DERANGEMENTS AND EIGENVALUE-FREE ELEMENTS IN FINITE CLASSICAL GROUPS

PETER M. NEUMANN AND CHERYL E. PRAEGER

1. *Introduction*

Permutations that have no fixed points have been known for a very long time as 'derangements'. Under that heading Rouse-Ball [**10**, p. 46] puts the matter in the following charming way: 'Suppose you have written a letter to each of n different friends, and addressed the n corresponding envelopes. In how many ways can you make the regrettable mistake of putting *every* letter into a wrong envelope?' He traces this problem back to 1713 and since then it has occurred in one form or another in many elementary texts on probability theory (see for example [**12**, p. 57] and references cited by Rouse-Ball). Let p_n be the probability that all the letters are put into the wrong envelope. It is well known that $p_n \to \mathrm{e}^{-1}$ as $n \to \infty$, and that, moreover, convergence is very fast. In fact, $p_n = \sum_0^n (-1)^r/r!$, so that $|p_n - \mathrm{e}^{-1}| < 1/(n+1)!$.

A derangement can be thought of as a fixed-point-free element of the symmetric group $\mathrm{Sym}(n)$. In this paper we turn our attention to eigenvalue-free elements of finite linear groups. Since an eigenvector of a linear transformation X in a vector space V corresponds to a fixed point of X in the projective space whose points are the 1-dimensional subspaces of V, eigenvalue-free invertible matrices correspond to derangements in projective groups.

Although most of our work deals with groups, we are also interested in the matrix ring $\mathrm{M}(n, q)$. It is not hard to understand that the proportion $v(\mathrm{M}; n, q)$ of eigenvalue-free $n \times n$ matrices over $\mathbb{F}_q$ should be approximately e^{-1} when q is large. For any fixed element λ of $\mathbb{F}_q$ the number of matrices that have λ as an eigenvalue is the number of solutions of the equation $\det(\lambda I - X) = 0$, and this is the same as the number of singular matrices. Therefore the number of matrices for which λ is not an eigenvalue is the same as the number of non-singular matrices, which is $\prod_{i=1}^n (q^n - q^i)$, and the probability that a randomly chosen matrix X does not have λ as an eigenvalue is $\prod_{i=1}^n (1 - q^{-i})$. If these probabilities were independent (for different values of λ) then the probability $v(\mathrm{M}; n, q)$ of X having no eigenvalue would be $(\prod_{i=1}^n (1 - q^{-i}))^q$. Since $(1 - q^{-1})^q \to \mathrm{e}^{-1}$ as $q \to \infty$ and $(1 - q^{-i})^q \to 1$ as $q \to \infty$ for $i \geqslant 2$ this number is close to e^{-1} when q is large.

There is another way of understanding why the probability that a randomly chosen matrix is eigenvalue-free should be close to e^{-1}. Let $p_n(q)$ denote the probability that a randomly chosen monic polynomial over a field F with q elements has no zeros in F. Using the inclusion–exclusion principle or generating function methods one can prove quite easily, as Zsigmondy [**14**] did over a hundred years ago (in the case where q is prime), that

Received 4 October 1996.

1991 *Mathematics Subject Classification* 15A52.

J. London Math. Soc. (2) 58 (1998) 564–586

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

$$p_n(q) = \sum_{r=0}^{\min\{q,\,n\}} (-1)^r \binom{q}{r} q^{-r}$$

so that $p_n(q) = (1-q^{-1})^q$ if $n \geqslant q$. Clearly, $p_n(q)$ is close to e^{-1}. Since monic polynomials of degree n can be expected to occur approximately uniformly as the characteristic polynomials of $n \times n$ matrices (and indeed they do, as Reiner [**9**] has made precise; see also Hansen and Schmutz [**7**]) we should also expect $v(\mathrm{M}; n, q)$ to be close to e^{-1}.

We find both the above arguments intuitively convincing. Unfortunately, we have not been able to work the first of them up into a satisfactory proof, and the second, although it can be made precise, does not give good enough estimates. They suggest that $v(\mathrm{M}; n, q)$ should converge to e^{-1} as both n and q tend to infinity, but they do not give any insight into how fast that convergence should be. In fact the behaviour of $v(\mathrm{M}; n, q)$ turns out to be very similar to that of $p_n(q)$. If $n \geqslant q$ then $\log p_n(q) = q \log(1-q^{-1})$, and expanding $\log(1-q^{-1})$ as a power series in q^{-1}, multiplying by q and exponentiating, one finds that

$$(1-q^{-1})^q = \mathrm{e}^{-1}(1 - \tfrac{1}{2}q^{-1} - \tfrac{5}{24}q^{-2} - \tfrac{5}{48}q^{-3} + O(q^{-4})).$$

Among other things, we shall prove that

$$\lim_{n\to\infty} v(\mathrm{M}; n, q) = \mathrm{e}^{-1}(1 - \tfrac{3}{2}q^{-1} - \tfrac{5}{24}q^{-2} - \tfrac{5}{16}q^{-3} + O(q^{-4}))$$

and that the convergence of $v(\mathrm{M}; n, q)$ as $n \to \infty$ is very rapid.

