases there is an expansion $p_G(\infty, q) = 1 - a_1 q^{-1} + a_2 q^{-2} + \cdots$ as a power series in q^{-1}.

PROBLEM 2. *Investigate the nature of the coefficients when $p_G(\infty, q)$ is expressed as a power series in q^{-1}.*

As far as we can calculate we find that the coefficients of powers of q^{-1} are integers for all of these limits, except for orthogonal groups where in some cases the coefficients are fractions with denominator 2 or 4. For separable matrices this has been proved and explained by Lehrer [**13**] (in the general linear case) and by Lehrer and Segal [**14**] (in general) in terms of cohomology and representation theory. For some of the probabilities for unitary groups it has recently been proved by one of us (JEF). But much about integrality remains to be proved and explained. It would, moreover, be valuable and interesting to have explicit information about the rate of growth of the coefficients.

In the case of semisimple matrices in $\mathrm{GL}(n, q)$ there is a remarkable formula for the limiting probability that was proved by Fulman [**5, 6**]:

$$ss_{\mathrm{GL}}(\infty, q) = \prod_{\substack{r \geqslant 1, \\ r \equiv 0, \pm 2 \pmod 5}} \frac{(1 - q^{1-r})}{(1 - q^{-r})}\,.$$

An important ingredient in the proof is a version of one of the Rogers–Ramanujan identities, namely the formula

$$1 + \sum_{n \geqslant 1} \frac{1}{|\mathrm{GL}(n, q)|} = \prod_{\substack{m \geqslant 1, \\ m \equiv \pm 1 \pmod 5}} \frac{1}{1 - q^{-m}}\,.$$

Sums analogous to the left side of this identity occur in our formulae for limiting probabilities of semisimple elements in other classical groups. This motivates the following question.

PROBLEM 3. *Are there analogues of the Rogers–Ramanujan identities that express*

$$1 + \sum_{n \geqslant 1} \frac{1}{|\mathrm{U}(n, q)|}\,, \qquad 1 + \sum_{m \geqslant 1} \frac{1}{|\mathrm{Sp}(2m, q)|}$$

and

$$1 + \sum_{m \geqslant 1} \Big(\frac{1}{|\mathrm{O}^+(2m, q)|} + \frac{1}{|\mathrm{O}^-(2m, q)|} \Big)$$

in a useful way as infinite products?

As has already been stated, our methods are developed from those of Fulman [**6**] and Wall [**23**]. They are differ significantly from those of Neumann & Praeger [**18**] and Guralnick & Lübeck [**12**] and they give significantly different results. On the one hand the generating function methods give far greater precision; on the other hand we have been able to succeed with them only for the classical groups themselves, and not for any other groups G in the range $\Omega \leqslant G \leqslant \mathrm{G}\Omega$, where Ω is the simple algebraic group that is normal in G and $\mathrm{G}\Omega$ is its normaliser (the so-called 'conformal' group) in the general linear group. In an earlier draft of this paper we had formulated as a fourth problem the need to develop a method for handling the generating functions associated with these other groups. Good progress on this has, however, recently been made by John Britnell in work for his Oxford DPhil thesis (see [**3**], [**4**]). For another approach to Britnell's results, using combinatorics of maximal tori, see [**8**].

1.2. Tables

Although in our studies of separable and cyclic matrices our focus is on the unitary, symplectic and orthogonal groups we include results about GL in our tables for comparison and for completeness. They are taken from Fulman [**5**], [**6**] and Wall [**23**].

$G =$	GL	U	Sp	O	O^ϵ
$n =$	m	m	$2m$	$2m+1$	$2m$

TABLE 1. Relationship between m and n.

Note that the group orders are given by

$$|\mathrm{GL}(n,q)| = \prod_{i=0}^{n-1}(q^n - q^i); \quad |\mathrm{U}(n,q)| = \prod_{i=0}^{n-1}(q^n - (-1)^{n-i}q^i)\,;$$

$$|\mathrm{Sp}(2m,q)| = \prod_{i=1}^{m} q^{2i-1}(q^{2i}-1); \quad |\mathrm{O}(2m+1,q)| = 2\prod_{i=1}^{m} q^{2i-1}(q^{2i}-1)\,;$$

$$|\mathrm{O}^\epsilon(2m,q)| = 2(q^m - \epsilon 1)\prod_{i=1}^{m-1} q^{2i}(q^{2i}-1) \quad \text{where } \epsilon \in \{+,-\}\,.$$

Group G	q	Limiting probability $s_G(\infty, q)$
$\mathrm{GL}(n,q)$	any	$1-\frac{1}{q}$
$\mathrm{U}(n,q)$	any	$\left(1+\frac{1}{q}\right)\prod_{d\,\mathrm{odd}}\left(1-\frac{2}{q^d(q^d+1)}\right)^{\widetilde{N}(q;d)}$
	any	$\frac{q^2-1}{q^2+1}\prod_{d\,\mathrm{odd}}\left(1-\frac{1}{(q^d+1)^2}\right)^{\widetilde{N}(q;d)}\prod_{d\geqslant 1}\left(1+\frac{1}{q^{4d}-1}\right)^{\widetilde{M}(q;d)}$
$\mathrm{Sp}(2m,q)$	odd	$\left(1-\frac{1}{q}\right)^2\prod_{d\geqslant 1}\left(1-\frac{2}{q^d(q^d+1)}\right)^{N^*(q;2d)}$
	even	$\left(1-\frac{1}{q}\right)\prod_{d\geqslant 1}\left(1-\frac{2}{q^d(q^d+1)}\right)^{N^*(q;2d)}$
	odd	$\frac{q(q-1)^3}{(q^2-1)^2}\prod_{d\geqslant 1}\left(1-\frac{1}{(q^d+1)^2}\right)^{N^*(q;2d)}\times\prod_{d\geqslant 1}\left(1+\frac{1}{(q^{2d}-1)}\right)^{M^*(q;d)}$
	even	$\frac{(q-1)^2}{(q^2-1)}\prod_{d\geqslant 1}\left(1-\frac{1}{(q^d+1)^2}\right)^{N^*(q;2d)}\times\prod_{d\geqslant 1}\left(1+\frac{1}{(q^{2d}-1)}\right)^{M^*(q;d)}$
$\mathrm{O}(2m+1,q)$	any	$s_{\mathrm{Sp}}(\infty,q)$
$\mathrm{O}^{\pm}(2m,q)$	odd	$s_{\mathrm{Sp}}(\infty,q)$
$\mathrm{O}^{\pm}(2m,q)$	even	$\frac{1}{2}s_{\mathrm{Sp}}(\infty,q)$

TABLE 2. Separable matrix limiting probabilities.

The numbers $\widetilde{M}$, $\widetilde{N}$, M^*, N^* enumerate certain kinds of irreducible polynomials—see Section 1.3, pp. 23, 26. For unitary and symplectic groups two forms are given. Theorems 2.1.3, 2.2.3 and 2.3.4 refer.

Group G	q	Limiting probability $s_G(\infty, q)$ mod $O(q^{-10})$
$\mathrm{GL}(n,q)$	any	$1 - q^{-1}$
$\mathrm{U}(n,q)$	any	$1 - q^{-1} - 2q^{-3} + 4q^{-4} - 6q^{-5} + 14q^{-6} - 28q^{-7} + 52q^{-8} - 106q^{-9} + \cdots$
$\mathrm{Sp}(2m,q)$	odd	$1 - 3q^{-1} + 5q^{-2} - 10q^{-3} + 23q^{-4} - 49q^{-5} + 100q^{-6} - 208q^{-7} + 439q^{-8} - 915q^{-9} + \cdots$
	even	$1 - 2q^{-1} + 2q^{-2} - 4q^{-3} + 9q^{-4} - 17q^{-5} + 32q^{-6} - 64q^{-7} + 130q^{-8} - 258q^{-9} + \cdots$
$\mathrm{O}(2m+1,q)$	any	$s_{\mathrm{Sp}}(\infty, q)$
$\mathrm{O}^{\pm}(2m,q)$	odd	$s_{\mathrm{Sp}}(\infty, q)$
$\mathrm{O}^{\pm}(2m,q)$	even	$\frac{1}{2} s_{\mathrm{Sp}}(\infty, q)$

TABLE 3. Separable matrix limiting probabilities as power series.

Group G	q	$s_G(\infty, q)$ lower bound	$s_G(\infty, q)$ upper bound
$\mathrm{GL}(n,q)$	any	$1 - q^{-1}$	$1 - q^{-1}$
$\mathrm{U}(n,q)$	any	$1 - q^{-1} - 2q^{-3} + 2q^{-4}$	$1 - q^{-1} - 2q^{-3} + 6q^{-4}$
	2	0.4147	0.4157
	3	0.6283	0.6286
$\mathrm{Sp}(2m,q)$	odd	$1 - 2q^{-1} + 2q^{-2} - 4q^{-3} + 4q^{-4}$	$1 - 2q^{-1} + 2q^{-2} - 4q^{-3} + 9q^{-4}$
	even	$1 - 3q^{-1} + 5q^{-2} - 10q^{-3} + 12q^{-4}$	$1 - 3q^{-1} + 5q^{-2} - 10q^{-3} + 23q^{-4}$
	2	0.2833	0.2881
	3	0.3487	0.3493
$\mathrm{O}(2m+1,q)$	any	same as for $S_{\mathrm{Sp}}(\infty, q)$	same as for $S_{\mathrm{Sp}}(\infty, q)$
$\mathrm{O}^{\pm}(2m,q)$	odd	same as for $S_{\mathrm{Sp}}(\infty, q)$	same as for $S_{\mathrm{Sp}}(\infty, q)$
$\mathrm{O}^{\pm}(2m,q)$	even	$\frac{1}{2}\times$bound for $S_{\mathrm{Sp}}(\infty, q)$	$\frac{1}{2}\times$bound for $S_{\mathrm{Sp}}(\infty, q)$

TABLE 4. Explicit bounds for separable matrix limiting probabilities.

Theorems 2.1.4, 2.2.6 and 2.3.5 refer.

Group G	q	First bound	Second bound
$\mathrm{GL}(n,q)$	any	$\frac{3(q-1)}{(2q-3)}\, p_2(n)\, q^{-n}$	$\frac{8(q-1)}{(2q-3)}\, \left(\frac{2}{3}\, q\right)^{-n}$
$\mathrm{U}(n,q)$	any	$\frac{3(q+1)}{(2q-3)}\, p_2(n)\, q^{-n}$	$\frac{8(q+1)}{(2q-3)}\, \left(\frac{2}{3}\, q\right)^{-n}$
$\mathrm{Sp}(2m,q)$	odd	$\frac{3(q-1)}{(2q-3)}\, p_3(m)\, q^{-m}$	$\frac{23(q-1)}{(2q-3)}\, \left(\frac{2}{3}\, q\right)^{-m}$
$\mathrm{Sp}(2m,q)$	even	$\frac{3(q-1)}{(2q-3)}\, p_2(m)\, q^{-m}$	$\frac{8(q-1)}{(2q-3)}\, \left(\frac{2}{3}\, q\right)^{-m}$
$\mathrm{O}(2m+1,q)$	odd	same as $S_{\mathrm{Sp}}(2m,q)$	same as $S_{\mathrm{Sp}}(2m,q)$
$\mathrm{O}(2m+1,q)$	even	same as $S_{\mathrm{Sp}}(2m,q)$	same as $S_{\mathrm{Sp}}(2m,q)$
$\mathrm{O}^{\pm}(2m,q)$	odd	$\frac{3(q-1)(2q-1)}{2(2q-3)}\, p_3(m)\, q^{-m}$	$\frac{23(q-1)(2q-3)}{2(2q-3)}\, \left(\frac{2}{3}\, q\right)^{-m}$
$\mathrm{O}^{\pm}(2m,q)$	even	$\frac{3(q-1)(q+2)}{2(2q-3)}\, p_2(m)\, q^{-m}$	$\frac{4(q-1)(q+2)}{2q-3}\, \left(\frac{2}{3}\, q\right)^{-m}$

TABLE 5. Convergence rates for separable matrices:

explicit upper bounds for $|s_G(\infty,q) - s_G(n,q)|$.

The second bound is weaker than the first but easier to compute.
The functions p_2 and p_3 are closely related to
the partition function—see Lemma 1.3.9.
Theorems 2.1.6, 2.2.5, 2.3.6 and 2.3.8 refer.

Group G	q	Limiting probability $c_G(\infty, q)$
$\mathrm{GL}(n,q)$	any	$\big(1-\frac{1}{q^5}\big)/\big(1+\frac{1}{q^3}\big)$
$\mathrm{U}(n,q)$	any	$\big(1+\frac{1}{q}\big)\prod_{d\,\mathrm{odd}}\big(1-\frac{1}{q^d(q^d+1)}\big)^{\widetilde{N}(q;d)} \times\prod_{d\geqslant 1}\big(1+\frac{1}{q^{2d}(q^{2d}-1)}\big)^{\widetilde{M}(q;d)}$
	any	$\big(1-\frac{1}{q^2}\big)\prod_{d\,\mathrm{odd}}\big(1+\frac{(q^d-1)}{q^{3d}(q^d+1)}\big)^{\widetilde{N}(q;d)} \times\prod_{d\geqslant 1}\big(1+\frac{1}{q^{6d}}\big)^{\widetilde{M}(q;d)}$
	any	$\frac{(q^2-1)(q^3-1)}{q(q^4+1)}\prod_{d\,\mathrm{odd}}\big(1+\frac{1}{(q^d+1)(q^{2d}-1)}\big)^{\widetilde{N}(q;d)} \times\prod_{d\geqslant 1}\big(1+\frac{1}{(q^{2d}-1)(q^{4d}+1)}\big)^{\widetilde{M}(q;d)}$
$\mathrm{Sp}(2m,q)$	any	$\prod_{d\geqslant 1}\big(1-\frac{1}{q^d(q^d+1)}\big)^{N^*(q;2d)}\prod_{d\geqslant 1}\big(1+\frac{1}{q^d(q^d-1)}\big)^{M^*(q;d)}$
	odd	$\frac{q^3(q^3-1)}{(q^2+1)(q^4-1)}\prod_{d\geqslant 1}\big(1+\frac{1}{(q^d+1)(q^{2d}-1)}\big)^{N^*(q;2d)} \times\prod_{d\geqslant 1}\big(1+\frac{1}{(q^d-1)(q^{2d}+1)}\big)^{M^*(q;d)}$
	even	$\frac{(q^3-1)}{q(q^2+1)}\prod_{d\geqslant 1}\big(1+\frac{1}{(q^d+1)(q^{2d}-1)}\big)^{N^*(q;2d)} \times\prod_{d\geqslant 1}\big(1+\frac{1}{(q^d-1)(q^{2d}+1)}\big)^{M^*(q;d)}$
$\mathrm{O}(2m+1,q)$	any	$\big(1-\frac{1}{q}\big)c_{\mathrm{Sp}}(\infty,q)$
$\mathrm{O}^{\pm}(2m,q)$	odd	$\big(1-\frac{1}{q}+\frac{1}{2q^2}\big)c_{\mathrm{Sp}}(\infty,q)$
$\mathrm{O}^{\pm}(2m,q)$	even	$\big(1-\frac{1}{2q}\big)c_{\mathrm{Sp}}(\infty,q)$

TABLE 6. Cyclic matrix limiting probabilities.

The numbers $\widetilde{M}$, $\widetilde{N}$, M^*, N^* enumerate certain kinds of irreducible polynomials—see Section 1.3, pp. 23, 26. For unitary groups three forms and for symplectic groups two forms are given. Theorems 2.1.9, 2.2.9 and 2.3.11 refer.

Group G	q	Limiting probability $c_G(\infty, q)$ mod $O(q^{-10})$
$\mathrm{GL}(n,q)$	any	$(1-q^{-5})/(1+q^{-3})$ $= 1-q^{-3}-q^{-5}+q^{-6}+q^{-8}-q^{-9}+\cdots$
$\mathrm{U}(n,q)$	any	$1-q^{-3}-q^{-5}+q^{-6}-2q^{-7}+3q^{-8}-5q^{-9}+\cdots$
$\mathrm{Sp}(2m,q)$	odd	$1-3q^{-3}+2q^{-4}-3q^{-5}+8q^{-6}$ $-11q^{-7}+19q^{-8}-32q^{-9}+\cdots$
	even	$1-2q^{-3}+q^{-4}-2q^{-5}+4q^{-6}$ $-5q^{-7}+9q^{-8}-14q^{-9}+\cdots$
$\mathrm{O}(2m+1,q)$	odd	$(1-q^{-1})\,c_{\mathrm{Sp}}(\infty,q)$ $= 1-q^{-1}-3q^{-3}+5q^{-4}-5q^{-5}+11q^{-6}$ $-19q^{-7}+30q^{-8}-51q^{-9}+\cdots$
	even	$(1-q^{-1})c_{\mathrm{Sp}}(\infty,q)$ $= 1-q^{-1}-2q^{-3}+3q^{-4}-3q^{-5}$ $+6q^{-6}-9q^{-7}+14q^{-8}-23q^{-9}+\cdots$
$\mathrm{O}^{\pm}(2m,q)$	odd	$(1-q^{-1}+\frac{1}{2}q^{-2})\,c_{\mathrm{Sp}}(\infty,q)$ $= 1-q^{-1}+\frac{1}{2}q^{-2}-3q^{-3}+5q^{-4}-\frac{13}{2}q^{-5}$ $+12q^{-6}-\frac{41}{2}q^{-7}+34q^{-8}-\frac{113}{2}q^{-9}+\cdots$
$\mathrm{O}^{\pm}(2m,q)$	even	$(1-\frac{1}{2}q^{-1})\,c_{\mathrm{Sp}}(\infty,q)$ $= 1-\frac{1}{2}q^{-1}-2q^{-3}+2q^{-4}-\frac{5}{2}q^{-5}$ $+5q^{-6}-7q^{-7}+\frac{23}{2}q^{-8}-\frac{37}{2}q^{-9}+\cdots$

TABLE 7. Cyclic matrix limiting probabilities as power series.

Group G	q	$c_G(\infty,q)$ lower bound	$c_G(\infty,q)$ upper bound
$\mathrm{GL}(n,q)$	any	$(1-q^{-5})/(1+q^{-3})$	$(1-q^{-5})/(1+q^{-3})$
$\mathrm{U}(n,q)$	any	$(1-q^{-3})/(1+q^{-4})$	$1-q^{-3}$
$\mathrm{Sp}(2m,q)$	odd	$1-3q^{-3}+q^{-4}-q^{-5}$	$1-3q^{-3}+2q^{-4}+q^{-5}$
	even	$1-2q^{-3}-q^{-5}$	$1-2q^{-3}+q^{-4}+q^{-5}$
$\mathrm{O}(2m+1,q)$	any	$k_1\times$bound for $c_{\mathrm{Sp}}(\infty,q)$	$k_1\times$bound for $c_{\mathrm{Sp}}(\infty,q)$
$\mathrm{O}^{\pm}(2m,q)$	odd	$k_2\times$bound for $c_{\mathrm{Sp}}(\infty,q)$	$k_2\times$bound for $c_{\mathrm{Sp}}(\infty,q)$
$\mathrm{O}^{\pm}(2m,q)$	even	$k_3\times$bound for $c_{\mathrm{Sp}}(\infty,q)$	$k_3\times$bound for $c_{\mathrm{Sp}}(\infty,q)$

TABLE 8. Explicit bounds for cyclic matrix limiting probabilities.

Here $k_1 := 1-q^{-1}$, $k_2 := 1-q^{-1}+\frac{1}{2}q^{-2}$ and $k_3 := 1-\frac{1}{2}q^{-1}$.
Theorems 2.1.12, 2.2.14, 2.3.11 (and 2.3.14) refer.

Group G	q	First bound	Second bound
$\mathrm{GL}(n,q)$	any	$\frac{3(q-1)}{2q^2-3}\,p_2(n)\,q^{-2n}$	$\frac{8(q-1)}{2q^2-3}\left(\frac{2}{3}\,q^2\right)^{-n}$
$\mathrm{U}(n,q)$	any	$\frac{3(q+1)}{2q^2-3}\,p_2(n)\,q^{-2n}$	$\frac{8(q+1)}{2q^2-3}\left(\frac{2}{3}\,q^2\right)^{-n}$
$\mathrm{Sp}(2m,q)$	odd	$\frac{3(q-1)}{2q^2-3}\,p_3(m)\,q^{-2m}$	$\frac{23(q-1)}{2q^2-3}\left(\frac{2}{3}\,q^2\right)^{-m}$
$\mathrm{Sp}(2m,q)$	even	$\frac{3(q-1)}{2q^2-3}\,p_2(m)\,q^{-2m}$	$\frac{8(q-1)}{2q^2-3}\left(\frac{2}{3}\,q^2\right)^{-m}$
$\mathrm{O}(2m+1,q)$	odd	$\frac{3q(q-1)}{2q^2-3}\,p_3(m)\,q^{-2m}$	$\frac{23q(q-1)}{2q^2-3}\left(\frac{2}{3}\,q^2\right)^{-m}$
$\mathrm{O}(2m+1,q)$	even	$\frac{3(q^2-1)}{2q^2-3}\,p_2(m)\,q^{-2m}$	$\frac{8(q^2-1)}{2q^2-3}\left(\frac{2}{3}\,q^2\right)^{-m}$
$\mathrm{O}^{\pm}(2m,q)$	odd	$\frac{3q^2(q-1)}{2q^2-3}\,p_3(m)\,q^{-2m}$	$\frac{23q^2(q-1)}{2q^2-3}\left(\frac{2}{3}\,q^2\right)^{-m}$
$\mathrm{O}^{\pm}(2m,q)$	even	$\frac{3q^2(q-1)}{2q^2-3}\,p_2(m)\,q^{-2m}$	$\frac{8q^2(q-1)}{2q^2-3}\left(\frac{2}{3}\,q^2\right)^{-m}$

TABLE 9. Convergence rates for cyclic matrices:

explicit upper bounds for $|c_G(\infty,q)-c_G(n,q)|$.

The second bound is weaker than the first but easier to compute.
Theorems 2.1.11, 2.2.13, 2.3.12 and 2.3.13 refer.

Group G	q	Limiting probability $ss_G(\infty, q)$
$\mathrm{GL}(n,q)$	any	$\prod_{r\equiv 0,\,\pm 2 \pmod 5} \big((1-\frac{1}{q^{r-1}})\big)/\big((1-\frac{1}{q^r})\big)$
$\mathrm{U}(n,q)$	any	$\big(1+\frac{1}{q}\big)\prod_{d\text{ odd}} A_{q,d}(1)^{\widetilde{N}(q;d)}\prod_{d\geqslant 1} B_{q^2,d}(1)^{\widetilde{M}(q;d)}$
$\mathrm{Sp}(2m,q)$	odd	$\big(1-\frac{1}{q}\big)^2 F(1)^2\prod_{d\geqslant 1} A_{q,d}(1)^{N^*(q;2d)}\prod_{d\geqslant 1} B_{q,d}(1)^{M^*(q;d)}$
	even	$\big(1-\frac{1}{q}\big)F(1)\prod_{d\geqslant 1} A_{q,d}(1)^{N^*(q;2d)}\prod_{d\geqslant 1} B_{q,d}(1)^{M^*(q;d)}$
$\mathrm{O}(2m+1,q)$	odd	$\big(1-\frac{1}{q}\big)^2 F_+(1)F(1)$ $\times\prod_{d\geqslant 1} A_{q,d}(1)^{N^*(q;2d)}\prod_{d\geqslant 1} B_{q,d}(1)^{M^*(q;d)}$
	even	$s_{\mathrm{Sp}}(\infty,q)$
$\mathrm{O}^{\pm}(2m,q)$	odd	$\frac{1}{2}\big(F_+(1)^2+F(1)^2\big)\big(1-\frac{1}{q}\big)^2$ $\times\prod_{d\geqslant 1} A_{q,d}(1)^{N^*(q;2d)}\prod_{d\geqslant 1} B_{q,d}(1)^{M^*(q;d)}$
$\mathrm{O}^{\pm}(2m,q)$	even	$\frac{1}{2}F_+(1)\big(1-\frac{1}{q}\big)\prod_{d\geqslant 1} A_{q,d}(1)^{N^*(q;2d)}\prod_{d\geqslant 1} B_{q,d}(1)^{M^*(q;d)}$

TABLE 10. Semisimple matrix limiting probabilities.

The numbers $\widetilde{M}$, $\widetilde{N}$, M^*, N^* enumerate certain kinds of irreducible polynomials—see Section 1.3;
$A_{q,d}(1)=\big(1-\frac{1}{q^d}\big)\big(1+\sum_{m\geqslant 1}\frac{1}{|\mathrm{U}(m,q^d)|}\big)$;
$B_{q,d}(1)=\big(1-\frac{1}{q^d}\big)\big(1+\sum_{m\geqslant 1}\frac{1}{|\mathrm{GL}(m,q^d)|}\big)$;
$F_+(1)=1+\sum_{m\geqslant 1}\big(\frac{1}{|\mathrm{O}^-(m,q)|}+\frac{1}{|\mathrm{O}^+(m,q)|}\big)$
$F(1)=1+\sum_{m\geqslant 1}\frac{1}{|\mathrm{Sp}(m,q)|}$; —see Section 3.1.
Theorems 3.1.13, 3.1.15 and 3.1.18 refer.

Group G	q	Limiting probability $ss_G(\infty, q)$ mod $O(q^{-10})$
$\mathrm{GL}(n,q)$	any	$1 - q^{-1} + q^{-3} - 2q^{-4} + 2q^{-5} - q^{-6} - q^{-7} + 3q^{-8} - 4q^{-9} + \cdots$
$\mathrm{U}(n,q)$	any	$1 - q^{-1} - q^{-3} + 2q^{-4} - 2q^{-5} + 5q^{-6} - 9q^{-7} + 11q^{-8} - 20q^{-9} + \cdots$
$\mathrm{Sp}(2m,q)$	odd	$1 - 3q^{-1} + 5q^{-2} - 7q^{-3} + 11q^{-4} - 19q^{-5} + 32q^{-6} - 56q^{-7} + 104q^{-8} - 195q^{-9} + \cdots$
	even	$1 - 2q^{-1} + 2q^{-2} - 2q^{-3} + 3q^{-4} - 5q^{-5} + 8q^{-6} - 15q^{-7} + 29q^{-8} - 52q^{-9} + \cdots$
$\mathrm{O}(2m+1,q)$	odd	$1 - 2q^{-1} + 2q^{-2} - 2q^{-3} + 3q^{-4} - 5q^{-5} + 8q^{-6} - 16q^{-7} + 34q^{-8} - 64q^{-9} + \cdots$
	even	$ss_{\mathrm{Sp}}(\infty, q)$
$\mathrm{O}^{\pm}(2m,q)$	odd	$1 - 2q^{-1} + \frac{5}{2}q^{-2} - \frac{7}{2}q^{-3} + \frac{11}{2}q^{-4} - \frac{19}{2}q^{-5} + \frac{33}{2}q^{-6} - \frac{61}{2}q^{-7} + \frac{117}{2}q^{-8} - \frac{215}{2}q^{-9} + \cdots$
	even	$\frac{1}{2} - \frac{1}{2}q^{-1} + \frac{1}{2}q^{-6} - 2q^{-7} + \frac{9}{2}q^{-8} - \frac{15}{2}q^{-9} + \cdots$

TABLE 11. Semisimple matrix limiting probabilities as power series.

Group G	q	$ss_G(\infty, q)$ lower bound	$ss_G(\infty, q)$ upper bound
$\mathrm{GL}(n, q)$	any	$1 - q^{-1} + q^{-3} - 2q^{-4}$	$1 - q^{-1} + q^{-3}$
$\mathrm{U}(n, q)$	any	$1 - q^{-1} - q^{-3} - 2q^{-4}$	$1 - q^{-1} - q^{-3} + 3q^{-4}$
	2	0.4698	0.4724
	3	0.6498	0.6501
$\mathrm{Sp}(2m, q)$	odd	$1 - 3q^{-1} + 5q^{-2} - 7q^{-3} + 6q^{-4}$	$1 - 3q^{-1} + 5q^{-2} - 7q^{-3} + 13q^{-4}$
	even	$1 - 2q^{-1} + 2q^{-2} - 2q^{-3} + q^{-4}$	$1 - 2q^{-1} + 2q^{-2} - 2q^{-3} + 5q^{-4}$
	2	0.3476	0.3481
	3	0.3819	0.3821
$\mathrm{O}(2m+1, q)$	odd	$1 - 2q^{-1} + 2q^{-2} - 2q^{-3} - 2q^{-4}$	$1 - 2q^{-1} + 2q^{-2} - 2q^{-3} + 7q^{-4}$
	3	0.5046	0.5053
$\mathrm{O}^{\pm}(2m, q)$	odd	$1 - 2q^{-1} + \frac{5}{2}q^{-2} - \frac{7}{2}q^{-3}$	$1 - 2q^{-1} + \frac{5}{2}q^{-2} - \frac{7}{2}q^{-3} + \frac{21}{2}q^{-4}$
	3	0.5244	0.5252
$\mathrm{O}^{\pm}(2m, q)$	even	$\frac{1}{2}\big(1 - q^{-1} - 3q^{-4}\big)$	$\frac{1}{2}\big(1 - q^{-1} + 5q^{-4}\big)$
	2	0.2513	0.2515

TABLE 12. Explicit bounds for semisimple matrix limiting probabilities.

Theorems 3.1.14, 3.1.17 and 3.1.20 refer.

Group G	q	First bound	Second bound
$\mathrm{GL}(n,q)$	any	$\frac{3(q-1)}{2q-3}\, p_2(n) q^{-n}$	$\frac{8(q-1)}{2q-3}\, \left(\frac{2}{3}\, q\right)^{-n}$
$\mathrm{U}(n,q)$	any	$\frac{3(q+1)}{2q-3}\, p_4(n) q^{-n}$	$\frac{63(q+1)}{2q-3}\, \left(\frac{2}{3}\, q\right)^{-n}$
$\mathrm{Sp}(2m,q)$	odd	$\frac{3(q+1)}{2q-3}\, p_3(m)\, q^{-m}$	$\frac{23(q+1)}{2q-3}\, \left(\frac{2}{3}\, q\right)^{-m}$
$\mathrm{Sp}(2m,q)$	even	$\frac{12q^2(q+1)}{(2q-3)(2q^2-3)}\, p_3(m)\, q^{-m}$	$\frac{92q^2(q+1)}{(2q-3)(2q^2-3)}\, \left(\frac{2}{3}\, q\right)^{-m}$
$\mathrm{O}(2m+1,q)$	odd	same as for $\mathrm{Sp}(2m,q)$	same as for $\mathrm{Sp}(2m,q)$
$\mathrm{O}(2m+1,q)$	even	same as for $\mathrm{Sp}(2m,q)$	same as for $\mathrm{Sp}(2m,q)$
$\mathrm{O}^{\pm}(2m,q)$	odd	$\frac{9(q+1)^2}{2(2q-3)}\, p_3(m)\, q^{-m}$	$\frac{69(q+1)^2}{2(2q-3)}\, \left(\frac{2}{3}\, q\right)^{-m}$
$\mathrm{O}^{\pm}(2m,q)$	even	$\frac{6q^2(q+1)(q+2)}{(2q-3)(2q^2-3)}\, p_3(m)\, q^{-m}$	$\frac{46q^2(q+1)(q+2)}{(2q-3)(2q^2-3)}\, \left(\frac{2}{3}\, q\right)^{-m}$

TABLE 13. Convergence rates for semisimple matrices:

explicit upper bounds for $|ss_G(\infty,q) - ss_G(n,q)|$.

The second bound is weaker than the first but easier to compute.
Theorems 3.1.22, 3.1.24, 3.1.27, 3.1.29 and 3.1.31 refer.

Group G	q	Limiting probability $r_G(\infty,q)$
$\mathrm{O}(2m+1,q)$	odd	$\left(1+\frac{1}{q^2(q+1)}\right) c_{\mathrm{Sp}}(\infty,q)$ $= 1 - 2q^{-3} + q^{-4} - 2q^{-5} + 4q^{-6} - 5q^{-7} + 10q^{-8} - 15q^{-9} + \cdots$
$\mathrm{O}(2m+1,q)$	even	$c_{\mathrm{Sp}}(\infty,q)$ $= 1 - 2q^{-3} + q^{-4} - 2q^{-5} + 4q^{-6} - 5q^{-7} + 9q^{-8} - 14q^{-9} + \cdots$
$\mathrm{O}^{\pm}(2m,q)$	odd	$\left(1+\frac{1}{q^2(q+1)}+\frac{1}{2q^4(q+1)^2}\right) c_{\mathrm{Sp}}(\infty,q)$ $= 1 - 2q^{-3} + q^{-4} - 2q^{-5} + \frac{9}{2}q^{-6} - 6q^{-7} + \frac{23}{2}q^{-8} - \frac{37}{2}q^{-9} + \cdots$
$\mathrm{O}^{\pm}(2m,q)$	even	$\left(1+\frac{1}{2q^2(q+1)}\right) c_{\mathrm{Sp}}(\infty,q)$ $= 1 - \frac{3}{2}q^{-3} + \frac{1}{2}q^{-4} - \frac{3}{2}q^{-5} + \frac{5}{2}q^{-6} - 3q^{-7} + 6q^{-8} - 9q^{-9} + \cdots$

TABLE 14. Regular orthogonal matrix limiting probabilities.

Theorems 3.2.3 and 3.2.5 refer.

1.3. Preliminaries

We shall be working with power series generating functions expressed as infinite products and with the characteristic and minimal polynomials of matrices in classical groups. The tools needed come from analysis and from the combinatorial theory of polynomials over finite fields. Some are well known, others less familiar. They are collected in this section in the forms most appropriate for our purposes.

Recall (see, for example, Ahlfors [**1**], Ch. 5, §2.2, pp. 189–191) that (if $a_n \neq -1$ for all n then) $\prod_n(1+a_n)$ is said to *converge* if there exists $l \neq 0$ such that $\prod_{n=1}^N(1+a_n) \to l$ as $N \to \infty$; it is said to *converge absolutely* if $\prod_{n=1}^N(1+|a_n|)$ converges. A product which converges absolutely certainly converges. Moreover, if the terms a_n are analytic functions of a complex variable u and convergence is uniform over a domain D in the complex plane then the limit will be analytic over D. A basic criterion for absolute convergence replaces products with sums:

LEMMA 1.3.1. *The following are equivalent:*

(a) $\prod(1+a_n)$ *converges absolutely* (*and uniformly over* D);
(b) $\sum\log(1+a_n)$ *converges absolutely* (*and uniformly over* D);
(c) $\sum|a_n|$ *converges absolutely* (*and uniformly over* D).

The form in which this is most useful in our work is

COROLLARY 1.3.2. *The product* $\prod\big(1+a_n(u)\big)^{m(n)}$, *where the exponents* $m(n)$ *are non-negative integers, converges absolutely* (*and uniformly over* D) *if and only if* $\sum m(n)\,|a_n(u)|$ *converges* (*uniformly over* D).

We write $D(R)$ throughout for the open disc $\{u \in \mathbb{C} \mid |u| < R\}$. In determining the limiting probabilities of the generating functions considered in this paper, we shall sometimes use the following standard result about analytic functions.

LEMMA 1.3.3. *Suppose that* $g(u) = \sum_{n\geqslant 0} a_n u^n$ *and* $g(u) = f(u)/(1-u)$ *for* $|u| < 1$. *If* $f(u)$ *is analytic in* $D(R)$, *where* $R > 1$, *then* $\lim_{n\to\infty} a_n = f(1)$ *and* $|a_n - f(1)| = o(r^{-n})$ *for any* r *such that* $1 < r < R$.

Proof. Define $F(1) := f'(1)$ and $F(u) := (f(1)-f(u))/(1-u)$ elsewhere in $D(R)$. Then F is analytic in that disc and must be represented by a Taylor series $\sum b_n u^n$ converging there. If $1 < r < R$ then $\sum b_n r^n$ converges and so $b_n r^n \to 0$ as $n \to \infty$, that is $|b_n| = o(r^{-n})$. Now $g(u) = f(1)/(1-u) - F(u)$ and therefore $a_n = f(1) - b_n$. Thus $a_n \to f(1)$ and $|a_n - f(1)| = o(r^{-n})$ as $n \to \infty$.

LEMMA 1.3.4. (a) *If* $0 \leqslant x \leqslant 1$ *and* $n \in \mathbb{N}$ *then*

$$1 - nx + \binom{n}{2}x^2 - \binom{n}{3}x^3 \leqslant (1-x)^n \leqslant 1 - nx + \binom{n}{2}x^2\,.$$

(b) *If* $0 < a_i < 1$ *for all* i *then* $\prod(1-a_i) \geqslant 1 - \sum a_i$.

Proof. The first of these is easily proved by elementary calculus or by induction on n. The second is proved for the finite case $\prod_1^n(1-a_i)$ by induction on n, and then for an infinite product by taking the limit as $n \to \infty$.

Following Wall [**23**], given formal power series $A(u) = \sum a_n u^n$ and $B(u) = \sum b_n u^n$, we write $A(u) \ll B(u)$ if $a_n \leqslant b_n$ for all n. We write $|A|(u)$ for the series $\sum|a_n|u^n$. In all cases of interest the power series that arise will converge in some neighbourhood of 0 in the complex plane, and then we work with the functions they represent. Care is needed: for example, it is not generally true that if

$A_1(u) \ll B_1(u)$ and $A_2(u) \ll B_2(u)$ then $A_1(u)A_2(u) \ll B_1(u)B_2(u)$. This is true, however, if $B_1(u)$, $B_2(u)$ are non-negative in the sense that all their coefficients are non-negative. In particular, if $A(u) = B(u)C(u)$ then $|A|(u) \ll |B|(u)\,|C|(u)$. It is not hard to see that these facts may be extended to infinite products. Similarly, it is not generally true that if $B_1(u) \ll B_2(u)$ then $A(B_1(u)) \ll A(B_2(u))$, but this does hold if $A(u)$, $B_1(u)$, $B_2(u)$ are non-negative.

LEMMA 1.3.5. (a) *If $a \geqslant 2$, $k \geqslant 1$ and $A(u) := (1 - au^k)/(1 - u)$ then $|A|(u) \ll (a - 1)/(1 - u)$.*

(b) *If $b \geqslant 2$, k is an even positive integer and $B(u) := (1 - bu^k)/(1 + u)$ then $|B|(u) \ll (b - 1)/(1 - u)$.*

(c) *Suppose that $C(u) = 1 + \sum_{n\geqslant 1} c_n u^n$ where $1 \geqslant c_1 \geqslant c_2 \geqslant \cdots \geqslant 0$. If $D(u) := C(u)/(1 + u)$ then $|D|(u) \ll 1/(1 - u)$.*

(d) *If $C(u) = \sum_{n\geqslant 0} c_n u^n$ where $c_n \geqslant 0$ for all n and $\sum c_n$ converges then $C(u)/(1 - u) \ll C(1)/(1 - u)$.*

Proof. For (a) note that the n^{th} coefficient of $A(u)$ is 1 if $0 \leqslant n \leqslant k - 1$ and is $-(a - 1)$ if $n \geqslant k$. Similarly, part (b) comes from the fact that the n^{th} coefficient of $B(u)$ is $(-1)^n$ if $0 \leqslant n \leqslant k - 1$ and is $(-1)^{n-1}(b - 1)$ if $n \geqslant k$.

For (c) write $D(u)$ as $1 + \sum_{n\geqslant 1} d_n u^n$. Then $d_n = (-1)^n\big(1 - c_1 + c_2 - \cdots + (-1)^n c_n\big)$. If n is even then

$$(1 - c_1) + \cdots + (c_{n-2} - c_{n-1}) + c_n = (-1)^n d_n = 1 - (c_1 - c_2) - \cdots - (c_{n-1} - c_n)\,,$$

while if n is odd then

$$(1 - c_1) + \cdots + (c_{n-1} - c_n) = (-1)^n d_n = 1 - (c_1 - c_2) - \cdots - (c_{n-2} - c_{n-1}) - c_n\,.$$

Thus $0 \leqslant (-1)^n d_n \leqslant 1$ and so $|D|(u) \ll 1 + \sum_{n\geqslant 1} u^n$, that is, $|D|(u) \ll 1/(1-u)$.

For (d) note that $C(u)/(1 - u) = \sum_{n\geqslant 0} d_n\, u^n$ where $d_n := \sum_{0\leqslant m\leqslant n} c_m \leqslant C(1)$, and so $C(u)/(1 - u) \ll C(1) \sum_{n\geqslant 0} u^n = C(1)/(1 - u)$.