Although $\mathrm{M}(n, q)$ is of considerable importance, we shall focus mainly on matrix groups. The results for $\mathrm{M}(n, q)$ can be derived very easily from those for $\mathrm{GL}(n, q)$: every element of $\mathrm{M}(n, q) \setminus \mathrm{GL}(n, q)$ has 0 as an eigenvalue, and therefore if $v(\mathrm{GL}; n, q)$ is the proportion of non-singular matrices that are eigenvalue-free then

$$v(\mathrm{M}; n, q) = \frac{|\mathrm{GL}(n, q)|\, v(\mathrm{GL}; n, q)}{|\mathrm{M}(n, q)|} = v(\mathrm{GL}; n, q) \prod_{i=1}^{n} (1-q^{-i}).$$

As we have already indicated, we are unable to transform the heuristics described above into rigorous mathematics giving precise enough estimates. Instead we shall use a generating function approach to obtain usable expressions for $v(\mathrm{GL}; n, q)$, and then also for $v(\mathrm{M}; n, q)$. The generating functions can all be expressed in terms of a function introduced by Euler [**5**, Article 306] (see also [**1**, p. 19]): namely, the function $G(x; z) := \prod_{i=1}^{\infty}(1 - x^{-i}z)$, where $|x| > 1$.

The method allows us to solve the analogous problem for all the finite classical groups, that is to say for the general linear groups, the symplectic groups, the unitary groups and the orthogonal groups over finite fields. We write $v(\mathrm{X}; n, q)$ for the probability that a matrix chosen at random from the group $\mathrm{X}(n, q)$ should turn out to be eigenvalue-free, where $\mathrm{X}(n, q)$ is one of the classical groups consisting of $n \times n$ matrices over the field $\mathbb{F}_q$ (or $\mathbb{F}_{q^2}$ in the case of the unitary groups). Define $v(\mathrm{X}; \infty, q) := \lim_{n\to\infty} v(\mathrm{X}; n, q)$. We shall show how $v(\mathrm{X}; \infty, q)$ can be expressed explicitly in terms of certain values of Euler's function $G(x; z)$, and that $v(\mathrm{X}; n, q)$ converges very rapidly to $v(\mathrm{X}; \infty, q)$ as $n \to \infty$. Convergence is, in fact, notably faster (for fixed q) than convergence in the classical problem of derangements. Our main results are summarised in Table 1. The first column lists the structure; the second gives two different forms for the limiting probability; the last gives an upper bound for the rate of convergence, that is for $|v(\mathrm{X}; \infty, q) - v(\mathrm{X}; n, q)|$, valid for large n.

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

TABLE 1.

Structure	Limiting probability (two forms)	Convergence rate
$\mathrm{M}(n,q)$	$G(q;1)^q$ $\mathrm{e}^{-1}(1-\frac{3}{2}q^{-1}+O(q^{-2}))$	$O(q^{-(n+1)(n+q)/(2(q-1))})$
$\mathrm{GL}(n,q)$	$G(q;1)^{q-1}$ $\mathrm{e}^{-1}(1-\frac{1}{2}q^{-1}+O(q^{-2}))$	$O(q^{-(n+1)(n+q)/(2(q-1))})$
$\mathrm{Sp}(2m,q)$, odd q	$G(q^2;q)^2\,G(q;1)^{(q-3)/2}$ $\mathrm{e}^{-1/2}(1-\frac{5}{4}q^{-1}+O(q^{-2}))$	$O(q^{-(m+1)^2/(q-1)})$
$\mathrm{Sp}(2m,q)$, even q	$G(q^2;q)\,G(q;1)^{(q-2)/2}$ $\mathrm{e}^{-1/2}(1-\frac{3}{4}q^{-1}+O(q^{-2}))$	$O(q^{-(m+1)^2/(q-1)})$
$\mathrm{U}(n,q)$	$G(-q;-1)^{q+1}\,G(q^2;1)^{(q^2-q-2)/2}$ $\mathrm{e}^{-3/2}(1+O(q^{-2}))$	$O(q^{-n(4n+q^2+3q+2)/(2(q^2+3q+2))})$
$\mathrm{O}^\varepsilon(2m,q)$, odd q	$\frac{1}{2}G(q^2;q)^2\,G(q;1)^{(q-3)/2}$ $\frac{1}{2}\mathrm{e}^{-1/2}(1-\frac{5}{4}q^{-1}+O(q^{-2}))$	$O(q^{-m(m+(q-1)/2)/(q-1)})$
$\mathrm{O}^\varepsilon(2m,q)$, even q	$\frac{1}{2}G(q^2;q)\,G(q;1)^{(q-2)/2}$ $\frac{1}{2}\mathrm{e}^{-1/2}(1-\frac{3}{4}q^{-1}+O(q^{-2}))$	$O(q^{-m(m+q/2)/(q-1)})$

Although $v(\mathrm{X};\infty,q)$ is here tabulated modulo order q^{-2}, in the body of the paper we compute modulo q^{-4}, and it would be a simple matter to give the answers to higher degrees of accuracy.

This table invites two observations about the orthogonal groups. First, the odd-dimensional orthogonal groups are missing. Over fields of characteristic 2 any odd-dimensional quadratic form is singular, so its isometry group is of no interest in the context of our work. And if q is odd then every element of $\mathrm{O}(2m+1,q)$ has eigenvalues. It is perhaps worth recalling the reason. Any quadratic form in $2m+1$ variables over $\mathbb{F}_q$ is equivalent under non-singular change of variable either to $\sum_1^{2m+1} x_i^2$ or to $\alpha\sum_1^{2m+1} x_i^2$, where α is a non-square in $\mathbb{F}_q$. Obviously, these two forms have the same orthogonal group, namely $\{X\in\mathrm{GL}(2m+1,q)\mid XX^{\mathrm{tr}}=I\}$. If $X\in\mathrm{O}(2m+1,q)$ then $\det X=\pm 1$. Moreover, if $\det X=-1$ then $\det(-X)=1$. Therefore it is sufficient to show that orthogonal matrices of determinant 1, that is, elements of $\mathrm{SO}(2m+1,q)$, have eigenvalues. Suppose that $XX^{\mathrm{tr}}=I$ and that $\det X=1$. Then also $\det X^{\mathrm{tr}}=1$ and so

$$\det(I-X)=\det(X^{\mathrm{tr}}-XX^{\mathrm{tr}})=\det(X-I)^{\mathrm{tr}}=\det(X-I)=-\det(I-X).$$

Therefore $\det(I-X)=0$ and so 1 is an eigenvalue of X. Thus odd-dimensional orthogonal groups over fields of odd characteristic contain no eigenvalue-free matrices.