LEMMA 1.3.6. *For each natural number n let c_n, d_n be real numbers and let m_n, r_n, s_n be non-negative integers. Define*

$$A(u) := \prod_n \Big(1 + \frac{c_n\, u^{r_n}}{1 + d_n\, u^{s_n}}\Big)^{m_n}.$$

Then

$$|A|(u) \ll \exp\Big(\sum_n \frac{m_n\,|c_n|\,u^{r_n}}{1 - |d_n|u^{s_n}}\Big)\,.$$

Proof. For a function $g(u)$ represented by a non-negative power series we have $1 + g(u) \ll \exp g(u)$, and as these are again represented by non-negative power series $(1+g(u))^m \ll \exp(mg(u))$ for non-negative integers m. If $B(u)$ is the power series expansion of $cu/(1+du)$ for real numbers c, d, then $|B|(u) = |c|u/(1-|d|u)$. It follows that if

$$C(u) := \Big(1 + \frac{c_n\, u^{r_n}}{1 + d_n\, u^{s_n}}\Big)^{m_n}$$

then

$$|C|(u) \ll \Big(1 + \frac{|c_n|\, u^{r_n}}{1 - |d_n|u^{s_n}}\Big)^{m_n} \ll \exp\Big(\frac{m_n\,|c_n|\,u^{r_n}}{1 - |d_n|u^{s_n}}\Big)\,,$$

and therefore that $|A|(u) \ll \exp\Big(\sum_n \dfrac{m_n\,|c_n|\,u^{r_n}}{1-|d_n|u^{s_n}}\Big)$, as the lemma states.

Just as in Wall's work, the technique of comparison of power series, applied to our generating functions, leads via the following lemma to the function $\Omega(u)$ defined by

$$\Omega(u) := \prod_{i\geqslant 1}(1-u^i)\,.$$

LEMMA 1.3.7. $$\exp\Big(\sum_{m\geqslant 1}\frac{1}{m}\,\frac{u^m}{1-u^m}\Big) = \Omega(u)^{-1}\,.$$

Proof. (See, for example, Wall [**23**, p. 272] or Apostol [**2**, p. 317].)

$$\begin{aligned}\log\Omega(u)^{-1} &= -\sum_{i\geqslant 1}\log(1-u^i) = \sum_{i\geqslant 1}\sum_{m\geqslant 1}\frac{u^{im}}{m}\\ &= \sum_{m\geqslant 1}\frac{1}{m}\sum_{i\geqslant 1}u^{im} = \sum_{m\geqslant 1}\frac{1}{m}\frac{u^m}{1-u^m}\,,\end{aligned}$$

and applying the exponential function gives the required result.

Let $p(n)$ be the number of partitions of n and let $p_r(n)$ for $r \geqslant 1$ be defined inductively by the prescription $p_1(n) := p(n)$ and $p_r(n) := 1 + \sum_{m=1}^{n} p_{r-1}(m)$ for $r > 1$. By a well-known theorem of Euler $\Omega(u)^{-1} = 1 + \sum_{n\geqslant 1} p(n)\,u^n$. The following has a straightforward inductive proof:

LEMMA 1.3.8. *If $r \geqslant 0$ then* $$\frac{1}{(1-u)^r}\,\Omega(u)^{-1} = 1 + \sum_{n\geqslant 1} p_{r+1}(n)\,u^n\,.$$

Since the product defining $\Omega(u)$ converges for $|u| < 1$, given $c > 1$ the series $\sum p(n)c^{-n}$ converges and therefore there exists $k > 0$ such that $p(n) \leqslant kc^n$ for all n. We shall need explicit forms of this inequality; we shall also need similar bounds for the functions $p_r(n)$.

LEMMA 1.3.9. *For $r := 1, 2, 3, \ldots$ let $p_r(n)$ be the function derived from summing the partition function $p(n)$ as above. Then:*

(a) *$p(n) \leqslant \frac{3}{2}p(n-1)$ for $n \geqslant 7$;*

(b) *$p(n) \leqslant (\frac{3}{2})^n$ for $n \geqslant 0$;*

(c) *for $r \geqslant 1$ there exists $N(r)$ such that $p_r(n) \leqslant \frac{3}{2}p_r(n-1)$ for $n \geqslant N(r)$;*

(d) *for $r \geqslant 1$ there exists $k(r) > 0$ such that $p_r(n) \leqslant k(r)\,(\frac{3}{2})^n$ for $n \geqslant 0$;*

(e) *for small r the following values of $N(r)$ and $k(r)$ are best possible:*

r:	1	2	3	4	5
$N(r)$:	7	7	10	12	14
$k(r)$:	1	$\frac{640}{243}$	$\frac{145\,408}{19\,683}$	$\frac{1\,230\,848}{59\,049}$	$\frac{94\,429\,184}{1\,594\,323}$
$k(r)$:	1	$2.633\cdots$	$7.387\cdots$	$20.844\cdots$	$59.228\cdots$
$k'(r)$:	1	8/3	23/3	21	178/3

The last line of this table records a number $k'(r)$, more convenient for our purposes than $k(r)$, for which $p_r(n) \leqslant k'(r)\,(\frac{3}{2})^n$ for $n \geqslant 0$.

Proof. Of course, clauses (a) and (b) are special cases of (c) and (d) respectively. We have picked them out for special mention because of their special importance and because they provide the base step of a proof by induction.

Define $p_0(n)$ to be the number of partitions of n that have no parts of size 1. Clearly $p(n) = p(n-1) + p_0(n)$ and we propose to show that $p_0(n) \leqslant \frac{1}{3}p(n)$ if $n \geqslant 7$. Given a partition λ with no parts of size 1 define new partitions λ' and λ'' as follows: λ' is the same as λ except that its smallest part a has been replaced by parts 1 and $a-1$; λ'' is the same as λ except that its largest part b has been replaced by b parts equal to 1. Then $\lambda' = \mu'$ if and only if $\lambda = \mu$ and similarly $\lambda'' = \mu''$ if and only if $\lambda = \mu$. Moreover, if n is odd then there are no coincidences amongst partitions λ, μ', ν'' (for partitions λ, μ, ν without parts of size 1), while if n is even then there is precisely one such coincidence, namely $\mu' = \nu''$ when $\mu = \nu = \frac{1}{2}n \times 2$ (that is, μ and ν consist of $\frac{1}{2}n$ parts of size 2). Thus $p(n) \geqslant 3p_0(n) - 1$ for $n \geqslant 1$. If $n \geqslant 7$ then there are partitions such as $3 \times 1 + (n-3)$ which are not of the form λ, λ' or λ'' where λ has no parts of size 1. Consequently $p(n) \geqslant 3p_0(n)$ if $n \geqslant 7$.

It follows immediately that $p(n) \leqslant p(n-1) + \frac{1}{3}p(n)$ if $n \geqslant 7$, whence $p(n) \leqslant \frac{3}{2}p(n-1)$, as stated in (a). That $p(n) \leqslant (\frac{3}{2})^n$ for $n \leqslant 6$ may be verified directly, and then (b) follows by induction from (a).

To prove (c) and (d) we proceed by induction on r. The generating function $\sum p_r(n)u^n$ is expressible as $(1-u)^{-(r-1)}\Omega(u)^{-1}$, and this is analytic in the unit disc $D(1)$. It follows that $\sum p_r(n)(\frac{2}{3})^n$ converges, and so certainly there must exist n_0 such that $p_r(n_0) \leqslant \frac{3}{2}p_r(n_0-1)$. If $n \geqslant \max\{N(r-1),\, n_0\}$ then

$$p_r(n) = p_r(n_0) + \sum_{m=n_0+1}^{n} p_{r-1}(m) \leqslant p_r(n_0) + \tfrac{3}{2}\sum_{m=n_0}^{n-1} p_{r-1}(m)\,,$$

that is, $p_r(n) \leqslant p_r(n_0) - \frac{3}{2}p_r(n_0-1) + \frac{3}{2}p_r(n-1)$, and so $p_r(n) \leqslant \frac{3}{2}p_r(n-1)$. This proves (c), and (d) follows immediately with

$$k(r) := \max\{p_r(n)(\tfrac{2}{3})^n \;\big|\; 0 \leqslant n \leqslant N(r)\}\,.$$

The verification of (e) is now routine and is left to the reader.

Although one might expect elementary facts like (a) and (b) to go back to Euler in the mid-eighteenth century we do not know if or where exactly they are to be found in the literature. A famous theorem of Hardy & Ramanujan tells us that $p(n) \sim \mathrm{e}^{\pi\sqrt{2n/3}}/(4\sqrt{3}n)$ as $n \to \infty$. Comparing the sum with an integral and using integration by parts one sees that $p_2(n) \sim \mathrm{e}^{\pi\sqrt{2n/3}}/(2\pi\sqrt{2n})$, that $p_3(n) \sim \sqrt{3}\mathrm{e}^{\pi\sqrt{2n/3}}/(2\pi^2)$ as $n \to \infty$, and that analogous formulae may be worked out for $p_r(n)$ in general. Several of our estimates below are of the form $|E_n| < k_0 \sum_{m>n} p_r(m)Q^{-m}$, where E_n is the difference between a member of a sequence and its limit, r is at most 5, and Q is q or q^2. Since $p_r(m+1) \leqslant \frac{3}{2}p_r(m)$ for large m such estimates yield that

$$|E_n| < k_0\, p_r(n)Q^{-n} \sum_{m\geqslant 1} (\tfrac{2}{3}Q)^{-m} = k\, p_r(n)Q^{-n}\,,$$

where $k := 3k_0/(2Q-3)$. Thus we have $|E_n| < KQ^{-(n-c\sqrt{n})}$ for suitable constants K and c. In this form these estimates are inexplicit in that we are unable to calculate appropriate values for K. There are explicit estimates with quite elementary

proofs, such as the bound $p(n) < \mathrm{e}^{\pi\sqrt{2n/3}}$ (see, for example, [**2**, Theorem 14.5]). They are, however, not quite as easy to exploit as the bounds given in Lemma 1.3.9 and, as the latter are more than adequate for practical purposes, we shall not need the more sophisticated theorems.

We turn now to polynomials over finite fields. For $d \geqslant 1$ let $N(q;d)$ denote the number of monic irreducible polynomials $\phi(t)$ of degree d over $\mathbb{F}_q$ for which $\phi(0) \neq 0$, that is, monic irreducible polynomials other than t. These numbers may be expressed using the Möbius function μ. Recall that for a positive integer n,

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n = p_1 p_2 \cdots p_r \text{ where } p_1, p_2, \ldots, p_r \\ & \text{are distinct prime numbers;} \\ 0 & \text{if } n \text{ is not square-free.} \end{cases}$$

LEMMA 1.3.10. (a) $N(q;1) = q-1$, *and if* $d > 1$, *then*

$$N(q;d) = \frac{1}{d}\sum_{r|d} \mu(r) q^{d/r} = \frac{1}{d}\, q^d - O(q^{d/2})\,.$$

(b) $$\prod_{d\geqslant 1} (1-u^d)^{-N(q;d)} = \frac{1-u}{1-qu} \quad \textit{for } |u| < q^{-1}\,.$$

(c) $$\prod_{d\geqslant 1} (1+u^d)^{-N(q;d)} = \frac{(1+u)(1-qu)}{1-qu^2} \quad \textit{for } |u| < q^{-1}\,.$$

Proof. Assertion (a) is well known (see for example [**15**, Theorem 3.25]). Assertion (b) is to be found in [**23**, p. 258] and is easily seen to be equivalent to [**6**, Lemma 4]. Since it provides a model for later theorems we nevertheless give a proof. Write $\prod_{d\geqslant 1}(1-u^d)^{-N(q;d)}$ as $\prod_\phi (1 + u^{\deg(\phi)} + u^{2\deg(\phi)} + \cdots)$ where ϕ ranges over monic irreducible polynomials such that $\phi(0) \neq 0$ (that is, monic irreducible polynomials $\phi(t)$ other than t). Expanding the product and using unique factorization we see that for $n \geqslant 1$ the coefficient of u^n is the number of monic polynomials $f(t)$ of degree n over $\mathbb{F}_q$ such that $f(0) \neq 0$, hence $q^n - q^{n-1}$. Since $N(q;d) < q^d/d$, by Corollary 1.3.2 the product converges for $|u| < q^{-1}$. The series $1 + \sum_{n\geqslant 1}(q^n - q^{n-1})u^n$ also converges for $|u| < q^{-1}$ and its sum is $(1-u)/(1-qu)$. Expansion of the product is valid whenever it, its factors, and the result all converge absolutely, and therefore (b) holds as an equality between complex functions for $|u| < q^{-1}$. Assertion (c) follows from (b) and the fact that $1 + x = (1-x^2) \div (1-x)$.

Next we consider the characteristic and minimal polynomials of matrices in the unitary groups. Since $\mathrm{U}(n,q)$ is a subgroup of $\mathrm{GL}(n,q^2)$, the relevant polynomials are monic polynomials over the field $\mathbb{F}_{q^2}$. The map $\sigma : x \mapsto x^q$ is an involutory automorphism of $\mathbb{F}_{q^2}$ and it induces an automorphism of the polynomial ring $\mathbb{F}_{q^2}[t]$ in an obvious way, namely $\sigma : \sum_{0\leqslant i\leqslant n} a_i t^i \mapsto \sum_{0\leqslant i\leqslant n} a_i^\sigma t^i$. An involutory map $\phi \mapsto \widetilde{\phi}$ is defined on those monic polynomials $\phi \in \mathbb{F}_{q^2}[t]$ that have non-zero constant coefficient, by

$$\widetilde{\phi}(t) := \phi(0)^{-\sigma} t^{\deg(\phi)} \phi^\sigma(t^{-1})\,.$$

Thus if

$$\phi(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$$

with $a_0 \neq 0$ then its $\sim$-conjugate is given by

$$\widetilde{\phi}(t) = t^n + (a_1 a_0^{-1})^\sigma t^{n-1} + \cdots + (a_{n-1} a_0^{-1})^\sigma t + (a_0^{-1})^\sigma \,,$$

and an element b in some extension field of $\mathbb{F}_{q^2}$ is a root of ϕ if and only if b^{-q} is a root of $\widetilde{\phi}$. We say that ϕ is *self-conjugate* (or $\sim$-self-conjugate) if $\phi(0) \neq 0$ and $\widetilde{\phi} = \phi$. In this case, an element b in some extension field of $\mathbb{F}_{q^2}$ is a root of ϕ if and only if b^{-q} is also a root; obviously, the roots b, b^{-q} are equal if and only if $b^{q+1} = 1$.

LEMMA 1.3.11. (a) *For $n \geqslant 1$, the number $\widetilde{P}(n)$ of self-conjugate monic polynomials ϕ of degree n in $\mathbb{F}_{q^2}[t]$ is $q^n + q^{n-1}$.*

(b) *If $\phi(t)$ is a self-conjugate monic irreducible polynomial over $\mathbb{F}_{q^2}$ then* $\deg(\phi)$ *is odd.*

Proof. Write n in the form $2k+\delta$, where δ is 0 or 1, and let $\phi(t) = \sum_{0 \leqslant i \leqslant n} a_i t^i$, with $a_n = 1$ and $a_0 \neq 0$. Then $\phi(t)$ is self-conjugate if and only if $a_{n-i} = (a_i a_0^{-1})^\sigma$ for $0 \leqslant i \leqslant k$. Thus all the coefficients of $\phi(t)$ are determined by $a_0, \ldots, a_k$. While $a_1, \ldots, a_{k-1}$ (and also a_k if n is odd) may be chosen arbitrarily, a_0 must satisfy $a_0^{q+1} = 1$. Thus if n is odd there are $q^n + q^{n-1}$ self-conjugate monic polynomials in $\mathbb{F}_{q^2}[t]$. If n is even then $a_k = (a_k a_0^{-1})^q$, whence either $a_k = 0$, or $a_k^{q-1} = a_0^q = a_0^{-1}$. For a given choice of a_0 (such that $a_0^{q+1} = 1$) the equation $a_k^{q-1} = a_0^{-1}$ has $q-1$ solutions for a_k. Thus in all there are q choices for a_k. Therefore when n is even there are $(q^2)^{k-1}(q+1)q$, that is, $q^n + q^{n-1}$ self-conjugate monic polynomials in $\mathbb{F}_{q^2}[t]$.

Now suppose that $\phi(t)$ is monic, self-conjugate and irreducible in $\mathbb{F}_{q^2}[t]$, and let $n := \deg(\phi)$. Let b be a root of ϕ in its splitting field K over $\mathbb{F}_{q^2}$ (so that b generates K over $\mathbb{F}_{q^2}$) and let Φ be the Frobenius automorphism $a \mapsto a^{q^2}$ of K. Then $\mathrm{ord}(\Phi) = |K : \mathbb{F}_{q^2}| = \deg(\phi) = n$. Since ϕ is self-conjugate b^{-q} is also a root of ϕ, and therefore there is an automorphism τ of K over $\mathbb{F}_{q^2}$ such that $\tau : b \mapsto b^{-q}$. Then $\tau^2 : b \mapsto b^{q^2}$ and so $\tau^2 = \Phi$. Since $\tau \in \langle \Phi \rangle \cong Z_n$, it follows that n is odd, as stated in (b).

Let $\widetilde{N}(q;d)$ denote the number of monic irreducible self-conjugate polynomials $\phi(t)$ of degree d over $\mathbb{F}_{q^2}$, and let $\widetilde{M}(q;d)$ denote the number of (unordered) conjugate pairs $\{\phi, \widetilde{\phi}\}$ of monic irreducible polynomials of degree d over $\mathbb{F}_{q^2}$ that are not self-conjugate.

LEMMA 1.3.12. *Let d be a positive integer.*

(a): ([**6**, Theorem 9]) *If d is even then $\widetilde{N}(q;d) = 0$, while if d is odd, then*

$$\widetilde{N}(q;d) = \frac{1}{d} \sum_{r|d} \mu(r)(q^{d/r} + 1) = \frac{1}{d}\, q^d - O(q^{d/3}) \,.$$

(b): ([**6**, Theorem 9])

$$\widetilde{M}(q;d) = \begin{cases} \frac{1}{2}(q^2 - q - 2) & \text{if } d = 1, \\ \dfrac{1}{2d} \displaystyle\sum_{r|d} \mu(r)(q^{2d/r} - q^{d/r}) & \text{if } d > 1 \text{ and } d \text{ is odd}, \\ \dfrac{1}{2d} \displaystyle\sum_{r|d} \mu(r) q^{2d/r} & \text{if } d \text{ is even}. \end{cases}$$

Thus $\widetilde{M}(q;d) = (q^{2d}/2d) - O(q^d)$.

COROLLARY 1.3.13. *If* $d > 1$ *then* $\widetilde{N}(q;d) = N(q;d)$ *if* d *is odd,* $\widetilde{N}(q;d) = 0$ *if* d *is even, and* $\widetilde{M}(q;d) = N(q;2d)$.

Proof. Suppose first that $d > 1$ and d is odd. By the lemma,

$$\widetilde{N}(q;d) = \frac{1}{d}\sum_{r|d} \mu(r)(q^{d/r}+1) = \frac{1}{d}\sum_{r|d} \mu(r)q^{d/r}$$

since $\displaystyle\sum_{r|d} \mu(r) = 0$ when $d > 1$. Thus $\widetilde{N}(q;d) = N(q;d)$. Also, from the definitions, $\widetilde{M}(q;d) = \frac{1}{2}\big(N(q^2;d) - \widetilde{N}(q;d)\big)$, and so

$$\begin{aligned}\widetilde{M}(q;d) &= \frac{1}{2d}\sum_{r|d} \mu(r)(q^{2d/r} - q^{d/r}) \\ &= \frac{1}{2d}\sum_{r|d} (\mu(r)q^{2d/r} + \mu(2r)q^{2d/2r}) = \frac{1}{2d}\sum_{r|2d} \mu(r)q^{2d/r}\,.\end{aligned}$$

Therefore $\widetilde{M}(q;d) = N(q;2d)$.

Now suppose that $d > 1$ and d is even. Then $\widetilde{N}(q;d) = 0$ and so $\widetilde{M}(q;d) = \frac{1}{2}N(q^2;d) = (2d)^{-1}\sum_{r|d} \mu(r)q^{2d/r}$. If $r \mid 2d$ and $r \nmid d$ then, since d is even, r is divisible by 4 and $\mu(r) = 0$. Therefore

$$\widetilde{M}(q;d) = (2d)^{-1}\sum_{r|d} \mu(r)q^{2d/r} = (2d)^{-1}\sum_{r|2d} \mu(r)q^{2d/r}\,,$$

and so $\widetilde{M}(q;d) = N(q;2d)$, as the corollary states.

The following infinite product expressions involving the numbers $\widetilde{N}(q;d)$ and $\widetilde{M}(q;d)$ are analogues of Lemma 1.3.10(b) and turn out to be fundamental for our calculations.

LEMMA 1.3.14. *For* $|u| < q^{-1}$,

(a) $$\prod_{d\,\text{odd}} (1-u^d)^{-\widetilde{N}(q;d)} \prod_{d\geqslant 1} (1-u^{2d})^{-\widetilde{M}(q;d)} = \frac{1+u}{1-qu}\,;$$

(b) $$\prod_{d\,\text{odd}} (1+u^d)^{-\widetilde{N}(q;d)} \prod_{d\geqslant 1} (1+u^{2d})^{-\widetilde{M}(q;d)} = \frac{(1+u^2)(1-qu)}{(1+u)(1-qu^2)}\,;$$

(c) $$\prod_{d\,\text{odd}} (1+u^d)^{-\widetilde{N}(q;d)} \prod_{d\geqslant 1} (1-u^{2d})^{-\widetilde{M}(q;d)} = \frac{1-u}{1+qu}\,;$$

(d) $$\prod_{d\,\text{odd}} \Big(\frac{1-u^d}{1+u^d}\Big)^{\widetilde{N}(q;d)} = \frac{(1-u)(1-qu)}{(1+u)(1+qu)}\,.$$

Proof. Define

$$B(u) := \prod_{d\,\text{odd}} (1-u^d)^{-\widetilde{N}(q;d)} \prod_{d\geqslant 1} (1-u^{2d})^{-\widetilde{M}(q;d)}\,.$$

Then

$$B(u) = \prod_{\phi=\widetilde{\phi}} \Big(1 + \sum_{n\geqslant 1} u^{n\deg(\phi)}\Big) \prod_{\phi\neq\widetilde{\phi}} \Big(1 + \sum_{n\geqslant 1} u^{2n\deg(\phi)}\Big)$$

where the polynomials ϕ are monic and irreducible with coefficients in $\mathbb{F}_{q^2}$ and the second product ranges over unordered pairs $\{\phi, \widetilde{\phi}\}$ such that $\phi \neq \widetilde{\phi}$. It is not hard to see that $B(u) = 1 + \sum_{d\geqslant 1} \widetilde{P}(d)\, u^d$, where $\widetilde{P}(d)$ is the number of monic polynomials f of degree d over $\mathbb{F}_{q^2}$, such that $f(0) \neq 0$ and $f = \tilde{f}$. By Lemma 1.3.11, this number is q^d+q^{d-1}. Substituting for $\widetilde{P}(d)$ and summing we find that $B(u) = (1+u)/(1-qu)$ as formal power series. But, just as in Lemma 1.3.10, by Corollary 1.3.2 the infinite products converge absolutely for $|u| < q^{-1}$ and so $B(u) = (1+u)/(1-qu)$ as functions of a complex variable u for $|u| < q^{-1}$, and this proves Part (a). To get (b) we use (a) twice, exploiting the fact that $(1+x) = (1-x^2)/(1-x)$. Substitution of $-u$ for u in (a) yields (c), and then (d) follows from (a) and (c) by division.

Now we consider the analogous theory for the symplectic groups $\mathrm{Sp}(n,q)$ and orthogonal groups $\mathrm{O}^\epsilon(n,q)$. Since these are subgroups of $\mathrm{GL}(n,q)$ the characteristic and minimal polynomials of their elements are monic polynomials over the field $\mathbb{F}_q$. For a monic polynomial $\phi(t) \in \mathbb{F}_q[t]$ of degree n with non-zero constant coefficient, we define the *$*$-conjugate* $\phi^*(t)$ by

$$\phi^*(t) := \phi(0)^{-1} t^n \phi(t^{-1}).$$

Thus if

$$\phi(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$$

then

$$\phi^*(t) = t^n + a_1 a_0^{-1} t^{n-1} + \cdots + a_{n-1}a_0^{-1} t + a_0^{-1};$$

moreover, an element b in some extension field of $\mathbb{F}_q$ satisfies $\phi(b) = 0$ if and only if it satisfies $\phi^*(b^{-1}) = 0$. We say that ϕ is *self-conjugate* (or $*$-self-conjugate) if $\phi(0) \neq 0$ and $\phi^* = \phi$. For a self-conjugate monic polynomial $\phi(t)$, an element b in some extension field of $\mathbb{F}_q$ is a root of ϕ if and only if b^{-1} is also a root. And of course $b^{-1} = b$ if and only if $b = \pm 1$.

This last observation points to the importance of ± 1 as roots of self-conjugate polynomials and therefore to a particular difference between fields of odd and of even characteristic: we define

$$e(q) := \begin{cases} 2 & \text{if } q \text{ is odd,} \\ 1 & \text{if } q \text{ is even,} \end{cases}$$

so that e is the number of square roots of 1 in $\mathbb{F}_q$.

LEMMA 1.3.15. (a) *If $\phi(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ then $\phi(t)$ is self-conjugate if and only if $a_0 = \pm 1$ and $a_{n-i} = a_0 a_i$ for $1 \leqslant i \leqslant n-1$. (In particular, if $a_0 = 1$ then $\phi(t)$ is self-conjugate if and only if it is palindromic.)*

(b) *For $n \geqslant 1$, let $P^*(n)$ be the number of monic self-conjugate polynomials $\phi(t)$ over $\mathbb{F}_q$ of degree n. Then*

$$P^*(n) = q^{\lfloor n/2 \rfloor} + (e-1)q^{\lfloor (n-1)/2 \rfloor},$$

where $e := e(q)$. Exactly $q^{\lfloor n/2 \rfloor}$ of these polynomials have constant term 1 (and, when q is odd, the rest have constant term -1).

(c) *If $\phi(t)$ is a monic self-conjugate irreducible polynomial over $\mathbb{F}_q$ then $\phi(t) = t+1$ or $\phi(t) = t-1$ or $\deg(\phi)$ is even.*

Proof. Let $\phi(t) = \sum_{0\leqslant i\leqslant n} a_i t^i$, with $a_n = 1$ and $a_0 \neq 0$. Then $\phi(t)$ is self-conjugate if and only if $a_{n-i} = a_i a_0^{-1}$ for $0 \leqslant i \leqslant n$. Taking i to be n we see that the constant coefficient a_0 satisfies $a_0^2 = 1$. Therefore $a_0 = \pm 1$ and $a_{n-i} = a_0 a_i$ for $0 \leqslant i \leqslant n$, and this proves (a).

Write n as $2k+\delta$, where δ is 0 or 1. All the coefficients of $\phi(t)$ are determined by $a_0, \ldots, a_k$. To define a monic self-conjugate polynomial $a_1, \ldots, a_{k-1}$ may be chosen arbitrarily. If n is odd then a_k may also be chosen arbitrarily and so $P^*(n) = eq^k$. If n is even then, since $a_k = a_0 a_k$, if $a_0 = 1$ then a_k may be chosen arbitrarily whereas if $a_0 \neq 1$ then $a_k = 0$. It follows that (when n is even) the number $P^*(n)$ of such polynomials is q^k if q is even and it is $q^k + q^{k-1}$ if q is odd. Thus the formula in (b) holds in all cases.

Now suppose that $\phi(t)$ is monic, irreducible and self-conjugate, and let b be a root of ϕ in some extension field of $\mathbb{F}_q$. Then, as we observed above, b^{-1} is also a root of ϕ. If for some root b we have $b = b^{-1}$, then as ϕ is irreducible, it follows that $\phi(t) = t \pm 1$. If this is not the case, then the roots occur in pairs and so $\deg(\phi)$ is even, as (c) states.

Let $N^*(q;d)$ denote the number of monic irreducible self-conjugate polynomials $\phi(t)$ of degree d over $\mathbb{F}_q$, and let $M^*(q;d)$ denote the number of (unordered) conjugate pairs $\{\phi, \phi^*\}$ of monic, irreducible non-self-conjugate polynomials of degree d over $\mathbb{F}_q$. The numbers $N^*(q;d)$ and $M^*(q;d)$ may be calculated as follows.

LEMMA 1.3.16. *Let d be a positive integer and let $e := e(q)$.*

(a) $$N^*(q;d) = \begin{cases} e & \text{if } d = 1, \\ 0 & \text{if } d \text{ is odd and } d > 1, \\ d^{-1} \displaystyle\sum_{r\mid d,\ r \text{ odd}} \mu(r)(q^{d/2r} + 1 - e) & \text{if } d \text{ is even.} \end{cases}$$

In particular, $N^*(q;d) = d^{-1}q^{d/2} + O(q^{d/6})$.

(b) $$M^*(q;d) = \begin{cases} \frac{1}{2}(q - e - 1) & \text{if } d = 1, \\ \frac{1}{2}N(q;d) & \text{if } d \text{ is odd and } d > 1, \\ \frac{1}{2}\big(N(q;d) - N^*(q;d)\big) & \text{if } d \text{ is even.} \end{cases}$$

In particular, $M^*(q;d) = (2d)^{-1}q^d + O(q^{d/2})$.

(c) $$N^*(q;2d) = \begin{cases} M^*(q;d) + 1 & \text{if } d = 1, \\ M^*(q;d) & \text{if } d \text{ is odd and } d > 1, \\ M^*(q;d) + N^*(q;d) & \text{if } d \text{ is even.} \end{cases}$$

Proof. By Lemma 1.3.15(c), $N^*(q;1) = e$ and $N^*(q;d) = 0$ if d is odd and $d > 1$. Suppose that d is even, say $d = 2m$. There is a bijection between the monic irreducible polynomials of degree d over $\mathbb{F}_q$ and the sets of roots of these polynomials, the latter being sets of algebraically conjugate elements of $\mathbb{F}_{q^d}$. Let $\phi(t)$ be a monic self-conjugate irreducible polynomial of degree d and let α be one of its roots in $\mathbb{F}_{q^d}$. Since ϕ is irreducible α generates $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$; since ϕ is self-conjugate α^{-1} is also a root of ϕ; since $d > 1$, $\alpha \neq \alpha^{-1}$. It follows that the assignment $\alpha \mapsto \alpha^{-1}$ extends to an automorphism σ of $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$ which is such

that $\sigma^2 = 1$ but $\sigma \neq 1$. The only involutory automorphism of $\mathbb{F}_{q^d}$ is the map $\tau : x \mapsto x^{q^m}$, and so $\sigma = \tau$, that is, $\sigma : x \mapsto x^{q^m}$ for all $x \in \mathbb{F}_{q^d}$. Therefore α satisfies $\alpha^{q^m+1} = 1$. Conversely, suppose that α generates $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$ and that $\alpha^{q^m+1} = 1$. Let ϕ be the minimal polynomial of α over $\mathbb{F}_q$. Then ϕ is monic and irreducible of degree d over $\mathbb{F}_q$. Moreover, if β is a root of ϕ then $\beta = \alpha^{q^i}$ for some i and so $\beta^{q^m+1} = 1$. Therefore $\beta^\tau = \beta^{-1}$ and since this is true of all the roots β, $\phi = \phi^*$. Thus the root-sets of self-conjugate monic irreducible polynomials of degree d over $\mathbb{F}_q$ are sets of d algebraically conjugate generators α of $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$ satisfying $\alpha^{q^m+1} = 1$ and it follows that

$$N^*(q;d) = \frac{1}{d}\left|\{\alpha \in \mathbb{F}_{q^d} \mid \alpha^{q^m+1} = 1 \text{ and } \alpha \text{ generates } \mathbb{F}_{q^d} \text{ over } \mathbb{F}_q\}\right|.$$

Consider elements $\alpha \in \mathbb{F}_{q^d}$ such that $\alpha^{q^m+1} = 1$ and $\alpha \neq \pm 1$. They are not fixed by τ and therefore $|\mathbb{F}_{q^d} : \mathbb{F}_q(\alpha)|$ is odd. For an odd divisor r of d define

$$E_r := \{\alpha \in \mathbb{F}_{q^{d/r}} \mid \alpha^{q^m+1} = 1 \text{ and } \alpha \neq \pm 1\}.$$

Then

$$E_r = \{\alpha \in \mathbb{F}_{q^d} \mid \alpha^{q^m+1} = 1,\ \alpha^{q^{d/r}-1} = 1 \text{ and } \alpha \neq \pm 1\}$$

and it follows that $|E_r| = \operatorname{hcf}(q^m+1, q^{d/r}-1) - e$, that is

$$|E_r| = \operatorname{hcf}(q^m+1, q^{2m/r}-1) - e = q^{m/r} + 1 - e.$$

Now α generates $\mathbb{F}_{q^d}$ if and only if

$$\alpha \in E_1 \setminus \Big(\bigcup \{E_r \mid r \mid m,\ r \text{ prime},\ r \text{ odd}\}\Big).$$

By the Inclusion-Exclusion Principle we therefore have that

$$N^*(q;d) = \sum_{r|m,\ r\,\text{odd}} \mu(r)(q^{m/r} + 1 - e),$$

and this completes the proof of (a). The asymptotic estimate follows immediately. Part (b) follows from (a) since $N(q;d) = N^*(q;d) + 2M^*(q;d)$.

To prove (c) we treat the cases d odd and d even separately. If $d = 1$ the result is immediate from (a) and (b). If $d > 1$ and d is odd then

$$M^*(q;d) = \frac{1}{2}N(q;d) = \frac{1}{2d}\sum_{r|d} \mu(r) q^{d/r},$$

and

$$\begin{aligned} N^*(q;2d) &= \frac{1}{2d} \sum_{r|2d,\ r\,\text{odd}} \mu(r)(q^{2d/2r} + 1 - e) \\ &= \frac{1}{2d}\sum_{r|d} \mu(r)(q^{d/r} + 1 - e). \end{aligned}$$

But $\sum_{r|d}\mu(r)=0$ since $d>1$, and so $N^*(q;2d)=M^*(q;d)$ as (c) states. Now suppose that d is even. Then

$$\begin{aligned}
&2d\big(N^*(q;2d)-M^*(q;d)\big)\\
&\quad=2d\,N^*(q;2d)-d\,N(q;d)+d\,N^*(q;d)\qquad\text{[by (b)]}\\
&\quad=\sum_{r|d,\ r\,\text{odd}}\mu(r)(q^{d/r}+1-e)-\sum_{r|d}\mu(r)q^{d/r}+\sum_{r|d,\ r\,\text{odd}}\mu(r)(q^{d/2r}+1-e)\\
&\quad=\sum_{r|d,\ r\,\text{odd}}\mu(r)q^{d/2r}-\sum_{r|d,\ r\,\text{even}}\mu(r)q^{d/r}+2\sum_{r|d,\ r\,\text{odd}}\mu(r)(1-e)\,.
\end{aligned}$$

Thus if $d=2m$ then

$$\begin{aligned}
&2d\big(N^*(q;2d)-M^*(q;d)\big)\\
&\qquad=\sum_{r|d,\ r\,\text{odd}}\mu(r)q^{m/r}-\sum_{s|m}\mu(2s)q^{m/s}+2\sum_{r|d,\ r\,\text{odd}}\mu(r)(1-e)\,.
\end{aligned}$$

But $\mu(2s)=0$ if s is even and $\mu(2s)=-\mu(s)$ if s is odd. Therefore

$$2d\big(N^*(q;2d)-M^*(q;d)\big)=2\sum_{r|m,\ r\,\text{odd}}\mu(r)q^{m/r}+2\sum_{r|d,\ r\,\text{odd}}\mu(r)(1-e)\,,$$

and it follows that $N^*(q;2d)-M^*(q;d)=N^*(q;d)$, as required.

There are important infinite product expressions analogous to those given in Lemmas 1.3.10 and 1.3.14.

LEMMA 1.3.17. *As usual, let $e:=e(q)$. If $|u|<q^{-1}$ then*

(a) $$\prod_{d\geqslant1}(1-u^d)^{-N^*(q;2d)}\prod_{d\geqslant1}(1-u^d)^{-M^*(q;d)}=\frac{(1-u)^e}{1-qu}\,;$$

(b) $$\prod_{d\geqslant1}(1+u^d)^{-N^*(q;2d)}\prod_{d\geqslant1}(1+u^d)^{-M^*(q;d)}=\frac{(1+u)^e(1-qu)}{1-qu^2}\,;$$

(c) $$\prod_{d\geqslant1}(1-u^d)^{-N^*(q;2d)}\prod_{d\geqslant1}(1+u^d)^{-M^*(q;d)}=\frac{(1-u)^{e-1}(1+u)^e}{1-qu^2}\,;$$

(d) $$\prod_{d\geqslant1}(1+u^d)^{-N^*(q;2d)}\prod_{d\geqslant1}(1-u^d)^{-M^*(q;d)}=1-u\,;$$

(e) $$\prod_{d\geqslant1}\left(\frac{1-u^d}{1+u^d}\right)^{N^*(q;2d)}=\frac{1-qu}{(1-u)^{e-1}}\,;$$

(f) $$\prod_{d\geqslant1}\left(\frac{1-u^d}{1+u^d}\right)^{M^*(q;d)}=\frac{(1+u)^e(1-qu)}{(1-u)(1-qu^2)}\,.$$

Proof. The proof of (a) is analogous to those of Lemmas 1.3.10(b) and 1.3.14(a). Define

$$B(z):=(1-z^2)^{-e}\prod_{d\geqslant1}(1-z^{2d})^{-N^*(q;2d)}\prod_{d\geqslant1}(1-z^{2d})^{-M^*(q;d)}\,.$$

Then

$$B(z) = \Big(1 + \sum_{m\geqslant 1} z^{2m}\Big)^e \prod_{\substack{\phi=\phi^*,\\ \deg(\phi)>1}} \Big(1 + \sum_{m\geqslant 1} z^{m\deg(\phi)}\Big) \prod_{\phi\neq\phi^*} \Big(1 + \sum_{m\geqslant 1} z^{2m\deg(\phi)}\Big)$$

where the polynomials ϕ are monic and irreducible with coefficients in $\mathbb{F}_q$. Multiplying out we find that the coefficient of z^n in $B(z)$ is 0 if n is odd and it is the number of self-conjugate monic polynomials f of degree n over $\mathbb{F}_q$ that are divisible by $(t-1)$ and $(t+1)$ with even multiplicity if n is even. These are precisely the self-conjugate monic polynomials f of degree n over $\mathbb{F}_q$ with $f(0) = 1$ and by Lemma 1.3.15 (b), there are exactly $q^{n/2}$ such polynomials. Thus $B(z) = 1 + \sum_{d\geqslant 1} q^d z^{2d} = 1/(1 - qz^2)$. Now replacing z^2 with u we obtain the required result as an equation between formal power series. Since $N^*(q; 2d) \sim (2d)^{-1}q^d$ and $M^*(q; 2d) \sim (2d)^{-1}q^d$ the infinite products and sums converge for $|u| < q^{-1}$ and so (a) holds as an equation between functions of the complex variable u in the open disc $D(q^{-1})$.

As in the unitary case, (b) follows immediately from (a) and the fact that $1 + x = (1 - x^2)/(1 - x)$. For (d) recall that $N(q; d) = N^*(q; d) + 2M^*(q; d)$, while $N^*(q; 1) = e$ and $N^*(q; d) = 0$ for odd $d > 1$. Substituting into Lemma 1.3.10(b) we find that

$$\prod_{d\geqslant 1} (1 - u^{2d})^{-N^*(q;2d)} \prod_{d\geqslant 1} (1 - u^d)^{-2M^*(q;d)} = \frac{(1-u)^{1+e}}{(1-qu)}\,.$$

Part (d) follows immediately from this and Part (a) by division. Substituting u^2 for u in (a) and dividing each side of the equation by the corresponding expression in (d) yields (c). Parts (e) and (f) follow from (a) and (d), and from (a) and (c) respectively, by division.

Remark 1.3.18. Parts (c), (d) may be interpreted as equations between functions of a complex variable valid in the open disc $D(q^{-1/2})$.

In the case of (c) the product $\prod_{d\geqslant 1} (1 - u^d)^{-N^*(q;2d)} \prod_{d\geqslant 1} (1 + u^d)^{-M^*(q;d)}$ may be rewritten as $\prod_{d\geqslant 1} (1 - u^{2d})^{-N^*(q;2d)} \prod_{d\geqslant 1} (1 + u^d)^{N^*(q;2d)-M^*(q;d)}$. Since $N^*(q; 2d) \sim q^d/2d$ the product $\prod_{d\geqslant 1} (1 - u^{2d})^{-N^*(q;2d)}$ converges absolutely if $q|u|^2 < 1$. Similarly, since $|N^*(q; 2d) - M^*(q; d)| = O(q^{d/2})$ the product $\prod_{d\geqslant 1} (1 + u^d)^{N^*(q;2d)-M^*(q;d)}$ converges absolutely if $q^{1/2}|u| < 1$. Thus the product on the right of (c) may be rearranged so as to converge for $|u| < q^{-1/2}$. Equation (d) may be treated similarly.

Lemma 1.3.19. (a) $$\frac{y}{x+y}\Big(1 + \frac{x}{y+1}\Big) = 1 - \frac{x}{(y+1)(x+y)}\,.$$

(b) $$\frac{y}{y-x}\Big(1 - \frac{x}{y(y+1)}\Big) = 1 + \frac{xy}{(y+1)(y-x)}\,.$$

The proof is a simple algebraic manipulation which we leave to the reader. We shall refer to Lemma 1.3.19(p)[U, Q] to mean part (p) (where p is a or b) with x, y replaced by U, Q respectively. Usually U and Q will be $\pm u^d$ and $\pm q^d$.

CHAPTER 2

Separable and cyclic matrices in classical groups

2.1. The unitary groups

The unitary group $\mathrm{U}(n,q)$ can be defined as the subgroup of $\mathrm{GL}(n,q^2)$ preserving a non-degenerate sesquilinear form. Recall that the map $x \mapsto x^q$ is an involutory automorphism of the field $\mathbb{F}_{q^2}$, and that a sesquilinear form with respect to this automorphism on an n-dimensional vector space V over $\mathbb{F}_{q^2}$ is a bi-additive map $\langle\ \rangle : V \times V \to \mathbb{F}_{q^2}$ such that $\langle ax, by\rangle = ab^q\langle x, y\rangle$ for all $a, b \in \mathbb{F}_{q^2}$. One such form is given by $\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i^q$, where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. It is well known (see for example [**21**, Chapter 10 and Theorem 7.4]) that any two non-degenerate sesquilinear forms are equivalent, so that the group $\mathrm{U}(n,q)$ is unique up to conjugacy in $\mathrm{GL}(n,q^2)$. The order of $\mathrm{U}(n,q)$ is $q^{n(n-1)/2}\prod_{i=1}^{n}(q^i - (-1)^i)$ (see [**21**, p.118]).

Separable unitary matrices. Let $S_{\mathrm{U}}(u)$ (or sometimes $S_{\mathrm{U}}(q;u)$) be the generating function for the probability $s_{\mathrm{U}}(n,q)$ that an element in a unitary group over $\mathbb{F}_{q^2}$ is separable. Thus

$$S_{\mathrm{U}}(u) := S_{\mathrm{U}}(q;u) := 1 + \sum_{n \geqslant 1} s_{\mathrm{U}}(n,q)\, u^n\,.$$

THEOREM 2.1.1. *Let $\widetilde{N}(q;d)$, $\widetilde{M}(q;d)$ be as defined on p. 23. Then*

$$S_{\mathrm{U}}(u) = \prod_{d\ \mathrm{odd}} \Big(1 + \frac{u^d}{q^d+1}\Big)^{\widetilde{N}(q;d)} \prod_{d \geqslant 1} \Big(1 + \frac{u^{2d}}{q^{2d}-1}\Big)^{\widetilde{M}(q;d)}\,.$$

Proof. This result may be deduced from the factorisation of the cycle index of the unitary groups derived in [**6**, Theorem 10]. One needs to note that an element X of $\mathrm{U}(n,q)$ is separable if and only if the partition $\lambda_\phi(X)$ (involved in the cycle index) associated with each monic irreducible polynomial $\phi(t)$ has norm at most 1. This is true because the characteristic polynomial of X is $\prod \phi(t)^{|\lambda_\phi(X)|}$. We shall, however, sketch a direct proof of the theorem.

For each separable matrix $X \in \mathrm{U}(n,q)$, its characteristic polynomial $c_X(t)$ is a product of distinct monic irreducible polynomials $\phi(t)$ such that $\phi(0) \neq 0$; moreover, if $\phi(t)$ divides $c_X(t)$, then also $\widetilde{\phi}(t)$ divides $c_X(t)$. Conversely, each monic polynomial $c(t)$ of degree n over $\mathbb{F}_{q^2}$ which has this property occurs as $c_X(t)$ for some X in $\mathrm{U}(n,q)$ (see [**22**]) and the set of matrices $X \in \mathrm{U}(n,q)$ such that $c_X(t) = c(t)$ forms a conjugacy class of $\mathrm{U}(n,q)$. Hence the proportion of elements $\mathrm{U}(n,q)$ with characteristic polynomial $c(t)$ is $|C_{\mathrm{U}(n,q)}(X)|^{-1}$, where X is one such and $C_{\mathrm{U}(n,q)}(X)$ is its centraliser.

Write $c(t)$ as $\prod_{i=1}^{r} \phi_i(t) \prod_{j=1}^{s} \psi_j(t)\widetilde{\psi}_j(t)$ where the irreducible factors ϕ_i are self-conjugate and the others are not. There is a corresponding primary decomposition $X = X_1 \oplus \cdots \oplus X_r \oplus Y_1 \oplus \cdots \oplus Y_s$, corresponding to an orthogonal direct sum decomposition of V, in which X_i has characteristic and minimal polynomial ϕ_i and Y_j has characteristic and minimal polynomial $\psi_j\widetilde{\psi}_j$. The centraliser $C_{\mathrm{U}(n,q)}(X)$ is the direct product of the centralisers $C_{\mathrm{U}(n_i,q)}(X_i)$, $C_{\mathrm{U}(2m_j,q)}(Y_j)$, where $n_i := \deg(\phi_i)$, $m_j := \deg(\psi_j)$. Now $|C_{\mathrm{U}(n_i,q)}(X_i)| = q^{n_i}+1$, and $C_{\mathrm{U}(2m_j,q)}(Y_j)$ is the centraliser in $\mathrm{GL}(m_j, q^2)$ of a matrix with characteristic polynomial $\psi_j(t)$, whence $|C_{\mathrm{U}(2m_j,q)}(Y_j)| = q^{2m_j}-1$ (see [**22**, p.34]). Thus the contribution to $s_{\mathrm{U}}(n,q)$ from matrices with characteristic polynomial $c(t)$ is $\left(\prod_i (q^{n_i}+1) \prod_j (q^{2m_j}-1)\right)^{-1}$ and the theorem is proved by writing

$$\prod_{d\,\mathrm{odd}} \Big(1+\frac{u^d}{q^d+1}\Big)^{\widetilde{N}(q;d)} \prod_{d\geqslant 1} \Big(1+\frac{u^{2d}}{q^{2d}-1}\Big)^{\widetilde{M}(q;d)}$$

as

$$\prod_{\phi=\widetilde{\phi}} \Big(1+\frac{u^{\deg(\phi)}}{q^{\deg(\phi)}+1}\Big) \prod_{\psi\neq\widetilde{\psi}} \Big(1+\frac{u^{2\deg(\psi)}}{q^{2\deg(\psi)}-1}\Big)$$

and expanding this product of products as a sum.

By using Lemma 1.3.14 we obtain a different infinite product expression for $S_{\mathrm{U}}(u)$ which, on applying Lemma 1.3.3, allows us to determine the limiting probability $s_{\mathrm{U}}(\infty, q)$. Define

$$\widetilde{V}(u) := \prod_{d\,\mathrm{odd}} \Big(1-\frac{u^d(u^d+1)}{q^d(q^d+1)}\Big)^{\widetilde{N}(q;d)} \prod_{d\geqslant 1} \Big(1-\frac{u^{2d}(u^{2d}-1)}{q^{2d}(q^{2d}-1)}\Big)^{\widetilde{M}(q;d)}$$

and

$$\widetilde{W}(u) := \prod_{d\,\mathrm{odd}} \Big(1-\frac{1}{q^d+1}\,\frac{u^d}{q^d+u^d}\Big)^{\widetilde{N}(q;d)} \prod_{d\geqslant 1} \Big(1+\frac{1}{q^{2d}-1}\,\frac{u^{2d}}{q^{2d}+u^{2d}}\Big)^{\widetilde{M}(q;d)}.$$

These are analogues for the unitary group of the functions $S(q,z)$ and $T(q,z)$ defined by Wall in Section 6 of [**23**]. Note that, by Corollary 1.3.2 and Lemma 1.3.12, the products defining $\widetilde{V}(u)$ converge for $|u| < \sqrt{q}$ and so $\widetilde{V}(u)$ is analytic in the open disc $D(\sqrt{q})$. Similarly, the products in the expression for $\widetilde{W}(u)$ converge for $|u| < q$ and so $\widetilde{W}(u)$ is analytic in $D(q)$.

THEOREM 2.1.2. *The generating function $S_{\mathrm{U}}(u)$ has an analytic extension to a function analytic in the open disc $D(q)$, except for a pole of order 1 at $u = 1$. Explicitly,*

$$S_{\mathrm{U}}(u) = \frac{(1+\frac{u}{q})}{1-u}\,\widetilde{V}(u) = \frac{(1-\frac{u^2}{q})(1+\frac{u}{q})}{(1-u)(1+\frac{u^2}{q^2})}\,\widetilde{W}(u),$$

where $\widetilde{V}(u)$, $\widetilde{W}(u)$ are as defined above.

Proof. From Lemma 1.3.14(a) (with u replaced by u/q), and Theorem 2.1.1 we have

$$\begin{aligned} S_{\mathrm{U}}(u) &= \frac{1+\frac{u}{q}}{1-u} \times \prod_{d\,\mathrm{odd}} \Big(\Big(1+\frac{u^d}{q^d+1}\Big)\Big(1-\frac{u^d}{q^d}\Big)\Big)^{\widetilde{N}(q;d)} \\ &\qquad \times \prod_{d\geqslant 1} \Big(\Big(1+\frac{u^{2d}}{q^{2d}-1}\Big)\Big(1-\frac{u^{2d}}{q^{2d}}\Big)\Big)^{\widetilde{M}(q;d)}, \end{aligned}$$

and so

$$\begin{aligned} S_{\mathrm{U}}(u) &= \frac{1+\frac{u}{q}}{1-u} \times \prod_{d\,\mathrm{odd}} \Big(1-\frac{u^d(u^d+1)}{q^d(q^d+1)}\Big)^{\widetilde{N}(q;d)} \\ &\qquad \times \prod_{d\geqslant 1} \Big(1-\frac{u^{2d}(u^{2d}-1)}{q^{2d}(q^{2d}-1)}\Big)^{\widetilde{M}(q;d)}. \end{aligned}$$

This proves the first equation and consequently also the first assertion of the theorem.

By using Lemma 1.3.14(b) with u replaced by u/q together with Theorem 2.1.1, we find that

$$S_{\mathrm{U}}(u) = \frac{\big(1-\frac{u^2}{q}\big)\big(1+\frac{u}{q}\big)}{\big(1-u\big)\big(1+\frac{u^2}{q^2}\big)}\, W_1(u)\, W_2(u)\,,$$

where

$$W_1(u) := \prod_{d\,\mathrm{odd}} \Big(\Big(\frac{1}{1+\big(\frac{u}{q}\big)^d}\Big)\Big(1+\frac{u^d}{q^d+1}\Big)\Big)^{\widetilde{N}(q;d)},$$

and

$$W_2(u) := \prod_{d\geqslant 1} \Big(\Big(\frac{1}{1+\big(\frac{u}{q}\big)^{2d}}\Big)\Big(1+\frac{u^{2d}}{q^{2d}-1}\Big)\Big)^{\widetilde{M}(q;d)}.$$

The second equation of the theorem now follows from Lemma 1.3.19(a)$[u^d, q^d]$ and from 1.3.19(a)$[-u^{2d}, -q^{2d}]$.

THEOREM 2.1.3.

$$\begin{aligned} s_{\mathrm{U}}(\infty,q) &= \Big(1+\frac{1}{q}\Big) \prod_{d\,\mathrm{odd}} \Big(1-\frac{2}{q^d(q^d+1)}\Big)^{\widetilde{N}(q;d)} \\ &= \frac{q^2-1}{q^2+1} \prod_{d\,\mathrm{odd}} \Big(1-\frac{1}{(q^d+1)^2}\Big)^{\widetilde{N}(q;d)} \prod_{d\geqslant 1} \Big(1+\frac{1}{q^{4d}-1}\Big)^{\widetilde{M}(q;d)}, \end{aligned}$$

and if $1<r<q$, *then* $|s_{\mathrm{U}}(n,q) - s_{\mathrm{U}}(\infty,q)| < o(r^{-n})$ *as* $n\to\infty$.

Proof. From the previous theorem $S_{\mathrm{U}}(u) = (1-u)^{-1} f(u)$, where f is analytic in the open disc $D(q)$ and

$$f(1) = \Big(1+\frac{1}{q}\Big)\widetilde{V}(1) = \Big(\frac{q^2-1}{q^2+1}\Big)\widetilde{W}(1)\,.$$

An application of Lemma 1.3.3 now gives the existence and the required values of $s_{\mathrm{U}}(\infty,q)$, and also the rate of convergence of $s_{\mathrm{U}}(n,q)$ to $s_{\mathrm{U}}(\infty,q)$.

We have been unable to simplify either of the infinite product expansions for $s_{\mathrm{U}}(\infty,q)$ and, in particular, we do not know whether or not it reduces to a rational function of q, as $s_{\mathrm{GL}}(\infty,q)$ does. It is expressible as a power series in q^{-1} whose first few terms can be calculated to be

$$1-\frac{1}{q}-\frac{2}{q^3}+\frac{4}{q^4}-\frac{6}{q^5}+\frac{14}{q^6}-\frac{28}{q^7}+\frac{52}{q^8}-\frac{106}{q^9}+O\Big(\frac{1}{q^{10}}\Big)$$

as in Table 3. For practical purposes the following estimates should suffice.

THEOREM 2.1.4. *For all q*

$$1-\frac{1}{q}-\frac{2}{q^3}+\frac{2}{q^4}<s_{\mathrm{U}}(\infty,q)<1-\frac{1}{q}-\frac{2}{q^3}+\frac{6}{q^4}\,.$$

For small q in fact

$$0.4147<s_{\mathrm{U}}(\infty,2)<0.4157 \quad \textit{and} \quad 0.6283<s_{\mathrm{U}}(\infty,3)<0.6286\,.$$

Proof. Taking $\alpha:=q^{2d}+q^d-1$ we may re-write the factor $1-2/q^d(q^d+1)$ appearing in the first expression for $s_{\mathrm{U}}(\infty,q)$ in Theorem 2.1.3 as $(1-\alpha^{-1})\div(1+\alpha^{-1})$. For $x>0$ the function $(1-x^{-1})/(1+x^{-1})$ is monotone increasing and so

$$\frac{1-\frac{1}{q^{2d}}}{1+\frac{1}{q^{2d}}}<1-\frac{2}{q^d(q^d+1)}\leqslant\frac{1-\frac{1}{(q^2+q-1)^d}}{1+\frac{1}{(q^2+q-1)^d}}$$

for all $d\geqslant 1$ since $q^{2d}<q^{2d}+q^d-1\leqslant(q^2+q-1)^d$. Therefore by Lemma 1.3.14(d)

$$\Big(1+\frac{1}{q}\Big)\frac{(1-\frac{1}{q^2})(1-\frac{1}{q})}{(1+\frac{1}{q^2})(1+\frac{1}{q})}<s_{\mathrm{U}}(\infty,q)<\Big(1+\frac{1}{q}\Big)\frac{(1-\frac{1}{q^2+q-1})(1-\frac{q}{q^2+q-1})}{(1+\frac{1}{q^2+q-1})(1+\frac{q}{q^2+q-1})}\,.$$

After simplification this yields that

$$\frac{(1-\frac{1}{q})(1-\frac{1}{q^2})}{(1+\frac{1}{q^2})}<s_{\mathrm{U}}(\infty,q)<\frac{(1-\frac{1}{q})(1+\frac{2}{q})(1-\frac{1}{q^2})}{(1+\frac{2}{q}-\frac{1}{q^2})}\,.$$

Here the lower bound is rather a poor one and we seek a better one in the next paragraph. The upper bound is quite good and leads to the one given in the statement of the theorem as follows. Suppose, seeking a contradiction, that

$$\frac{(1-\frac{1}{q})(1+\frac{2}{q})(1-\frac{1}{q^2})}{(1+\frac{2}{q}-\frac{1}{q^2})}\geqslant 1-\frac{1}{q}-\frac{2}{q^3}+\frac{6}{q^4}\,.$$

Multiplying both sides by $(1+\frac{2}{q}-\frac{1}{q^2})$, expanding and simplifying, we find that $14q-6\leqslant 0$, which is plainly false. Thus $s_{\mathrm{U}}(\infty,q)\leqslant 1-\frac{1}{q}-\frac{2}{q^3}+\frac{6}{q^4}$.

To derive an acceptable lower bound we use the second expression for $s_{\mathrm{U}}(\infty,q)$ in Theorem 2.1.3 to write

$$s_{\mathrm{U}}(\infty,q)=\frac{1-\frac{1}{q^2}}{1+\frac{1}{q^2}}\times A\times B\,,$$

where

$$A:=\prod_{d\,\mathrm{odd}}\Big(1-\frac{1}{q^{2d}}\Big)^{\widetilde{N}(q;d)}\prod_{d\geqslant 1}\Big(1+\frac{1}{q^{4d}}\Big)^{\widetilde{M}(q;d)},$$

and

$$B:=\prod_{d\,\mathrm{odd}}\Big(\frac{1-\frac{1}{(q^d+1)^2}}{1-\frac{1}{q^{2d}}}\Big)^{\widetilde{N}(q;d)}\prod_{d\geqslant 1}\Big(\frac{1+\frac{1}{q^{4d}-1}}{1+\frac{1}{q^{4d}}}\Big)^{\widetilde{M}(q;d)}.$$

Lemma 1.3.14(b) with u replaced by $-1/q^2$, yields that

$$A = \frac{(1-\frac{1}{q^2})(1-\frac{1}{q^3})}{(1+\frac{1}{q^4})(1+\frac{1}{q})} = \frac{(1-\frac{1}{q})(1-\frac{1}{q^3})}{(1+\frac{1}{q^4})}\,.$$

To deal with B we note that $1-\frac{1}{(q^d+1)^2} > 1-\frac{1}{q^{2d}}$ and $1+\frac{1}{(q^{4d}-1)} > 1+\frac{1}{q^{4d}}$. Therefore, since $\widetilde{N}(q;1) = q+1$, we have that $B > \big((1-\frac{1}{(q+1)^2})/(1-\frac{1}{q^2})\big)^{q+1}$ and

$$s_{\mathrm{U}}(\infty,q) > \frac{(1-\frac{1}{q})(1-\frac{1}{q^2})(1-\frac{1}{q^3})}{(1-\frac{1}{q^8})} \times C \quad \text{where} \quad C := \frac{\big(1-\frac{1}{(q+1)^2}\big)^{q+1}}{\big(1-\frac{1}{q^2}\big)^{q}}\,.$$

Now

$$\log\Big(1-\frac{1}{(q+1)^2}\Big)^{q+1} = -\sum_{m\geqslant 1}\frac{1}{m\,(q+1)^{2m-1}}$$

and

$$\log\Big(1-\frac{1}{q^2}\Big)^{q} = -\sum_{m\geqslant 1}\frac{1}{m\,q^{2m-1}}\,,$$

and therefore

$$\begin{aligned}\log C &= \sum_{m\geqslant 1}\frac{1}{m}\Big(\frac{1}{q^{2m-1}} - \frac{1}{(q+1)^{2m-1}}\Big)\\ &> \frac{1}{q} - \frac{1}{q+1} + \frac{1}{2\,q^3} - \frac{1}{2\,(q+1)^3}\\ &> \frac{1}{q(q+1)} + \frac{3}{2q^2(q+1)^2}\,.\end{aligned}$$

It is elementary algebra to check that if $q \geqslant 7$ then

$$\frac{1}{q(q+1)} + \frac{3}{2q^2(q+1)^2} > \frac{1}{q^2} - \frac{1}{q^3} + \frac{2}{q^4}\,.$$

Thus if $q \geqslant 7$ then $\log C > \frac{1}{q^2} - \frac{1}{q^3} + \frac{2}{q^4}$ and so $C > 1 + \frac{1}{q^2} - \frac{1}{q^3} + \frac{2}{q^4}$. This inequality can be checked directly for $3 \leqslant q < 7$. It fails for $q = 2$, but the inequality $C > 1 + \frac{1}{q^2} - \frac{1}{q^3} + \frac{2}{q^4} - \frac{1}{q^8}$ may be calculated to hold for $q = 2$ and therefore holds for all $q \geqslant 2$. Now

$$\begin{aligned}\Big(1-\frac{1}{q^8}\Big)^{-1} C &> \Big(1+\frac{1}{q^8}\Big)\Big(1+\frac{1}{q^2}-\frac{1}{q^3}+\frac{2}{q^4}-\frac{1}{q^8}\Big)\\ &> 1+\frac{1}{q^2}-\frac{1}{q^3}+\frac{2}{q^4}\,,\end{aligned}$$

by Lemma 1.3.4, and it is again a matter of elementary algebra to prove that

$$\Big(1-\frac{1}{q^2}\Big)\Big(1-\frac{1}{q^3}\Big)\Big(1+\frac{1}{q^2}-\frac{1}{q^3}+\frac{2}{q^4}\Big) > 1-\frac{2}{q^3}\,.$$

It follows that

$$s_{\mathrm{U}}(\infty,q) > \frac{(1-\frac{1}{q})(1-\frac{1}{q^2})(1-\frac{1}{q^3})}{(1-\frac{1}{q^8})}\,C > \Big(1-\frac{1}{q}\Big)\Big(1-\frac{2}{q^3}\Big)\,,$$

that is, $s_{\mathrm{U}}(\infty,q) > 1-\frac{1}{q}-\frac{2}{q^3}+\frac{2}{q^4}$ which is the promised lower bound.

These bounds are not good enough to be useful for small values of q. They can be somewhat improved as follows. Using the transformation exploited in the first paragraph of this proof we find that

$$s_{\mathrm{U}}(\infty,q) = \Big(1+\frac{1}{q}\Big)\Big(\frac{1-\frac{1}{q^2+q-1}}{1+\frac{1}{q^2+q-1}}\Big)^{q+1} \prod_{d\,\mathrm{odd},\,d\geqslant 3} \Big(\frac{1-\frac{1}{q^{2d}+q^d-1}}{1+\frac{1}{q^{2d}+q^d-1}}\Big)^{\widetilde{N}(q;d)}.$$

If $d \geqslant 3$ then

$$\Big(q^2+\frac{1}{4q}\Big)^d < q^{2d}+q^d-1 < \Big(q^2+\frac{1}{3q}\Big)^d,$$

and so, arguing as in the first part of the proof, we find that

$$\Big(1+\frac{1}{q}\Big)\lambda^{q+1}\Big(\frac{(1-\frac{4q}{4q^3+1})(1-\frac{4q^2}{4q^3+1})}{(1+\frac{4q}{4q^3+1})(1+\frac{4q^2}{4q^3+1})}\Big) < s_{\mathrm{U}}(\infty,q) < \Big(1+\frac{1}{q}\Big)\mu^{q+1}\Big(\frac{(1-\frac{3q}{3q^3+1})(1-\frac{3q^2}{3q^3+1})}{(1+\frac{3q}{3q^3+1})(1+\frac{3q^2}{3q^3+1})}\Big),$$

where

$$\lambda := \frac{\big(1-\frac{1}{q^2+q-1}\big)\big(1+\frac{4q}{4q^3+1}\big)}{\big(1+\frac{1}{q^2+q-1}\big)\big(1-\frac{4q}{4q^3+1}\big)} \quad \text{and} \quad \mu := \frac{\big(1-\frac{1}{q^2+q-1}\big)\big(1+\frac{3q}{3q^3+1}\big)}{\big(1+\frac{1}{q^2+q-1}\big)\big(1-\frac{3q}{3q^3+1}\big)}.$$

We do not pursue this analysis further in general. The expressions for the bounds, although complicated, are easy to calculate with. Substituting $q=2$ and $q=3$ we find that $0.4147 < s_{\mathrm{U}}(\infty,2) < 0.4157$ and $0.6283 < s_{\mathrm{U}}(\infty,3) < 0.6286$, and this completes the proof.

The convergence rate given in Theorem 2.1.3 is too inexplicit to be useful in practice. The method of Wall [**23**, §6] may be adapted to unitary matrices as follows. Recall from pp. 18–20 that, given two power series $A(u) = \sum a_n u^n$, $B(u) = \sum b_n u^n$, we write $A(u) \ll B(u)$ if $a_n \leqslant b_n$ for all n and we write $|A|(u)$ for $\sum |a_n| u^n$; also that $\Omega(u) := \prod_{i\geqslant 1}(1-u^i)$, so that $\Omega(u)^{-1} = \sum_{n\geqslant 0} p(n)\,u^n$ where $p(n)$ is the number of partitions of n (and $p(0)=1$); and that $p_2(n) := \sum_{m=0}^{n} p(m)$.

LEMMA 2.1.5. (a) *Let* $A(u) := (1-qu)S_{\mathrm{U}}(qu)$. *Then*

$$|A|(u) \ll \frac{(1+qu^2)}{(1-u)}\,\Omega(u)^{-1}.$$

(b) $|s_{\mathrm{U}}(n,q) - s_{\mathrm{U}}(n-1,q)| < (q+1)p_2(n)q^{-n}$ *for* $n \geqslant 2$.

Proof. Theorem 2.1.2 gives that

$$A(u) = \frac{(1-qu^2)(1+u)}{(1+u^2)}\,\widetilde{W}(qu),$$

where $\widetilde{W}(u)$ is the product defined on p. 32. It follows that

$$|A|(u) \ll \frac{(1+qu^2)(1+u)}{(1-u^2)}\,|\widetilde{W}|(qu) = \frac{(1+qu^2)}{(1-u)}\,|\widetilde{W}|(qu).$$

Applying Lemma 1.3.6 to the definition of $\widetilde{W}(qu)$ we see that

$$|\widetilde{W}|(qu) \ll \exp\Big(\sum_{d \text{ odd}} \frac{\widetilde{N}(q;d)\, u^d}{(q^d+1)(1-u^d)} + \sum_{d \geqslant 1} \frac{\widetilde{M}(q;d)\, u^{2d}}{(q^{2d}-1)(1-u^{2d})} \Big) .$$

Now $\widetilde{N}(q;d) \leqslant (q^d+1)/d$ and $\widetilde{M}(q;d) \leqslant (q^{2d}-1)/(2d)$ (see Lemma 1.3.12). Therefore

$$\begin{aligned} |\widetilde{W}|(qu) &\ll \exp\Big(\sum_{d \text{ odd}} \frac{u^d}{d(1-u^d)} + \sum_{d \geqslant 1} \frac{u^{2d}}{2d(1-u^{2d})} \Big) \\ &= \exp\Big(\sum_{d \geqslant 1} \frac{u^d}{d(1-u^d)} \Big) . \end{aligned}$$

Thus $|\widetilde{W}|(qu) \ll \Omega(u)^{-1}$ by Lemma 1.3.7, and the first assertion of the lemma follows.

Taking the coefficient of u^n on both sides of (a) and using Lemma 1.3.8 we see that if $n \geqslant 2$ then $|s_{\mathrm{U}}(n,q) - s_{\mathrm{U}}(n-1,q)|q^n \leqslant c_n$ where $c_n := p_2(n) + q\, p_2(n-2)$. Since $p_2(n)$ is monotone increasing we certainly have $c_n < (q+1)p_2(n)$ and so $|s_{\mathrm{U}}(n,q) - s_{\mathrm{U}}(n-1,q)| < (q+1)p_2(n)q^{-n}$ for $n \geqslant 2$, as the lemma states.

We use this to improve the convergence rate in Theorem 2.1.3 and to produce an explicit estimate.

THEOREM 2.1.6. *If $6 \leqslant n < n' \leqslant \infty$ and $k := (q+1)/(2q-3)$ then*

$$|s_{\mathrm{U}}(n',q) - s_{\mathrm{U}}(n,q)| < 3k\, p_2(n) q^{-n} < 8k \left(\tfrac{2}{3}\, q\right)^{-n} .$$

Proof. If $n < n' \leqslant \infty$ then

$$\begin{aligned} |s_{\mathrm{U}}(n',q) - s_{\mathrm{U}}(n,q)| &\leqslant \sum_{m=n+1}^{n'} |s_{\mathrm{U}}(m,q) - s_{\mathrm{U}}(m-1,q)| \\ &< \sum_{m=n+1}^{n'} (q+1) p_2(m) q^{-m} . \end{aligned}$$

By Lemma 1.3.9, if $n \geqslant 6$ then

$$\sum_{m=n+1}^{n'} (q+1) p_2(m) q^{-m} \leqslant (q+1) p_2(n) q^{-n} \sum_{m=1}^{n'-n} (\tfrac{3}{2})^m q^{-m} < 3k\, p_2(n) q^{-n} .$$

Thus $|s_{\mathrm{U}}(n',q) - s_{\mathrm{U}}(n,q)| < 3k\, p_2(n) q^{-n}$ if $6 \leqslant n < n' \leqslant \infty$, and the fact that $|s_{\mathrm{U}}(n',q) - s_{\mathrm{U}}(n,q)| < 8k\, (\frac{2}{3} q)^{-n}$ now follows from Lemma 1.3.9(e).

As was observed in §1.3 the Hardy–Ramanujan estimates for $p(n)$ give more precise information of the form $|s_{\mathrm{U}}(\infty,q) - s_{\mathrm{U}}(n,q)| < q^{-n+O(\sqrt{n})}$, but we do not propose to pursue details here.

Cyclic unitary matrices. Let $C_{\mathrm{U}}(u)$ be the generating function for the probability $c_{\mathrm{U}}(n,q)$ that an element in a unitary group over $\mathbb{F}_{q^2}$ is cyclic, that is,

$$C_{\mathrm{U}}(u) := 1 + \sum_{n \geqslant 1} c_{\mathrm{U}}(n,q)\, u^n .$$

The proof of the following theorem is similar to that of Theorem 2.1.1. Since an element X of $\mathrm{U}(n,q)$ is cyclic if and only if the partition $\lambda_\phi(X)$ in the cycle index has at most 1 row for all ϕ, it may also be deduced from the factorisation of the cycle index for the unitary groups derived in [**6**, Theorem 10].

THEOREM 2.1.7.

$$C_{\mathrm{U}}(u) = \prod_{d\,\mathrm{odd}} \Big(1 + \frac{u^d}{(q^d+1)(1-(u/q)^d)}\Big)^{\widetilde{N}(q;d)} \times \prod_{d\geqslant 1} \Big(1 + \frac{u^{2d}}{(q^{2d}-1)(1-(u/q)^{2d})}\Big)^{\widetilde{M}(q;d)}.$$

Proof. The characteristic polynomial $c_X(t)$ of a cyclic matrix $X \in \mathrm{U}(n,q)$, is monic of degree n over $\mathbb{F}_{q^2}$ and is a product of monic irreducible polynomials $\phi(t)$, such that $\phi(t) \neq t$ and $\phi(t)^a$ divides $c_X(t)$ if and only if $\widetilde{\phi}(t)^a$ does also. Each such polynomial $c(t)$ arises as $c_X(t)$ for some X in $\mathrm{U}(n,q)$, and the subset of matrices $X \in \mathrm{U}(n,q)$ such that $c_X(t) = c(t)$ forms a conjugacy class of $\mathrm{U}(n,q)$ (see [**22**]). Thus the proportion of elements of $\mathrm{U}(n,q)$ with characteristic polynomial $c(t)$ is $|C_{\mathrm{U}(n,q)}(X)|^{-1}$, where X is one such.

In the primary decomposition of a cyclic matrix X, there is a unique summand corresponding to each irreducible polynomial $\phi(t)$ dividing $c(t)$, and, as in the case of separable matrices, $|C_{\mathrm{U}(n,q)}(X)|$ is a certain product with one term for each self-conjugate monic irreducible $\phi(t)$ dividing $c(t)$, and one term for each pair $\{\phi(t), \widetilde{\phi}(t)\}$ of non-self-conjugate monic irreducible polynomials dividing $c(t)$. Suppose that the monic irreducible polynomial $\phi(t)$ of degree d divides $c(t)$ with multiplicity $a \geqslant 1$. If $\phi(t)$ is self-conjugate then the term for $\phi(t)$ in $|C_{\mathrm{U}(n,q)}(X)|$ is the order of the centraliser in $\mathrm{U}(da,q)$ of a cyclic matrix $X_\phi \in \mathrm{U}(da,q)$ with characteristic polynomial $\phi(t)^a$, which is $q^{d(a-1)}(q^d+1)$ (see [**22**, p. 34]). The term for a pair $\{\phi(t), \widetilde{\phi}(t)\}$ of non-self-conjugate monic irreducible polynomials is the order of the centraliser in $\mathrm{GL}(da,q^2)$ of a cyclic matrix $X_\phi \in \mathrm{GL}(da,q^2)$ with characteristic polynomial $\phi(t)^a$, and this is $q^{2d(a-1)}(q^{2d}-1)$ (see [**22**, p. 34]). Exactly as in the case of separable matrices (see the proof of Theorem 2.1.1) it follows that

$$C_{\mathrm{U}}(u) = \prod_{d\,\mathrm{odd}} \Big(1 + \frac{u^d}{q^d+1} + \frac{u^{2d}}{q^d(q^d+1)} + \frac{u^{3d}}{q^{2d}(q^d+1)} + \cdots\Big)^{\widetilde{N}(q;d)} \times \prod_{d\geqslant 1} \Big(1 + \frac{u^{2d}}{q^{2d}-1} + \frac{u^{4d}}{q^{2d}(q^{2d}-1)} + \frac{u^{6d}}{q^{4d}(q^{2d}-1)} + \cdots\Big)^{\widetilde{M}(q;d)}.$$

Summing the infinite series occurring for each d in the infinite products yields the result.

Wall has discovered a direct relationship between the generating functions for separable and cyclic probabilities in the case of the general linear groups [**23**]. There is a similar relationship between the generating functions $S_{\mathrm{U}}(u)$ and $C_{\mathrm{U}}(u)$. Later we shall show that in fact the functions for the unitary groups may be expressed in terms of those for the general linear groups, and that therefore the following theorem follows from Wall's.

THEOREM 2.1.8. $\displaystyle C_{\mathrm{U}}(u) = \frac{(1+u/q)\, S_{\mathrm{U}}(-u/q)}{1-u}.$

Proof. By Theorem 2.1.7, Lemma 1.3.19(b)$[u^d, q^d]$ and 1.3.19(b)$[-u^{2d}, -q^{2d}]$,

$$\begin{aligned} C_{\mathrm{U}}(u) &= \prod_{d\,\mathrm{odd}} \Big(1 + \frac{u^d}{(q^d+1)(1-(u/q)^d)}\Big)^{\widetilde{N}(q;d)} \\ &\qquad \times \prod_{d\geqslant 1} \Big(1 + \frac{u^{2d}}{(q^{2d}-1)(1-(u/q)^{2d})}\Big)^{\widetilde{M}(q;d)} \\ &= \prod_{d\,\mathrm{odd}} \Big(\Big(\frac{1}{1-(u/q)^d}\Big)\Big(1 - \frac{(u/q)^d}{q^d+1}\Big)\Big)^{\widetilde{N}(q;d)} \\ &\qquad \times \prod_{d\geqslant 1} \Big(\Big(\frac{1}{1-(u/q)^{2d}}\Big)\Big(1 + \frac{(u/q)^{2d}}{q^{2d}-1}\Big)\Big)^{\widetilde{M}(q;d)}. \end{aligned}$$

Applying Lemma 1.3.14(a) we see that

$$C_{\mathrm{U}}(u) = \frac{1+u/q}{1-u} \prod_{d\,\mathrm{odd}} \Big(1 - \frac{(u/q)^d}{q^d+1}\Big)^{\widetilde{N}(q;d)} \prod_{d\geqslant 1} \Big(1 + \frac{(u/q)^{2d}}{q^{2d}-1}\Big)^{\widetilde{M}(q;d)}.$$

Therefore by Theorem 2.1.1, $C_{\mathrm{U}}(u) = (1+u/q)\, S_{\mathrm{U}}(-u/q)/(1-u)$, as claimed.

We may now determine the limiting value $c_{\mathrm{U}}(\infty, q)$ (in three different forms) and the rate of convergence to this limit.

THEOREM 2.1.9.

$$\begin{aligned} c_{\mathrm{U}}(\infty,q) &= \Big(1+\frac{1}{q}\Big) \prod_{d\,\mathrm{odd}} \Big(1 - \frac{1}{q^d(q^d+1)}\Big)^{\widetilde{N}(q;d)} \prod_{d\geqslant 1} \Big(1 + \frac{1}{q^{2d}(q^{2d}-1)}\Big)^{\widetilde{M}(q;d)} \\ &= \Big(1-\frac{1}{q^2}\Big) \prod_{d\,\mathrm{odd}} \Big(1 + \frac{q^d-1}{q^{3d}(q^d+1)}\Big)^{\widetilde{N}(q;d)} \prod_{d\geqslant 1} \Big(1 + \frac{1}{q^{6d}}\Big)^{\widetilde{M}(q;d)} \\ &= \frac{(1-\frac{1}{q^2})(1-\frac{1}{q^3})}{1+\frac{1}{q^4}} \prod_{d\,\mathrm{odd}} \Big(1 + \frac{1}{(q^d+1)(q^{2d}-1)}\Big)^{\widetilde{N}(q;d)} \\ &\qquad \times \prod_{d\geqslant 1} \Big(1 + \frac{1}{(q^{2d}-1)(q^{4d}+1)}\Big)^{\widetilde{M}(q;d)}, \end{aligned}$$

and if $1 < r < q^2$ *then* $|c_{\mathrm{U}}(n,q) - c_{\mathrm{U}}(\infty,q)| < o(r^{-n})$ *as* $n \to \infty$.

This comes from Theorems 2.1.8, 2.1.1, 2.1.2 and Lemma 1.3.3. The second and third expressions for $c_{\mathrm{U}}(\infty,q)$ are $(1-q^{-2})\,\widetilde{V}(-q^{-1})$ and $\frac{(1-q^{-2})(1-q^{-3})}{(1+q^{-4})}\,\widetilde{W}(-q^{-1})$ respectively.

Our next observation yields a far more explicit bound for the convergence rate than the last assertion of the theorem above, which is therefore more useful in practice. It is an intriguing relationship between the numbers $c_{\mathrm{U}}(n,q)$ and $s_{\mathrm{U}}(n,q)$ implied by Theorem 2.1.8 and analogous to Wall's formula (3.17) in [**23**]. A direct proof of this relationship would be desirable.

THEOREM 2.1.10. *For* $n \geqslant 2$

$$c_{\mathrm{U}}(n,q) - c_{\mathrm{U}}(n-1,q) = (-q)^{-n}\big(s_{\mathrm{U}}(n,q) - s_{\mathrm{U}}(n-1,q)\big).$$

This comes from taking the coefficient of u^n on both sides of Theorem 2.1.8 in the form $(1-u)C_{\mathrm{U}}(u) = (1+u/q)\, S_{\mathrm{U}}(-u/q)$.

THEOREM 2.1.11. *If* $6 \leqslant n < n' \leqslant \infty$ *and* $k := (q+1)/(2q^2-3)$ *then*

$$|c_{\mathrm{U}}(n',q) - c_{\mathrm{U}}(n,q)| < 3k\, p_2(n)\, q^{-2n} < 8k\left(\tfrac{2}{3}\, q^2\right)^{-n}.$$

Proof. It follows from the previous theorem and Lemma 2.1.5(b) that

$$|c_{\mathrm{U}}(n,q) - c_{\mathrm{U}}(n-1,q)| < (q+1)p_2(n)q^{-2n}$$

for $n \geqslant 2$. Arguing as in the proof of Theorem 2.1.6 we find that if $6 \leqslant n < n' \leqslant \infty$ then

$$|c_{\mathrm{U}}(n',q) - c_{\mathrm{U}}(n,q)| < (q+1)p_2(n)q^{-2n} \sum_{m=1}^{n'-n} (\tfrac{3}{2})^m q^{-2m},$$

from which it follows that $|c_{\mathrm{U}}(n',q) - c_{\mathrm{U}}(n,q)| < 3kp_2(n)q^{-2n}$. Lemma 1.3.9 gives, $|c_{\mathrm{U}}(n',q) - c_{\mathrm{U}}(n,q)| < 8k\big(\frac{2}{3}q^2\big)^{-n}$, as our theorem states.