The second noteworthy point about the orthogonal groups concerns the factor $\frac{1}{2}$ that comes at the front of the formulae for the probabilities. The algebraic group $\mathrm{O}^\varepsilon(2m,q)$ is disconnected. The connected component containing the identity matrix I is $\mathrm{SO}^\varepsilon(2m,q)$, which is a subgroup of index 2. A simple variant of the argument in the preceding paragraph proves that all elements of the non-trivial coset do have eigenvalues (see Theorem 7.1 below). Thus the quantities $G(q^2;q)^2\,G(q;1)^{(q-3)/2}$ (when q is odd) and $G(q^2;q)\,G(q;1)^{(q-2)/2}$ (when q is even) measure the limiting probability (as $m\to\infty$) that a matrix X chosen at random from $\mathrm{SO}^\varepsilon(2m,q)$ should turn out to be eigenvalue-free.

The paper is organised as follows: §2 contains a preparatory account of Euler's function and its powers; §3 contains other preparatory material on the classical

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

groups over finite fields; §§4–7 are devoted to treatments of the general linear, symplectic, unitary and orthogonal groups respectively; §8 deals with a closely related matter, namely, the probability that a matrix X chosen at random from one of the classical groups does not have a given field element λ as an eigenvalue. The present work emerged from, and its results are applied in, our study of cyclic matrices [**8**]. In that paper our general method for estimating an upper bound for the proportion of non-cyclic matrices in classical groups was inadequate for orthogonal groups over fields of small order, and failed to produce a usable bound in the case where the field size was 2. There is an exploitable connection between eigenvalue-free matrices and cyclic matrices, and the results of this paper have led to satisfactory estimates for the proportions of cyclic matrices in these orthogonal groups. They have also yielded improved estimates for other classical groups.

Acknowledgements. For an earlier version of our theorem in the case of orthogonal groups over fields of characteristic 2 we required to know the number of unipotent elements in $O^\varepsilon(2n,q)\setminus\Omega^\varepsilon(2n,q)$. This was calculated for us by Jean Michel, Gus Lehrer and Bob Howlett. Although that result is no longer needed here, we thank them for their help. We are grateful also to Professor Harald Niederreiter for the reference to Zsigmondy.

We record our sincere thanks to several bodies for research and travel grants that have supported our continued collaboration in general, and the work reported here in particular: the Engineering and Physical Sciences Research Council of the United Kingdom (Visiting Fellowship Research Grant GR/K69186), the Australian Research Council, and the Royal Society of London.

2. *Some generating functions*

Let x be a complex number with $|x|>1$; usually we shall take x to be q or q^2, sometimes $-q$. As has already been announced in §1, Euler's function defined by $G(x;z):=\prod_{i=1}^{\infty}(1-x^{-i}z)$ will play a central role in our work. Since the product converges absolutely and uniformly over any compact set of complex numbers (see, for example, Copson [**3**, p. 104]) it represents an integral function (that is, a function holomorphic over the whole of $\mathbb{C}$) which has simple zeros at $x, x^2, x^3, \ldots$ and no other zeros. Because it is holomorphic everywhere, $G(x;z)$ must have a power-series expansion $\sum_0^\infty g(n)z^n$ (or $\sum_0^\infty g_x(n)z^n$ if the dependence of $g(n)$ on x needs to be shown explicitly in the notation) converging everywhere in $\mathbb{C}$.

The function $G(x;z)^{-1}$ is nearly as important as $G(x;z)$. It is meromorphic in the complex plane, with simple poles at $x, x^2, x^3, \ldots$ and with no zeros, and it has a Taylor series converging for $|z|<|x|$.

THEOREM 2.1 (Euler, 1748).
(1) $G(x;z)=\sum_{n=0}^{\infty}g(n)z^n$ *where* $g(n)=(-1)^n x^{-n(n+1)/2}\prod_{i=1}^{n}(1-x^{-i})^{-1}$;
(2) $G(x;z)^{-1}=\sum_{n=0}^{\infty}h(n)z^n$ *where* $h(n)=x^{-n}\prod_{i=1}^{n}(1-x^{-i})^{-1}$.

Proof. (1) From the definition, $G(x;xz)=(1-z)G(x;z)$. Comparison of power-series coefficients yields that $x^n g(n)=g(n)-g(n-1)$. Therefore $g(n)=-g(n-1)/(x^n-1)$. Since $g(0)=1$ it follows that

$$g(n)=(-1)^n\prod_{i=1}^{n}(x^i-1)^{-1}=(-1)^n x^{-n(n+1)/2}\prod_{i=1}^{n}(1-x^{-i})^{-1}.$$

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

(2) Similarly, from the equation $(1-z)\,G(x;xz)^{-1} = G(x;z)^{-1}$ we have that $x^n h(n) - x^{n-1}h(n-1) = h(n)$. Solving this recurrence relation we find that $h(n) = x^{-n}\prod_{i=1}^{n}(1-x^{-i})^{-1}$.

Prompted by this theorem and mindful of later developments we are led to define

$$c_n(x) := \prod_{i=1}^{n}(1-x^{-i})^{-1} \quad \text{and} \quad c(x) := \lim_{n\to\infty} c_n(x),$$

so that $g(n) = (-1)^n\, c_n(x)\, x^{-n(n+1)/2}$ and $h(n) = x^{-n}c_n(x)$. For future use we record the following inequalities.