As in the case of $s_{\mathrm{U}}(\infty,q)$, we do not know whether or not $c_{\mathrm{U}}(\infty,q)$ is, in fact, a rational function of q. It may be expressed as a power-series in q^{-1} whose first few terms may be calculated to be

$$1 - \frac{1}{q^3} - \frac{1}{q^5} + \frac{1}{q^6} - \frac{2}{q^7} + \frac{3}{q^8} - \frac{5}{q^9} + \frac{8}{q^{10}} - \frac{11}{q^{11}} + \frac{21}{q^{12}} + O\Big(\frac{1}{q^{13}}\Big).$$

For practical purposes we prove:

THEOREM 2.1.12. $$\frac{1-q^{-3}}{1+q^{-4}} < c_{\mathrm{U}}(\infty,q) < 1 - q^{-3}.$$

Proof. Since $c_{\mathrm{U}}(q) = \big((1-q^{-2})(1-q^{-3})/(1+q^{-4})\big)\,\widetilde{W}(-q^{-1})$ we seek estimates for $\widetilde{W}(-q^{-1})$. From the definition on p. 32,

$$\widetilde{W}(-q^{-1}) \;=\; \prod_{d\,\mathrm{odd}} \Big(1 + \frac{1}{(q^d+1)(q^{2d}-1)}\Big)^{\widetilde{N}(q;d)} \times \prod_{d\geqslant 1} \Big(1 + \frac{1}{(q^{2d}-1)(q^{4d}+1)}\Big)^{\widetilde{M}(q;d)},$$

and so certainly

$$\widetilde{W}(-q^{-1}) > \Big(1 + \frac{1}{(q+1)(q^2-1)}\Big)^{q+1} > 1 + \frac{1}{q^2-1}.$$

Therefore

$$c_{\mathrm{U}}(\infty,q) > \frac{(1-q^{-2})(1-q^{-3})}{(1+q^{-4})}\,\big(1 + \frac{1}{q^2-1}\big),$$

that is, $c_{\mathrm{U}}(\infty,q) > (1-q^{-3})(1+q^{-4})^{-1}$, which is the promised lower bound.

For the upper bound we use the fact that if $x > 0$ then $1 + x < \mathrm{e}^x$. This tells us that

$$\log \widetilde{W}(-q^{-1}) < \sum_{d\,\mathrm{odd}} \frac{\widetilde{N}(q;d)}{(q^d+1)(q^{2d}-1)} + \sum_{d\geqslant 1} \frac{\widetilde{M}(q;d)}{(q^{2d}-1)(q^{4d}+1)}.$$

In each of these sums we treat the first term separately; also, we use the fact that if $d > 1$ then $\widetilde{N}(q;d) < (q^d-1)/d$ and $\widetilde{M}(q;d) < (q^{2d}-1)/(2d)$. Thus

$$\log \widetilde{W}(-q^{-1}) < \tilde{A} + \sum_{d\,\mathrm{odd}} \frac{1}{dq^{2d}} + \sum_{d\geqslant 1} \frac{1}{2dq^{4d}} = \tilde{A} + \sum_{m\geqslant 1} \frac{1}{mq^{2m}},$$

where $\tilde{A} := \dfrac{\widetilde{N}(q;1)}{(q+1)(q^2-1)} - \dfrac{1}{q^2} + \dfrac{\widetilde{M}(q;1)}{(q^2-1)(q^4+1)} - \dfrac{1}{2q^4}$. Therefore

$$\log \widetilde{W}(-q^{-1}) < \tilde{A} + \log \frac{1}{1-q^{-2}}\,.$$

It follows that $\widetilde{W}(-q^{-1}) < \mathrm{e}^{\tilde{A}}/(1-q^{-2})$ and

$$c_{\mathrm{U}}(\infty,q) < \frac{(1-q^{-2})(1-q^{-3})}{(1+q^{-4})} \times \frac{\mathrm{e}^{\tilde{A}}}{(1-q^{-2})} = (1-q^{-3}) \times \frac{\mathrm{e}^{\tilde{A}}}{(1+q^{-4})}\,,$$

and what remains is to prove that $\mathrm{e}^{\tilde{A}} < 1+q^{-4}$. Here is a sketch of a proof. Since $\widetilde{N}(q;1) = q+1$ and $\widetilde{M}(q;1) = \frac{1}{2}(q^2-q-2)$,

$$\begin{aligned}\tilde{A} &= \frac{1}{q^2-1} - \frac{1}{q^2} + \frac{q^2-q-2}{2(q^2-1)(q^4+1)} - \frac{1}{2q^4} \\ &= \frac{2q^6-q^5-q^4+q^2+1}{2q^4(q^2-1)(q^4+1)}\,.\end{aligned}$$

It follows easily that

$$\tilde{A} < \frac{1}{q^4} - \frac{1}{2(q+1)(q^4+1)} < \frac{1}{q^4} - \frac{1}{2q^8} < \log(1+q^{-4})\,.$$

Therefore $\mathrm{e}^{\tilde{A}} < 1+q^{-4}$ and $c_{\mathrm{U}}(\infty,q) < 1-q^{-3}$, as the theorem states.

A relationship between the unitary and general linear groups. Let $S_{\mathrm{GL}}(q;u)$ and $C_{\mathrm{GL}}(q;u)$ be the generating functions for the probabilities that an element of $\mathrm{GL}(n,q)$ is separable or cyclic, respectively. In [**23**] Wall starts from the observation that

$$\begin{aligned}S_{\mathrm{GL}}(q;u) &= \prod_{d\geqslant 1} \Bigl(1 + \frac{u^d}{q^d-1}\Bigr)^{N(q;d)}\,, \\ C_{\mathrm{GL}}(q;u) &= \prod_{d\geqslant 1} \Bigl(1 + \frac{u^d}{q^d-1} + \frac{u^{2d}}{q^d(q^d-1)} + \frac{u^{3d}}{q^{2d}(q^d-1)} + \cdots\Bigr)^{N(q;d)}\,,\end{aligned}$$

and proves the lovely theorems that we have taken as the model for our treatment of the unitary groups. He proves that $C_{\mathrm{GL}}(q;u) = (1-u/q)\,S_{\mathrm{GL}}(q;u)/(1-u)$ and that $S_{\mathrm{GL}}(q;u)$ has an analytic continuation analytic in the open disc $D(q)$, except for a simple pole at $u=1$. The fact that the functions $S_{\mathrm{U}}(q;u)$, $C_{\mathrm{U}}(q;u)$ behave in the same way turns out to be no accident, as the following theorem shows.

THEOREM 2.1.13. $\quad S_{\mathrm{U}}(q;u) = \dfrac{S_{\mathrm{GL}}(q^2;u^2)}{S_{\mathrm{GL}}(-q;-u)}\,, \quad C_{\mathrm{U}}(q;u) = \dfrac{C_{\mathrm{GL}}(q^2;u^2)}{C_{\mathrm{GL}}(-q;-u)}\,.$

Proof. From Theorem 2.1.1 and Corollary 1.3.13 we know that

$$S_{\mathrm{U}}(q;u) = \prod_{d\,\mathrm{odd}} \Bigl(1 + \frac{u^d}{q^d+1}\Bigr)^{N(q;d)} \prod_{d\geqslant 1} \Bigl(1 + \frac{u^{2d}}{q^{2d}-1}\Bigr)^{N(q;2d)}\,.$$

Replacing q by $-q$ and u by $-u$ we find that

$$S_{\mathrm{U}}(-q;-u) = \prod_{d\,\mathrm{odd}} \Bigl(1 + \frac{u^d}{q^d-1}\Bigr)^{N(-q;d)} \prod_{d\geqslant 1} \Bigl(1 + \frac{u^{2d}}{q^{2d}-1}\Bigr)^{N(-q;2d)}\,,$$

where now $N(q';d)$ for negative q' has to be defined by Lemma 1.3.10(a). Clearly, $N(-q;d) = -N(q;d)$ if d is odd and so

$$S_{\mathrm{U}}(-q;-u) = S_{\mathrm{GL}}(q;u)^{-1} \times F(q;u)\,,$$

where

$$F(q;u) := \prod_{d\geqslant 1} \Big(1 + \frac{u^{2d}}{q^{2d}-1}\Big)^{N(q;2d)+N(-q;2d)}\,.$$

From Lemma 1.3.10(a) it is easy to see that $N(q;2d)+N(-q;2d) = N(q^2;d)$ for all d. Therefore $F(q;u) = S_{\mathrm{GL}}(q^2;u^2)$ and $S_{\mathrm{U}}(q;u) = S_{\mathrm{GL}}(-q;-u)^{-1}\, S_{\mathrm{GL}}(q^2;u^2)$.

The analogous fact for C_{U} can be proved in the same way or it can be deduced from Theorem 2.1.8 and the corresponding theorem proved by Wall for the general linear groups.

Two points about this theorem are worthy of note. First, the method can be applied to the generating functions for probabilities of quite a wide range of events in the unitary groups. It is applicable whenever the property of the matrix X (such as being separable, being cyclic, or being semisimple) is such that the restriction on the partitions associated to irreducible polynomials by the rational canonical form of X (as described by Fulman in his work on cycle index generating functions [**5, 6**]) is independent of the polynomial. Secondly, one might hope that since the residue of $S_{\mathrm{GL}}(u)$ at its pole at $u = 1$ is a rational function of q, it might be possible to deduce that the same was true of the residue of $S_{\mathrm{U}}(u)$ there, hence of $s_{\mathrm{U}}(\infty, q)$. We have been unable to do this and do not know whether or not $s_{\mathrm{U}}(\infty, q)$ is a rational function of q.

2.2. The symplectic groups

The symplectic group $\mathrm{Sp}(2m,q)$ is that subgroup of $\mathrm{GL}(2m,q)$ which preserves a non-degenerate alternating form on V, the vector space $\mathbb{F}_q^{2m}$ on which $\mathrm{GL}(2m,q)$ naturally acts. Recall that an alternating form on V is a bilinear map $\langle\rangle : V\times V \to \mathbb{F}_q$ such that $\langle x,x\rangle = 0$ for all $x \in V$, and that non-degenerate alternating forms exist only on even dimensional spaces. One such form on V is given by $\langle x,y\rangle = \sum_{i=1}^{m}(x_{2i-1}y_{2i} - x_{2i}y_{2i-1})$, where $x = (x_1,\ldots,x_{2m})$ and $y = (y_1,\ldots,y_{2m})$, and any other is equivalent to this (see, for example, [**21**, Chapter 8 and Theorem 7.4]), so $\mathrm{Sp}(2m,q)$ is unique up to conjugacy in $\mathrm{GL}(2m,q)$. The order of $\mathrm{Sp}(2m,q)$ is $q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)$.

Separable symplectic matrices. Let $S_{\mathrm{Sp}}(u)$ (or $S_{\mathrm{Sp}}(q;u)$ when the dependence on q needs to be made explicit) be the generating function for the probability $s_{\mathrm{Sp}}(2m,q)$ that an element of a finite symplectic group over $\mathbb{F}_q$ is separable. It turns out to be convenient to index the terms of the generating function by the parameter (in this case Lie rank) m, where $n = 2m$ as in Table 1 (p. 7). Thus,

$$S_{\mathrm{Sp}}(u) := S_{\mathrm{Sp}}(q;u) := 1 + \sum_{m\geqslant 1} s_{\mathrm{Sp}}(2m,q)\,u^m\,.$$

First we derive an infinite product expression for $S_{\mathrm{Sp}}(u)$ analogous to Wall's product expansion for $S_{\mathrm{GL}}(u)$ and to the expression for $S_{\mathrm{U}}(u)$ in Theorem 2.1.1. As for both those theorems, this result can be derived from the factorisation of the cycle index for the symplectic groups in [**6**, Theorem 12]. We sketch a direct proof analogous to the proof given for Theorem 2.1.1 above.

THEOREM 2.2.1. *With $N^*(q;d)$ and $M^*(q;d)$ defined as on p. 26 we have*

$$S_{\mathrm{Sp}}(u) = \prod_{d\geqslant 1}\Big(1+\frac{u^d}{q^d+1}\Big)^{N^*(q;2d)} \prod_{d\geqslant 1}\Big(1+\frac{u^d}{q^d-1}\Big)^{M^*(q;d)}.$$

Proof. Let X be a separable symplectic matrix. The vector space V has even dimension and admits an X-invariant primary decomposition with one summand for each monic irreducible $*$-self-conjugate (as defined on p. 25) polynomial dividing $c_X(t)$, and one summand for each conjugate pair of monic irreducible non-self-conjugate polynomials dividing $c_X(t)$. In particular, each primary summand is nonsingular and therefore has even dimension. It follows that the polynomials $t-1$ and $t+1$ do not divide $c_X(t)$, and hence that the characteristic polynomial $c_X(t)$ of a separable matrix $X \in \mathrm{Sp}(2m,q)$ is a product of monic irreducible self-conjugate polynomials of even degree (see Lemma 1.3.15(c)), and conjugate pairs of monic irreducible non-self-conjugate polynomials.

The remainder of the proof is very similar to that given for Theorem 2.1.1. We simply note (see [**22**, p.38] for proofs) that, if the characteristic polynomial of $X \in \mathrm{Sp}(2d,q)$ is a monic irreducible self-conjugate polynomial, then $|C_{\mathrm{Sp}(2d,q)}(X)| = q^d+1$, while if $c_X(t) = \phi(t)\phi^*(t)$, with $\phi(t)$ irreducible and non-self-conjugate, then $|C_{\mathrm{Sp}(2d,q)}(X)| = q^d-1$.

Just as in the general linear and unitary cases, there are other infinite product expansions for $S_{\mathrm{Sp}}(u)$ which exhibit the fact that it has a continuation to a larger disc, in which it is analytic apart from a simple pole at $u=1$. These allow us to apply Lemma 1.3.3 to prove the existence and determine the limiting probability $s_{\mathrm{Sp}}(\infty,q)$. In the symplectic case the function corresponding to Wall's $S(q,z)$ in [**23**, §6] is defined by

$$V^*(u) := \prod_{d\geqslant 1}\Big(1-\frac{u^d(u^d+1)}{q^d(q^d+1)}\Big)^{N^*(q;2d)} \prod_{d\geqslant 1}\Big(1-\frac{u^d(u^d-1)}{q^d(q^d-1)}\Big)^{M^*(q;d)},$$

and there are two functions which are analogues of his $T(q,z)$, namely,

$$W_1^*(u) := \prod_{d\geqslant 1}\Big(1-\frac{1}{q^d+1}\,\frac{u^d}{q^d+u^d}\Big)^{N^*(q;2d)} \prod_{d\geqslant 1}\Big(1+\frac{1}{q^d-1}\,\frac{u^d}{q^d+u^d}\Big)^{M^*(q;d)},$$

and

$$W_2^*(u) := \prod_{d\geqslant 1}\Big(1+\frac{1}{q^d+1}\,\frac{u^d}{q^d-u^d}\Big)^{N^*(q;2d)} \prod_{d\geqslant 1}\Big(1+\frac{1}{q^d-1}\,\frac{u^d}{q^d+u^d}\Big)^{M^*(q;d)}.$$

From Corollary 1.3.2 it follows easily that V^* is analytic in the open disc $D(\sqrt{q})$ and W_1^*, W_2^* are analytic in $D(q)$.

THEOREM 2.2.2. *Let $e := e(q)$ (that is, recall, $e=1$ if q is even and $e=2$ if q is odd). Then*

$$S_{\mathrm{Sp}}(u) \;=\; \frac{(1-\frac{u}{q})^e}{1-u}V^*(u) \;=\; \frac{(1-\frac{u^2}{q})}{(1-u)(1+\frac{u}{q})^e}\,W_1^*(u),$$

where $V^*(u)$ and $W_1^*(u)$ are as defined above.

Proof. From Lemma 1.3.17(a) (with u replaced by u/q), and Theorem 2.2.1, we have that

$$\begin{aligned} S_{\mathrm{Sp}}(u) &= \frac{(1-\frac{u}{q})^e}{1-u}\prod_{d\geqslant 1}\Big(\Big(1+\frac{u^d}{q^d+1}\Big)\Big(1-\frac{u^d}{q^d}\Big)\Big)^{N^*(q;2d)} \\ &\qquad\qquad \times\prod_{d\geqslant 1}\Big(\Big(1+\frac{u^d}{q^d-1}\Big)\Big(1-\frac{u^d}{q^d}\Big)\Big)^{M^*(q;d)} \\ &= \frac{(1-\frac{u}{q})^e}{1-u}\prod_{d\geqslant 1}\Big(1-\frac{u^d(u^d+1)}{q^d(q^d+1)}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1-\frac{u^d(u^d-1)}{q^d(q^d-1)}\Big)^{M^*(q;d)} \\ &= \frac{(1-\frac{u}{q})^e}{1-u}\,V^*(u)\,. \end{aligned}$$

To derive the second expression for $S_{\mathrm{Sp}}(u)$ we start from Theorem 2.2.1 and use Lemma 1.3.17(a) twice, once with u replaced by u/q and once with u replaced by $(u/q)^2$, to get that

$$S_{\mathrm{Sp}}(u) = \frac{(1-\frac{u^2}{q})(1-\frac{u}{q})^e}{(1-u)(1-\frac{u^2}{q^2})^e}\,S(u)T(u) = \frac{(1-\frac{u^2}{q})}{(1-u)(1+\frac{u}{q})^e}\,S(u)T(u)\,,$$

where

$$S(u) := \prod_{d\geqslant 1}\Big(\Big(\frac{1-(\frac{u}{q})^d}{1-(\frac{u}{q})^{2d}}\Big)\Big(1+\frac{u^d}{q^d+1}\Big)\Big)^{N^*(q;2d)}$$

and

$$T(u) := \prod_{d\geqslant 1}\Big(\Big(\frac{1-(\frac{u}{q})^d}{1-(\frac{u}{q})^{2d}}\Big)\Big(1+\frac{u^d}{q^d-1}\Big)\Big)^{M^*(q;d)}\,.$$

The proof is now completed in exactly the same way as that of Theorem 2.1.2.

THEOREM 2.2.3. *Let $e := e(q)$. Then*

$$\begin{aligned} s_{\mathrm{Sp}}(\infty,q) &= \Big(1-\frac{1}{q}\Big)^e V^*(1) \\ &= \Big(1-\frac{1}{q}\Big)^e\prod_{d\geqslant 1}\Big(1-\frac{2}{q^d(q^d+1)}\Big)^{N^*(q;2d)}. \end{aligned}$$

Also,

$$\begin{aligned} s_{\mathrm{Sp}}(\infty,q) &= \frac{(1-\frac{1}{q})^{e+1}}{(1-\frac{1}{q^2})^e}\,W_1^*(1) \\ &= \frac{(1-\frac{1}{q})^{e+1}}{(1-\frac{1}{q^2})^e}\prod_{d\geqslant 1}\Big(1-\frac{1}{(q^d+1)^2}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\frac{1}{(q^{2d}-1)}\Big)^{M^*(q;d)}. \end{aligned}$$

If $1<r<q$ then $|s_{\mathrm{Sp}(2m,q)} - s_{\mathrm{Sp}(\infty,q)}| < o(r^{-m})$ as $m\to\infty$.

This follows immediately from the previous theorem and Lemma 1.3.3. As in the case of the unitary groups (see Theorem 2.1.5), the last assertion of this theorem can be made more explicit.

LEMMA 2.2.4. (a) *Let $A(u) := (1-qu)S_{\mathrm{Sp}}(qu)$. Then*

$$|A|(u) \ll \frac{(q-1)}{(1-u)^e}\Omega(u)^{-1}\,,$$

where $e = e(q)$ *and* $\Omega(u)$ *is as defined on p.* 20.

(b) $|s_{\mathrm{Sp}}(2m,q) - s_{\mathrm{Sp}}(2m-2,q)| < (q-1)p_{e+1}(m)q^{-m}$, *where* $p_r(m)$ *is as defined on p.* 20.

Proof. By Theorem 2.2.2 $(1-qu)S_{\mathrm{Sp}}(qu) = \dfrac{1-qu^2}{(1+u)^e}\, W_1^*(qu)$, where

$$W_1^*(qu) = \prod_{d\geqslant 1}\Big(1 - \frac{1}{q^d+1}\,\frac{u^d}{1+u^d}\Big)^{N^*(q;2d)} \prod_{d\geqslant 1}\Big(1 + \frac{1}{q^d-1}\,\frac{u^d}{1+u^d}\Big)^{M^*(q;d)}.$$

Lemma 1.3.5(b) gives that $|A|(u) \ll \dfrac{(q-1)}{(1-u)^e}\,|W_1^*|(qu)$. Apply Lemma 1.3.6:

$$|W_1^*|(qu) \ll \exp\sum_{d\geqslant 1}\Big(\frac{N^*(q;2d)}{q^d+1}\,\frac{u^d}{1-u^d} + \frac{M^*(q;d)}{q^d-1}\,\frac{u^d}{1-u^d}\Big).$$

From Lemma 1.3.16 we know that $N^*(q;2d) < (q^d+1)/(2d)$ and $M^*(q;2d) \leqslant (q^d-1)/(2d)$. Therefore

$$|W_1^*|(qu) \ll \exp\sum_{d\geqslant 1}\Big(\frac{1}{2d}\,\frac{u^d}{1-u^d} + \frac{1}{2d}\,\frac{u^d}{1-u^d}\Big) = \exp\sum_{d\geqslant 1}\Big(\frac{1}{d}\,\frac{u^d}{1-u^d}\Big).$$

Thus $|W_1^*|(qu) \ll \Omega(u)^{-1}$ by Lemma 1.3.7 and so we have (a). Part (b) follows immediately from Lemma 1.3.8.

In the same way as for the unitary groups we can now derive the following explicit estimates for the rate of convergence of $s_{\mathrm{Sp}}(2m,q)$ to $s_{\mathrm{Sp}}(\infty,q)$.

THEOREM 2.2.5. *Let* $k := (q-1)/(2q-3)$.
If q *is odd and* $9 \leqslant m < m' \leqslant \infty$ *then*

$$|s_{\mathrm{Sp}}(2m',q) - s_{\mathrm{Sp}}(2m,q)| < 3k\,p_3(m)q^{-m} < 23k\,\big(\tfrac{2}{3}\,q\big)^{-m}.$$

If q *is even and* $6 \leqslant m < m' \leqslant \infty$ *then*

$$|s_{\mathrm{Sp}}(2m',q) - s_{\mathrm{Sp}}(2m,q)| < 3k\,p_2(m)q^{-m} < 8k\,\big(\tfrac{2}{3}\,q\big)^{-m}.$$

The derivation of this from the previous lemma using Lemma 1.3.9 is exactly the same as that of Theorem 2.1.6 from Lemma 2.1.5 and is therefore omitted.

Using Theorem 2.2.3 and Lemma 1.3.16(a), one may express $s_{\mathrm{Sp}}(\infty,q)$ as a power series in q^{-1}. Its leading terms are not hard to calculate: if q is odd they are

$$1 - \frac{3}{q} + \frac{5}{q^2} - \frac{10}{q^3} + \frac{23}{q^4} - \frac{49}{q^5} + \frac{100}{q^6} - \frac{208}{q^7} + \frac{439}{q^8} - \frac{915}{q^9} + O\Big(\frac{1}{q^{10}}\Big),$$

while if q is even they are

$$1 - \frac{2}{q} + \frac{2}{q^2} - \frac{4}{q^3} + \frac{9}{q^4} - \frac{17}{q^5} + \frac{32}{q^6} - \frac{64}{q^7} + \frac{130}{q^8} - \frac{258}{q^9} + O\Big(\frac{1}{q^{10}}\Big).$$

The following explicit bounds are useful in practice.

THEOREM 2.2.6. *If* q *is odd then*

$$1 - \frac{3}{q} + \frac{5}{q^2} - \frac{10}{q^3} + \frac{12}{q^4} < s_{\mathrm{Sp}}(\infty,q) < 1 - \frac{3}{q} + \frac{5}{q^2} - \frac{10}{q^3} + \frac{23}{q^4},$$

and if q is even then

$$1-\frac{2}{q}+\frac{2}{q^2}-\frac{4}{q^3}+\frac{4}{q^4}<s_{\mathrm{Sp}}(\infty,q)<1-\frac{2}{q}+\frac{2}{q^2}-\frac{4}{q^3}+\frac{9}{q^4}\,.$$

For small values of q we have

$$0.2833<s_{\mathrm{Sp}}(\infty,2)<0.2881 \quad \textit{and} \quad 0.3487<s_{\mathrm{Sp}}(\infty,3)<0.3493\,.$$

Proof. The calculation has to be done with a little care if errors are to be of order at most q^{-4}. For the lower bound we use the first expression for $s_{\mathrm{Sp}}(\infty,q)$ and seek estimates for the infinite product in Theorem 2.2.3. We start from the observation that

$$\frac{1-1/q^{2d}}{1+1/q^{2d}}=1-\frac{2}{q^{2d}+1}<1-\frac{2}{q^d(q^d+1)}\,.$$

Define

$$A_1^*:=\prod_{d\geqslant 1}\left(\Big(\frac{1+\frac{1}{q^{2d}}}{1-\frac{1}{q^{2d}}}\Big)\Big(1-\frac{2}{q^d(q^d+1)}\Big)\right)^{N^*(q;2d)}\,.$$

Then

$$s_{\mathrm{Sp}}(\infty,q)=\Big(1-\frac{1}{q}\Big)^e A_1^*\prod_{d\geqslant 1}\left(\frac{1-\frac{1}{q^{2d}}}{1+\frac{1}{q^{2d}}}\right)^{N^*(q;2d)}\,.$$

Substituting $u:=1/q^2$ into the equation of Lemma 1.3.17(e) we find that

$$s_{\mathrm{Sp}}(\infty,q)=A_1^*\,\frac{\big(1-\frac{1}{q}\big)^{e+1}}{\big(1-\frac{1}{q^2}\big)^{e-1}}\,,$$

and it remains to bound A_1^* from below. It is easy to calculate that

$$\left(\frac{1+\frac{1}{q^{2d}}}{1-\frac{1}{q^{2d}}}\right)\left(1-\frac{2}{q^d(q^d+1)}\right)=1+\frac{2}{q^d(q^d+1)^2}\,,$$

and so $A_1^*=\displaystyle\prod_{d\geqslant 1}\Big(1+\frac{2}{q^d(q^d+1)^2}\Big)^{N^*(q;2d)}$. In the product defining A_1^* each factor >1, and so

$$A_1^*>\Big(1+\frac{2}{q(q+1)^2}\Big)^{\frac{1}{2}(q+1-e)}\Big(1+\frac{2}{q^2(q^2+1)^2}\Big)^{\frac{1}{4}(q^2+1-e)}\,.$$

Substituting small values of q we find that $s_{\mathrm{Sp}}(\infty,2)>0.2833\cdots$ and $s_{\mathrm{Sp}}(\infty,3)>0.3487\cdots$. For general q we use the fact that

$$1+\frac{2}{q^d(q^d+1)^2}>1+\frac{2}{q^{3d}}-\frac{4}{q^{4d}}$$

to see that

$$\begin{aligned}
A_1^* &> \Big(1+\frac{2}{q^3}-\frac{4}{q^4}\Big)^{\frac{1}{2}(q+1-e)}\Big(1+\frac{2}{q^6}-\frac{4}{q^8}\Big)^{\frac{1}{4}(q^2+1-e)}\\
&> 1+\Big(\frac{q+1-e}{2}\Big)\Big(\frac{2}{q^3}-\frac{4}{q^4}\Big)+\Big(\frac{q^2+1-e}{4}\Big)\Big(\frac{2}{q^6}-\frac{4}{q^8}\Big)\\
&= 1+\frac{1}{q^2}-\frac{1+e}{q^3}+\frac{2(e-1)}{q^4}+\frac{1}{2q^4}-\frac{1+e}{2q^6}+\frac{e-1}{q^8}\\
&> 1+\frac{1}{q^2}-\frac{1+e}{q^3}+\frac{2(e-1)}{q^4}\,.
\end{aligned}$$

Now if q is odd then

$$s_{\mathrm{Sp}}(\infty,q) > \Big(1+\frac{1}{q^2}-\frac{3}{q^3}+\frac{2}{q^4}\Big)\,\frac{(1-\frac{1}{q})^2}{(1+\frac{1}{q})}\,,$$

and the bound $s_{\mathrm{Sp}}(\infty,q) > 1-\frac{3}{q}+\frac{5}{q^2}-\frac{10}{q^3}+\frac{12}{q^4}$ follows by elementary algebra. If q is even then

$$s_{\mathrm{Sp}}(\infty,q) > \Big(1+\frac{1}{q^2}-\frac{2}{q^3}\Big)\Big(1-\frac{1}{q}\Big)^2\,,$$

and our lower bound for $s_{\mathrm{Sp}}(\infty,q)$ follows again by elementary algebra.

For the upper bound we use the second expression for $s_{\mathrm{Sp}}(\infty,q)$ in Theorem 2.2.3 and seek a good bound for $W_1^*(1)$. We have

$$\begin{aligned} W_1^*(1) &= \prod_{d\geqslant 1}\Big(1-\frac{1}{(q^d+1)^2}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\frac{1}{(q^{2d}-1)}\Big)^{M^*(q;d)} \\ &= A_2^*\prod_{d\geqslant 1}\Big(\Big(1-\frac{1}{(q^d+1)^2}\Big)\Big(1+\frac{1}{q^{2d}-1}\Big)\Big)^{N^*(q;2d)}\,, \end{aligned}$$

where

$$A_2^* := \prod_{d\geqslant 1}\Big(1+\frac{1}{q^{2d}-1}\Big)^{M^*(q;d)-N^*(q;2d)} = \prod_{d\geqslant 1}\Big(1-\frac{1}{q^{2d}}\Big)^{N^*(q;2d)-M^*(q;d)}\,.$$

Now define $A_3^* := \prod_{d\geqslant 1}\alpha(q^d)^{N^*(q;2d)}$, where

$$\alpha(x) := \Big(1-\frac{1}{(x+1)^2}\Big)\Big(1+\frac{1}{x^2-1}\Big)\Big(\frac{x^3-1}{x^3+1}\Big)\,.$$

Then

$$\begin{aligned} s_{\mathrm{Sp}}(\infty,q) &= \frac{(1-\frac{1}{q})^{e+1}}{(1-\frac{1}{q^2})^e}\,A_2^*\,A_3^*\prod_{d\geqslant 1}\Big(\frac{1+\frac{1}{q^{3d}}}{1-\frac{1}{q^{3d}}}\Big)^{N^*(q;2d)} \\ &= \frac{(1-\frac{1}{q})^{e+1}(1-\frac{1}{q^3})^{e-1}}{(1-\frac{1}{q^2})^{e+1}}\,A_2^*\,A_3^* \end{aligned}$$

by Lemma 1.3.17(e). Since $1-\frac{1}{q^{2d}}<1$ for $d\geqslant 1$ and $N^*(q;2d)-M^*(q;d)\geqslant 0$ (see Lemma 1.3.16(c)) we know that

$$A_2^* < \Big(1-\frac{1}{q^2}\Big)^{N^*(q;2)-M^*(q;1)}\Big(1-\frac{1}{q^4}\Big)^{N^*(q;4)-M^*(q;2)}\,,$$

and so by Lemma 1.3.16(c) again

$$A_2^* < \Big(1-\frac{1}{q^2}\Big)\Big(1-\frac{1}{q^4}\Big)^{N^*(q;2)} = \Big(1-\frac{1}{q^2}\Big)\Big(1-\frac{1}{q^4}\Big)^{\frac{1}{2}(q+1-e)}\,.$$

Also, $\alpha(q^d)<1$ for all d and so $A_3^* < \alpha(q)^{\frac{1}{2}(q+1-e)}$. Thus we find that

$$s_{\mathrm{Sp}}(\infty,q) < \frac{(1-\frac{1}{q})^{e+1}(1-\frac{1}{q^3})^{e-1}}{(1-\frac{1}{q^2})^e}\,\Big(\Big(1-\frac{1}{q^4}\Big)\alpha(q)\Big)^{\frac{1}{2}(q+1-e)}\,.$$

Substituting $q=2,\ e=1$ we find that $s_{\mathrm{Sp}}(\infty,2) < 0.2880\cdots$ and substituting $q=3,\ e=2$ we get $s_{\mathrm{Sp}}(\infty,3) < 0.3492\cdots$ by direct calculation. For larger values

of q we use the facts (which we leave the reader to check) that $\left(1-\frac{1}{q^4}\right)\alpha(q) < 1-\frac{4}{q^4}+\frac{6}{q^5}$ and

$$\left(1-\frac{4}{q^4}+\frac{6}{q^5}\right)^{\frac{1}{2}(q+1-e)} < 1-\frac{2}{q^3}+\frac{2e+1}{q^4}+\frac{2-e}{q^5}\,.$$

It is now routine manipulation to show that if q is odd (so that $e=2$) then

$$\frac{(1-\frac{1}{q})^3(1-\frac{1}{q^3})}{(1-\frac{1}{q^2})^2}\left(1-\frac{2}{q^3}+\frac{5}{q^4}\right) < 1-\frac{3}{q}+\frac{5}{q^2}-\frac{10}{q^3}+\frac{23}{q^4}\,,$$

while if q is even (so that $e=1$) then

$$\frac{(1-\frac{1}{q})^2}{(1-\frac{1}{q^2})}\left(1-\frac{2}{q^3}+\frac{3}{q^4}+\frac{1}{q^5}\right) < 1-\frac{2}{q}+\frac{2}{q^2}-\frac{4}{q^3}+\frac{9}{q^4}\,,$$

and this completes the proof of the theorem.

Cyclic symplectic matrices. Let $C_{\mathrm{Sp}}(u)$ be the generating function for the probability $c_{\mathrm{Sp}}(2m,q)$ that an element of a finite symplectic group over $\mathbb{F}_q$ is cyclic. As in the case of separable symplectic matrices, we index the terms of the power series by the Lie rank m. Thus

$$C_{\mathrm{Sp}}(u) := 1+\sum_{m\geqslant 1} c_{\mathrm{Sp}}(2m,q)\,u^m\,.$$

First we state an infinite product expression for $C_{\mathrm{Sp}}(u)$ which is analogous to the expression for $C_{\mathrm{U}}(u)$ in Theorem 2.1.7.

THEOREM 2.2.7. *Let $e := e(q)$. Then*

$$C_{\mathrm{Sp}}(u) = \left(\frac{1}{1-\frac{u}{q}}\right)^e \prod_{d\geqslant 1}\left(1+\frac{u^d}{(q^d+1)(1-\frac{u^d}{q^d})}\right)^{N^*(q;2d)} \times \prod_{d\geqslant 1}\left(1+\frac{u^d}{(q^d-1)(1-\frac{u^d}{q^d})}\right)^{M^*(q;d)}.$$

As for Theorem 2.1.7, this result can be derived from the factorisation of the cycle index for the symplectic groups given in [**6**]. There is also a direct proof which is analogous to that given for unitary groups. There are two variations from the unitary case. First, the form of the infinite product expression is a little different from that for the unitary groups. The reason is that the polynomials $t-1$ and $t+1$, as the only self-conjugate polynomials of odd degree (see Theorem 1.3.16), require a separate term in the product. These polynomials correspond to plus and minus cyclic unipotent symplectic matrices. Secondly, computing this term causes a slight complication, since if $m\geqslant 2$, the cyclic unipotent matrices in $\mathrm{Sp}(2m,q)$ form two conjugacy classes (rather than a single class), with each such matrix having a centraliser of order $2q^m$ (see [**22**, p.36]). We leave further details to the reader and turn to two different infinite product expressions for $C_{\mathrm{Sp}}(u)$.

THEOREM 2.2.8. *Let $e := e(q)$ and let $W_2^*(u)$ be as defined on p. 43. Then*

(a)

$$C_{\mathrm{Sp}}(u) = \frac{1}{1-u}\prod_{d\geqslant 1}\Big(1-\frac{u^d}{q^d(q^d+1)}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\frac{u^d}{q^d(q^d-1)}\Big)^{M^*(q;d)}.$$

(b) $$C_{\mathrm{Sp}}(u) = \frac{(1-\frac{u^2}{q^3})(1-\frac{u}{q^2})}{(1-u)(1-\frac{u^2}{q^4})^e}\,W_2^*(u/q)\,.$$

(c) *In particular, $C_{\mathrm{Sp}}(u)$ has a continuation to a function which is analytic in the open disc $D(q^2)$ except for a simple pole at $u=1$.*

Proof. Since

$$\Big(1-\frac{u^d}{q^d}\Big)\Big(1+\frac{u^d}{(q^d+1)(1-\frac{u^d}{q^d})}\Big) = 1-\frac{u^d}{q^d(q^d+1)}\,,$$

and

$$\Big(1-\frac{u^d}{q^d}\Big)\Big(1+\frac{u^d}{(q^d-1)(1-\frac{u^d}{q^d})}\Big) = 1+\frac{u^d}{q^d(q^d-1)}\,,$$

part (a) follows from Theorem 2.2.7 by means of Lemma 1.3.17(a) with u replaced by u/q. To derive (b) we divide each factor $1-(u^d/q^d(q^d+1))$ in (a) by $(1-(u^d/q^{2d}))$ and each factor $1+(u^d/q^d(q^d-1))$ by $(1+(u^d/q^{2d}))$. Then from Lemma 1.3.19(a)$[-(u/q)^d, q^d]$ and Lemma 1.3.19(a)$[-(u/q)^d, -q^d]$, together with definition of $W_2^*(u)$, it follows that

$$C_{\mathrm{Sp}}(u)\prod_{d\geqslant 1}\Big(1-\frac{u^d}{q^{2d}}\Big)^{-N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\frac{u^d}{q^{2d}}\Big)^{-M^*(q;d)} = \frac{1}{1-u}\,W_2^*(u/q)\,.$$

It now follows from Lemma 1.3.17(c) that

$$C_{\mathrm{Sp}}(u)\,\frac{(1-\frac{u}{q^2})^{e-1}(1+\frac{u}{q^2})^e}{(1-\frac{u^2}{q^3})} = \frac{1}{1-u}\,W_2^*(u/q)\,,$$

and (b) follows, as does (c) since $W_2^*(u)$ is analytic in the disc $D(q)$.

We can now determine the limiting value $c_{\mathrm{Sp}}(\infty, q)$. The following theorem is an immediate consequence of the preceding one and Corollary 1.3.2.

THEOREM 2.2.9.

$$c_{\mathrm{Sp}}(\infty,q) = \prod_{d\geqslant 1}\Big(1-\frac{1}{q^d(q^d+1)}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\frac{1}{q^d(q^d-1)}\Big)^{M^*(q;d)}$$

and

$$\begin{aligned} c_{\mathrm{Sp}}(\infty,q) &= \frac{(1-q^{-3})(1-q^{-2})}{(1-q^{-4})^e}\,W_2^*(q^{-1}) \\ &= \frac{(1-q^{-3})(1-q^{-2})}{(1-q^{-4})^e}\prod_{d\geqslant 1}\Big(1+\frac{1}{(q^d+1)(q^{2d}-1)}\Big)^{N^*(q;2d)} \\ &\qquad\qquad \times\prod_{d\geqslant 1}\Big(1+\frac{1}{(q^d-1)(q^{2d}+1)}\Big)^{M^*(q;d)}. \end{aligned}$$

Furthermore, if $1<r<q^2$ then $|c_{\mathrm{Sp}}(2m,q)-c_{\mathrm{Sp}}(\infty,q)|<o(r^{-m})$ as $m\to\infty$.

Our next result, which has some curiosity value in its own right, and is analogous to, though rather different from, Theorem 2.1.10 and Wall's formula (3.17) in [**23**], leads to an explicit convergence-rate.

THEOREM 2.2.10. *Let $s'_{\mathrm{Sp}}(m,q)$ be the probability that an element of $\mathrm{Sp}(2m,q)$ is separable and its characteristic polynomial has an even number of self-conjugate irreducible factors, and define $s''_{\mathrm{Sp}}(m,q)$ to be the probability that an element is separable and its characteristic polynomial has an odd number of self-conjugate irreducible factors. Then*

$$c_{\mathrm{Sp}}(2m,q) - c_{\mathrm{Sp}}(2m-2,q) = q^{-m}\big(s'_{\mathrm{Sp}}(m,q) - s''_{\mathrm{Sp}}(m,q)\big)\,.$$

Proof. From Theorem 2.2.8 (a)

$$(1-u)C_{\mathrm{Sp}}(u) = \prod_{d\geqslant 1}\Big(1-\frac{(u/q)^d}{q^d+1}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\frac{(u/q)^d}{q^d-1}\Big)^{M^*(q;d)}.$$

The coefficient of u^m in $(1-u)C_{\mathrm{Sp}}(u)$ is $c_{\mathrm{Sp}}(2m,q) - c_{\mathrm{Sp}}(2m-2,q)$, while the coefficient of u^m in the infinite product expression on the right side of this equation is $q^{-m}p_m$, where p_m is the coefficient of u^m in

$$\prod_{d\geqslant 1}\Big(1-\frac{u^d}{q^d+1}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\frac{u^d}{q^d-1}\Big)^{M^*(q;d)}.$$

It follows from Theorem 2.2.1 that $p_m = s'_{\mathrm{Sp}}(m,q) - s''_{\mathrm{Sp}}(m,q)$ and the theorem is proved.

COROLLARY 2.2.11. $\quad |c_{\mathrm{Sp}}(\infty,q) - c_{\mathrm{Sp}}(2m,q)| \leqslant \dfrac{1}{(q-1)q^m}\,.$

Proof. Since, obviously, $|s'_{\mathrm{Sp}}(k,q) - s''_{\mathrm{Sp}}(k,q)| \leqslant 1$ for all k, we have as required that $|c_{\mathrm{Sp}}(\infty,q) - c_{\mathrm{Sp}}(2m,q)| < \displaystyle\sum_{k\geqslant m+1} q^{-k} = 1/((q-1)q^m)$.

In order to improve the estimate in this corollary one may use Wall's method of comparison of power series. Recall that $\Omega(u) = \prod_{i\geqslant 1}(1-u^i)$.

LEMMA 2.2.12. *Let $A(u) := (1-q^2u)C_{\mathrm{Sp}}(q^2u)$. Then*

$$|A|(u) \ll \frac{(q-1)}{(1-u)^e}\,\Omega(u)^{-1}\,,$$

where $e = e(q)$ and $\Omega(u)$ is as defined on p. 20.

Proof. By Theorem 2.2.8(b),

$$A(u) = \frac{(1-qu^2)(1-u)}{(1-u^2)^e}\,W_2^*(qu) = \frac{(1-qu^2)}{(1+u)(1-u^2)^{e-1}}\,W_2^*(qu)\,.$$

Using Lemma 1.3.5(b) and the fact that $(1-u^2)^{-1} \ll (1-u)^{-1}$ we derive that $|A|(u) \ll (q-1)(1-u)^{-e}\,|W_2^*|(qu)$. Now

$$W_2^*(qu) = \prod_{d\geqslant 1}\Big(1+\frac{1}{q^d+1}\,\frac{u^d}{1-u^d}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\frac{1}{q^d-1}\,\frac{u^d}{1+u^d}\Big)^{M^*(q;d)}$$

and the method of proof of Lemma 2.2.4 yields that $|W_2^*(qu)| \ll \Omega(u)^{-1}$. Thus $|A|(u) \ll (q-1)(1-u)^{-e}\,\Omega(u)^{-1}$, as the lemma states.

Comparing this lemma with Lemma 2.2.4(a) we see that essentially the same theorem will follow, except for a change of q to q^2 at certain points:

THEOREM 2.2.13. *Let $k := (q-1)/(2q^2-3)$. If q is odd and $9 \leqslant m < m' \leqslant \infty$ then*

$$|c_{\mathrm{Sp}}(2m', q) - c_{\mathrm{Sp}}(2m, q)| < 3k\, p_3(m) q^{-2m} < 23k \left(\tfrac{2}{3}\, q^2\right)^{-m}.$$

If q is even and $6 \leqslant m < m' \leqslant \infty$ then

$$|c_{\mathrm{Sp}}(2m', q) - c_{\mathrm{Sp}}(2m, q)| < 3k\, p_2(m) q^{-2m} < 8k \left(\tfrac{2}{3}\, q^2\right)^{-m}.$$

Details of the proofs are left to the reader.

Using the values of $N^*(2d)$ and $M^*(d)$ given in Lemma 1.3.16, one may express $c_{\mathrm{Sp}}(\infty, q)$ as a power series in q^{-1}. For odd q the leading terms are

$$1 - \frac{3}{q^3} + \frac{2}{q^4} - \frac{3}{q^5} + \frac{8}{q^6} - \frac{11}{q^7} + \frac{19}{q^8} - \frac{32}{q^9} + O\Big(\frac{1}{q^{10}}\Big),$$

while for even q they are

$$1 - \frac{2}{q^3} + \frac{1}{q^4} - \frac{2}{q^5} + \frac{4}{q^6} - \frac{5}{q^7} + \frac{9}{q^8} - \frac{14}{q^9} + O\Big(\frac{1}{q^{10}}\Big).$$

For practical purposes the following bounds are more helpful, however.

THEOREM 2.2.14. *If q is odd then*

$$1 - \frac{3}{q^3} + \frac{1}{q^4} - \frac{1}{q^5} < c_{\mathrm{Sp}}(\infty, q) < 1 - \frac{3}{q^3} + \frac{2}{q^4} + \frac{1}{q^5}$$

and if q is even then

$$1 - \frac{2}{q^3} - \frac{1}{q^5} < c_{\mathrm{Sp}}(\infty, q) < 1 - \frac{2}{q^3} + \frac{1}{q^4} + \frac{1}{q^5}$$

Proof. We use the second expression for $c_{\mathrm{Sp}}(\infty, q)$ given in Theorem 2.2.9:

$$\begin{aligned} W_2^*(q^{-1}) &> \Big(1 + \frac{1}{(q+1)(q^2-1)}\Big)^{N^*(q;2)} \Big(1 + \frac{1}{(q-1)(q^2+1)}\Big)^{M^*(q;1)} \\ &= \Big(1 + \frac{1}{(q+1)(q^2-1)}\Big)^{\frac{1}{2}(q+1-e)} \Big(1 + \frac{1}{(q-1)(q^2+1)}\Big)^{\frac{1}{2}(q-1-e)}, \end{aligned}$$

and so by Lemma 1.3.4(b),

$$\begin{aligned} W_2^*(q^{-1}) &> 1 + \frac{q+1-e}{2(q+1)(q^2-1)} + \frac{q-1-e}{2(q-1)(q^2+1)} \\ &= 1 + \frac{q^2}{q^4-1} - \frac{e\,(q^3-1)}{(q^2-1)(q^4-1)} \\ &> 1 + \frac{1}{q^2} - \frac{e}{q(q^2-1)}. \end{aligned}$$

Therefore

$$\begin{aligned} c_{\mathrm{Sp}}(\infty, q) &> \frac{(1-q^{-3})(1-q^{-2})}{(1-q^{-4})^e} \Big(1 + q^{-2} - \frac{e}{q(q^2-1)}\Big) \\ &= \frac{(1-q^{-3})}{(1-q^{-4})^e} (1 - q^{-4} - e\, q^{-3}) \\ &> (1 - (e+1)q^{-3} - q^{-4})(1 + e\, q^{-4}). \end{aligned}$$

From this it is not at all hard to derive that

$$c_{\mathrm{Sp}}(\infty, q) > 1 - (e+1)q^{-3} + (e-1)q^{-4} - q^{-5},$$

which is the lower bound given in the theorem.

As in the proof of Theorem 2.1.12, for the upper bound we use the fact that if $x > 0$ then $\log(1+x) < x$. This tells us that

$$\log W_2^*(q^{-1}) < \sum_{d \geqslant 1} \Big(\frac{N^*(q;2d)}{(q^d+1)(q^{2d}-1)} + \frac{M^*(q;d)}{(q^d-1)(q^{2d}+1)} \Big) .$$

In this sum we treat the first term separately; also, we use the fact that $N^*(q;2d) \leqslant q^d/(2d)$ and if $d > 1$ then $M^*(q;d) < (q^d - q)/(2d)$. After a little manipulation we find that

$$\log W_2^*(q^{-1}) < A^* + \sum_{d \geqslant 1} \frac{1}{d q^{2d}} ,$$

where $A^* := \dfrac{N^*(q;2)}{(q+1)(q^2-1)} + \dfrac{M^*(q;1)}{(q-1)(q^2+1)} - \dfrac{1}{q^2}$. Thus

$$\log W_2^*(q^{-1}) < A^* + \log \frac{1}{1-q^{-2}} ,$$

and it follows that $W_2^*(q^{-1}) < \exp(A^*)/(1-q^{-2})$ and

$$c_{\mathrm{Sp}}(\infty, q) < \frac{(1-q^{-2})(1-q^{-3})}{(1-q^{-4})^e} \times \frac{\exp(A^*)}{(1-q^{-2})} = \frac{(1-q^{-3})}{(1-q^{-4})^e} \times \exp(A^*) .$$

To finish the calculation we need to estimate $\exp(A^*)$. Now

$$\begin{aligned} A^* &= \frac{q+1-e}{2\,(q+1)(q^2-1)} + \frac{q-1-e}{2\,(q-1)(q^2+1)} - \frac{1}{q^2} \\ &= \frac{1}{q^2(q^4-1)} - \frac{e\,(q^3-1)}{(q^2-1)(q^4-1)} \\ &\leqslant -e \Big(\frac{(q^3-1)}{(q^2-1)(q^4-1)} - \frac{1}{q^2(q^4-1)} \Big) , \end{aligned}$$

and it is routine to check that the coefficient of $-e$ here is greater than q^{-3}. Thus $A^* < -e\,q^{-3}$ and

$$\begin{aligned} c_{\mathrm{Sp}}(\infty, q) &< \frac{(1-q^{-3})}{(1-q^{-4})^e} \exp(-e/q^3) \\ &< (1-q^{-3})(1 - e\,q^{-3} + \tfrac{1}{2} e^2\, q^{-6})(1 + e\,q^{-4}) . \end{aligned}$$

It is not hard to check from this that

$$c_{\mathrm{Sp}}(\infty, q) < 1 - (e+1)\,q^{-3} + e\,q^{-4} + q^{-5} ,$$

and this completes the proof of the theorem.

2.3. The orthogonal groups

The orthogonal groups $\mathrm{O}^\epsilon(n,q)$ are defined as subgroups of $\mathrm{GL}(n,q)$ preserving a non-degenerate quadratic form Q on an n-dimensional vector space V over $\mathbb{F}_q$ (see, for example, [**21**, Chapter 11] for details). If n is even, say $n = 2m \geqslant 2$, and $V = \mathbb{F}_q^n$ then there are two such forms up to equivalence under linear transformations of V. Choose $a \in \mathbb{F}_q$ such that $t^2 + t + a$ is irreducible in $\mathbb{F}_q[t]$. Any non-degenerate quadratic form is equivalent either to Q^+ or to Q^-, where $Q^+(x_1,\dots,x_n) = \sum_{i=1}^m x_{2i-1}x_{2i}$ and $Q^-(x_1,\dots,x_n) = x_1^2 + x_1x_2 + ax_2^2 + \sum_{i=2}^m x_{2i-1}x_{2i}$. The subgroups of $\mathrm{GL}(n,q)$ preserving these forms are $\mathrm{O}^+(n,q)$ and $\mathrm{O}^-(n,q)$ respectively. Their orders are given by $|\mathrm{O}^\epsilon(2m,q)| = 2q^{m^2-m}(q^m - \epsilon 1)\prod_{i=1}^{m-1}(q^{2i}-1)$.

Now take n to be odd, say $n = 2m+1 \geqslant 1$. If q is even then every non-degenerate quadratic form is equivalent to $x_1^2 + \sum_{i=1}^m x_{2i}x_{2i+1}$, and so there is just one orthogonal group $\mathrm{O}(2m+1,q)$. For the orthogonal group of this canonical form the vector e_1, where $e_1 = (1,0,\dots,0)$, is invariant, and the action of $\mathrm{O}(2m+1,q)$ on the quotient space $V/\langle e_1\rangle$ yields the famous isomorphism $\mathrm{O}(2m+1,q) \to \mathrm{Sp}(2m,q)$. If q is odd any non-degenerate quadratic form is equivalent under linear transformations either to Q or to bQ, where $Q(x_1,\dots,x_n) = \sum x_i^2$ and b is a fixed non-square in $\mathbb{F}_q$. Thus, although there are two inequivalent forms, they give rise to the same group $\mathrm{O}(2m+1,q)$. For odd q the order of $\mathrm{O}(2m+1,q)$ is $2q^{m^2}\prod_{i=1}^m (q^{2i}-1)$.

The concept of type of an orthogonal space may be modified and extended to spaces of odd dimension in such a way that the types of a collection of summands in an orthogonal decomposition of V determine the type of V. Define

$$\tau(V) := \begin{cases} \epsilon\, 1 & \text{if } n \text{ is even and } V \text{ has type } \epsilon\,, \\ 1 & \text{if } n \text{ is odd, } q \text{ is even,} \\ 1 & \text{if } n \text{ is odd, } q \equiv 1 \pmod 4,\ Q \sim \sum x_i^2\,, \\ -1 & \text{if } n \text{ is odd, } q \equiv 1 \pmod 4,\ Q \sim b\sum x_i^2\,, \\ \mathrm{i}^n & \text{if } n \text{ is odd, } q \equiv 3 \pmod 4,\ Q \sim \sum x_i^2\,, \\ (-\mathrm{i})^n & \text{if } n \text{ is odd, } q \equiv 3 \pmod 4,\ Q \sim b\sum x_i^2\,, \end{cases}$$

where $\mathrm{i} = \sqrt{-1} \in \mathbb{C}$ and b is a non-square in $\mathbb{F}_q$. It is not hard to prove that if $V = V_1 \oplus^\perp \cdots \oplus^\perp V_k$ then $\tau(V) = \prod \tau(V_i)$.

Separable orthogonal matrices. It turns out to be sensible to define generating functions $S_{\mathrm{O}^\epsilon}(u)$, $S_{\mathrm{O}}(u)$ for the chance that an element of $\mathrm{O}^\epsilon(2m,q)$, $\mathrm{O}(2m+1,q)$ respectively, is separable, as follows (these functions depend on q and could well be denoted $S_{\mathrm{O}^\epsilon}(q;u)$, $S_{\mathrm{O}}(q;u)$, but since we think of q as fixed we suppress the dependence on q):

$$S_{\mathrm{O}^+}(u) := 1 + \sum_{m\geqslant 1} s_{\mathrm{O}^+}(2m,q)\,u^m\,; \quad S_{\mathrm{O}^-}(u) := \sum_{m\geqslant 1} s_{\mathrm{O}^-}(2m,q)\,u^m\,;$$
$$S_{\mathrm{O}}(u) := 1 + \sum_{m\geqslant 1} s_{\mathrm{O}}(2m+1,q)\,u^m\,.$$

Effectively this treats the zero-dimensional space as being of $+$ type. We shall express these generating functions in terms of two other functions. The first is

$S_{\mathrm{Sp}}(u)$, for which, recall from Theorem 2.2.1, we have

$$S_{\mathrm{Sp}}(u) = \prod_{d\geqslant 1}\Big(1+\frac{u^d}{q^d+1}\Big)^{N^*(q;2d)} \prod_{d\geqslant 1}\Big(1+\frac{u^d}{q^d-1}\Big)^{M^*(q;d)}.$$

The second is the function $X_{\mathrm{O}}(u)$ (or $X_{\mathrm{O}}(q;u)$) defined by

$$X_{\mathrm{O}}(u) := \prod_{d\geqslant 1}\Big(1-\frac{u^d}{q^d+1}\Big)^{N^*(q;2d)} \prod_{d\geqslant 1}\Big(1+\frac{u^d}{q^d-1}\Big)^{M^*(q;d)}.$$

By Lemma 1.3.16, $N^*(q;2d)$ and $M^*(q;d)$ have size $O(q^d/(2d))$, and it follows from Corollary 1.3.2 that $X_{\mathrm{O}}(u)$ is analytic in the open unit disc. We shall prove later that it is in fact analytic in the disc $D(q)$.

THEOREM 2.3.1. *Let $e := e(q)$, the number of square roots of 1 in $\mathbb{F}_q$. Then*

(a) $S_{\mathrm{O}^+}(u^2) + S_{\mathrm{O}^-}(u^2) + e\,uS_{\mathrm{O}}(u^2) = (1+u)^e S_{\mathrm{Sp}}(u^2)$,

(b) $S_{\mathrm{O}^+}(u^2) - S_{\mathrm{O}^-}(u^2) = X_{\mathrm{O}}(u^2)$.

Proof. The proofs are similar in strategy to those of Theorems 2.1.1 and 2.2.1, but care is needed to account for the type of the quadratic forms involved. All unproved assertions we make about conjugacy classes and centraliser sizes can be found in [**22**, p. 40]. Suppose that X is an orthogonal matrix, preserving a non-degenerate quadratic form Q on an n-dimensional vector space V over $\mathbb{F}_q$, where n may be even or odd. Then $c_X(t)$ is $*$-self-conjugate as defined on p. 25, and there is a unique primary decomposition of V, that is, an X-invariant orthogonal direct sum decomposition with one summand of V for each monic irreducible self-conjugate polynomial $\phi(t)$ dividing $c_X(t)$, and one summand for each conjugate pair $\{\phi(t), \phi^*(t)\}$ of monic irreducible non-self-conjugate polynomials dividing $c_X(t)$. Each primary summand is non-singular with respect to the quadratic form. The centraliser of X in the orthogonal group is the direct product of the centralisers of the orthogonal transformations induced by X on the primary summands. Now suppose that X is separable. For a monic irreducible self-conjugate polynomial $\phi(t)$ of degree $2d$, the corresponding summand in the primary decomposition is of negative type, and the corresponding centraliser order is q^d+1 (the same as in the symplectic case). For a pair $\{\phi,\phi^*\}$ of monic irreducible non-self-conjugate polynomial divisors, each of degree d, the corresponding summand in the primary decomposition is of positive type, and the corresponding centraliser order is q^d-1 (again the same as in the symplectic case). However, in contrast to the case of symplectic groups, it is possible for the polynomials $t-1$ and $t+1$ to divide $c_X(t)$, since there are non-singular 1-dimensional orthogonal spaces; in these cases the corresponding centraliser has order 2 if q is odd and order 1 if q is even.

Now if q is odd consider the right side of the equation in part (a) in the form:

$$(1+\tfrac{1}{2}u+\tfrac{1}{2}u)^e \prod_{d\geqslant 1}\Big(1+\frac{u^{2d}}{q^d+1}\Big)^{N^*(q;2d)} \prod_{d\geqslant 1}\Big(1+\frac{u^{2d}}{q^d-1}\Big)^{M^*(q;d)}.$$

One of the factors $1+\frac{1}{2}u+\frac{1}{2}u$ is there to track whether or not $t-1$ occurs as a divisor of $c_X(t)$: each of the two terms $\frac{1}{2}u$ corresponds to a 1-dimensional summand of V with eigenvalue 1; there are two of them since the quadratic form on this summand can be either x_1^2 or bx_1^2 where b is a non-square; the coefficients $\frac{1}{2}$ account for the fact that the centralisers have order 2. This factor occurs a second time to account for the identical situation which occurs for a possible divisor $t+1$ of $c_X(t)$. It

follows from the remarks in the previous paragraph that, for n even and positive, the coefficient of u^n in the expansion of the product is $s_{\mathrm{O}^+}(n,q)+s_{\mathrm{O}^-}(n,q)$, while for n odd, the coefficient of u^n in this expansion is $2s_{\mathrm{O}}(n,q)$ accounting for the two types of forms. The constant term on each side of equation (a) is clearly 1. These considerations prove part (a) when q is odd. If q is even the factor $1+u$ tracks whether or not $t-1$ is a divisor of $c_X(t)$ but in this case there is only one possibility for the one-dimensional summand and its centraliser is of order 1. The rest of the argument proceeds as before.

We prove (b) by modifying the product on the right side of (a). In that product each factor $1+u^{2d}/(q^d+1)$ corresponds to a self-conjugate irreducible polynomial ϕ of degree $2d$ and is of the form $1+|C_{\mathrm{O}}(X_\phi)|^{-1}u^{2d}$, where X_ϕ is an orthogonal matrix with characteristic polynomial ϕ, and $C_{\mathrm{O}}(X_\phi)$ denotes its centraliser in the appropriate orthogonal group. Similarly, each factor $1+u^{2d}/(q^d-1)$ is of the form $1+|C_{\mathrm{O}}(X_\phi)|^{-1}u^{2d}$, and the factor $1+\frac{1}{2}u+\frac{1}{2}u$ or $1+u$ is of the form $1+|C_{\mathrm{O}}(X_\phi)|^{-1}u+|C_{\mathrm{O}}(X_\phi)|^{-1}u$ or $1+|C_{\mathrm{O}}(X_\phi)|^{-1}u$, respectively. Now modify the right side of equation (a) by replacing each coefficient $|C_{\mathrm{O}}(X_\phi)|^{-1}$ with $\tau_\phi|C_{\mathrm{O}}(X_\phi)|^{-1}$, where $\tau_\phi := \tau(V_\phi)$ and V_ϕ is the orthogonal space on which X_ϕ is acting. When q is odd the two summands $\frac{1}{2}u$, $\frac{1}{2}u$ in the factors corresponding to irreducible polynomials $t-1$ and $t+1$ cancel (since they are multiplied by 1 and -1 or i and $-$i respectively), and therefore the factor $(1+u)^2$ is replaced by a factor 1; when q is even we may delete the factor $1+u$ because the left side of (b) deals only with even-dimensional spaces, whereas the summand u corresponds to odd-dimensional spaces. Also the factors $1+u^{2d}/(q^d+1)$ are replaced by $1-u^{2d}/(q^d+1)$ and the factors $1+u^{2d}/(q^d-1)$ are unchanged. The product therefore becomes

$$\prod_{d\geqslant 1}\Big(1-\frac{u^{2d}}{q^d+1}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\frac{u^{2d}}{q^d-1}\Big)^{M^*(q;d)},$$

and, because of the multiplicative property of τ, when it is expanded it gives positive weighting to spaces of type $+$ and negative weighting to spaces of type $-$. Then the usual argument proves (b).

THEOREM 2.3.2. *Define $e' := e(q)-1$, so that $e'=0$ if q is even, $e'=1$ if q is odd. Then*

(a) $S_{\mathrm{O}}(u) = S_{\mathrm{Sp}}(u)$,

(b) $S_{\mathrm{O}^\epsilon}(u) = \frac{1}{2}(1+e'u)S_{\mathrm{Sp}}(u)+\frac{1}{2}\epsilon X_{\mathrm{O}}(u)$.

where $X_{\mathrm{O}}(u)$ is as defined on p. 54 above.

Proof. In Theorem 2.3.1(a), the terms contributing to the coefficient of an odd power u^{2m+1} in the left side of the equation arise from choosing $2u$ from the factor $(1+u)^2$, or u from $(1+u)$ respectively, on the right side. Part (a) follows immediately. Similarly, comparing even powers on each side of this equation we see that

$$S_{\mathrm{O}^+}(u^2)+S_{\mathrm{O}^-}(u^2) = (1+e'u^2)S_{\mathrm{Sp}}(u^2),$$

and parts (b), (c) follow from this and Theorem 2.3.1(b).

LEMMA 2.3.3. *Let $e := e(q)$ as usual, and let $W_2^*(u)$ be as defined on p. 43. Then*

$$X_{\mathrm{O}}(u) = \frac{1-\frac{u^2}{q}}{\left(1-\frac{u}{q}\right)^{e-1}\left(1+\frac{u}{q}\right)^{e}}\, W_2^*(u)\,,$$

and this provides an analytic continuation of $X_{\mathrm{O}}(u)$ *to the disc* $D(q)$*.*

Proof. We use Lemma 1.3.17(c) with u replaced by u/q to get that

$$X_{\mathrm{O}}(u) = \frac{1-\frac{u^2}{q}}{\left(1-\frac{u}{q}\right)^{e-1}\left(1+\frac{u}{q}\right)^{e}}\, X_1(u)X_2(u)\,,$$

where

$$X_1(u) := \prod_{d\geqslant 1}\Big(\Big(\frac{1}{1-(\frac{u}{q})^d}\Big)\Big(1-\frac{u^d}{q^d+1}\Big)\Big)^{N^*(q;2d)}$$

and

$$X_2(u) := \prod_{d\geqslant 1}\Big(\Big(\frac{1}{1+(\frac{u}{q})^d}\Big)\Big(1+\frac{u^d}{q^d-1}\Big)\Big)^{M^*(q;d)}\,.$$

The proof is now completed in exactly the same way as that of Theorem 2.1.2.

If q is odd then, by Theorem 2.3.2, $S_{\mathrm{O}^+}(u) - S_{\mathrm{Sp}}(u) = -\frac{1}{2}(1-u)S_{\mathrm{Sp}}(u) + \frac{1}{2}X_{\mathrm{O}}(u)$ and from Theorem 2.2.2 it follows that $(1-u)S_{\mathrm{Sp}}(u)$ is analytic in $D(q)$. By the above lemma therefore, $S_{\mathrm{O}^+}(u)-S_{\mathrm{Sp}}(u)$ is (or may be analytically continued to a function which is) analytic in the disc $D(q)$. Exactly the same argument applies to $S_{\mathrm{O}^-}(u)-S_{\mathrm{Sp}}(u)$. Thus if q is odd then each of $S_{\mathrm{O}^+}(u)$, $S_{\mathrm{O}^-}(u)$, $S_{\mathrm{O}}(u)$ is of the form $f(u)/(1-u)$, where $f(u)$ is analytic in $D(q)$ and $f(1) = S_{\mathrm{Sp}}(\infty, q)$. Similarly, but more obviously, if q is even then each of $S_{\mathrm{O}^+}(u)$, $S_{\mathrm{O}^-}(u)$, $S_{\mathrm{O}}(u)$ is of the form $f(u)/(1-u)$, where $f(u)$ is analytic in $D(q)$, but $f(1) = \frac{1}{2}S_{\mathrm{Sp}}(\infty, q)$ in the O^+ and O^- cases and $f(1) = S_{\mathrm{Sp}}(\infty, q)$ in the odd-dimensional case. Consequently, by Lemma 1.3.3 and Theorem 2.2.3 we have the following theorem.

THEOREM 2.3.4. *For separable orthogonal matrices the limiting probabilities are given by*

$$s_{\mathrm{O}}(\infty, q) = s_{\mathrm{Sp}}(\infty, q) \quad \textit{and} \quad s_{\mathrm{O}^+}(\infty, q) = s_{\mathrm{O}^-}(\infty, q) = 2^{e-2}s_{\mathrm{Sp}}(\infty, q)\,,$$

where

$$s_{\mathrm{Sp}}(\infty, q) = \Big(1-\frac{1}{q}\Big)^{e}\prod_{d\geqslant 1}\Big(1-\frac{2}{q^d(q^d+1)}\Big)^{N^*(q;2d)}\,.$$

Moreover, if $1 < r < q$ *then* $|s_{\mathrm{O}}(2m+1, q) - s_{\mathrm{O}}(\infty, q)| < o(r^{-m})$ *and* $|s_{\mathrm{O}^\epsilon}(2m, q) - s_{\mathrm{O}^\epsilon}(\infty, q)| < o(r^{-m})$ *as* $m \to \infty$*.*

From Theorem 2.2.6 we have the immediate corollary

THEOREM 2.3.5. *If* q *is odd and* s *is any of* $s_{\mathrm{O}}(\infty, q)\,,\ s_{\mathrm{O}^+}(\infty, q)\,,\ s_{\mathrm{O}^-}(\infty, q)\,,$ *then*

$$1-\frac{3}{q}+\frac{5}{q^2}-\frac{10}{q^3}+\frac{12}{q^4} \;<\; s \;<\; 1-\frac{3}{q}+\frac{5}{q^2}-\frac{10}{q^3}+\frac{23}{q^4}\,.$$

If q *is even then*

$$1-\frac{2}{q}+\frac{2}{q^2}-\frac{4}{q^3}+\frac{4}{q^4} \;<\; s_{\mathrm{O}}(\infty, q) < 1-\frac{2}{q}+\frac{2}{q^2}-\frac{4}{q^3}+\frac{9}{q^4}\,,$$

while if s *is either of* $s_{\mathrm{O}^+}(\infty, q)\,,\ s_{\mathrm{O}^-}(\infty, q)\,,$ *then*

$$\frac{1}{2}\Big(1-\frac{2}{q}+\frac{2}{q^2}-\frac{4}{q^3}+\frac{4}{q^4}\Big) \;<\; s < \frac{1}{2}\Big(1-\frac{2}{q}+\frac{2}{q^2}-\frac{4}{q^3}+\frac{9}{q^4}\Big)\,.$$

As with the other classical groups, the convergence rate given in the last sentence of Theorem 2.3.4 can be made more explicit. Since $S_{\mathrm{O}}(u) = S_{\mathrm{Sp}}(u)$ the following theorem is an immediate consequence of what we have proved for separable symplectic matrices.

THEOREM 2.3.6. (a) *Let* $A(u) := (1-qu)S_{\mathrm{O}}(qu)$ *and let* $e = e(q)$. *Then*

$$|A|(u) \ll \frac{(q-1)}{(1-u)^e}\Omega(u)^{-1}\,.$$

(b) *Let* $k := (q-1)/(2q-3)$. *If* q *is odd and* $9 \leqslant m < m' \leqslant \infty$ *then*

$$|s_{\mathrm{O}}(2m'+1,q) - s_{\mathrm{O}}(2m+1,q)| < 3k\,p_3(m)q^{-m} < 23k\left(\tfrac{2}{3}\,q\right)^{-m}.$$

If q *is even and* $6 \leqslant m < m' \leqslant \infty$ *then*

$$|s_{\mathrm{O}}(2m'+1,q) - s_{\mathrm{O}}(2m+1,q)| < 3k\,p_2(m)q^{-m} < 8k\left(\tfrac{2}{3}\,q\right)^{-m}.$$

For even-dimensional orthogonal groups the situation is similar to that for symplectic groups but not quite the same.

LEMMA 2.3.7. *Define* $A^\epsilon(u) := (1-qu)S_{\mathrm{O}^\epsilon}(qu)$. *Then*

$$|A^\epsilon|(u) \ll \begin{cases} \frac{1}{2}(q-1)(2q-1)\times(1-u)^{-2}\,\Omega(u)^{-1} & \text{if } q \text{ is odd,}\\ \frac{1}{2}(q-1)(q+2)\times(1-u)^{-1}\,\Omega(u)^{-1} & \text{if } q \text{ is even,}\end{cases}$$

where $\Omega(u)$ *is as defined on p.* 20.

Proof. It is convenient to treat the cases q even and q odd separately. Suppose first that q is odd, so that $e = 2$. By Theorem 2.3.2

$$2A^\epsilon(u) = (1-qu)(1+qu)S_{\mathrm{Sp}}(qu) + \epsilon\,(1-qu)X_{\mathrm{O}}(qu)$$

and so by Theorem 2.2.2 and Lemma 2.3.3

$$2A^\epsilon(u) = \frac{(1+qu)(1-qu^2)}{(1+u)^2}\,W_1^*(qu) + \epsilon\,\frac{(1-qu)(1-qu^2)}{(1-u^2)(1+u)}\,W_2^*(qu)\,,$$

where W_1^* and W_2^* are as defined on p. 43. It follows from Lemma 1.3.5 that if $A(u) := (1+qu)(1-qu^2)/(1+u)^2$ then $|A|(u) \ll (q-1)^2/(1-u)^2$. Similarly, examining coefficients we see that $(1-qu)/(1-u^2) \ll q/(1-u)$, and from Lemma 1.3.5(b) we have that $(1-qu^2)/(1+u) \ll (q-1)/(1-u)$, and therefore if $A(u) := (1-qu)(1-qu^2)/(1-u^2)(1+u)$ then $|A|(u) \ll (q^2-q)/(1-u)^2$. In the course of proving Lemmas 2.2.4 and 2.2.12 it was shown that $|W_1^*(qu)| \ll \Omega(u)^{-1}$ and $|W_2^*(qu)| \ll \Omega(u)^{-1}$. The assertion made in the lemma follows immediately.

Now suppose that q is even, so that $e = 1$. By Theorem 2.3.2

$$2A^\epsilon(u) = (1-qu)S_{\mathrm{Sp}}(qu) + \epsilon\,(1-qu)X_{\mathrm{O}}(qu)\,,$$

and so by Theorem 2.2.2 and Lemma 2.3.3

$$2A^\epsilon(u) = \frac{(1-qu^2)}{(1+u)}\,W_1^*(qu) + \epsilon\,\frac{(1-qu)(1-qu^2)}{(1+u)}\,W_2^*(qu)\,.$$

By Lemma 1.3.5, if $A(u) := (1-qu^2)/(1+u)$ then $|A|(u) \ll (q-1)/(1-u)$ and it follows easily that if $A(u) := (1-qu)(1-qu^2)/(1+u)$ then $|A|(u) \ll (q^2-1)/(1-u)$. As we noted, one has the inequalities $|W_1^*(qu)| \ll \Omega(u)^{-1}$ and $|W_2^*(qu)| \ll \Omega(u)^{-1}$. Again, the assertion made in the lemma follows immediately.

Now the argument that produced Theorem 2.2.5 from Lemma 2.2.4(a) yields the following theorem.

THEOREM 2.3.8. *Let p_2, p_3 be as defined on p. 20. If q is odd, $9 \leqslant m < m' \leqslant \infty$, and $k := (q-1)(2q-1)/2(2q-3)$ then*

$$|s_{\mathrm{O}^\epsilon}(2m', q) - s_{\mathrm{O}^\epsilon}(2m, q)| < 3k\, p_3(m) q^{-m} < 23k \left(\tfrac{2}{3}\, q\right)^{-m};$$

if q is even, $6 \leqslant m < m' \leqslant \infty$, and $k := (q-1)(q+2)/2(2q-3)$ then

$$|s_{\mathrm{O}^\epsilon}(2m', q) - s_{\mathrm{O}^\epsilon}(2m, q)| < 3k\, p_2(m) q^{-m} < 8k \left(\tfrac{2}{3}\, q\right)^{-m}.$$

The fact that $S_{\mathrm{O}}(u) = S_{\mathrm{Sp}}(u)$ when q is even can be seen directly. A non-degenerate form Q on an odd dimensional vector space V over $\mathbb{F}_q$ is singular (when q is even) in the sense that the associated bilinear form φ, which is defined by $\varphi(u, v) := Q(u+v) - Q(u) - Q(v)$, has a radical $V^\perp$ of dimension 1. The corresponding orthogonal group $\mathrm{O}(2m+1, q)$ acts faithfully on the quotient space $V/V^\perp$ as the symplectic group $\mathrm{Sp}(2m, q)$. If $X \in \mathrm{O}(2m+1, q)$ then X fixes $V^\perp$ elementwise, and so $c_X(t)$ is divisible by $t-1$. Recall from the proof of Theorem 2.2.1 that $t-1$ does not divide the characteristic polynomial of any separable matrix in $\mathrm{Sp}(2m, q)$. Therefore a matrix $X \in \mathrm{O}(2m+1, q)$ is separable if and only if the element of $\mathrm{Sp}(2m, q)$ induced by X is separable. It follows that $s_{\mathrm{O}}(2m+1, q) = s_{\mathrm{Sp}}(2m, q)$ for all m, and this explains the equality $S_{\mathrm{O}}(u) = S_{\mathrm{Sp}}(u)$ when q is even. We have found no such explanation for the phenomenon when q is odd.

Cyclic orthogonal matrices. For the same reasons as for separable matrices we define the generating functions for the probability that an orthogonal matrix is cyclic according to the convention that the zero-dimensional space has type $+$. Thus

$$C_{\mathrm{O}^+}(u) := 1 + \sum_{m \geqslant 1} c_{\mathrm{O}^+}(2m, q)\, u^m; \quad C_{\mathrm{O}^-}(u) := \sum_{m \geqslant 1} c_{\mathrm{O}^-}(2m, q)\, u^m;$$
$$C_{\mathrm{O}}(u) := 1 + \sum_{m \geqslant 1} c_{\mathrm{O}}(2m+1, q)\, u^m.$$

Our first result is a partner to Theorem 2.3.1. Define

$$X'_{\mathrm{O}}(u) := \prod_{d \geqslant 1} \Big(1 - \frac{u^d}{(q^d+1)(1+(\frac{u}{q})^d)}\Big)^{N^*(q;2d)} \times \prod_{d \geqslant 1} \Big(1 + \frac{u^d}{(q^d-1)(1-(\frac{u}{q})^d)}\Big)^{M^*(q;d)},$$

the analogue for the cyclic case of the function $X_{\mathrm{O}}(u)$ that appeared in the separable case.

THEOREM 2.3.9. *Let $e := e(q)$ (so that, recall, e is the number of square roots of 1 in $\mathbb{F}_q$). Then*

(a) $C_{\mathrm{O}}(u) = (1 - \frac{u}{q})\, C_{\mathrm{Sp}}(u)$,

(b) $C_{\mathrm{O}^\epsilon}(u) = \frac{1}{2}\left((1-\frac{u}{q})^e + u\right) C_{\mathrm{Sp}}(u) + \frac{1}{2}\,\epsilon\, X'_{\mathrm{O}}(u)$.

Proof. As for other classical groups, the theorem can be deduced from factorizations of the sum and difference of the cycle index generating functions for the orthogonal groups, but it can also be proved directly. What lies behind it is an

argument similar to that for Theorem 2.3.2. To deal with the case where q is odd we consider the product

$$\Big(1+\frac{u}{1-\frac{u^2}{q}}\Big)^2\prod_{d\geqslant 1}\Big(1+\frac{u^{2d}}{q^d+1}\,\frac{q^d}{q^d-u^{2d}}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\frac{u^{2d}}{q^d-1}\,\frac{q^d}{q^d-u^{2d}}\Big)^{M^*(q;d)}.$$

The proof that on expansion this yields $C_{\mathrm{O}^+}(u^2)+C_{\mathrm{O}^-}(u^2)+2u\,C_{\mathrm{O}}(u^2)$ is similar to that of Theorem 2.3.1, using information about conjugacy classes and centraliser sizes that may be found in the final section of [**22**]. Special care is needed only for the primary components corresponding to the irreducible polynomials $t-1$ and $t+1$. If the primary component of a cyclic orthogonal matrix corresponding to either of these is non-zero then it has odd dimension and can have type $+$ or $-$. There is a single conjugacy class of cyclic elements of $\mathrm{O}(2m+1,q)$ with characteristic polynomial $(t-1)^{2m+1}$, and a single class with characteristic polynomial $(t+1)^{2m+1}$. The centraliser has order $2q^m$. Thus for each of the polynomials $t-1$ and $t+1$ the generating function should have a factor $1+\dfrac{u}{1}+\dfrac{u^3}{q}+\dfrac{u^5}{q^2}+\cdots$, and this explains the term $\Big(1+\dfrac{u}{1-\frac{u^2}{q}}\Big)^2$.

Now suppose that q is even. The situation is similar to that for odd q, except that now a cyclic primary component correponding to the irreducible polynomial $t-1$ must either have dimension 1 or have even dimension. If the dimension is 1 then the centraliser order is 1; if the dimension is $2m$, where $m\geqslant 1$, then the component corresponding to the polynomial $(t-1)^{2m}$ can have type $+$ or $-$ and for either type the centraliser order is $2q^{m-1}$. Thus there should be a factor

$$1+u+u^2+\frac{u^4}{q}+\frac{u^6}{q^2}+\frac{u^8}{q^3}+\cdots,$$

and we find that

$$\begin{aligned}C_{\mathrm{O}^+}(u^2)+C_{\mathrm{O}^-}(u^2)+u\,C_{\mathrm{O}}(u^2)&=\Big(1+u+\frac{u^2}{1-\frac{u^2}{q}}\Big)\\&\times\prod_{d\geqslant 1}\Big(1+\frac{u^{2d}}{q^d+1}\,\frac{q^d}{q^d-u^{2d}}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\frac{u^{2d}}{q^d-1}\,\frac{q^d}{q^d-u^{2d}}\Big)^{M^*(q;d)}.\end{aligned}$$

Focussing on the terms of odd degree we see that, whatever the parity of q,

$$\begin{aligned}C_{\mathrm{O}}(u^2)\;=\;\Big(\frac{1}{1-\frac{u^2}{q}}\Big)^{e-1}&\prod_{d\geqslant 1}\Big(1+\frac{u^{2d}}{q^d+1}\,\frac{q^d}{q^d-u^{2d}}\Big)^{N^*(q;2d)}\\&\times\prod_{d\geqslant 1}\Big(1+\frac{u^{2d}}{q^d-1}\,\frac{q^d}{q^d-u^{2d}}\Big)^{M^*(q;d)},\end{aligned}$$

where $e:=e(q)$, and part (a) of the theorem follows from Theorem 2.2.7. Focussing on the terms of even degree we find that

$$\begin{aligned}C_{\mathrm{O}^+}(u^2)+C_{\mathrm{O}^-}(u^2)\;=\;\Big(1+\frac{u^2}{(1-\frac{u^2}{q})^e}\Big)&\prod_{d\geqslant 1}\Big(1+\frac{u^{2d}}{q^d+1}\,\frac{q^d}{q^d-u^{2d}}\Big)^{N^*(q;2d)}\\&\times\prod_{d\geqslant 1}\Big(1+\frac{u^{2d}}{q^d-1}\,\frac{q^d}{q^d-u^{2d}}\Big)^{M^*(q;d)},\end{aligned}$$

and so, again by Theorem 2.2.7,

$$C_{\mathrm{O}^+}(u^2) + C_{\mathrm{O}^-}(u^2) = \Big(1 + \frac{u^2}{(1-\frac{u^2}{q})^e}\Big)\Big(1 - \frac{u^2}{q}\Big)^e C_{\mathrm{Sp}}(u^2)\,.$$

Thus $C_{\mathrm{O}^+}(u) + C_{\mathrm{O}^-}(u) = \big((1-\frac{u}{q})^e + u\big)\, C_{\mathrm{Sp}}(u)$. Arguing as for Theorem 2.3.1(b) we find also that $C_{\mathrm{O}^+}(u^2) - C_{\mathrm{O}^-}(u^2) = X'_{\mathrm{O}}(u^2)$, and part (b) of the theorem follows immediately.