LEMMA 2.2. *If x is real and $x \geqslant 2$ then*
(1) $1 \leqslant c_n(x) < c(x) \leqslant c(2) < \frac{32}{9}$ (*in fact* $c(2) = 3.4627\ldots$),
(2) $1 < c(x) < x^2/(x^2-x-1)$,
(3) $c(x^2)^2 < c(x)$, *and*
(4) $(2+3x^{-1/2})\,c(x) < 16$.

Proof. That the inequalities $1 \leqslant c_n(x) < c(x) \leqslant c(2)$ hold when $x \geqslant 2$ should be clear; what is required for (1) therefore is to estimate $c(2)$. Use induction to see that if $0 < x_i < 1$ for $1 \leqslant i \leqslant m$ then $\prod_{i=1}^{m}(1-x_i) > 1 - \sum_{i=1}^{m} x_i$. Then

$$c(2)^{-1} = (\tfrac{1}{2})(\tfrac{3}{4})\prod_{i=3}^{\infty}(1-2^{-i}) > \tfrac{3}{8}\left(1-\sum_{i=3}^{\infty}2^{-i}\right) = \tfrac{9}{32}.$$

Similarly,

$$\begin{aligned} c(x)^{-1} = (1-x^{-1})\prod_{i=2}^{\infty}(1-x^{-i}) &> (1-x^{-1})\left(1-\sum_{i=2}^{\infty}x^{-i}\right) \\ &= (1-x^{-1})\,(1-x^{-2}(1-x^{-1})^{-1}) \\ &= 1-x^{-1}-x^{-2}, \end{aligned}$$

and part (2) of the lemma follows immediately. For part (3) note that

$$c(x^2)^2 = \prod_{1}^{\infty}(1-x^{-2i})^{-2} < \prod_{1}^{\infty}(1-x^{-(2i-1)})^{-1}\,(1-x^{-2i})^{-1} = c(x)$$

(and this only requires that $x > 1$). For part (4) a quick calculation shows that if $x \geqslant 2$ then $2+3x^{-1/2} < \frac{9}{2}$, and so by part (1), $(2+3x^{-1/2})\,c(x) < \frac{9}{2}\times\frac{32}{9} = 16$.

Many of the generating functions that arise in this work have the property that their Taylor coefficients are alternately positive and negative. It will be useful to know that the class of such functions is closed under multiplication.

LEMMA 2.3. *Suppose that $A(z) = \sum(-1)^n a_n z^n$ and $B(z) = \sum(-1)^n b_n z^n$, where $a_n > 0$, $b_n > 0$. If $C(z) := A(z)\,B(z)$ then $C(z) = \sum(-1)^n c_n z^n$, where $c_n > 0$.*

For, $c_n = \sum_{s=0}^{n}(-1)^s a_s (-1)^{n-s} b_{n-s} = (-1)^n \sum_{s=0}^{n} a_s b_{n-s}$ and $\sum_{s=0}^{n} a_s b_{n-s} > 0$. We apply this, in particular, to powers of $G(x;z)$:

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

THEOREM 2.4. *For $r \geqslant 1$ let $(-1)^n g^{(r)}(n)$ be the nth coefficient in the Taylor series for $G(x;z)^r$, so that $g^{(1)}(n) = (-1)^n g(n)$ and $G(x;z)^r = \sum_0^\infty (-1)^n g^{(r)}(n) z^n$. Suppose that x is real and $x \geqslant 2$. Then*

$$0 < g^{(r)}(n) < (2+3x^{-1/2})^{r-1} c(x)^r x^{-n(n+r)/2r} < \tfrac{1}{2} 16^r x^{-n(n+r)/2r}$$

for all $n \geqslant 0$. Moreover, $g^{(r)}(n+1) < g^{(r)}(n)$ for all $n > 5r^2$.

We believe that in fact $g^{(r)}(n) < (1+kx^{-1})^r x^{-n(n+r)/2r}$, where k is some constant that is independent of r, x and n, but we have not been able to prove this.

Proof of Theorem 2.4. We use induction on r. The assertion is certainly true for $r = 1$ by Theorem 2.1 and Lemma 2.2. That $g^{(r)}(n)$ is positive comes directly from Lemma 2.3, and so the heart of the matter is to justify the upper bound. Suppose therefore that $r \geqslant 2$ and that

$$0 < g^{(r-1)}(n) < (2+3x^{-1/2})^{r-2} c(x)^{r-1} x^{-n(n+r-1)/(2(r-1))}$$

for all $n \geqslant 0$. Then

$$g^{(r)}(n) = \sum_{s=0}^{n} g^{(r-1)}(s) g^{(1)}(n-s) < (2+3x^{-1/2})^{r-2} c(x)^r \sum_{s=0}^{n} x^{-\left(\frac{s(s+r-1)}{2(r-1)} + \frac{(n-s)(n-s+1)}{2}\right)}.$$

Define

$$j_s := -\frac{n(n+r)}{2r} + \frac{s(s+r-1)}{2(r-1)} + \frac{(n-s)(n-s+1)}{2}$$

so that

$$g^{(r)}(n) < (2+3x^{-1/2})^{r-2} c(x)^r x^{-n(n+r)/2r} \sum_{s=0}^{n} x^{-j_s}$$

and

$$\begin{aligned} j_s &= \frac{r(r-1)(n-s)(n-s+1) + rs(s+r-1) - (r-1)n(n+r)}{2r(r-1)} \\ &= \frac{(r-1)^2 n^2 - 2r(r-1)sn + r^2 s^2}{2r(r-1)} \\ &= \frac{((r-1)n - rs)^2}{2r(r-1)}. \end{aligned}$$

Writing $(r-1)n$ as $ar+b$, where a, b are integers and $-\frac{1}{2}r < b \leqslant \frac{1}{2}r$, we have that $j_s = ((a-s)r+b)^2/2r(r-1)$. Substitution of t for $a-s$ then gives that

$$\sum_{s=0}^{n} x^{-j_s} < \sum_{t=-\infty}^{\infty} x^{-(rt+b)^2/(2r(r-1))}.$$

Replacement of b by $-b$ leaves the sum unaltered (as one sees by also replacing t by $-t$) and therefore we may assume that $0 \leqslant b \leqslant \frac{1}{2}r$. Then

$$\sum_{s=0}^{n} x^{-j_s} < 2 \sum_{t=0}^{\infty} x^{-(rt+b)^2/(2r(r-1))} \leqslant 2 \sum_{t=0}^{\infty} x^{-rt^2/2(r-1)} < 2 \sum_{t=0}^{\infty} x^{-t^2/2}.$$

Now $\sum_{t=0}^{\infty} x^{-t^2/2} < 1 + x^{-1/2} + \sum_{t=1}^{\infty} x^{-2t} = 1 + x^{-1/2}(1 + x^{1/2}(x^2-1)^{-1})$ and it is not hard to see that $x^{1/2}(x^2-1)^{-1} < \frac{1}{2}$ since $x \geqslant 2$. Therefore $\sum_{s=0}^{n} x^{-j_s} < 2(1+\frac{3}{2}x^{-1/2}) =$

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

$2+3x^{-1/2}$ and so $g^{(r)}(n) < (2+3x^{-1/2})^{r-1}\, c(x)^r\, x^{-n(n+r)/(2r)}$. From Lemma 2.2(4) we know that $(2+3x^{-1/2})\, c(x) < 16$, and so

$$g^{(r)}(n) < (2+3x^{-1/2})^{r-1}\, c(x)^r\, x^{-n(n+r)/2r} < \tfrac{1}{2} 16^r\, x^{-n(n+r)/2r},$$

as the first part of the theorem states.

To show that the coefficients $g^{(r)}(n)$ become monotone decreasing for $n > 5r^2$ we first need a lower bound for them. Write n as $ar-b$ where $0 < b \leqslant r$. Then $n = (a-1)\, b + a(r-b)$ and, making z^n by taking z^{a-1} from the first b factors and z^a from the remaining $r-b$ factors of $G(x;z)^r$, we find that

$$g^{(r)}(n) > c_{a-1}(x)^b\, x^{-ba(a-1)/2} c_a(x)^{r-b}\, x^{-(r-b)\, a(a+1)/2} > x^{-a(b(a-1)+(r-b)\, (a+1))/2}.$$

Now $ra(b(a-1)+(r-b)\,(a+1)) = (n+b)\,(n+r-b) = (n+\frac{1}{2}r)^2 - (b-\frac{1}{2}r)^2 \leqslant (n+\frac{1}{2}r)^2$. Therefore $g^{(r)}(n) > x^{-(n+r/2)^2/2r}$.

Using this lower bound we can compare $g^{(r)}(n+1)$ with $g^{(r)}(n)$:

$$\frac{g^{(r)}(n+1)}{g^{(r)}(n)} < \frac{\frac{1}{2} 16^r\, x^{-(n+1)\, (n+1+r)/(2r)}}{x^{-(n+r/2)^2/2r}} = K x^{-n/r},$$

where

$$K := \tfrac{1}{2} 16^r\, x^{(r^2-4r-4)/8r} < \tfrac{1}{2}(16 x^{1/8})^r < x^{5r}.$$

It follows that $g^{(r)}(n+1) < g^{(r)}(n)$ as soon as $x^{n/r} > K$, and that this is certainly true when $x^n \geqslant x^{5r^2}$. Therefore if $n \geqslant 5r^2$ then $g^{(r)}(n+1) < g^{(r)}(n)$ as required.

3. *Notation for the classical groups*

Throughout we shall use F for the field over which our groups are defined – usually $\mathbb{F}_q$, but $\mathbb{F}_{q^2}$ in the case of the unitary groups $\mathrm{U}(n,q)$. We shall use V to denote the space F^n of $1 \times n$ row vectors, on which $n \times n$ matrices act by right multiplication. Although this conflicts mildly with later usage, where V also denotes a generating function, the intended meaning will always be clear from the context. An $n \times n$ matrix is said to be *unipotent* if its characteristic polynomial is $(t-1)^n$. Where we use the term *λ-potent* (for $\lambda \in F^\times$) we refer to a matrix whose characteristic polynomial is $(t-\lambda)^n$. Note that the λ-potent matrices are precisely the matrices of the form λU, where U is unipotent; equally, they are the matrices $\lambda I + Z$ where Z is nilpotent.