PROPOSITION 2.3.10. *The function $X'_{\mathrm{O}}(u)$ defined on p. 58 satisfies $X'_{\mathrm{O}}(u) = (1-\frac{u}{q})S_{\mathrm{Sp}}(\frac{u}{q})$, and is analytic in the open disc $D(q^2)$.*

Proof. From the definition of $X'_{\mathrm{O}}(u)$ and Lemma 1.3.17 (d) with u replaced by u/q, we find that

$$\frac{X'_{\mathrm{O}}(u)}{1-\frac{u}{q}} = \prod_{d\geqslant 1} a(q;u)^{N^*(q;2d)} \prod_{d\geqslant 1} b(q;u)^{M^*(q;d)}\,,$$

where $$a(q;u) := \Big(1 - \frac{u^d}{(q^d+1)(1+(\frac{u}{q})^d)}\Big)\Big(1 + (\frac{u}{q})^d\Big)$$

and $$b(q;u) := \Big(1 + \frac{u^d}{(q^d-1)(1-(\frac{u}{q})^d)}\Big)\Big(1 - (\frac{u}{q})^d\Big)\,.$$

Simple algebra then yields that

$$\begin{aligned}\frac{X'_{\mathrm{O}}(u)}{1-\frac{u}{q}} &= \prod_{d\geqslant 1}\Big(1 + \frac{u^d}{q^d(q^d+1)}\Big)^{N^*(q;2d)} \prod_{d\geqslant 1}\Big(1 + \frac{u^d}{q^d(q^d-1)}\Big)^{M^*(q;d)}\\ &= S_{\mathrm{Sp}}(\frac{u}{q})\,,\end{aligned}$$

by Theorem 2.2.1. By Theorem 2.2.2, $(1-u)S_{\mathrm{Sp}}(u)$ is analytic in the open disc $D(q)$, and hence $X'_{\mathrm{O}}(u)$ is analytic in $D(q^2)$.

Our next theorem records the limiting probabilities and an inexplicit estimate for the convergence rates for cyclic orthogonal matrices.

THEOREM 2.3.11. (a) *The limiting probabilities for orthogonal matrices are related to those for symplectic matrices as follows:*

$$\begin{aligned} c_{\mathrm{O}}(\infty,q) &= (1-\tfrac{1}{q})\, c_{\mathrm{Sp}}(\infty,q)\,;\\ c_{\mathrm{O}^+}(\infty,q) = c_{\mathrm{O}^-}(\infty,q) &= \tfrac{1}{2}\big((1-\tfrac{1}{q})^e + 1\big)\, c_{\mathrm{Sp}}(\infty,q)\\ &= \begin{cases}(1-\frac{1}{q}+\frac{1}{2q^2})\, c_{\mathrm{Sp}}(\infty,q) & \text{if } q \text{ is odd,}\\ (1-\frac{1}{2q})\, c_{\mathrm{Sp}}(\infty,q) & \text{if } q \text{ is even.}\end{cases}\end{aligned}$$

where $e := e(q)$ as usual, so that $e = 1$ if q is even and $e = 2$ if q is odd.

(b) *If $1 < r < q^2$ then $|c_{\mathrm{O}}(2m+1,q) - c_{\mathrm{O}}(\infty,q)| < o(r^{-m})$ as $m \to \infty$ and $|c_{\mathrm{O}^\epsilon}(2m,q) - c_{\mathrm{O}^\epsilon}(\infty,q)| < o(r^{-m})$ as $m \to \infty$.*

This follows immediately from the form of the generating functions given in Theorem 2.3.9, together with Lemma 1.3.3 and Proposition 2.3.10. The fact that $1 - C_{\mathrm{O}}(\infty,q) = q^{-1} + O(q^{-2})$ and $1 - C_{\mathrm{O}^\pm}(\infty,q) = \frac{e}{2}q^{-1} + O(q^{-2})$ is a manifestation of the fact that the non-cyclic matrices form a subvariety of codimension 1 in an orthogonal group.

To make Part (b) explicit we use Wall's method again.

THEOREM 2.3.12. (a) *If* $A(u) := (1-q^2u)C_{\mathrm{O}}(q^2u)$ *then*

$$|A|(u) \ll \begin{cases} \dfrac{(q^2-q)}{(1-u)^2}\,\Omega(u)^{-1} & \text{if } q \text{ is odd,} \\ \dfrac{(q^2-1)}{(1-u)}\,\Omega(u)^{-1} & \text{if } q \text{ is even,} \end{cases}$$

where $\Omega(u)$ *is as defined on p.* 20.

(b) *Let* p_2, p_3 *be as defined on p.* 20. *If* q *is odd,* $9 \leqslant m < m' \leqslant \infty$, *and* $k := q(q-1)/(2q^2-3)$ *then*

$$|c_{\mathrm{O}}(2m'+1,q) - c_{\mathrm{O}}(2m+1,q)| < 3k\,p_3(m)q^{-2m} < 23k\left(\tfrac{2}{3}\,q^2\right)^{-m};$$

if q *is even,* $6 \leqslant m < m' \leqslant \infty$, *and* $k := (q^2-1)/(2q^2-3)$ *then*

$$|c_{\mathrm{O}}(2m'+1,q) - c_{\mathrm{O}}(2m+1,q)| < 3k\,p_2(m)q^{-2m} < 8k\left(\tfrac{2}{3}\,q^2\right)^{-m}.$$

Proof. We know from Theorems 2.3.9(a) and 2.2.8 that

$$A(u) = \frac{(1-qu)(1-qu^2)}{(1+u)(1-u^2)^{e-1}}\,W_2^*(qu),$$

where $e = e(q)$. We proved Part (a) in the course of proving Lemma 2.3.7, and Part (b) follows by an argument we have now used several times before.

For the even-dimensional groups we have a similar theorem:

THEOREM 2.3.13. *Let* ϵ *be* $+$ *or* $-$ *and let* $e := e(q)$.

(a) *If* $A^\epsilon(u) := (1-q^2u)C_{\mathrm{O}^\epsilon}(q^2u)$ *then* $|A^\epsilon|(u) \ll \dfrac{q^2(q-1)}{(1-u)^e}\,\Omega(u)^{-1}$, *where* $\Omega(u)$ *is as defined on p.* 20.

(b) *Let* $k := q^2(q-1)/(2q^2-3)$ *and let* p_2, p_3 *be as defined on p.* 20. *If* q *is odd and* $9 \leqslant m < m' \leqslant \infty$ *then*

$$|c_{\mathrm{O}^\epsilon}(2m',q) - c_{\mathrm{O}^\epsilon}(2m,q)| < 3k\,p_3(m)q^{-2m} < 23k\left(\tfrac{2}{3}\,q^2\right)^{-m},$$

If q *is even and* $6 \leqslant m < m' \leqslant \infty$ *then*

$$|c_{\mathrm{O}^\epsilon}(2m',q) - c_{\mathrm{O}^\epsilon}(2m,q)| < 3k\,p_2(m)q^{-2m} < 8k\left(\tfrac{2}{3}\,q^2\right)^{-m}.$$

Proof. Suppose first that q is even, so that $e = 1$. From Theorem 2.3.9 and Proposition 2.3.10 we know that

$$2A^\epsilon(u) = (1+(q^2-q)u)(1-q^2u)C_{\mathrm{Sp}}(q^2u) + \epsilon(1-q^2u)(1-qu)S_{\mathrm{Sp}}(qu)\,,$$

and therefore, from Theorems 2.2.2 and 2.2.8(b),

$$2A^\epsilon(u) = \frac{(1+(q^2-q)u)(1-qu^2)}{(1+u)}\,W_2^*(qu) + \epsilon\frac{(1-q^2u)(1-qu^2)}{(1+u)}\,W_1^*(qu)\,.$$

Examining the coefficients of the power series defined by

$$B(u) := \frac{(1+(q^2-q)u)(1-qu^2)}{1+u}$$

we find that $|B|(u) \ll (q-1)(q^2-1)/(1-u)$ (in fact, for $q > 2$ we have $|B|(u) \ll (q^3-2q^2+1)/(1-u)$ but we will ignore this). Similarly, note that if one defines $C(u) := (1-q^2u)(1-qu^2)/(1+u)$ then $|C|(u) \ll (q-1)(q^2+1) \div (1-u)$. We

already know that $|W_1^*|(qu) \ll \Omega(u)^{-1}$ and $|W_2^*|(qu) \ll \Omega(u)^{-1}$. It follows that $|A^\epsilon|(u) \ll \big(q^2(q-1)/(1-u)\big)\Omega(u)^{-1}$, as required in this case.

Now suppose that q is odd. Using the same theorems as in the case where q is even we see that

$$\begin{aligned} 2A^\epsilon(u) \;=\; & (1+(q^2-2q)u+q^2u^2)(1-q^2u)C_{\mathrm{Sp}}(q^2u) \\ & + \epsilon\,(1-q^2u)(1-qu)S_{\mathrm{Sp}}(qu)\,, \end{aligned}$$

and that

$$\begin{aligned} 2A^\epsilon(u) \;=\; & \frac{(1+(q^2-2q)u+q^2u^2)(1-qu^2)}{(1+u)(1-u^2)}\,W_2^*(qu) \\ & + \epsilon\,\frac{(1-q^2u)(1-qu^2)}{(1+u)^2}\,W_1^*(qu)\,. \end{aligned}$$

For

$$B(u) := \frac{(1+(q^2-2q)u+q^2u^2)(1-qu^2)}{(1+u)(1-u^2)}$$

we find that $B(u) = B_0(u)/(1-u^2)$ where

$$B_0(u) := 1+(q^2-2q-1)u+(q+1)u^2-(q^3-2q^2+q+1)u^3-(q^2-q-1)\sum_{m\geqslant 4}(-u)^m,$$

from which it follows easily that $|B|(u) \ll (q-1)(q^2-1)/(1-u)^2$. For $C(u) := (1-q^2u)(1-qu^2)/(1+u)^2$ we have $|C|(u) \ll (q-1)(q^2+1)/(1-u)^2$. It follows as above that $|A^\epsilon|(u) \ll \big(q^2(q-1)/(1-u)^2\big)\Omega(u)^{-1}$, as was to be shown for part (a).

Part (b) follows in the same way as Theorem 2.2.13 from Lemma 2.2.12.

From Theorem 2.3.11(a) and Theorem 2.2.14 one may derive explicit upper and lower bounds for $c_{\mathrm{O}}(\infty,q)$ and $c_{\mathrm{O}^\pm}(\infty,q)$. After a little simplification to remove terms of higher order than q^{-4}, the results are:

THEOREM 2.3.14. *If q is odd then*

$$1-\frac{1}{q}-\frac{3}{q^3}+\frac{3}{q^4} < c_{\mathrm{O}}(\infty,q) < 1-\frac{1}{q}-\frac{3}{q^3}+\frac{5}{q^4}$$

and

$$1-\frac{1}{q}+\frac{1}{2q^2}-\frac{3}{q^3}+\frac{5}{2q^4} < c_{\mathrm{O}^\pm}(\infty,q) < 1-\frac{1}{q}+\frac{1}{2q^2}-\frac{3}{q^3}+\frac{5}{q^4}\,.$$

If q is even then

$$1-\frac{1}{q}-\frac{2}{q^3}+\frac{1}{q^4} < c_{\mathrm{O}}(\infty,q) < 1-\frac{1}{q}-\frac{2}{q^3}+\frac{3}{q^4}$$

and

$$1-\frac{1}{2q}-\frac{2}{q^3}+\frac{1}{2q^4} < c_{\mathrm{O}^\pm}(\infty,q) < 1-\frac{1}{2q}-\frac{2}{q^3}+\frac{5}{2q^4}\,.$$

CHAPTER 3

Semisimple and regular matrices in classical groups

3.1. Semisimple matrices

The previous chapter was devoted to developing the ideas of Wall [**23**] for the cases of separable and cyclic matrices in the unitary, symplectic and orthogonal groups. Here we turn to semisimple matrices. For a classical group X define $ss_{\mathrm{X}}(m,q)$ to be the probability that an element of $\mathrm{X}(n,q)$ is semisimple (*i.e.* diagonalizable over an algebraic closure of $\mathbb{F}_q$), where m is related to the dimension n as in Table 1. Then, as usual, define $ss_{\mathrm{X}}(\infty,q) := \lim_{m\to\infty} ss_{\mathrm{X}}(m,q)$.

Every separable matrix is semisimple; moreover, a semisimple matrix is either separable or non-cyclic; if $n \geqslant 2$ then the $n \times n$ identity matrix I_n is semisimple but not separable. The following is an immediate consequence:

PROPOSITION 3.1.1. *For any classical group* X *and for* $2 \leqslant m \leqslant \infty$,

$$s_{\mathrm{X}}(m,q) < ss_{\mathrm{X}}(m,q) \leqslant s_{\mathrm{X}}(m,q) + 1 - c_{\mathrm{X}}(m,q)\,.$$

The lower bound is the basis of the work [**12**] by Guralnick and Lübeck, who, in order to estimate $ss_{\mathrm{X}}(m,q)$ use geometric-combinatorial ideas related to, although different from, those used in [**17**] and [**18**], to give upper bounds for $1 - s_{\mathrm{X}}(m,q)$. Their methods have, however, not yielded useful bounds when $q \leqslant 4$, values of q that are quite important in computational contexts, whereas the generating function methods succeed for all q. From the proposition and the values for $s_{\mathrm{X}}(\infty,q)$ and $c_{\mathrm{X}}(\infty,q)$ given in the case of GL in [**23**] and [**6**], and for other classical groups in preceding sections of this paper, one obtains estimates for $ss_{\mathrm{X}}(\infty,q)$. For example,

PROPOSITION 3.1.2.
$$1 - \frac{1}{q} < ss_{\mathrm{GL}}(\infty,q) < 1 - \frac{1}{q} + \frac{1}{q^3} + \frac{1}{q^5}\,;$$
$$1 - \frac{1}{q} - \frac{2}{q^3} + \frac{4}{q^4} < ss_{\mathrm{U}}(\infty,q) < 1 - \frac{1}{q} - \frac{1}{q^3} + \frac{7}{q^4}\,;$$

if q *is odd then*

$$1 - \frac{3}{q} + \frac{5}{q^2} - \frac{10}{q^3} + \frac{12}{q^4} < ss_{\mathrm{Sp}}(\infty,q) < 1 - \frac{3}{q} + \frac{5}{q^2} - \frac{7}{q^3} + \frac{23}{q^4}\,;$$

and if q *is even then*

$$1 - \frac{2}{q} + \frac{2}{q^2} - \frac{4}{q^3} + \frac{4}{q^4} < ss_{\mathrm{Sp}}(\infty,q) < 1 - \frac{2}{q} + \frac{2}{q^2} - \frac{2}{q^3} + \frac{10}{q^4}\,.$$

This approach is unnecessary for GL where Fulman's infinite product formula quoted on p. 66 not only makes such estimates unnecessary but also yields better inequalities such as

$$1 - \frac{1}{q} + \frac{1}{q^3} - \frac{2}{q^4} < ss_{\mathrm{GL}}(\infty,q) < 1 - \frac{1}{q} + \frac{1}{q^3}\,.$$

It is somewhat unsatisfactory for the unitary group since it cannot yield estimates correct to order q^{-3}. It is seriously unsatisfactory for the symplectic groups when q is small, and it is even less satisfactory for the orthogonal groups, for which $1 - c_G(\infty, q) = O(q^{-1})$.

To obtain exact formulae that may be used to compute to any desired accuracy or to obtain better estimates for $ss_{\mathrm{X}}(\infty, q)$, and to obtain the rates of convergence of $ss_{\mathrm{X}}(m, q)$ to $ss_{\mathrm{X}}(\infty, q)$, we use the generating functions defined as follows:

$$SS_{\mathrm{X}}(u) := 1 + \sum_{m \geqslant 1} ss_{\mathrm{X}}(m, q)\, u^m\,,$$

with the exception that

$$SS_{\mathrm{O}^-}(u) := \sum_{m \geqslant 1} ss_{O^-}(m, q)\, u^m\,,$$

because the zero-dimensional orthogonal space should be treated as being of positive type. For these generating functions we have the following theorems.

THEOREM 3.1.3. (See [**6**]) $\displaystyle SS_{\mathrm{GL}}(u) = \prod_{d \geqslant 1} \Big(1 + \sum_{m \geqslant 1} \frac{u^{dm}}{|\mathrm{GL}(m, q^d)|}\Big)^{N(q;d)}.$

THEOREM 3.1.4.

$$SS_{\mathrm{U}}(u) = \prod_{d\ \mathrm{odd}} \Big(1 + \sum_{m \geqslant 1} \frac{u^{dm}}{|\mathrm{U}(m, q^d)|}\Big)^{\widetilde{N}(q;d)} \prod_{d \geqslant 1} \Big(1 + \sum_{m \geqslant 1} \frac{u^{2dm}}{|\mathrm{GL}(m, q^{2d})|}\Big)^{\widetilde{M}(q;d)}.$$

To simplify the corresponding statements in the symplectic and orthogonal cases we make some more definitions:

$$Y_1^*(u) := \prod_{d \geqslant 1} \Big(1 + \sum_{m \geqslant 1} \frac{u^{dm}}{|\mathrm{U}(m, q^d)|}\Big)^{N^*(q;2d)} \prod_{d \geqslant 1} \Big(1 + \sum_{m \geqslant 1} \frac{u^{dm}}{|\mathrm{GL}(m, q^d)|}\Big)^{M^*(q;d)};$$

$$Y_2^*(u) := \prod_{d \geqslant 1} \Big(1 + \sum_{m \geqslant 1} \frac{(-1)^m\, u^{dm}}{|\mathrm{U}(m, q^d)|}\Big)^{N^*(q;2d)} \prod_{d \geqslant 1} \Big(1 + \sum_{m \geqslant 1} \frac{u^{dm}}{|\mathrm{GL}(m, q^d)|}\Big)^{M^*(q;d)};$$

$$F(u) := 1 + \sum_{m \geqslant 1} \frac{u^m}{|\mathrm{Sp}(2m, q)|};$$

$$F_+(u) := 1 + \sum_{m \geqslant 1} \Big(\frac{1}{|\mathrm{O}^+(2m, q)|} + \frac{1}{|\mathrm{O}^-(2m, q)|}\Big)\, u^m;$$

$$F_-(u) := 1 + \sum_{m \geqslant 1} \Big(\frac{1}{|\mathrm{O}^+(2m, q)|} - \frac{1}{|\mathrm{O}^-(2m, q)|}\Big)\, u^m.$$

Since $|\mathrm{Sp}(2m, q)| = O(q^{m(2m+1)})$ and $|\mathrm{O}^{\pm}(2m, q)| = O(q^{m(2m-1)})$ these three power series converge everywhere in $\mathbb{C}$ and so $F(u)$, $F_+(u)$, $F_-(u)$ are entire functions (analytic in the whole complex plane). Note that, since $|\mathrm{O}(2m+1, q)| = e|\mathrm{Sp}(2m, q)|$, we have

$$F(u) = 1 + e \sum_{m \geqslant 1} \frac{u^m}{|\mathrm{O}(2m+1, q)|} = e \sum_{m \geqslant 0} \frac{u^m}{|\mathrm{O}(2m+1, q)|}\,.$$

The functions $Y_1^*(u)$ and $Y_2^*(u)$ may be thought of as perturbations of $S_{\mathrm{Sp}}(u)$ and the function $X_{\mathrm{O}}(u)$ defined on p. 54 respectively.

THEOREM 3.1.5. *Let* $e := e(q)$. *Then* $SS_{\mathrm{Sp}}(u) = F(u)^e\, Y_1^*(u)$.

THEOREM 3.1.6. *Let* $e := e(q)$. *Then*

$$SS_{\mathrm{O}^+}(u^2) + SS_{\mathrm{O}^-}(u^2) + e\,u\,SS_{\mathrm{O}}(u^2) = \big(F_+(u^2) + uF(u^2)\big)^e\, Y_1^*(u^2)$$

and

$$SS_{\mathrm{O}^+}(u^2) - SS_{\mathrm{O}^-}(u^2) = F_-(u^2)^e\, Y_2^*(u^2)\,.$$

These two theorems may be derived by specialisation from product factorisations of the cycle index generating functions of the symplectic and orthogonal groups; they can also be proved by arguments similar to those sketched for Theorems 2.1.7, 2.2.1, and 2.3.1. We therefore leave the details to the reader. From Theorem 3.1.6 it is a simple matter to separate out the individual generating functions $SS_{\mathrm{O}}(u)$, $SS_{\mathrm{O}^+}(u)$ and $SS_{\mathrm{O}^-}(u)$:

THEOREM 3.1.7. *Let* $e := e(q)$. *Then*

$$\begin{aligned} SS_{\mathrm{O}}(u) &= F_+(u)^{e-1}\,F(u)\,Y_1^*(u)\,,\\ SS_{\mathrm{O}^\epsilon}(u) &= \tfrac{1}{2}\big(F_+(u)^e + (e-1)uF(u)^2\big)\,Y_1^*(u) + \tfrac{1}{2}\epsilon\,F_-(u)^e\,Y_2^*(u)\,. \end{aligned}$$

As with the probability of separable and cyclic matrices, our main objective is to use the above theorems to give information about $ss_{\mathrm{X}}(\infty;q)$ for classical groups X. We approach the problems of evaluating $ss_{\mathrm{X}}(\infty;q)$ and estimating the rate of convergence of $ss_{\mathrm{X}}(m;q)$ to $ss_{\mathrm{X}}(\infty;q)$ through the following theorem.

THEOREM 3.1.8. *Let* X *be one of the classical groups. Then*

(a) $SS_{\mathrm{X}}(u) = \dfrac{T_{\mathrm{X}}(u)}{1-u}$, *where* $T_{\mathrm{X}}(u)$ *is analytic in the open disc* $D(q)$;

(b) *if* $1 < r < q$ *then* $|ss_{\mathrm{X}}(\infty,q) - ss_{\mathrm{X}}(m,q)| < o(r^{-m})$ *as* $m \to \infty$.

Proof. We treat only the case where $\mathrm{X} = \mathrm{GL}$ in detail: the others are similar and are left to the reader. Using Lemma 1.3.10(c) we find that

$$SS_{\mathrm{GL}}(u)\,\frac{(1-u)(1+\frac{u}{q})}{1-\frac{u^2}{q}} = \prod_{d\geqslant 1}\Big(\Big(1+\sum_{m\geqslant 1}\frac{u^{dm}}{|\mathrm{GL}(m,q^d)|}\Big)\Big(1+\frac{u^d}{q^d}\Big)^{-1}\Big)^{N(q;d)}\,.$$

Now

$$\Big(1+\sum_{m\geqslant 1}\frac{u^{dm}}{|\mathrm{GL}(m,q^d)|}\Big)\Big(1+\frac{u^d}{q^d}\Big)^{-1} = 1+\sum_{n\geqslant 1} c_{d,n}\,\frac{u^{dn}}{q^{dn}}$$

where

$$\begin{aligned} c_{d,n} &:= (-1)^n + \frac{(-1)^{n-1}q^d}{q^d-1} + \sum_{k=2}^{n}\frac{(-1)^{n-k}q^{dk}}{|\mathrm{GL}(k,q^d)|}\\ &= (-1)^n\Big(\frac{-1}{q^d-1} + \sum_{k=2}^{n}\frac{(-1)^k q^{dk}}{|\mathrm{GL}(k,q^d)|}\Big)\,. \end{aligned}$$

In this sum the terms are alternating in sign and strictly decreasing in magnitude. Therefore $|c_{d,n}| \leqslant 1/(q^d-1)$ for $n \geqslant 1$, and

$$\Big|\sum_{n\geqslant 1} c_{d,n}\,\frac{u^{dn}}{q^{dn}}\Big| < \sum_{n\geqslant 1}\frac{|u|^{dn}}{q^{dn}(q^d-1)} = \frac{1}{q^d-1}\,\frac{|u|^d}{q^d}\,\frac{1}{1-(|u|^d/q^d)}$$

provided that $|u|^d < q^d$, that is, $|u| < q$. Now we apply Corollary 1.3.2 together with the inequality $N(q;d) < q^d/d$ to see that

$$\prod\big(1+\sum_{n\geqslant 1} c_{d,n}\,\frac{u^{dn}}{q^{dn}}\big)^{N(q;d)}$$

defines a function $T_0(u)$ which is analytic in the open disc $D(q)$. Then

$$SS_{\mathrm{GL}}(u) = \frac{1}{1-u}\,\frac{1-(u^2/q)}{1+(u/q)}\,T_0(u)\,,$$

and this is the required result with $T_{\mathrm{GL}}(u) := (1-\frac{u^2}{q})\,T_0(u)/(1+\frac{u}{q})$. Part (b) now follows immediately from Lemma 1.3.3, and the proof is complete.

We turn now to the evaluation of $ss_{\mathrm{X}}(\infty,q)$. In [**5**] and [**6**] the first author has used one of the Rogers–Ramanujan identities to show that

$$ss_{\mathrm{GL}}(\infty,q) = \prod_{\substack{r\geqslant 1\\ r\equiv 0,\pm 2 \pmod 5}} \frac{(1-\frac{1}{q^{r-1}})}{(1-\frac{1}{q^r})}\,.$$

We have been unable to prove analogous formulae for the other classical groups. Nevertheless, we can produce infinite product expansions which converge sufficiently fast to be useful. They are expressed in terms of the following functions:

$$A_{q,d}(u) := 1 - \frac{u^d}{q^d(q^d+1)} - \sum_{m\geqslant 2}\Big(\frac{1}{q^d\,|\mathrm{U}(m-1,q^d)|} - \frac{1}{|\mathrm{U}(m,q^d)|}\Big)\,u^{dm}\,;$$

$$B_{q,d}(u) := 1 + \frac{u^d}{q^d(q^d-1)} - \sum_{m\geqslant 2}\Big(\frac{1}{q^d\,|\mathrm{GL}(m-1,q^d)|} - \frac{1}{|\mathrm{GL}(m,q^d)|}\Big)\,u^{dm}\,.$$

The usefulness of these functions comes from the following observations.

Lemma 3.1.9. (a) $A_{q,d}(u) = \Big(1-\dfrac{u^d}{q^d}\Big)\Big(1+\displaystyle\sum_{m\geqslant 1}\frac{u^{dm}}{|\mathrm{U}(m,q^d)|}\Big)$.

(b) $B_{q,d}(u) = \Big(1-\dfrac{u^d}{q^d}\Big)\Big(1+\displaystyle\sum_{m\geqslant 1}\frac{u^{dm}}{|\mathrm{GL}(m,q^d)|}\Big)$.

(c) *If* $|u|<q$ *then* $A_{q,d}(u) = 1 - \dfrac{u^d(u^d+1)}{q^d(q^d+1)} + \alpha$, *where* $|\alpha| < 3|u|^{2d}q^{-4d}$.

(d) *If* $|u|<q$ *then* $B_{q,d}(u) = 1 - \dfrac{u^d(u^d-1)}{q^d(q^d-1)} + \beta$, *where* $|\beta| < 3|u|^{2d}q^{-4d}$.

(e) $Y_1^*(u) = \dfrac{(1-\frac{u}{q})^e}{1-u}\displaystyle\prod_{d\geqslant 1}A_{q,d}(u)^{N^*(q;2d)}\prod_{d\geqslant 1}B_{q,d}(u)^{M^*(q;2d)}$.

Proof. For parts (a) and (b) we simply multiply out the right sides of their equations and collect terms of degree dm in u. For (c) recall that $|\mathrm{U}(m,q^d)| = \prod_{1\leqslant i\leqslant m}(q^{dm}-(-1)^i q^{d(m-i)})$, and so $A_{q,d}(u) = 1 - \frac{u^d(u^d+1)}{q^d(q^d+1)} + \alpha$, where

$$\alpha := \frac{u^{2d}}{q^d(q^d+1)(q^{2d}-1)} - \sum_{m\geqslant 3}\Big(\frac{1}{q^d\,|\mathrm{U}(m-1,q^d)|} - \frac{1}{|\mathrm{U}(m,q^d)|}\Big)\,u^{dm}.$$

Estimating quite crudely we see that $\big|u^{2d}/\big(q^d(q^d+1)(q^{2d}-1)\big)\big| < |u|^{2d}/q^{4d}$ and also that if $m\geqslant 3$ then

$$0 < \frac{1}{q^d\,|\mathrm{U}(m-1,q^d)|} - \frac{1}{|\mathrm{U}(m,q^d)|} < \frac{1}{q^d\,|\mathrm{U}(m-1,q^d)|} < \frac{1}{q^{5d(m-2)}}\,.$$

Therefore if $|u| < q$ then certainly

$$\Big| \sum_{m\geqslant 3} \Big(\frac{1}{q^d\,|\mathrm{U}(m-1,q^d)|} - \frac{1}{|\mathrm{U}(m,q^d)|} \Big)\, u^{dm} \Big| < \frac{2|u|^{3d}}{q^{5d}} < \frac{2|u|^{2d}}{q^{4d}}\,,$$

and the inequality $|\alpha| < 3|u|^{2d}/q^{4d}$ follows immediately. This proves (c), and (d) is similar. Part (e) is an immediate consequence of the definition of $Y_1^*(u)$ (see p. 64) together with Lemma 1.3.17(a).

Corollary 3.1.10. *The function $Y_1^*(u)$ is analytic in the open disc $D(q^{\frac12})$ except for a simple pole at $u = 1$.*

Proof. Focus on the description of $Y_1^*(u)$ given in (e) of the lemma. Using parts (c) and (d) and Corollary 1.3.2 together with the facts that $N^*(q;2d) < q^d - 1$ and $M^*(q;d) < q^d - 1$, we see that the infinite products $\prod_{d\geqslant 1} A_{q,d}(u)^{N^*(q;2d)}$ and $\prod_{d\geqslant 1} B_{q,d}(u)^{M^*(q;2d)}$ converge provided that $\sum \big(|u|^d(|u|^d+1)q^{-d} + 3|u|^{2d}q^{-3d}\big)$ converges, which it does if $|u|^2 < q$. Therefore Y_1^* is analytic in $D(q^{\frac12})$.

For future use we record the following inequalities.

Lemma 3.1.11. $$\Big(1 - \frac{1}{q^d(q^d+1)}\Big)^2 < A_{q,d}(1) < \Big(1 - \frac{1}{q^d(q^d+1)}\Big)^2 + \frac{1}{q^{9d}}$$

and $$1 + \frac{1}{q^{2d}(q^{2d}-1)} < B_{q,d}(1) < 1 + \frac{1}{q^{2d}(q^{2d}-1)} + \frac{2}{q^{9d}}\,.$$

Proof. From the definition of $A_{q,d}(u)$ we see that

$$A_{q,d}(1) = \Big(1 - \frac{1}{q^d(q^d+1)}\Big)^2 + \sum_{m\geqslant 3} \frac{q^d-1}{q^d\,|\mathrm{U}(m,q^d)|}\,.$$

Since $|U(m,q^d)| = \prod_{1\leqslant i\leqslant m} (q^{dm} - (-1)^i q^{d(m-i)})$, estimating quite crudely we find that

$$\begin{aligned}\sum_{m\geqslant 3} \frac{q^d-1}{q^d\,|\mathrm{U}(m,q^d)|} &< \frac{1}{q^{4d}(q^d+1)^2(q^{3d}+1)} \Big(1 + \frac{1}{q^{3d}} + \frac{1}{q^{6d}} + \cdots\Big) \\ &= \frac{1}{q^d(q^d+1)^2(q^{6d}-1)} < \frac{1}{q^{9d}}\,.\end{aligned}$$

Therefore

$$\Big(1 - \frac{1}{q^d(q^d+1)}\Big)^2 < A_{q,d}(1) < \Big(1 - \frac{1}{q^d(q^d+1)}\Big)^2 + \frac{1}{q^{9d}}\,.$$

A very similar calculation, which we omit, proves the second assertion.

Lemma 3.1.12. $$A_{q,d}(1) > \Big(\frac{1-\frac{1}{q^{2d}}}{1+\frac{1}{q^{2d}}}\Big)\Big(\frac{1+\frac{1}{q^{3d}}}{1-\frac{1}{q^{3d}}}\Big)\Big(\frac{1-\frac{1}{q^{4d}}}{1+\frac{1}{q^{4d}}}\Big)\Big(1 - \frac{1}{q^{4d}}\Big)\,,$$

$$A_{q,d}(1) < \Big(\frac{1-\frac{1}{q^{2d}}}{1+\frac{1}{q^{2d}}}\Big)\Big(\frac{1+\frac{1}{q^{3d}}}{1-\frac{1}{q^{3d}}}\Big)\Big(\frac{1-\frac{1}{q^{4d}}}{1+\frac{1}{q^{4d}}}\Big)\Big(1 - \frac{1}{q^{4d}}\Big)\Big(1 + \frac{1}{q^{5d}}\Big)^4,$$

and $$1 + \frac{1}{q^{4d}} < B_{q,d}(1) < \Big(1 + \frac{1}{q^{4d}}\Big)\Big(1 + \frac{1}{q^{5d}}\Big)\,.$$

The proof is omitted. Although somewhat tedious in the case of $A_{q,d}(1)$, it is a routine calculation using the previous lemma.

With this preparation we can embark now on our promised exploitation of the generating functions $ss_{\mathrm{X}}(u)$. Our first aim is to find exact formulae and good bounds for $ss_{\mathrm{X}}(\infty, q)$ and we begin with the unitary case.

THEOREM 3.1.13. *With $A_{q,d}$ and $B_{q,d}$ as defined above we have that*

$$ss_{\mathrm{U}}(\infty, q) = \Big(1 + \frac{1}{q}\Big) \prod_{d \text{ odd}} A_{q,d}(1)^{\widetilde{N}(q;d)} \prod_{d \geqslant 1} B_{q^2,d}(1)^{\widetilde{M}(q;d)} .$$

Proof. Lemma 1.3.14(a) with u replaced by u/q may be used to re-write the formula for $SS_{\mathrm{U}}(u)$ given in Theorem 3.1.4. The calculation is essentially the same as for Theorem 2.1.2 and, together with Lemma 3.1.9(a), (b), yields that

$$SS_{\mathrm{U}}(u) = \frac{1 + \frac{u}{q}}{1 - u} \prod_{d \text{ odd}} A_{q,d}(u)^{\widetilde{N}(q;d)} \prod_{d \geqslant 1} B_{q^2,d}(u^2)^{\widetilde{M}(q;d)}.$$

It is not hard to calculate from Lemma 3.1.9(c), (d) that the two products represent functions that are analytic in the open discs $D(q^{1/2})$ and $D(q^{3/4})$ respectively, and so Lemma 1.3.3 delivers the given value of $ss_{\mathrm{U}}(\infty, q)$.

This description of $ss_{\mathrm{U}}(\infty, q)$, though complicated, may be used to show that in the unitary case the upper bound given in Proposition 3.1.2 is more realistic than the lower bound.

THEOREM 3.1.14. $\quad 1 - \dfrac{1}{q} - \dfrac{1}{q^3} - \dfrac{2}{q^4} < ss_{\mathrm{U}}(\infty, q) < 1 - \dfrac{1}{q} - \dfrac{1}{q^3} + \dfrac{3}{q^4}$.

For small values of q we have the better bounds

$$0.4698 < ss_{\mathrm{U}}(\infty, 2) < 0.4724 \quad \textit{and} \quad 0.6498 < ss_{\mathrm{U}}(\infty, 3) < 0.6501 .$$

Proof. From Theorem 3.1.13, Lemma 3.1.12 and Lemma 1.3.14 we derive that

$$\begin{aligned} ss_{\mathrm{U}}(\infty, q) > {} & \Big(1 + \frac{1}{q}\Big) \prod_{d \text{ odd}} \Big(\frac{1 - \frac{1}{q^{2d}}}{1 + \frac{1}{q^{2d}}}\Big)^{\widetilde{N}(q;d)} \prod_{d \text{ odd}} \Big(\frac{1 + \frac{1}{q^{3d}}}{1 - \frac{1}{q^{3d}}}\Big)^{\widetilde{N}(q;d)} \\ & \times \prod_{d \text{ odd}} \Big(\frac{1 - \frac{1}{q^{4d}}}{1 + \frac{1}{q^{4d}}}\Big)^{\widetilde{N}(q;d)} \prod_{d \text{ odd}} \Big(1 - \frac{1}{q^{4d}}\Big)^{\widetilde{N}(q;d)} \prod_{d \geqslant 1} \Big(1 + \frac{1}{q^{8d}}\Big)^{\widetilde{M}(q;d)} \\ = {} & \Big(1 + \frac{1}{q}\Big) \times \frac{(1 - \frac{1}{q^2})(1 - \frac{1}{q})}{(1 + \frac{1}{q^2})(1 + \frac{1}{q})} \times \frac{(1 + \frac{1}{q^3})(1 + \frac{1}{q^2})}{(1 - \frac{1}{q^3})(1 - \frac{1}{q^2})} \\ & \times \frac{(1 - \frac{1}{q^4})(1 - \frac{1}{q^3})}{(1 + \frac{1}{q^4})(1 + \frac{1}{q^3})} \times \frac{(1 - \frac{1}{q^4})(1 - \frac{1}{q^7})}{(1 + \frac{1}{q^8})(1 + \frac{1}{q^3})} \\ = {} & \frac{(1 - \frac{1}{q})(1 - \frac{1}{q^4})^2(1 - \frac{1}{q^7})}{(1 + \frac{1}{q^3})(1 + \frac{1}{q^4})(1 + \frac{1}{q^8})} . \end{aligned}$$

Now

$$\begin{aligned} \frac{(1 - \frac{1}{q})(1 - \frac{1}{q^4})^2(1 - \frac{1}{q^7})}{(1 + \frac{1}{q^3})(1 + \frac{1}{q^4})(1 + \frac{1}{q^8})} &= \frac{(1 - \frac{1}{q})(1 - \frac{1}{q^3})(1 - \frac{1}{q^4})^3(1 - \frac{1}{q^7})}{(1 - \frac{1}{q^6})(1 - \frac{1}{q^{16}})} \\ &> (1 - \tfrac{1}{q})(1 - \tfrac{1}{q^3})(1 - \tfrac{1}{q^4})^3 , \end{aligned}$$

and the inequality $ss_{\mathrm{U}}(\infty,q) > 1-\frac{1}{q}-\frac{1}{q^3}-\frac{2}{q^4}$ follows easily.

For the upper bound we note that, by Lemma 3.1.12, if L is the lower bound treated above then $ss_{\mathrm{U}}(\infty,q) < L\times M$, where

$$M := \prod_{d\,\mathrm{odd}}\Big(1+\frac{1}{q^{5d}}\Big)^{4\widetilde{N}(q;d)}\prod_{d\geqslant 1}\Big(1+\frac{1}{q^{10d}}\Big)^{\widetilde{M}(q;d)}.$$

From Lemma 1.3.14 we see that

$$M = \left(\frac{(1+\frac{1}{q^5})(1-\frac{1}{q^9})}{(1+\frac{1}{q^{10}})(1-\frac{1}{q^4})}\right)^4\prod_{d\geqslant 1}\Big(1+\frac{1}{q^{10d}}\Big)^{-3\widetilde{M}(q;d)} < \frac{(1+\frac{1}{q^5})^4(1-\frac{1}{q^9})^4}{(1-\frac{1}{q^4})^4}.$$

Therefore

$$\begin{aligned} ss_{\mathrm{U}}(\infty,q) &< \frac{(1-\frac{1}{q})(1-\frac{1}{q^4})^2(1-\frac{1}{q^7})}{(1+\frac{1}{q^3})(1+\frac{1}{q^4})(1+\frac{1}{q^8})}\times\frac{(1+\frac{1}{q^5})^4(1-\frac{1}{q^9})^4}{(1-\frac{1}{q^4})^4}\\ &= \frac{(1-\frac{1}{q})(1+\frac{1}{q^4})(1+\frac{1}{q^5})^4(1-\frac{1}{q^7})(1-\frac{1}{q^9})^4}{(1+\frac{1}{q^3})(1-\frac{1}{q^8})(1-\frac{1}{q^{16}})}. \end{aligned}$$

Since $(1-\frac{1}{q^7})(1-\frac{1}{q^9})^4 < (1-\frac{1}{q^8})(1-\frac{1}{q^{16}})$, we have

$$ss_{\mathrm{U}}(\infty,q) < \frac{(1-\frac{1}{q})(1+\frac{1}{q^4})(1+\frac{1}{q^5})^4}{(1+\frac{1}{q^3})},$$

and it is easy (if a little tedious) to deduce that $ss_{\mathrm{U}}(\infty,q) < 1-\frac{1}{q}-\frac{1}{q^3}+\frac{3}{q^4}$, as required.