By a classical group G is meant one of $\mathrm{GL}(m,q)$, $\mathrm{Sp}(2m,q)$, $\mathrm{U}(m,q)$, $\mathrm{O}^\varepsilon(2m,q)$ where $\varepsilon \in \{+,-\}$, and $\mathrm{O}(2m+1,q)$ where q is odd. The dimension n of the natural G-module V is m, $2m$, m, $2m$, or $2m+1$ accordingly. As explained in §1, however, we can ignore the odd-dimensional orthogonal groups. For $\mathrm{X} \in \{\mathrm{GL}, \mathrm{Sp}, \mathrm{U}, \mathrm{O}^+, \mathrm{O}^-\}$ define

$$v(\mathrm{X}; m, q) := |\{\text{eigenvalue-free elements of } G\}| \div |G|$$

and the generating function

$$V(X; q; z) := \sum_{m=0}^{\infty} v(\mathrm{X}; m, q)\, z^m,$$

where G is of type X and appropriate dimension over F. The eigenvalue-free elements of G may be approached by way of a connection with unipotent matrices. For X and G as above, define

$$u(\mathrm{X}; m, q) := \begin{cases} |\{\text{unipotent elements of } G\}| \div |G| & \text{if } \mathrm{X} \in \{\mathrm{GL}, \mathrm{Sp}, \mathrm{U}\}, \\ |\{\text{unipotent elements of } \mathrm{SO}^\varepsilon(V)\}| \div |G| & \text{if } \mathrm{X} = \mathrm{O}^\varepsilon, \end{cases}$$

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

and

$$U(\mathrm{X};q;z) := \sum_{m=0}^{\infty} u(\mathrm{X};m,q)\, z^m.$$

Here we are using the convention (compare Carter [**2**, p. 26] or Taylor [**13**, p. 160]) that if char $F = 2$ then $\mathrm{SO}^\varepsilon(V)$ denotes the subgroup of index 2 in $\mathrm{O}^\varepsilon(V)$ that is often denoted $\Omega^\varepsilon(V)$. We also observe the rather important convention that

$$u(\mathrm{X};0,q) := v(\mathrm{X};0,q) := \begin{cases} 1 & \text{if } \mathrm{X} \in \{\mathrm{GL}, \mathrm{Sp}, \mathrm{U}, \mathrm{O}^+\}, \\ 0 & \text{if } \mathrm{X} = \mathrm{O}^-. \end{cases}$$

Our strategy is to derive a formula that expresses $V(\mathrm{X};m,q)$ in terms of certain of the functions $U(\mathrm{X}';m',q')$, and to obtain the latter functions explicitly from a theorem of Steinberg [**11**] enumerating unipotent elements. It will turn out that these generating functions can all be expressed in terms of Euler's function $G(x;z)$.

The orthogonal groups require a variant of this strategy. Since the groups of dimension $2m$ involve orthogonal groups of both $+$ and $-$ types in smaller dimensions the generating functions for O^+ and O^- have to be combined. Therefore we define

$$u^\pm(\mathrm{O};m,q) := u(\mathrm{O}^+;m,q) \pm u(\mathrm{O}^-;m,q), \quad v^\pm(\mathrm{O};m,q) := v(\mathrm{O}^+;m,q) \pm v(\mathrm{O}^-;m,q),$$

and

$$U^+(\mathrm{O};q;z) := \sum_{0}^{\infty} u^+(\mathrm{O};m,q)\, z^m, \quad U^-(\mathrm{O};q;z) := \sum_{0}^{\infty} u^-(\mathrm{O};m,q)\, z^m,$$

$$V^+(\mathrm{O};q;z) := \sum_{0}^{\infty} v^+(\mathrm{O};m,q)\, z^m, \quad V^-(\mathrm{O};q;z) := \sum_{0}^{\infty} v^-(\mathrm{O};m,q)\, z^m.$$

For the even-dimensional orthogonal groups it is these functions U^ε, V^ε that can be expressed in terms of Euler's function.

To derive the relationship between eigenvalue-free and unipotent matrices we consider the primary decomposition of V relative to a matrix X. The characteristic polynomial $c_X(t)$ of an invertible $n \times n$ matrix X can be factorised as $f_0(t) \prod_{\lambda \in F^\times} (t-\lambda)^{n_\lambda}$, where f_0 has no zeros in F. There is a corresponding

$$\text{Primary Decomposition: } V = V_0 \oplus \bigoplus_{\lambda \in F^\times} V_\lambda,$$

where the subspaces V_0, V_λ are X-invariant, X is eigenvalue-free on V_0, and X acts as a λ-potent matrix on V_λ for $\lambda \in F^\times$.

There is a similar primary decomposition for matrices in the classical groups of types other than GL. Such a group G leaves a non-singular form on V invariant. This form is alternating bilinear for the symplectic group, hermitian for the unitary group, and symmetric bilinear for the orthogonal groups. In the symplectic and unitary cases G is the full isometry group of the pair $(V,\ )$, but in the orthogonal cases there is a quadratic form Q with polar form such that G is the isometry group of (V,Q). In the unitary case, where is hermitian, we write $X \mapsto \bar{X}$ for the map

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

induced by the automorphism $x \mapsto x^q$ of $\mathbb{F}_{q^2}$. Now if A is the matrix of (with respect to some basis of V) then $X \in G$ if and only if $XAX^{\mathrm{tr}} = A$ in the bilinear cases and $XA\bar{X}^{\mathrm{tr}} = A$ when is hermitian. Define

$$X^* := \begin{cases} (X^{\mathrm{tr}})^{-1} & \text{if } \text{ is bilinear,} \\ (\bar{X}^{\mathrm{tr}})^{-1} & \text{if } \text{ is hermitian.} \end{cases}$$

Since A is non-singular the matrices X and X^* are similar. Now for $\lambda \in F^\times$ define

$$\lambda^* := \begin{cases} \lambda^{-1} & \text{in the symplectic and orthogonal cases,} \\ \lambda^{-q} & \text{in the unitary case.} \end{cases}$$

Then define $\Theta := \{\theta \in F^\times \mid \theta = \theta^*\}$ and let Ψ be a set of representatives, one from each pair $\{\lambda, \lambda^*\}$ of members of $F^\times \setminus \Theta$. Since X, X^* are similar they have the same characteristic polynomials, and it follows that the characteristic polynomial $c_X(t)$ has a factorisation of the form:

$$c_X(t) = f_0(t) \prod_{\theta \in \Theta} (t-\theta)^{n_\theta} \prod_{\psi \in \Psi} ((t-\psi)(t-\psi^*))^{m_\psi}$$

where $f_0(t)$ has no zeros in F. Correspondingly the vector space V splits uniquely as an orthogonal direct sum

$$\text{Primary Decomposition: } V = V_0 \oplus^\perp \bigoplus_{\theta \in \Theta}{}^\perp V_\theta \oplus^\perp \bigoplus_{\psi \in \Psi}{}^\perp V_\psi$$

of X-invariant subspaces on which the restrictions of X have characteristic polynomials

$$f_0(t), \quad (t-\theta)^{n_\theta}, \quad ((t-\psi)(t-\psi^*))^{m_\psi},$$

respectively. Since they are pairwise orthogonal, the spaces V_0, V_θ, V_ψ have to be non-singular relative to our standard form . Moreover, there are uniquely determined X-invariant subspaces W_ψ, W_ψ^* of V_ψ on which the characteristic polynomials of X are $(t-\psi)^{m_\psi}$ and $(t-\psi^*)^{m_\psi}$ respectively. Then $V_\psi = W_\psi \oplus W_\psi^*$ (a non-orthogonal direct sum), the spaces W_ψ, W_ψ^* are totally isotropic and, given a basis for W_ψ, there is a dual basis for W_ψ^* such that, if the matrix of X restricted to W_ψ is X_ψ, then the matrix of X restricted to W_ψ^* is X_ψ^*. Conversely, suppose we are given:

(i) a family $\mathbf{n}$ of non-negative integers n_0, n_θ, m_ψ such that $n_0 + \sum_\Theta n_\theta + \sum_\Psi 2m_\psi = n$ (that is, an ordered partition of n into $1 + |\Theta| + |\Psi|$ non-negative parts), with the restriction on n_0 and n_θ that vector spaces of these dimensions can support non-singular forms of the requisite kind;

(ii) a decomposition of V as an orthogonal direct sum $V_0 \oplus^\perp \bigoplus_{\theta \in \Theta}^\perp V_\theta \oplus^\perp \bigoplus_{\psi \in \Psi}^\perp V_\psi$, of non-singular subspaces of the appropriate dimensions;

(iii) for each $\psi \in \Psi$ a decomposition of V_ψ as a vector-space direct sum $W_\psi \oplus W_\psi^*$ of totally isotropic subspaces of dimension m_ψ;

(iv) an eigenvalue-free isometry X_0 of V_0;

(v) unipotent isometries X_θ of V_θ (for all $\theta \in \Theta$); and

(vi) invertible linear transformations X_ψ of W_ψ (for all $\psi \in \Psi$).

Then the direct sum $X_0 \oplus \bigoplus_{\theta \in \Theta} \theta X_\theta \oplus \bigoplus_{\psi \in \Psi} (\psi X_\psi \oplus (\psi X_\psi)^*)$ belongs to G. We shall refer to the partition $\mathbf{n}$ of n as the *dimension partition* of the direct sum decomposition. To prove our theorems we shall count the elements of G according to dimension partitions and primary decompositions.

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

4. *The general linear groups*

The relationship between the proportions of unipotent and eigenvalue-free elements in $\mathrm{GL}(m,q)$ may be expressed by the following connection between the generating functions $U(\mathrm{GL};q;z)$ and $V(\mathrm{GL};q;z)$.

THEOREM 4.1. $V(\mathrm{GL};q;z)\,U(\mathrm{GL};q;z)^{q-1} = (1-z)^{-1}$.

Proof. We count the elements of $\mathrm{GL}(n,q)$ according to their primary decomposition. For a given (ordered) partition $\sum_{\lambda\in F} n_\lambda$ of n, the number of decompositions $V = \bigoplus_{\lambda\in F} V_\lambda$ in which $\dim V_\lambda = n_\lambda$ is $|\mathrm{GL}(n,q)| \div \prod |\mathrm{GL}(n_\lambda,q)|$. Also, the number of eigenvalue-free $n_0\times n_0$ matrices is $v(\mathrm{GL};n_0,q)\,|\mathrm{GL}(n_0,q)|$ and the number of λ-potent $n_\lambda\times n_\lambda$ matrices is the same as the number of $n_\lambda\times n_\lambda$ unipotent matrices, which is $u(\mathrm{GL};n_\lambda,q)\,|\mathrm{GL}(n_\lambda,q)|$. Conducting a census of $\mathrm{GL}(n,q)$ we therefore find that

$$|\mathrm{GL}(n,q)| = \sum_{\mathbf{n}} \frac{|\mathrm{GL}(n,q)|}{\prod_{\lambda\in F}|\mathrm{GL}(n_\lambda,q)|}\,(v(\mathrm{GL};n_0,q)\,|\mathrm{GL}(n_0,q)|)\prod_{\lambda\in F^\times}(u(\mathrm{GL};n_\lambda,q)\,|\mathrm{GL}(n_\lambda,q)|),$$

where the sum is over appropriate partitions $\mathbf{n}$ of n. This leads immediately to the following fundamental recurrence relation:

$$\sum_{\mathbf{n}}\left(v(\mathrm{GL};n_0,q)\prod_{\lambda\in F^\times} u(\mathrm{GL};n_\lambda,q)\right) = 1 \quad \text{for } n\geqslant 0$$

(recall that $u(\mathrm{GL};0,q) = v(\mathrm{GL};0,q) = 1$). Multiplying both sides of the equation by z^n and summing, we get that $V(\mathrm{GL};q;z)\,U(\mathrm{GL};q;z)^{q-1} = (1-z)^{-1}$, as the theorem states.