To get more accurate estimates for small values of q we use the facts, easily proved by the arguments above, that

$$\begin{aligned} ss_{\mathrm{U}}(\infty,q) &= C\times\frac{(1-\frac{1}{q})(1-\frac{1}{q^4})^2(1-\frac{1}{q^7})}{(1+\frac{1}{q^3})(1+\frac{1}{q^4})(1+\frac{1}{q^8})}\\ &= D\times\frac{(1-\frac{1}{q})(1-\frac{1}{q^4})^2(1-\frac{1}{q^7})}{(1+\frac{1}{q^3})(1+\frac{1}{q^4})(1+\frac{1}{q^8})}\times\left(\frac{(1+\frac{1}{q^5})(1-\frac{1}{q^9})}{(1+\frac{1}{q^{10}})(1-\frac{1}{q^4})}\right)^4, \end{aligned}$$

where $C := \displaystyle\prod_{d\,\mathrm{odd}} C_{q,d}^{\widetilde{N}(q;d)}\prod_{d\geqslant 1} C'_{q,d}{}^{\widetilde{M}(q;d)}$, $D := \displaystyle\prod_{d\,\mathrm{odd}} D_{q,d}^{\widetilde{N}(q;d)}\prod_{d\geqslant 1} D'_{q,d}{}^{\widetilde{M}(q;d)}$ and

$$\begin{aligned} C_{q,d} &:= A_{q,d}(1)\times\Big(\frac{1+\frac{1}{q^{2d}}}{1-\frac{1}{q^{2d}}}\Big)\Big(\frac{1-\frac{1}{q^{3d}}}{1+\frac{1}{q^{3d}}}\Big)\Big(\frac{1+\frac{1}{q^{4d}}}{1-\frac{1}{q^{4d}}}\Big)\Big(\frac{1}{1-\frac{1}{q^{4d}}}\Big),\\ C'_{q,d} &:= B_{q^2,d}(1)\times\Big(\frac{1}{1+\frac{1}{q^{8d}}}\Big),\\ D_{q,d} &:= C_{q,d}\times\Big(\frac{1}{(1+\frac{1}{q^{5d}})^4}\Big),\\ D'_{q,d} &:= C'_{q,d}\times\Big(\frac{1}{(1+\frac{1}{q^{10d}})^4}\Big). \end{aligned}$$

Lemma 3.1.12 tells us that $C_{q,d}>1$, $C'_{q,d}>1$ and $D_{q,d}<1$, $D'_{q,d}<1$. Therefore $C > C_{q,1}^{\widetilde{N}(q;1)} = C_{q,1}^{\,q+1}$ and $D < D_{q,1}^{\widetilde{N}(q;1)} = D_{q,1}^{\,q+1}$. Using these bounds in the

above formulae for $ss_{\mathrm{U}}(\infty,q)$ and using also Lemma 3.1.11 modified in the case where $q=2$ to say that $A_{2,1}(1) > (1-\frac{1}{2})\big(1+\sum_{1\leqslant m\leqslant 3}\frac{1}{|\mathrm{U}(m,2)|}\big)$, we find that $0.4698 < ss_{\mathrm{U}}(\infty,2) < 0.4724$ and $0.6498 < ss_{\mathrm{U}}(\infty,3) < 0.6501$, as the theorem states.

We turn now to the symplectic groups.

THEOREM 3.1.15. *Define* $a(q) := \prod_{d\geqslant 1} A_{q,d}(1)^{N^*(q;2d)} \prod_{d\geqslant 1} B_{q,d}(1)^{M^*(q;d)}$ *and let* $e := e(q)$ *as usual. Then* $ss_{\mathrm{Sp}}(\infty,q) = \Big(1-\frac{1}{q}\Big)^e F(1)^e\, a(q)$, *where* $F(u)$ *is as defined on p.* 64, *so that* $F(1) = 1+\sum_{m\geqslant 1}\frac{1}{|\mathrm{Sp}(2m,q)|}$.

The proof of is very similar to that of Theorem 3.1.13 and is omitted. Our next aim is to find usable bounds for $ss_{\mathrm{Sp}}(\infty,q)$. To this end we first bound $a(q)$.

LEMMA 3.1.16. *Let* $a(q)$ *be as defined in Theorem* 3.1.15 *and let* $e := e(q)$ *as usual. Then*

$$1-\frac{1}{q}+\frac{e}{q^2}-\frac{2e}{q^3}+\frac{2e-2}{q^4} < a(q) < 1-\frac{1}{q}+\frac{e}{q^2}-\frac{2e}{q^3}+\frac{3e+3}{q^4}.$$

Also, $0.5953 < a(2) < 0.5956$ *and* $0.7919 < a(3) < 0.7921$.

Proof. Since $a(q) = \prod_{d\geqslant 1} A_{q,d}(1)^{N^*(q;2d)} \prod_{d\geqslant 1} B_{q,d}(1)^{M^*(q;d)}$, Lemmas 3.1.12 and 1.3.17 imply that

$$\frac{(1-\frac{1}{q})}{(1-\frac{1}{q^2})^{e-1}}\,\frac{(1-\frac{1}{q^3})^{e-1}}{(1-\frac{1}{q^2})}\,\frac{(1-\frac{1}{q^3})}{(1-\frac{1}{q^4})^{e-1}}\,\frac{(1-\frac{1}{q^4})(1-\frac{1}{q^7})}{(1-\frac{1}{q^8})^e} < a(q)$$

and

$$\begin{aligned} a(q) < {} & \frac{(1-\frac{1}{q})}{(1-\frac{1}{q^2})^{e-1}}\,\frac{(1-\frac{1}{q^3})^{e-1}}{(1-\frac{1}{q^2})}\,\frac{(1-\frac{1}{q^3})}{(1-\frac{1}{q^4})^{e-1}}\,\frac{(1-\frac{1}{q^4})(1-\frac{1}{q^7})}{(1-\frac{1}{q^8})^e} \\ & \times \frac{(1-\frac{1}{q^9})^4}{(1-\frac{1}{q^4})^4(1+\frac{1}{q^5})^{4e}} \prod_{d\geqslant 1}\Big(1+\frac{1}{q^{5d}}\Big)^{-3M^*(q;d)}. \end{aligned}$$

It follows that

$$\frac{(1-\frac{1}{q})(1-\frac{1}{q^3})^e(1-\frac{1}{q^4})^{2-e}(1-\frac{1}{q^7})}{(1-\frac{1}{q^2})^e} < a(q) < \frac{(1-\frac{1}{q})(1-\frac{1}{q^3})^e}{(1-\frac{1}{q^2})^e(1-\frac{1}{q^4})^{e+2}},$$

and it is now routine algebra to check that

$$1-\frac{1}{q}+\frac{e}{q^2}-\frac{2e}{q^3}+\frac{2e-2}{q^4} < a(q) < 1-\frac{1}{q}+\frac{e}{q^2}-\frac{2e}{q^3}+\frac{3e+3}{q^4}.$$

For small values of q these inequalities are rather too crude to be helpful but using the same technique as in the unitary case we find that

$$\begin{aligned} a(q) = {} & \frac{(1-\frac{1}{q})}{(1-\frac{1}{q^2})^{e-1}}\,\frac{(1-\frac{1}{q^3})^{e-1}}{(1-\frac{1}{q^2})}\,\frac{(1-\frac{1}{q^3})}{(1-\frac{1}{q^4})^{e-1}}\,\frac{(1-\frac{1}{q^4})(1-\frac{1}{q^7})}{(1-\frac{1}{q^8})^e} \\ & \times \prod_{d\geqslant 1} C_d(q)^{N^*(q;2d)} \prod_{d\geqslant 1} D_d(q)^{M^*(q;d)}, \end{aligned}$$

where

$$C_d(q) := \frac{q^{2d}+1}{q^{2d}-1}\,\frac{q^{3d}-1}{q^{3d}+1}\,\frac{q^{4d}+1}{q^{4d}-1}\,\frac{q^{4d}}{q^{4d}-1} \times A_{q,d}(1)$$

and

$$D_d(q) := \frac{q^{4d}}{q^{4d}+1} \times B_{q,d}(1)\,.$$

Now $C_d(q) > 1$ and $D_d(q) > 1$ by Lemma 3.1.12, and it follows that

$$a(q) > \frac{(1-\frac{1}{q})}{(1-\frac{1}{q^2})^{e-1}}\,\frac{(1-\frac{1}{q^3})^{e-1}}{(1-\frac{1}{q^2})}\,\frac{(1-\frac{1}{q^3})}{(1-\frac{1}{q^4})^{e-1}}\,\frac{(1-\frac{1}{q^4})(1-\frac{1}{q^7})}{(1-\frac{1}{q^8})^{e}} \times \prod_{1\leqslant d\leqslant k} C_d(q)^{N^*(q;2d)} \prod_{1\leqslant d\leqslant k} D_d(q)^{M^*(q;d)}\,,$$

for any $k \geqslant 0$. Using the bounds $A_{d,q}(1) > \big(1-\frac{1}{q^d}\big)\big(1+\sum_{1\leqslant m\leqslant 3}\frac{1}{|\mathrm{U}(m,q^d)|}\big)$ and $B_{d,q}(1) > \big(1-\frac{1}{q^d}\big)\big(1+\sum_{1\leqslant m\leqslant 3}\frac{1}{|\mathrm{GL}(m,q^d)|}\big)$ which follow immediately from Lemma 3.1.9(a), (b), and taking $k := 3$ when $q = 2$ and $k := 2$ when $q = 3$ we calculate that $a(2) > 0.59534\cdots$ and $a(3) > 0.79195\cdots$.

Upper bounds for $a(q)$ for particular values of q may be found in a similar way. But here is an alternative technique. It follows from Lemma 3.1.11 that $A_{q,d}(1) < 1$ and $A_{q,d}(1)\,B_{q,d}(1) < 1$. Also $N^*(q;2d) \geqslant M^*(q;d)$ by Lemma 1.3.16(c), and so

$$\begin{aligned} &A_{q,d}(1)^{N^*(q;2d)} B_{q,d}(1)^{M^*(q;d)} \\ &\quad = A_{q,d}(1)^{(N^*(q;2d)-M^*(q;d))}\big(A_{q,d}(1)\,B_{q,d}(1)\big)^{M^*(q;d)} \\ &\quad < 1\,. \end{aligned}$$

It follows that

$$a(q) < \prod_{1\leqslant d\leqslant k} A_{q,d}(1)^{N^*(q;2d)} B_{q,d}(1)^{M^*(q;d)}$$

for any $k \geqslant 0$. Using the upper bounds for $A_{q,d}(1)$ and $B_{q,d}(1)$ in Lemma 3.1.11 (except in the case $q = 2$, $d = 1$ when we use the better bound $A_{q,d}(1) < \big(1-\frac{1}{q}\big)\big(1+\frac{1}{q^{16}}+\sum_{1\leqslant m\leqslant 3}\frac{1}{|\mathrm{U}(m,q^d)|}\big)$), and taking $k := 8$ when $q = 2$ and $k := 6$ when $q = 3$ we calculate that $a(2) < 0.59558\cdots$ and $a(3) < 0.79205\cdots$. This completes the proof of the lemma.

THEOREM 3.1.17. *If q is odd then*

$$1-\frac{3}{q}+\frac{5}{q^2}-\frac{7}{q^3}+\frac{6}{q^4} < ss_{\mathrm{Sp}}(\infty,q) < 1-\frac{3}{q}+\frac{5}{q^2}-\frac{7}{q^3}+\frac{13}{q^4}\,,$$

and if q is even then

$$1-\frac{2}{q}+\frac{2}{q^2}-\frac{2}{q^3}+\frac{1}{q^4} < ss_{\mathrm{Sp}}(\infty,q) < 1-\frac{2}{q}+\frac{2}{q^2}-\frac{2}{q^3}+\frac{5}{q^4}\,.$$

Also, $0.3476 < ss_{\mathrm{Sp}}(\infty,2) < 0.3481$ *and* $0.3819 < ss_{\mathrm{Sp}}(\infty,3) < 0.3821$.

Proof. By Theorem 3.1.15, $ss_{\mathrm{Sp}}(\infty,q) = \big(1-\frac{1}{q}\big)^e F(1)^e\,a(q)$. From the facts that $F(1) = 1+\sum_{m\geqslant 1}\frac{1}{|\mathrm{Sp}(2m,q)|}$ and $|\mathrm{Sp}(2m,q)| = \prod_{1\leqslant i\leqslant m}(q^{2i}-1)q^{2i-1}$ it follows (see Lemma 3.1.19 below) that

$$1+\frac{1}{q(q^2-1)}+\frac{1}{q^4(q^2-1)(q^4-1)} < F(1) < 1+\frac{1}{q(q^2-1)}+\frac{2}{q^{10}}\,.$$

Our lower and upper bounds for $ss_{\mathrm{Sp}}(\infty,q)$ when q is 2 or 3 can be calculated immediately from the corresponding bounds for $a(2)$ and $a(3)$ given in the previous lemma.

For general q we use the fact (see Lemma 3.1.19 below) that

$$\Big(1+\frac{1}{q^3}\Big)\Big(1+\frac{1}{q^5}\Big) < F(1) < \frac{(1+\frac{1}{q^5})}{(1-\frac{1}{q^3})}\,.$$

In the proof of Lemma 3.1.16 we showed that

$$\frac{(1-\frac{1}{q})(1-\frac{1}{q^3})^e(1-\frac{1}{q^4})^{2-e}(1-\frac{1}{q^7})}{(1-\frac{1}{q^2})^e} < a(q) < \frac{(1-\frac{1}{q})(1-\frac{1}{q^3})^e}{(1-\frac{1}{q^2})^e(1-\frac{1}{q^4})^{e+2}}\,,$$

and it follows that

$$ss_{\mathrm{Sp}}(\infty,q) > \frac{(1-\frac{1}{q})^{e+1}(1-\frac{1}{q^6})^e(1-\frac{1}{q^4})^{2-e}(1+\frac{1}{q^5})^e(1-\frac{1}{q^7})}{(1-\frac{1}{q^2})^e}$$

and

$$ss_{\mathrm{Sp}}(\infty,q) < \frac{(1-\frac{1}{q})^{e+1}(1+\frac{1}{q^5})^e}{(1-\frac{1}{q^2})^e(1-\frac{1}{q^4})^{e+2}}\,.$$

It is now straightforward to check the inequalities displayed in the statement of the theorem.

We turn now to the orthogonal groups.

THEOREM 3.1.18. *Let $e := e(q)$, let $a(q)$ be as defined in Theorem* 3.1.15*, and let $F(u)$, $F_+(u)$ be as defined on p.*64*. Then*

$$ss_{\mathrm{O}}(\infty,q) = F_+(1)^{e-1}\,F(1)\,(1-q^{-1})^e\,a(q)\,,$$

and $\quad ss_{\mathrm{O}^+}(\infty,q) = ss_{\mathrm{O}^-}(\infty,q) = \frac{1}{2}\big(F_+(1)^e + (e-1)F(1)^2\big)\,(1-q^{-1})^e\,a(q)\,.$

In particular, if q is even then $ss_{\mathrm{O}}(\infty,q) = ss_{\mathrm{Sp}}(\infty,q)$.

Proof. By Theorem 3.1.7

$$\begin{aligned} SS_{\mathrm{O}}(u) &= F_+(u)^{e-1}\,F(u)\,Y_1^*(u)\,,\\ SS_{\mathrm{O}^\epsilon}(u) &= \tfrac{1}{2}\big(F_+(u)^e + (e-1)uF(u)^2\big)\,Y_1^*(u) + \tfrac{1}{2}\epsilon\,F_-(u)^e\,Y_2^*(u)\,,\end{aligned}$$

where the functions $Y_1^*(u)$, $Y_2^*(u)$, $F(u)$, $F_+(u)$, $F_-(u)$ are defined near the beginning of this chapter. We have observed that $F(u)$, $F_+(u)$ and $F_-(u)$ are analytic in the whole plane. In Corollary 3.1.10 we have seen that $Y_1^*(u)$ is analytic in the open disc $D(q^{\frac{1}{2}})$ except for a simple pole at $u=1$. It is not hard to show that $Y_2^*(u)$ behaves like the function $X_{\mathrm{O}}(u)$ defined on p. 54 and is analytic in $D(q)$ (*cf.* Lemma 2.3.3). Thus if y_1^* is the residue of $Y_1^*(u)$ at its pole at $u=1$ then the residues of the functions

$$\begin{aligned} &F_+(u)^{e-1}\,F(u)\,Y_1^*(u) \qquad \text{and}\\ &\big(F_+(u)^e + (e-1)uF(u)^2\big)\,Y_1^*(u) + \epsilon F_-(u)^e\,Y_2^*(u)\end{aligned}$$

at $u=1$ are

$$F_+(1)^{e-1}\,F(1)\,y_1^* \quad \text{and} \quad \big(F_+(1)^e + (e-1)F(1)^2\big)\,y_1^*\,,$$

respectively. From Lemma 3.1.9(e) and Corollary 3.1.10 we know that $y_1^* = \big(1-\frac{1}{q}\big)^e a(q)$ and the theorem now follows from Lemma 1.3.3 in the usual way.

The equation $ss_{\mathrm{O}}(\infty, q) = ss_{\mathrm{Sp}}(\infty, q)$ when q is even, which can be read off from our formulae for these limiting probabilities, is a manifestation of the fact that, since semisimple elements correspond under the isomorphism $\mathrm{O}(2m+1, q) \cong \mathrm{Sp}(2m, q)$, we have $ss_{\mathrm{O}}(2m+1, q) = ss_{\mathrm{Sp}}(2m, q)$ for all m.

In order to obtain bounds for the limiting probabilities in the orthogonal case we need bounds for $F(1)$, $F_+(1)$ and $F_+(1)^2 + F(1)^2$. Those are given in the following lemma.

LEMMA 3.1.19. *For all q*

$$1 + \frac{1}{q(q^2-1)} + \frac{1}{q^4(q^2-1)(q^4-1)} < F(1) < 1 + \frac{1}{q(q^2-1)} + \frac{2}{q^{10}},$$

and

$$1 + \frac{q}{q^2-1} + \frac{1}{(q^2-1)(q^4-1)} < F_+(1) < 1 + \frac{q}{q^2-1} + \frac{2}{q^6}.$$

Also, if $q \geqslant 3$ then

$$1 + \frac{1}{q} + \frac{1}{2q^2} + \frac{2}{q^3} + \frac{1}{q^4} < \tfrac{1}{2}\big(F_+(1)^2 + F(1)^2\big) < 1 + \frac{1}{q} + \frac{1}{2q^2} + \frac{2}{q^3} + \frac{3}{q^4}.$$

Proof. By definition $F(1) = 1 + \sum_{m \geqslant 1} \frac{1}{|\mathrm{Sp}(2m, q)|}$, and from the well-known formula $|\mathrm{Sp}(2m, q)| = \prod_{i=1}^{m} q^{2m-1}(q^{2m} - 1)$, certainly

$$F(1) > 1 + \frac{1}{q(q^2-1)} + \frac{1}{q^4(q^2-1)(q^4-1)}.$$

For an upper bound we start from the fact that if $m \geqslant 2$ then, as is easily established,

$$|\mathrm{Sp}(2m, q)| > q^4(q^2-1)(q^4-1) \times q^{10(m-2)}.$$

Therefore

$$\begin{aligned} F(1) &< 1 + \frac{1}{q(q^2-1)} + \frac{1}{q^4(q^2-1)(q^4-1)} \sum_{m \geqslant 2} \frac{1}{q^{10(m-2)}} \\ &= 1 + \frac{1}{q(q^2-1)} + \frac{q^6}{(q^2-1)(q^4-1)(q^{10}-1)}. \end{aligned}$$

Since $(q^2-1)(q^4-1)(q^{10}-1) > \frac{1}{2}q^{16}$ we have

$$F(1) < 1 + \frac{1}{q(q^2-1)} + \frac{2}{q^{10}}$$

as stated in the first part of the lemma.

Recall that $|\mathrm{O}^{\epsilon}(2m, q)| = 2q^{m^2-m}(q^m - \epsilon) \prod_{i=1}^{m-1} (q^{2i} - 1)$. From the definition (p. 64) of $F_+(u)$ we have

$$F_+(1) = 1 + \sum_{m \geqslant 1} \Big(\frac{1}{|\mathrm{O}^+(2m, q)|} + \frac{1}{|\mathrm{O}^-(2m, q)|} \Big).$$

Certainly therefore

$$\begin{aligned} F_+(1) &> 1 + \frac{1}{2(q-1)} + \frac{1}{2(q+1)} + \frac{1}{2q^2(q^2-1)^2} + \frac{1}{2q^2(q^4-1)} \\ &= 1 + \frac{q}{q^2-1} + \frac{1}{(q^2-1)(q^4-1)}. \end{aligned}$$

Also

$$\begin{aligned}\frac{1}{|\mathrm{O}^+(2m,q)|}+\frac{1}{|\mathrm{O}^-(2m,q)|} &= \frac{1}{2q^{m^2-m}}\Big(\prod_{i=1}^{m-1}\frac{1}{q^{2i}-1}\Big)\Big(\frac{1}{q^m-1}+\frac{1}{q^m+1}\Big)\\ &= \frac{1}{q^{m^2-2m}}\prod_{i=1}^{m}\frac{1}{q^{2i}-1}\\ &\leqslant \frac{1}{(q^2-1)(q^4-1)q^{8(m-2)}} \quad \text{if } m\geqslant 2\,.\end{aligned}$$

Therefore

$$\begin{aligned}F_+(1) &< 1+\frac{q}{q^2-1}+\frac{1}{(q^2-1)(q^4-1)}\sum_{m\geqslant 2}\frac{1}{q^{8(m-2)}}\\ &= 1+\frac{q}{q^2-1}+\frac{q^8}{(q^2-1)(q^4-1)(q^8-1)}\,.\end{aligned}$$

Now $(q^2-1)(q^4-1)(q^8-1)>\frac{1}{2}q^{14}$ and so

$$F_+(1)<1+\frac{q}{q^2-1}+\frac{2}{q^6}$$

and this is the upper bound for $F_+(1)$ in the statement of the lemma.

From what has already been proved it follows that $F_+(1)>1+q^{-1}+q^{-3}$ and that $F(1)>1+q^{-3}$. Therefore

$$F_+(1)^2>1+\frac{2}{q}+\frac{1}{q^2}+\frac{2}{q^3}+\frac{2}{q^4}\,,\quad F(1)^2>1+\frac{2}{q^3}\,,$$

and

$$\tfrac{1}{2}\big(F_+(1)^2+F(1)^2\big)>1+\frac{1}{q}+\frac{1}{2q^2}+\frac{2}{q^3}+\frac{1}{q^4}\,,$$

which is the required lower bound. For an upper bound, note that if $q\geqslant 3$ then $F_+(1)<1+q^{-1}+q^{-3}+2q^{-5}$ and $F(1)<1+q^{-3}+2q^{-5}$. Therefore

$$F_+(1)^2+F(1)^2<2+\frac{2}{q}+\frac{1}{q^2}+\frac{4}{q^3}+\frac{2}{q^4}+\frac{8}{q^5}+\frac{6}{q^6}+\frac{8}{q^8}+\frac{8}{q^{10}}\,,$$

and if $q\geqslant 3$ we easily find that

$$\tfrac{1}{2}\big(F_+(1)^2+F(1)^2\big)<1+\frac{1}{q}+\frac{1}{2q^2}+\frac{2}{q^3}+\frac{3}{q^4}\,.$$

This completes the proof of the lemma.

THEOREM 3.1.20. *If q is odd then*

$$1-\frac{2}{q}+\frac{2}{q^2}-\frac{2}{q^3}-\frac{2}{q^4}<ss_{\mathrm{O}}(\infty,q)<1-\frac{2}{q}+\frac{2}{q^2}-\frac{2}{q^3}+\frac{7}{q^4}$$

and

$$1-\frac{2}{q}+\frac{5}{2q^2}-\frac{7}{2q^3}<ss_{\mathrm{O}^\pm}(\infty,q)<1-\frac{2}{q}+\frac{5}{2q^2}-\frac{7}{2q^3}+\frac{21}{2q^4}\,.$$

For $q=3$ we have

$$0.5046<ss_{\mathrm{O}}(\infty,3)<0.5053\quad \textit{and}\quad 0.5244<ss_{\mathrm{O}^\pm}(\infty,3)<0.5252\,.$$

If q is even then $ss_{\mathrm{O}}(\infty,q)=ss_{\mathrm{Sp}}(\infty,q)$, for which Theorem 3.1.17 gives bounds, and

$$\frac{1}{2}-\frac{1}{2q}-\frac{3}{2q^4}<ss_{\mathrm{O}^\pm}(\infty,q)<\frac{1}{2}-\frac{1}{2q}+\frac{5}{2q^4}\,.$$

For $q = 2$ we have $0.2513 < ss_{\mathrm{O}^\pm}(\infty, 2) < 0.2515$.

Proof. The values of $ss_{\mathrm{O}}(\infty, q)$ and $ss_{\mathrm{O}^\pm}(\infty, q)$ are given by Theorem 3.1.18. If q is odd then $ss_{\mathrm{O}}(\infty, q) = \big(1 - \frac{1}{q}\big)^2 F_+(1)F(1)a(q)$. It is straightforward to check that $(1 - \frac{1}{q})(1 + \frac{q}{q^2-1}) = 1 - \frac{1}{q(q+1)}$, that $(1 - \frac{1}{q})(1 + \frac{1}{q(q^2-1)}) = 1 - \frac{1}{q} + \frac{1}{q^2(q+1)}$, and that

$$\begin{aligned}\Big(1 - \frac{1}{q(q+1)}\Big)\Big(1 - \frac{1}{q} + \frac{1}{q^2(q+1)}\Big) &= 1 - \frac{1}{q} + \frac{1}{q^2} + \frac{3}{q^3} - \frac{3q+4}{q^3(q+1)^2} \\ &> 1 - \frac{1}{q} - \frac{1}{q^2} + \frac{3}{q^3} - \frac{3}{q^4}\,.\end{aligned}$$

Therefore by Lemmas 3.1.16 and 3.1.19 we have

$$ss_{\mathrm{O}}(\infty, q) > \Big(1 - \frac{1}{q} - \frac{1}{q^2} + \frac{3}{q^3} - \frac{3}{q^4}\Big)\Big(1 - \frac{1}{q} + \frac{2}{q^2} - \frac{4}{q^3} + \frac{2}{q^4}\Big)$$

and the lower bound given in the theorem follows easily. For the upper bound a very similar argument proves that

$$\Big(1 - \frac{1}{q}\Big)^2 F_+(1)F(1) < 1 - \frac{1}{q} - \frac{1}{q^2} + \frac{3}{q^3} - \frac{2}{q^4}\,,$$

so we have

$$ss_{\mathrm{O}}(\infty, q) < \Big(1 - \frac{1}{q} - \frac{1}{q^2} + \frac{3}{q^3} - \frac{2}{q^4}\Big)\Big(1 - \frac{1}{q} + \frac{2}{q^2} - \frac{4}{q^3} + \frac{9}{q^4}\Big)\,,$$

and again the upper bound given in the theorem follows easily.

If q is odd then $ss_{\mathrm{O}^\pm}(\infty, q) = \frac{1}{2}\big(F_+(1)^2 + F(1)^2\big)\big(1 - \frac{1}{q}\big)^2 a(q)$ and so we find that

$$\begin{aligned}ss_{\mathrm{O}^\pm}(\infty, q) &< \Big(1 + \frac{1}{q} + \frac{1}{2q^2} + \frac{2}{q^3} + \frac{3}{q^4}\Big)\Big(1 - \frac{1}{q}\Big)^2\Big(1 - \frac{1}{q} + \frac{2}{q^2} - \frac{4}{q^3} + \frac{9}{q^4}\Big) \\ &< \Big(1 - \frac{1}{q} - \frac{1}{2q^2} + \frac{2}{q^3} + \frac{1}{2q^4}\Big)\Big(1 - \frac{1}{q} + \frac{2}{q^2} - \frac{4}{q^3} + \frac{7}{q^4}\Big) \\ &< 1 - \frac{2}{q} + \frac{5}{2q^2} - \frac{7}{2q^3} + \frac{21}{2q^4}\,.\end{aligned}$$

The calculations for the lower bound, and for the bounds when q is even, are very similar and are omitted. Given all the information we have collected, calculations of the bounds for $q = 2$ and $q = 3$ are also straightforward (although for $q = 2$ we use a variant of the upper bound for $F_+(1)$ given in Lemma 3.1.19, namely $F_+(1) < 1 + \frac{q}{q^2-1} + \frac{1}{(q^2-1)(q^4-1)} + \frac{2}{q^{15}}$), and these complete the proof.

It is worth observing that when q is even all semisimple elements of the orthogonal groups $\mathrm{O}^\pm(2m, q)$ lie in the subgroup $\Omega^\pm(2m, q)$ of index 2. Thus, with an obvious notation, $ss_{\mathrm{O}^\pm}(\infty, q) = \frac{1}{2} ss_{\Omega^\pm}(\infty, q)$, and to some extent this explains the factor $\frac{1}{2}$ in the bounds in this case.

From Fulman's product formula for $ss_{\mathrm{GL}}(\infty, q)$ cited above (p. 66) it is very easy to compute the first few terms of the formal power series in q^{-1} that represents this limiting probability in the sense of [**23**, §7]. The formulae given in Theorems 3.1.13, 3.1.15 and 3.1.18 permit a similar calculation of $ss_G(\infty, q)$ for the other classical groups G. For the unitary groups we calculated $\log A_{q,d}(1)$ and

$\log B_{q,d}(1)$, then $\sum_{d\,\mathrm{odd}} \widetilde{N}(q;d)\log A_{q,d}(1)$ and $\sum_{d\geqslant 1}\widetilde{M}(q;d)\log B_{q,d}(1)$ to the desired accuracy—in our case modulo $O(q^{-10})$. This gave $\log\big(\prod_{d\,\mathrm{odd}} A_{q,d}(1)^{\widetilde{N}(q;d)}\times \prod_{d\geqslant 1} B_{q^2,d}(1)^{\widetilde{M}(q;d)}\big)$, which, after exponentiation and multiplication by $(1+q^{-1})$, yielded $ss_{\mathrm{U}}(\infty,q)$ as

$$1-\frac{1}{q}-\frac{1}{q^3}+\frac{2}{q^4}-\frac{2}{q^5}+\frac{5}{q^6}-\frac{9}{q^7}+\frac{11}{q^8}-\frac{20}{q^9}+O\Big(\frac{1}{q^{10}}\Big).$$

For the symplectic and othogonal groups we used the same strategy to compute $a(q)$ (defined in Theorem 3.1.15). When q is odd it turns out to be

$$1-\frac{1}{q}+\frac{2}{q^2}-\frac{4}{q^3}+\frac{7}{q^4}-\frac{13}{q^5}+\frac{22}{q^6}-\frac{42}{q^7}+\frac{77}{q^8}-\frac{138}{q^9}+O\Big(\frac{1}{q^{10}}\Big),$$

and when q is even it turns out to be

$$1-\frac{1}{q}+\frac{1}{q^2}-\frac{2}{q^3}+\frac{3}{q^4}-\frac{5}{q^5}+\frac{8}{q^6}-\frac{15}{q^7}+\frac{27}{q^8}-\frac{46}{q^9}+O\Big(\frac{1}{q^{10}}\Big).$$

The values of $ss_{\mathrm{Sp}}(\infty,q)$, $ss_{\mathrm{O}}(\infty,q)$ and $ss_{\mathrm{O}^{\pm}}(\infty,q)$ listed in Table 11 were then obtained quite easily from the formulae in Theorems 3.1.15 and 3.1.18.

To complete our study of the probability that an element of a classical group is semisimple we study convergence rates. Recall (see p. 20) that $p_r(n)$ is defined inductively by the prescription $p_1(n):=p(n)$, where $p(n)$ is the number of partitions of n (and $p(0):=1$), and $p_r(n):=\sum_{m=0}^{n} p_{r-1}(m)$.

Lemma 3.1.21. *Let* $A(u):=(1-qu)SS_{\mathrm{GL}}(qu)$. *Then*

$$|A|(u)\ll \frac{(q-1)}{(1-u)}\,\Omega(u)^{-1},$$

where $\Omega(u)$ *is as defined on p.* 20. *Therefore (by Lemma* 1.3.8*),*

$$|ss_{\mathrm{GL}}(n,q)-ss_{\mathrm{GL}}(n-1,q)|\leqslant (q-1)p_2(n)q^{-n}.$$

Proof. By the proof of Theorem 3.1.8,

$$A(u)=\frac{1-qu^2}{1+u}\prod_{d\geqslant 1}\Big(1+\sum_{n\geqslant 1} c_{d,n}\,u^{dn}\Big)^{N(q;d)},$$

where $|c_{d,n}|\leqslant 1/(q^d-1)$ for $n\geqslant 1$. Thus, by Lemma 1.3.5(b),

$$\begin{aligned}|A|(u)&\ll \Big(\frac{q-1}{1-u}\Big)\prod_{d\geqslant 1}\Big(1+\sum_{n\geqslant 1}\frac{u^{dn}}{q^d-1}\Big)^{N(q;d)}\\ &=\Big(\frac{q-1}{1-u}\Big)\prod_{d\geqslant 1}\Big(1+\frac{1}{q^d-1}\,\frac{u^d}{1-u^d}\Big)^{N(q;d)}.\end{aligned}$$

From Lemma 1.3.6 and the fact that $N(q;d)\leqslant (q^d-1)/d$,

$$\begin{aligned}|A|(u)&\ll \Big(\frac{q-1}{1-u}\Big)\exp\Big(\sum_{d\geqslant 1}\frac{N(q;d)}{q^d-1}\,\frac{u^d}{1-u^d}\Big)\\ &\ll \Big(\frac{q-1}{1-u}\Big)\exp\Big(\sum_{d\geqslant 1}\frac{1}{d}\,\frac{u^d}{1-u^d}\Big).\end{aligned}$$

Thus $|A|(u)\ll\Big(\frac{q-1}{1-u}\Big)\Omega(u)^{-1}$ by Lemma 1.3.7, as the lemma states.

THEOREM 3.1.22. *If* $6 \leqslant n < n' \leqslant \infty$ *and* $k := (q-1)/(2q-3)$ *then*

$$|ss_{\mathrm{GL}}(n',q) - ss_{\mathrm{GL}}(n,q)| < 3k\, p_2(n) q^{-n} < 8k \left(\tfrac{2}{3}\, q\right)^{-n}.$$

This is an immediate consequence of the previous lemma and Lemma 1.3.9.

LEMMA 3.1.23. *Let* $A(u) := (1-qu)SS_{\mathrm{U}}(qu)$. *Then*

$$|A|(u) \ll \frac{(q+1)}{(1-u)^3}\, \Omega(u)^{-1},$$

where $\Omega(u)$ *is as defined on p.* 20. *Therefore*

$$|ss_{\mathrm{U}}(n,q) - ss_{\mathrm{U}}(n-1,q)| \leqslant (q+1)\, p_4(n)\, q^{-n}.$$

Proof. By Theorem 3.1.4

$$SS_{\mathrm{U}}(u) = \prod_{d\,\mathrm{odd}} \Big(1 + \sum_{m\geqslant 1} \frac{u^{dm}}{|\mathrm{U}(m,q^d)|}\Big)^{\widetilde{N}(q;d)} \prod_{d\geqslant 1} \Big(1 + \sum_{m\geqslant 1} \frac{u^{2dm}}{|\mathrm{GL}(m,q^{2d})|}\Big)^{\widetilde{M}(q;d)},$$

and so by Lemma 1.3.14(b),

$$A(u) = \frac{(1-qu^2)(1+u)}{(1+u^2)} \prod_{d\,\mathrm{odd}} B_d(u)^{\widetilde{N}(q;d)} \prod_{d\geqslant 1} C_d(u)^{\widetilde{M}(q;d)},$$

where

$$B_d(u) := \Big(1 + \sum_{m\geqslant 1} \frac{q^{dm}\, u^{dm}}{|\mathrm{U}(m,q^d)|}\Big)\Big(\frac{1}{1+u^d}\Big)$$

and

$$C_d(u) := \Big(1 + \sum_{m\geqslant 1} \frac{q^{2dm}\, u^{2dm}}{|\mathrm{GL}(m,q^{2d})|}\Big)\Big(\frac{1}{1+u^{2d}}\Big).$$

Writing $B_d(u) = 1 + \sum_{n\geqslant 1} b_{d,n} u^{dn}$ we find that

$$b_{d,n} = (-1)^n \Big(1 - \frac{q^d}{q^d+1} + \varepsilon\Big) = (-1)^n \Big(\frac{1}{q^d+1} + \varepsilon\Big),$$

where $\varepsilon := \displaystyle\sum_{m=2}^{n} \frac{(-1)^m q^{dm}}{|\mathrm{U}(m,q^d)|}$. In this sum the terms are alternating in sign and decreasing monotonically in magnitude. Thus $0 \leqslant \varepsilon \leqslant q^d \big/ \big((q^d+1)(q^{2d}-1)\big)$ and

$$|b_{d,1}| = \frac{1}{q^d+1} \quad \text{while} \quad |b_{d,n}| < \frac{q^d}{q^{2d}-1} \ \text{ for } n \geqslant 2.$$

Therefore

$$|B_d|(u) = 1 + \sum_{n\geqslant 1} |b_{d,n}| u^{dn} \ll 1 + \frac{1}{q^d-1} \sum_{n\geqslant 1} u^{dn} = 1 + \frac{1}{q^d-1}\, \frac{u^d}{1-u^d}.$$

The factors $C_d(u)$ may be treated similarly. If we write $C_d(u) = 1 + \sum_{n\geqslant 1} c_{d,n} u^{2dn}$ we find, as in the proofs of Theorem 3.1.8 and Lemma 3.1.21 (with q there replaced by q^2 here), that $|c_{d,n}| \leqslant 1/(q^{2d}-1)$, so that

$$|C_d|(u) \ll 1 + \frac{1}{q^{2d}-1}\, \frac{u^{2d}}{1-u^{2d}}.$$

Now let

$$A_0(u) := \frac{(1-qu^2)(1+u)}{(1+u^2)}, \quad A_1(u) := \prod_{d \text{ odd}} B_d(u)^{\widetilde{N}(q;d)} \prod_{d\geqslant 1} C_d(u)^{\widetilde{M}(q;d)}\,.$$

Clearly,

$$|A_0|(u) \ll \frac{(1+qu^2)(1+u)}{(1-u^2)} = \frac{1+qu^2}{1-u}\,,$$

and so $|A_0|(u) \ll (q+1)/(1-u)$. To treat $A_1(u)$ we use Lemma 1.3.6 together with the facts that $\widetilde{N}(q;1) = q+1$, $\widetilde{N}(q;d) \leqslant (q^d-1)/d$ for odd $d \geqslant 1$, and $\widetilde{M}(q;d) \leqslant (q^{2d}-1)/(2d)$:

$$\begin{aligned}
|A_1|(u) &\ll \big(|B_1|(u)\big)^{q+1} \prod_{\substack{d\geqslant 3,\\ d \text{ odd}}} \big(|B_d|(u)\big)^{\widetilde{N}(q;d)} \prod_{d\geqslant 1} \big(|C_d|(u)\big)^{\widetilde{M}(q;d)} \\
&\ll \big(|B_1|(u)\big)^2 \exp\Big(\sum_{\substack{d\geqslant 1,\\ d \text{ odd}}} \frac{1}{d}\,\frac{u^d}{1-u^d} + \sum_{d\geqslant 1} \frac{1}{2d}\,\frac{u^{2d}}{1-u^{2d}}\Big) \\
&= \big(|B_1|(u)\big)^2 \exp\Big(\sum_{d\geqslant 1} \frac{1}{d}\,\frac{u^d}{1-u^d}\Big)\,.
\end{aligned}$$

Thus $|A_1|(u) \ll \big(|B_1|(u)\big)^2\,\Omega(u)^{-1}$ by Lemma 1.3.7. We have seen that

$$|B_1|(u) \ll 1 + \frac{1}{q-1}\,\frac{u}{1-u}$$

and therefore trivially

$$|B_1|(u) \ll 1 + \frac{u}{1-u} = \frac{1}{1-u}\,.$$

Putting this all together we find that $|A|(u) \ll (q+1)(1-u)^{-3}\Omega(u)^{-1}$. It follows from Lemma 1.3.8 that $|ss_{\mathrm{U}}(n,q) - ss_{\mathrm{U}}(n-1,q)|q^n \leqslant (q+1)p_4(n)$, that is, $|ss_{\mathrm{U}}(n,q) - ss_{\mathrm{U}}(n-1,q)| \leqslant (q+1)\,p_4(n)\,q^{-n}$, as was to be proved.

As a corollary we have from Lemma 1.3.9 the following bounds:

THEOREM 3.1.24. *If $11 \leqslant n < n' \leqslant \infty$ and $k := (q+1)/(2q-3)$ then*

$$|ss_{\mathrm{U}}(n',q) - ss_{\mathrm{U}}(n,q)| < 3k\,p_4(n)q^{-n} < 63\,k\,\big(\tfrac{2}{3}\,q\big)^{-n}.$$

In preparation for our treatment of the symplectic and orthogonal groups we first prove the following lemma.

LEMMA 3.1.25. *Define*

$$A_1(u) := Y_1^*(qu) \prod_{d\geqslant 1}(1+u^d)^{-N^*(q;2d)} \prod_{d\geqslant 1}(1+u^d)^{-M^*(q;d)}\,,$$

and

$$A_2(u) := Y_2^*(qu) \prod_{d\geqslant 1}(1-u^d)^{-N^*(q;2d)} \prod_{d\geqslant 1}(1+u^d)^{-M^*(q;d)}\,,$$

where $Y_1^*(u)$, $Y_2^*(u)$ are as defined on p. 64. Define also $e := e(q)$, and $k_0 := 1$ if q is odd and $k_0 := \frac{4q^2}{2q^2-3}$ if q is even. Then

$$|A_i|(u) \ll k_0\,(1-u)^{e-2}\,\Omega(u)^{-1}$$

for $i = 1, 2$, where $\Omega(u)$ is as defined on p. 20.

Proof. We deal first with $A_1(u)$. We have

$$\begin{aligned} A_1(u) &= \prod_{d\geqslant 1}\Big(\Big(1+\sum_{m\geqslant 1}\frac{q^{dm}\,u^{dm}}{|\mathrm{U}(m,q^d)|}\Big)\Big(\frac{1}{1+u^d}\Big)\Big)^{N^*(q;2d)} \\ &\qquad\qquad \times \prod_{d\geqslant 1}\Big(\Big(1+\sum_{m\geqslant 1}\frac{q^{dm}\,u^{dm}}{|\mathrm{GL}(m,q^d)|}\Big)\Big(\frac{1}{1+u^d}\Big)\Big)^{M^*(q;d)} \\ &= \prod_{d\geqslant 1}\Big(1+\sum_{n\geqslant 1} b_{d,n}u^{dn}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\sum_{n\geqslant 1} c_{d,n}u^{dn}\Big)^{M^*(q;d)}, \end{aligned}$$

where $b_{d,n}$ is as in our treatment of the unitary case and $c_{d,n}$ is as in the general linear and unitary cases. Thus

$$|b_{d,1}| = \frac{1}{q^d+1}\,, \quad |b_{d,n}| < \frac{q^d}{q^{2d}-1} \text{ for } n\geqslant 2, \quad \text{and} \quad |c_{d,n}| \leqslant \frac{1}{q^d-1}\,.$$

Also, $N^*(q;2d) = (q^d+1-e)/2d$ if d is a power of 2, $N^*(q;2d) \leqslant (q^d-1)/2d$ otherwise, and $M^*(q;d) \leqslant (q^d-1)/2d$ for $d\geqslant 1$ (see Lemma 1.3.16).

If q is odd, so that $e=2$ and $N^*(q;2d)\leqslant (q^d-1)/2d$ for all d, then

$$\begin{aligned} &\prod_{d\geqslant 1}\Big(1+\sum_{n\geqslant 1}|b_{d,n}|u^{dn}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\sum_{n\geqslant 1}|c_{d,n}|u^{dn}\Big)^{M^*(q;d)} \\ &\quad\ll \exp\Big(\sum_{d\geqslant 1}\Big(N^*(q;2d)\sum_{n\geqslant 1}|b_{d,n}|u^{dn}\Big)+\sum_{d\geqslant 1}\Big(M^*(q;d)\sum_{n\geqslant 1}|c_{d,n}|u^{dn}\Big)\Big) \\ &\quad\ll \exp\Big(\sum_{d\geqslant 1}\Big(\sum_{n\geqslant 1}\frac{u^{dn}}{2d}\Big)+\sum_{d\geqslant 1}\Big(\sum_{n\geqslant 1}\frac{u^{dn}}{2d}\Big)\Big) \;=\; \exp\sum_{d\geqslant 1}\Big(\sum_{n\geqslant 1}\frac{u^{dn}}{d}\Big), \end{aligned}$$

and it follows that in this case (q odd) $|A_1|(u) \ll \Omega(u)^{-1}$ as required.

Suppose now that q is even, so that $e=1$. Define $N^{**}(q;2d)$ to be equal to $N^*(q;2d)-1$ if d is a power of 2 and to be $N^*(q;2d)$ otherwise. Then

$$\prod_{d\geqslant 1}\Big(1+\sum_{n\geqslant 1} b_{d,n}u^{dn}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\sum_{n\geqslant 1} c_{d,n}u^{dn}\Big)^{M^*(q;d)} = B(u)\,C(u)\,,$$

where

$$B(u) := \prod_{m\geqslant 0}\Big(1+\sum_{n\geqslant 1} b_{2^m,\,n}\,u^{2^m n}\Big)$$

and

$$C(u) := \prod_{d\geqslant 1}\Big(1+\sum_{n\geqslant 1} b_{d,n}\,u^{dn}\Big)^{N^{**}(q;2d)}\prod_{d\geqslant 1}\Big(1+\sum_{n\geqslant 1} c_{d,n}\,u^{dn}\Big)^{M^*(q;d)}.$$

The same calculation as that for odd q yields that $|C|(u) \ll \Omega(u)^{-1}$.

To deal with $B(u)$ we define $B_d(u) := 1+\sum_{n\geqslant 1} b_{d,n}\,u^{dn}$ and note (see the definition of $b_{d,n}$ above) that $B_d(u) = (1+u^d)^{-1}\big(1+\sum_{m\geqslant 1}\frac{q^{dm}\,u^{dm}}{|\mathrm{U}(m,q^d)|}\big)$. It is a well known observation by Euler that since $(1-u)\prod_{m=0}^{n-1}(1+u^{2^m}) = 1-u^{2^n}$, we have

$\prod_{m\geqslant 0}(1+u^{2^m}) = 1/(1-u)$, and so

$$B(u) = \prod_{m\geqslant 0} B_{2^m}(u) = (1-u)\prod_{m\geqslant 0}\Big(1+\sum_{n\geqslant 1}\frac{q^{2^m n}\,u^{2^m n}}{|\mathrm{U}(n,q^{2^m})|}\Big)\,.$$

We shall prove that

$$\prod_{m\geqslant 0}\Big(1+\sum_{n\geqslant 1}\frac{q^{2^m n}\,u^{2^m n}}{|\mathrm{U}(n,q^{2^m})|}\Big) \ll \Big(\frac{2q^2}{2q^2-3}\Big)\,(1-u)^{-1}\,.$$

The first step is to note that if $n\geqslant 1$ then $\dfrac{q^{dn}}{|\mathrm{U}(n,q^d)|} < \dfrac{1}{q^{2d(n-1)}} + \dfrac{1}{q^{2dn}}$: this is easily checked if $n=1$ or $n\geqslant 3$, and if $n=2$ we observe that

$$\frac{q^{2d}}{|\mathrm{U}(2,q^d)|} = \frac{q^d}{(q^d+1)(q^{2d}-1)} < \frac{1}{q^{2d}} + \frac{1}{q^{4d}}\,.$$

Therefore

$$1+\sum_{n\geqslant 1}\frac{q^{dn}\,u^{dn}}{|\mathrm{U}(n,q^d)|} \ll \big(1+u^d\big)\Big(1+\sum_{n\geqslant 1}\frac{u^{dn}}{q^{2dn}}\Big) = \big(1+u^d\big)\Big(1-\frac{u^d}{q^{2d}}\Big)^{-1}\,,$$

and

$$\begin{aligned}\prod_{m\geqslant 0}\Big(1+\sum_{n\geqslant 1}\frac{q^{2^m n}\,u^{2^m n}}{|\mathrm{U}(n,q^{2^m})|}\Big) &\ll \prod_{m\geqslant 0}(1+u^{2^m})\prod_{m\geqslant 0}\Big(1-\frac{u^{2^m}}{q^{2^{m+1}}}\Big)^{-1}\\ &\ll \prod_{m\geqslant 0}(1+u^{2^m})\prod_{k\geqslant 1}\Big(1-\frac{u^k}{q^{2k}}\Big)^{-1}\\ &= (1-u)^{-1}\Omega(u/q^2)^{-1}\,.\end{aligned}$$

Now $\Omega(u/q^2)^{-1} = \sum p(n)q^{-2n}\,u^n$ and we know from Lemma 1.3.9 that $p(n)q^{-2n} \leqslant \big(2q^2/3\big)^{-n}$ for all $n\geqslant 0$. Thus $\Omega(u/q^2)^{-1} \ll (1-(3u/2q^2))^{-1}$, and

$$\prod_{m\geqslant 0}\Big(1+\sum_{n\geqslant 1}\frac{q^{2^m n}\,u^{2^m n}}{|\mathrm{U}(n,q^{2^m})|}\Big) \ll \frac{1}{(1-u)(1-(3u/2q^2))} \ll \frac{2q^2}{2q^2-3}\,(1-u)^{-1}\,,$$

where the last assertion comes from Lemma 1.3.5(d). It now follows that $|B|(u) \ll (1+u)\times\frac{2q^2}{2q^2-3}(1-u)^{-1} \ll \frac{4q^2}{2q^2-3}(1-u)^{-1}$, and so in this case ($q$ even) we have $|A_1|(u) \ll \frac{4q^2}{2q^2-3}(1-u)^{-1}\Omega(u)^{-1}$. This completes the proof of the lemma for $A_1(u)$.

To deal with $A_2(u)$ notice that, when expressed as the product of two infinite products, it is the same as $A_1(u)$ except that in the first factor u^d is replaced by $-u^d$ throughout. Thus

$$A_2(u) = \prod_{d\geqslant 1}\Big(1+\sum_{n\geqslant 1}(-1)^n b_{d,n}u^{dn}\Big)^{N^*(q;2d)}\prod_{d\geqslant 1}\Big(1+\sum_{n\geqslant 1}c_{d,n}u^{dn}\Big)^{M^*(q;d)}\,,$$

where $b_{d,n}$ and $c_{d,n}$ are exactly as in our analysis of $A_1(u)$. The rest of the proof for $A_1(u)$ therefore applies to give the result for $A_2(u)$, and this completes the proof of the lemma.

We now turn to the symplectic groups.

LEMMA 3.1.26. *Define* $A(u) := (1-qu)SS_{\mathrm{Sp}}(qu)$, *and let* $k_0 := 1$ *if* q *is odd,* $k_0 := \frac{4q^2}{2q^2-3}$ *if* q *is even, as in Lemma* 3.1.25. *Then*

$$|A|(u) \ll (q+1)k_0\,(1-u)^{-2}\Omega(u)^{-1}\,,$$

where $\Omega(u)$ *is as defined on p.* 20. *Consequently, by Lemma* 1.3.8,

$$|ss_{\mathrm{Sp}}(2m,q) - ss_{\mathrm{Sp}}(2m-2,q)| < (q+1)k_0\,p_3(m)q^{-m}.$$

Proof. By Theorem 3.1.5, $SS_{\mathrm{Sp}}(u) = F(u)^e\,Y_1^*(u)$, where $e = e(q)$ (so that, recall, $e = 2$ if q is odd and $e = 1$ if q is even), $F(u) = 1 + \sum_{m\geqslant 1} \dfrac{u^m}{|\mathrm{Sp}(2m,q)|}$, and

$$Y_1^*(u) = \prod_{d\geqslant 1}\Big(1+\sum_{m\geqslant 1}\frac{u^{dm}}{|\mathrm{U}(m,q^d)|}\Big)^{N^*(q;2d)} \prod_{d\geqslant 1}\Big(1+\sum_{m\geqslant 1}\frac{u^{dm}}{|\mathrm{GL}(m,q^d)|}\Big)^{M^*(q;d)}.$$

By Lemma 1.3.17(b),

$$A(u) = \frac{1-qu^2}{(1+u)^e}\,F(qu)^e\,Y_1^*(qu)\prod_{d\geqslant 1}(1+u^d)^{-N^*(q;2d)}\prod_{d\geqslant 1}(1+u^d)^{-M^*(q;d)}\,,$$

and so $A(u) = A_1(u)\,A_3(u)$ where $A_1(u)$ is as defined in the preceding lemma and

$$A_3(u) := \frac{1-qu^2}{(1+u)^e}\,F(qu)^e\,.$$

Now $F(qu) = 1+\dfrac{1}{q^2-1}\,u+\dfrac{1}{q^2(q^2-1)(q^4-1)}\,u^2+\cdots$, and Lemma 1.3.5(c) applied e times shows that $|A_3|(u) \ll (1+qu^2)(1-u)^{-e} \ll (1+q)(1-u)^{-e}$. The result now follows from Lemma 3.1.25.

Exactly as for the general linear and unitary cases we now have the following theorem.

THEOREM 3.1.27. *Let* $k := \dfrac{q+1}{2q-3}$ *if* q *is odd and* $k := \dfrac{4q^2(q+1)}{(2q-3)(2q^2-3)}$ *if* q *is even. If* $9 \leqslant m < m' \leqslant \infty$ *then*

$$|ss_{\mathrm{Sp}}(2m',q) - ss_{\mathrm{Sp}}(2m,q)| \leqslant 3k\,p_3(m)\,q^{-m} < 23\,k\,\left(\tfrac{2}{3}\,q\right)^{-m}.$$

The analysis for the orthogonal groups is similar. We treat the odd-dimensional groups first.

LEMMA 3.1.28. *Let* $A(u) := (1-qu)SS_{\mathrm{O}}(qu)$, *and let* $k_0 := 1$ *if* q *is odd,* $k_0 := \frac{4q^2}{2q^2-3}$ *if* q *is even, as in Lemma* 3.1.25. *Then*

$$|A|(u) \ll (q+1)k_0\,(1-u)^{-2}\Omega(u)^{-1}\,,$$

where $\Omega(u)$ *is as defined on p.* 20. *Consequently, by Lemma* 1.3.8,

$$|ss_{\mathrm{O}}(2m+1,q) - ss_{\mathrm{O}}(2m-1,q)| < (q+1)k_0\,p_3(m)q^{-m}.$$

Proof. Write $A(u)$ as $A_1(u)\,A_3(u)$ where, as in the proof of Lemma 3.1.26, $A_1(u)$ is the function defined in Lemma 3.1.25 and

$$A_3(u) := \frac{1-qu^2}{(1+u)^e}\,F_+(qu)^{e-1}\,F(qu)\,.$$

It follows from Lemma 1.3.5(c) that $F(qu)/(1+u) \ll (1-u)^{-1}$. Although the same result does not quite suffice to prove that $F_+(qu)/(1+u) \ll (1-u)^{-1}$, the argument

used in its proof does: for, examining coefficients we see that $F_+(qu)/(1+u) = \sum_{n\geqslant 1} d_n u^n$, where $d_0 = 1$, $d_1 = -1/(q^2-1)$, and $d_1 < d_n < 0$ for $n \geqslant 2$. Therefore

$$|A_3|(u) \ll (1+qu^2)(1-u)^{-e} \ll (1+q)(1-u)^{-e}\,,$$

and the result now follows from Lemma 3.1.25.

The following is an immediate consequence.

THEOREM 3.1.29. *Let* $k := \dfrac{q+1}{2q-3}$ *if* q *is odd and* $k := \dfrac{4q^2(q+1)}{(2q-3)(2q^2-3)}$ *if* q *is even. If* $9 \leqslant m < m' \leqslant \infty$ *then*

$$|ss_{\mathrm{O}}(2m'+1,q) - ss_{\mathrm{O}}(2m+1,q)| \leqslant 3k\, p_3(m)\, q^{-m} < 23\, k\, \left(\tfrac{2}{3}\, q\right)^{-m}.$$

For the even-dimensional orthogonal groups the situation is similar.

LEMMA 3.1.30. *Let* ϵ *be* $+$ *or* $-$ *and let* $A(u) := (1-qu)SS_{\mathrm{O}^\epsilon}(qu)$. *Also, let* $k_0 := \frac{3}{2}\,(q+1)^2$ *if* q *is odd and let* $k_0 := \dfrac{2q^2(q+1)(q+2)}{2q^2-3}$ *if* q *is even. Then* $|A|(u) \ll k_0(1-u)^{-2}\,\Omega(u)^{-1}$, *where* $\Omega(u)$ *is as defined on p.* 20. *Thus*

$$|ss_{\mathrm{O}^\epsilon}(2m,q) - ss_{\mathrm{O}^\epsilon}(2m-2,q)| < k_0\, p_3(m) q^{-m}\,.$$

Proof. By Theorem 3.1.7 and Lemma 1.3.17(b), (c),

$$A(u) = \tfrac{1}{2} A_1(u)\, A_3(u) + \tfrac{1}{2}\epsilon\, A_2(u)\, A_4(u)$$

where $A_1(u)$ and $A_2(u)$ are as defined in Lemma 3.1.25 and

$$A_3(u) := \frac{1-qu^2}{(1+u)^e}\left(F_+(qu)^e + (e-1)qu\, F(qu)^2\right)$$

and

$$A_4(u) := \frac{(1-qu)(1-qu^2)}{(1-u)^{e-1}(1+u)^e}\, F_-(qu)^e\,.$$

Arguing as in the proof of Lemma 3.1.28 (and treating the cases $e=1$ and $e=2$ separately), we find that

$$|A_3|(u) \ll \begin{cases} (q+1)^2/(1-u)^2 & \text{if } q \text{ is odd,} \\ (q+1)/(1-u) & \text{if } q \text{ is even.} \end{cases}$$

Also, if q is odd so that $e=2$ then

$$A_4(u) = \frac{(1-qu)(1-qu^2)}{(1-u^2)}\, \frac{F_-(qu)}{1+u}\, F_-(qu)\,.$$

Since all the coefficients of $F_-(qu)$ lie between 0 and 1, by Lemma 1.3.5(c)

$$|A_4|(u) \ll \frac{(1+qu)(1+qu^2)}{(1-u^2)}\, \frac{1}{1-u}\, F_-(qu) \ll \frac{(q+1)^2}{(1-u)}\, \frac{F_-(qu)}{(1-u)}\,.$$

Then Lemma 1.3.5(d) applies to give that $|A_4|(u) \ll (q+1)^2 F_-(q)(1-u)^{-2}$. Now $F_-(q) = 1 + \frac{q}{q^2-1} + \frac{1}{(q^2-1)(q^2+1)} + \cdots$ and it is not hard to see that $F_-(q) < 2$. Thus if q is odd then $|A_4|(u) \ll 2(q+1)^2/(1-u)^2$. If q is even, so that $e=1$ then

$$A_4(u) = (1-qu)(1-qu^2)\frac{F_-(qu)}{(1+u)}\,,$$

and so we find that $|A_4|(u) \ll (q+1)^2/(1-u)$ in this case.

Now

$$|A|(u) \ll \tfrac{1}{2}\,|A_1|(u)\,|A_3|(u) + \tfrac{1}{2}\,|A_2|(u)\,|A_4|(u)\,,$$

and so from Lemma 3.1.25

$$|A|(u) \ll \begin{cases} \frac{3}{2}(q+1)^2\,(1-u)^{-2}\,\Omega(u)^{-1} & \text{if } q \text{ is odd,} \\ \dfrac{2q^2(q+1)(q+2)}{2q^2-3}\,(1-u)^{-2}\,\Omega(u)^{-1} & \text{if } q \text{ is even,} \end{cases}$$

as claimed.

As usual, the following theorem is an immediate consequence.

THEOREM 3.1.31. *Let* $\epsilon \in \{+,-\}$*, and let* $k := \dfrac{3(q+1)^2}{2(2q-3)}$ *if* q *is odd and* $k := \dfrac{2q^2(q+1)(q+2)}{(2q-3)(2q^2-3)}$ *if* q *is even. If* $9 \leqslant m < m' \leqslant \infty$ *then*

$$|ss_{\mathrm{O}^\epsilon}(2m',q) - ss_{\mathrm{O}^\epsilon}(2m,q)| \leqslant 3k\,p_3(m)\,q^{-m} < 23\,k\,\left(\tfrac{2}{3}\,q\right)^{-m}.$$

3.2. Regular elements

Recall that an element of a finite classical group G is said to be regular if its centraliser in the corresponding algebraic group over the algebraic closure of the appropriate prime field has minimal possible dimension, namely, the Lie rank of the group. As was mentioned in the introduction, for the groups GL, U and Sp an element is regular if and only if it is cyclic, but, as was pointed out in [**17**], this is not true in the orthogonal case. In this section we focus on the finite orthogonal groups.

Let $r_{\mathrm{O}^\epsilon}(2m,q)$ and $r_{\mathrm{O}}(2m+1,q)$ be the probabilities that elements of $\mathrm{O}^\epsilon(2m,q)$ and of $\mathrm{O}(2m+1,q)$ respectively are regular. Of particular interest are the limiting values

$$r_{\mathrm{O}^\epsilon}(\infty,q) := \lim_{m\to\infty} r_{\mathrm{O}^\epsilon}(2m,q) \quad \text{and} \quad r_{\mathrm{O}}(\infty,q) := \lim_{m\to\infty} r_{\mathrm{O}}(2m+1,q)\,.$$

These limits do not obviously exist but we shall use generating functions to prove that they do and to evaluate them. Define

$$R_{\mathrm{O}^+}(u) := 1 + \sum_{m\geqslant 1} r_{\mathrm{O}^+}(2m,q)\,u^m\,; \quad R_{\mathrm{O}^-}(u) := \sum_{m\geqslant 1} r_{\mathrm{O}^-}(2m,q)\,u^m\,;$$

$$R_{\mathrm{O}}(u) := 1 + \sum_{m\geqslant 1} r_{\mathrm{O}}(2m+1,q)\,u^m\,.$$

To simplify the description of regular elements in the orthogonal groups we introduce a little *ad hoc* terminology. Let U be a vector space over $\mathbb{F}_q$ equipped with an orthogonal form φ, let $X \in \mathrm{Aut}\,(U,\varphi)$, and suppose that the characteristic polynomial of X is $(t-\eta)^n$, where $\eta = \pm 1$ (that is, X is unipotent or (-1)-potent). We shall call X, or the X-module U, *nearly cyclic* if either $U = \{0\}$ or there is an X-invariant orthogonal direct sum decomposition $U = U_0 \oplus^\perp U_1$ in which $\dim U_0 = 1$ and U_1 is cyclic as X-module. Note that under these circumstances if q is odd then $\dim U_1$ will be odd and $\dim U$ will therefore be even, whereas if q is even then $\dim U_1$ will be even and $\dim U$ will be odd.

We shall treat fields of odd and even characteristic separately, dealing first with odd q.

THEOREM 3.2.1. (See [**11**]). *Let q be an odd prime power and X an orthogonal matrix over $\mathbb{F}_q$. Then X is regular if and only if*

(a) *for every monic irreducible polynomial ϕ other than $t-1$ and $t+1$ the ϕ-primary component of X is cyclic and*
(b) *for $\eta = \pm 1$, the $(t-\eta)$-primary component of X is cyclic if it is odd-dimensional and nearly cyclic if it is even-dimensional.*

What this means is that when q is odd:

an element of $\mathrm{SO}^\epsilon(2m,q)$ is regular if and only if it is of the form $Y \oplus^\perp X_1 \oplus^\perp X_{-1}$, where Y is cyclic and does not have 1 or -1 as an eigenvalue, X_1 is unipotent and nearly cyclic, X_{-1} is (-1)-potent and nearly cyclic;

an element of $\mathrm{O}^\epsilon(2m,q) \setminus \mathrm{SO}^\epsilon(2m,q)$ is regular if and only if it is cyclic;

an element of $\mathrm{SO}(2m+1,q)$ is regular if and only if it is of the form $Y \oplus^\perp X_{-1}$, where Y is cyclic and does not have -1 as an eigenvalue, and X_{-1} is (-1)-potent and nearly cyclic;

an element of $\mathrm{O}(2m+1,q) \setminus \mathrm{SO}(2m+1,q)$ is regular if and only if it is of the form $Y \oplus^\perp X_1$, where Y is cyclic and does not have 1 as an eigenvalue, and X_1 is unipotent and nearly cyclic.

With this preparation we can relate the generating functions for regular orthogonal matrices to well-studied functions, namely $C_{\mathrm{Sp}}(u)$ as defined on p. 48 and X'_{O} as defined on p. 58, in the following way.

THEOREM 3.2.2. *Suppose that q is odd. For the odd-dimensional orthogonal groups we have*

$$R_{\mathrm{O}}(u) = \Big(1 + \frac{u}{q(q^2-1)} - \frac{u^2}{q^2(q^2-1)}\Big)\, C_{\mathrm{Sp}}(u)\,.$$

For the even-dimensional groups

$$\begin{aligned} R_{\mathrm{O}^+}(u) + R_{\mathrm{O}^-}(u) &= \left(\Big(1 + \frac{u}{q(q^2-1)} - \frac{u^2}{q^2(q^2-1)}\Big)^2 + u\right) C_{\mathrm{Sp}}(u)\,, \\ R_{\mathrm{O}^+}(u) - R_{\mathrm{O}^-}(u) &= \Big(1 + \frac{u}{q^2-1}\Big)^2 X'_{\mathrm{O}}(u)\,. \end{aligned}$$

Proof. The strategy is to consider the structure of the natural module V for a regular orthogonal matrix X. The argument is the same as that for Theorem 2.3.9 except that special care is needed for the factors $F_1(u)$, $F_{-1}(u)$ of the infinite product which enumerate primary components corresponding to the irreducible polynomials $t-1$ and $t+1$. It follows as in the proof of Theorem 2.3.9 that

$$\begin{aligned} R_{\mathrm{O}^+}(u^2) + R_{\mathrm{O}^-}(u^2) + 2uR_{\mathrm{O}}(u^2) &= F_1(u)\,F_{-1}(u) \times \\ &\times \prod_{d\geqslant 1} \Big(1 + \frac{u^{2d}}{q^d+1}\,\frac{q^d}{q^d-u^{2d}}\Big)^{N^*(q;2d)} \prod_{d\geqslant 1} \Big(1 + \frac{u^{2d}}{q^d-1}\,\frac{q^d}{q^d-u^{2d}}\Big)^{M^*(q;d)}\,, \end{aligned}$$

and then from Theorem 2.2.7 that

$$R_{\mathrm{O}^+}(u^2) + R_{\mathrm{O}^-}(u^2) + 2uR_{\mathrm{O}}(u^2) = \Big(1 - \frac{u^2}{q}\Big)^2 F_1(u)\,F_{-1}(u)\,C_{\mathrm{Sp}}(u^2)\,.$$

To find $F_1(u)$, $F_{-1}(u)$ we argue as follows. Clearly, $F_1(u) = F_{-1}(u)$, so it is sufficient to focus on the primary component for the polynomial $t-1$, that is, the unipotent component. This is either cyclic and of odd dimension or nearly cyclic

and of even dimension; in either case it can have type $+$ or $-$. There is a single conjugacy class of unipotent cyclic elements of $\mathrm{O}(2m+1,q)$; the centraliser order is $2q^m$ (see [**22**]). There is a single class of nearly cyclic unipotent elements in $\mathrm{O}^\epsilon(2,q)$, namely I_2, and the centraliser order is $|\mathrm{O}^\epsilon(2,q)|$, that is, $2(q-\epsilon 1)$. For $m \geqslant 2$ there are two classes of nearly cyclic unipotent matrices in $\mathrm{O}^\epsilon(2m,q)$. For each class $V = V_0 \oplus^\perp V_1$ where $\dim V_0 = 1$ and V_1 is a cyclic X-module. They are distinguished by the type of V_0. The centraliser order is $4q^m$ (see [**22**]). Thus

$$F_1(u) = F_{-1}(u) = 1 + f_1(u) + f_2(u)\,,$$

where

$$f_1(u) = \frac{u}{1} + \frac{u^3}{q} + \frac{u^5}{q^2} + \cdots = \frac{u}{1-(u^2/q)}$$

and

$$\begin{aligned} f_2(u) &= \frac{u^2}{2(q-1)} + \frac{u^2}{2(q+1)} + 4\frac{u^4}{4q^2} + 4\frac{u^6}{4q^3} + \cdots \\ &= \frac{qu^2}{q^2-1} + \frac{u^4}{q^2(1-(u^2/q))}\,. \end{aligned}$$

Here the coefficient 4 multiplying the term $u^{2m}/4q^m$ in $f_2(u)$ comes from the fact that there are 4 classes of unipotent matrices of size $2m$ corresponding to the 2 choices for $\mathrm{type}(V)$ and the 2 independent choices for $\mathrm{type}(V_0)$. We now have that

$$\begin{aligned} &R_{\mathrm{O}^+}(u^2) + R_{\mathrm{O}^-}(u^2) + 2uR_{\mathrm{O}}(u^2) \\ &\quad = \Big(1-\frac{u^2}{q}\Big)^2\Big(1 + \frac{u}{1-(u^2/q)} + \frac{qu^2}{q^2-1} + \frac{u^4}{q^2(1-(u^2/q))}\Big)^2 C_{\mathrm{Sp}}(u^2)\,. \end{aligned}$$

The terms of odd degree yield, after some calculation, that

$$R_{\mathrm{O}}(u) = \Big(1 + \frac{u}{q(q^2-1)} - \frac{u^2}{q^2(q^2-1)}\Big)\, C_{\mathrm{Sp}}(u)$$

which is the first assertion of the theorem. Similarly, picking out the terms of even degree we find that

$$R_{\mathrm{O}^+}(u) + R_{\mathrm{O}^-}(u) = \Big(\Big(1 - \frac{u}{q} + \frac{u(q^3-u)}{q^2(q^2-1)}\Big)^2 + u\Big)\, C_{\mathrm{Sp}}(u)\,,$$

which, after simple algebraic rearrangement, is the second assertion. The third assertion is proved similarly, using the extended notion of type $\tau(V)$ defined on p. 53 in the same way as it is used in §2.3.

THEOREM 3.2.3. *For odd q, with $c_{\mathrm{Sp}}(\infty,q)$ as described in Theorem* 2.2.9 *we have*

$$\begin{aligned} r_{\mathrm{O}}(\infty,q) &= \Big(1 + \frac{1}{q^2(q+1)}\Big)\, c_{\mathrm{Sp}}(\infty,q)\,; \\ r_{\mathrm{O}^+}(\infty,q) = r_{\mathrm{O}^-}(\infty,q) &= \Big(1 + \frac{1}{q^2(q+1)} + \frac{1}{2q^4(q+1)^2}\Big)\, c_{\mathrm{Sp}}(\infty,q)\,. \end{aligned}$$

Proof. Since $C_{\mathrm{Sp}}(u)$ has a pole at $u = 1$ with residue $c_{\mathrm{Sp}}(\infty, q)$, using Lemma 1.3.3 in the usual way we find that

$$\begin{aligned} r_{\mathrm{O}}(\infty, q) &= \Big(1 + \frac{1}{q(q^2-1)} - \frac{1}{q^2(q^2-1)}\Big)\, c_{\mathrm{Sp}}(\infty, q) \\ &= \Big(1 + \frac{1}{q^2(q+1)}\Big)\, c_{\mathrm{Sp}}(\infty, q)\,, \end{aligned}$$

as required. Since $X'_{\mathrm{O}}(u)$ is analytic in the open disc $D(q^2)$ (see Prop. 2.3.10), the third assertion of Theorem 3.2.2 implies that $r_{\mathrm{O}^+}(2m, q) - r_{\mathrm{O}^-}(2m, q) \to 0$ as $m \to \infty$, so that $r_{\mathrm{O}^+}(\infty, q) = r_{\mathrm{O}^-}(\infty, q)$. Then, examining residues at $u = 1$ of the functions occurring in the second assertion of that theorem we find that

$$r_{\mathrm{O}^+}(\infty, q) = r_{\mathrm{O}^-}(\infty, q) = \frac{1}{2}\Big(\Big(1 + \frac{1}{q^2(q+1)}\Big)^2 + 1\Big)\, c_{\mathrm{Sp}}(\infty, q)\,,$$

and, after a very little elementary algebra, this completes the proof.

Corollary 3.2.4. *Suppose that q is odd. Then*

$$r_{\mathrm{O}}(\infty, q) = 1 - 2q^{-3} + O(q^{-4}) \quad \textit{and} \quad r_{\mathrm{O}^\pm}(\infty, q) = 1 - 2q^{-3} + O(q^{-4})\,.$$

This follows immediately from the fact that $c_{\mathrm{Sp}}(\infty, q) = 1 - 3q^{-3} + O(q^{-4})$ when q is odd. It illustrates Steinberg's theorem that the non-regular elements form a subvariety of codimension 3 in an orthogonal group.

For the case when q is even, the theory is similar and we simply sketch what happens. If $X \in \mathrm{O}(2m+1, q)$ then X is regular if and only if all primary summands for monic irreducible polynomials other than $t - 1$ are cyclic and the unipotent summand is nearly cyclic. In this case the natural homomorphism $\mathrm{O}(2m+1, q) \to \mathrm{Sp}(2m, q)$ maps regular elements to regular elements bijectively, and so the proportion of regular elements in $\mathrm{O}(2m+1, q)$ is exactly the same as the proportion of cyclic elements in $\mathrm{Sp}(2m, q)$, that is $r_{\mathrm{O}}(2m+1, q) = c_{\mathrm{Sp}}(2m, q)$. For even dimensions the analogue of Theorem 3.2.1 holds in the form: the matrix X in $\mathrm{O}^\pm(2m, q)$ is regular if and only if for every monic irreducible polynomial ϕ other than $t - 1$ the ϕ-primary component of X is cyclic, and the unipotent component of X has one of the four following forms:

(1) cyclic (of even dimension $2k$);
(2) I_2 (the two-dimensional identity matrix);
(3) $J_2 \oplus^\perp J_2$, where J_2 is cyclic unipotent of dimension 2;
(4) $J_2 \oplus^\perp J_{2k-2}$, where $k \geqslant 3$ and J_{2k-2} is cyclic unipotent of dimension $2k - 2$.

In Case (1) the type of the underlying vector space summand can be $+$ or $-$, and the order of the centraliser C is $2q^{k-1}$; in Case (2) the type can be $+$ or $-$, and $|C| = |\mathrm{O}^\epsilon(2, q)| = 2(q - \epsilon 1)$; in Case (3) the type can be $+$ or $-$, and $|C| = 2q^2$; and in Case (4) there are four types (depending on the type of the summand affording J_2 and the type of that affording J_{2k-2}), and $|C| = 4q^k$. We find that

$$R_{\mathrm{O}^+}(u) + R_{\mathrm{O}^-}(u) = f_1(u)\,\big(1 - (u/q)\big)\, C_{\mathrm{Sp}}(u)\,,$$

where

$$f_1(u) = 1 + \sum_{k=1}^{\infty} \frac{u^k}{q^{k-1}} + \frac{u}{2(q-1)} + \frac{u}{2(q+1)} + \sum_{k=2}^{\infty} \frac{u^k}{q^k}$$
$$= 1 + \frac{u}{1-(u/q)} + \frac{q\,u}{q^2-1} + \frac{u^2}{q^2\big(1-(u/q)\big)}\,.$$

Moreover, as in the proof of Theorem 2.3.9,

$$R_{\mathrm{O}^+}(u) - R_{\mathrm{O}^-}(u) = \Big(1 + \frac{u}{q^2-1}\Big) X'_{\mathrm{O}}(u)\,,$$

and so, since X'_{O} is analytic in the disc $D(q^2)$, $r_{\mathrm{O}^+}(2m,q) - r_{\mathrm{O}^-}(2m,q) \to 0$ as $m \to \infty$.

THEOREM 3.2.5. *When q is even $r_{\mathrm{O}}(\infty,q) = c_{\mathrm{Sp}}(\infty,q)$ and*

$$r_{\mathrm{O}^\pm}(\infty,q) = \Big(1 + \frac{1}{2q^2(q+1)}\Big)\, c_{\mathrm{Sp}}(\infty,q) = 1 - \tfrac{3}{2}q^{-3} + O(q^{-4})\,.$$

Proof. Evaluating the residue of $R_{\mathrm{O}^+}(u) + R_{\mathrm{O}^-}(u)$ at its pole at $u = 1$ in the usual way we find that

$$r_{\mathrm{O}^+}(\infty,q) + r_{\mathrm{O}^-}(\infty,q) = \Big(2 + \frac{1}{q^2(q+1)}\Big)\, c_{\mathrm{Sp}}(\infty,q)\,,$$

and the assertion of the theorem follows immediately.

In fact, using the expansions for $c_{\mathrm{Sp}}(\infty,q)$ given on p. 51 we find that if q is odd then

$$r_{\mathrm{O}}(\infty,q) = 1 - \frac{2}{q^3} + \frac{1}{q^4} - \frac{2}{q^5} + \frac{4}{q^6} - \frac{5}{q^7} + \frac{10}{q^8} - \frac{15}{q^9} + O\Big(\frac{1}{q^{10}}\Big)$$

and

$$r_{\mathrm{O}^\pm}(\infty,q) = 1 - \frac{2}{q^3} + \frac{1}{q^4} - \frac{2}{q^5} + \frac{9}{2q^6} - \frac{6}{q^7} + \frac{23}{2q^8} - \frac{37}{2q^9} + O\Big(\frac{1}{q^{10}}\Big)\,.$$

If q is even then

$$r_{\mathrm{O}^\pm}(\infty,q) = 1 - \frac{3}{2q^3} + \frac{1}{2q^4} - \frac{3}{2q^5} + \frac{5}{2q^6} - \frac{3}{q^7} + \frac{6}{q^8} - \frac{9}{q^9} + O\Big(\frac{1}{q^{10}}\Big)\,.$$

Good upper bounds, lower bounds, and convergence rates can be derived for the frequency of regular elements just as they can for cyclic matrices in orthogonal groups. But what we have done is enough to emphasize the point that regular elements in orthogonal groups are not the same as cyclic matrices and to exhibit techniques that can give good statistical information. That is enough, and we stop here.

Bibliography

[1] Lars V. Ahlfors, *Complex analysis* (second edition). McGraw-Hill, New York etc., 1966.

[2] Tom M. Apostol, *Introduction to analytic number theory*. Springer-Verlag, New York etc., 1976.

[3] John R. Britnell, Cyclic and separable matrices in the special linear groups over a finite field, *J. London Math. Soc.* (2), 66 (2002), 605–622.

[4] John R. Britnell, *Cycle index methods for matrix groups over finite fields*. DPhil thesis, University of Oxford, 2003.

[5] Jason Fulman, *Probability in the classical groups over finite fields: symmetric functions, stochastic algorithms, and cycle indices*. PhD thesis, Harvard University, 1997.

[6] Jason Fulman, Cycle indices for the finite classical groups, *J. Group Theory*, 2 (1999), 251–289.

[7] Jason Fulman and Robert M. Guralnick, Derangements in simple and primitive groups. In *Groups, combinatorics and geometry: Durham 2001*, A. A. Ivanov, M. W. Liebeck and J. Saxl eds, World Scientific, 2003, pp. 99–121.

[8] Jason Fulman and Robert M. Guralnick, Derangements in subspace actions of finite classical groups. Preprint, 2002.

[9] Jason Fulman and Robert M. Guralnick, The probability of generating an irreducible subgroup. Preprint 2002.

[10] Jason Fulman and Robert M. Guralnick, Conjugacy class properties of the extension of $\mathrm{GL}(n, q)$ generated by the inverse transpose involution, *J. Algebra*, 275 (2004), 356–396.

[11] Jason Fulman, Peter M. Neumann and Cheryl E. Praeger, Conjugacy in the classical groups as a classification of indecomposable objects. Preprint 1999.

[12] Robert M. Guralnick and Frank Lübeck, On p-singular elements in Chevalley groups in characteristic p. In *Groups and computation III* (Procs Internat. Conf. Ohio State U., June 1999). William M. Kantor and Ákos Seress eds, Walter de Gruyter, Berlin and New York 2001, pp. 169–182.

[13] G. I. Lehrer, The cohomology of the regular semisimple variety, *J. Algebra*, 199 (1998), 666–689.

[14] G. I. Lehrer and G. B. Segal, Homology stability for classical regular semisimple varieties, *Math. Z.*, 236 (2001), 251–290.

[15] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications* (revised edition). Cambridge University Press, Cambridge, 1994.

[16] Peter M. Neumann and Cheryl E. Praeger, A recognition algorithm for special linear groups, *Proc. London Math. Soc.* (3), 65 (1992), 555–603.

[17] Peter M. Neumann and Cheryl E. Praeger, Cyclic matrices over finite fields, *J. London Math. Soc.* (2), 52 (1995), 263–284.

[18] Peter M. Neumann and Cheryl E. Praeger, Cyclic matrices in classical groups over finite fields, *J. Algebra*, 234 (2000), 367–418.

[19] Peter M. Neumann and Cheryl E. Praeger, Cyclic matrices and the meataxe. In *Groups and Computation, III*, (Procs Conf. on Computational Group Theory, OSU 1999, eds A. Seress and W. M. Kantor), Ohio State University Math. Res. Inst. Publ. 8, Walter de Gruyter, Berlin 2001, pp. 291–300.

[20] R. Steinberg, Regular elements of semisimple algebraic groups, *Publ. Math. Inst. Hautes Études Sci.*, 25 (1965), 49–80.

[21] D. E. Taylor, *The geometry of the classical groups*. Heldermann Verlag, Berlin, 1992.

[22] G. E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, *J. Australian Math. Soc.*, 3 (1963), 1–62.

[23] G. E. Wall, Counting cyclic and separable matrices over a finite field, *Bull. Australian Math. Soc.*, 60 (1999), 253–284.