THEOREM 4.2. $U(\mathrm{GL};q;z) = G(q;z)^{-1}$.

Proof. By a theorem of Fine and Herstein [**6**] (see also [**11**, Theorem 15.1]), the number of nilpotent $n\times n$ matrices over F is q^{n^2-n}; consequently the number of unipotent matrices in $\mathrm{GL}(n,q)$ is q^{n^2-n} also. Therefore

$$u(\mathrm{GL};n,q) = q^{n^2-n}\,|\mathrm{GL}(n,q)|^{-1} = q^{n^2-n}\prod_{i=0}^{n-1}(q^n-q^i)^{-1} = q^{-n}\prod_{j=1}^{n}(1-q^{-j})^{-1} = q^{-n}c_n(q),$$

and so by Theorem 2.1(2), $U(q;z) = G(q;z)^{-1}$.

THEOREM 4.3. *Defining* $v(\mathrm{GL};\infty,q) := \lim_{n\to\infty} v(\mathrm{GL};n,q)$ *we have that* $v(\mathrm{GL};\infty,q) = G(q;1)^{q-1}$. *Moreover,* $v(\mathrm{GL};\infty,q) - v(\mathrm{GL};n,q) = (-1)^{n+1}\varepsilon_n$, *where*

$$0 < \varepsilon_n < \tfrac{1}{2}16^{q-1}q^{-(n+1)(n+q)/(2(q-1))}$$

whenever $n > 5(q-1)^2$.

Proof. By the previous results, $V(\mathrm{GL};q;z) = (1-z)^{-1}G(q;z)^{q-1}$. Therefore $v(\mathrm{GL};n,q) = \sum_{i=0}^{n}(-1)^i g^{(q-1)}(i)$, where $(-1)^i g^{(q-1)}(i)$ is, as in §2, the ith Taylor coefficient of $G(q;z)^{q-1}$. Now $G(q,1)^{q-1} = \sum_{i=0}^{\infty}(-1)^i g^{(q-1)}(i)$ and therefore

$$v(\mathrm{GL};n,q)\to G(q,1)^{q-1} \quad \text{as} \quad n\to\infty.$$

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

Moreover, since the terms of the series alternate in sign, and since by the last part of Theorem 2.4, when $n > 5(q-1)^2$ they decrease monotonically in absolute value, $v(\mathrm{GL}; n, q) = G(q;1)^{q-1} + (-1)^{n+1}\varepsilon_n$, where $0 < \varepsilon_n < g^{(q-1)}(n+1)$ for sufficiently large n. The given estimate therefore comes from Theorem 2.4.

THEOREM 4.4. $G(q;1)^{q-1} = \mathrm{e}^{-1}(1 - \frac{1}{2}q^{-1} + \frac{7}{24}q^{-2} - \frac{25}{48}q^{-3} + O(q^{-4}))$.

Proof. From the definition of $G(q;z)$ we have that $G(q;1)^{q-1} = \prod_{i=1}^{\infty}(1-q^{-i})^{q-1}$. Take logarithms and reorganise:

$$\begin{aligned}
\log G(q;1)^{q-1} &= (q-1)\sum_{i=1}^{\infty}\log(1-q^{-i}) \\
&= -(q-1)\sum_{i=1}^{\infty}\sum_{j=1}^{\infty}\frac{q^{-ij}}{j} \\
&= -(q-1)\sum_{i=1}^{\infty}q^{-i} - (q-1)\sum_{i=1}^{\infty}\sum_{j=2}^{\infty}\frac{q^{-ij}}{j} \\
&= -1 - (q-1)\sum_{k=2}^{\infty}\left(\sum_{j\geqslant 2;\, j|k}\frac{1}{j}\right)q^{-k}.
\end{aligned}$$

Now

$$\begin{aligned}
(q-1)\sum_{k=2}^{\infty}\left(\sum_{j\geqslant 2;\, j|k}\frac{1}{j}\right)q^{-k} &= (q-1)\left(\frac{1}{2q^2} + \frac{1}{3q^3} + \frac{3}{4q^4} + O(q^{-5})\right) \\
&= \tfrac{1}{2}q^{-1} - \tfrac{1}{6}q^{-2} + \tfrac{5}{12}q^{-3} + O(q^{-4}),
\end{aligned}$$

and so

$$\begin{aligned}
G(q;1)^{q-1} &= \mathrm{e}^{-1}\exp(-\tfrac{1}{2}q^{-1} + \tfrac{1}{6}q^{-2} - \tfrac{5}{12}q^{-3} + O(q^{-4})) \\
&= \mathrm{e}^{-1}(1 - \tfrac{1}{2}q^{-1} + \tfrac{7}{24}q^{-2} - \tfrac{25}{48}q^{-3} + O(q^{-4})),
\end{aligned}$$

as the theorem states.

Theorems 4.3 and 4.4 lead directly to the proportion $v(\mathrm{M}; n, q)$ of eigenvalue-free matrices in $\mathrm{M}(n,q)$. Any element of $\mathrm{M}(n,q)$ outside of $\mathrm{GL}(n,q)$ is certainly not eigenvalue-free because it has 0 as an eigenvalue. Therefore, as was pointed out in §1,

$$v(\mathrm{M}; n, q) = \frac{v(\mathrm{GL}; n, q)\,|\mathrm{GL}(n,q)|}{|\mathrm{M}(n,q)|} = v(\mathrm{GL}; n, q)\prod_{i=1}^{n}(1-q^{-i})$$

and we deduce the following:

THEOREM 4.5. *If* $v(\mathrm{M}; \infty, q) := \lim_{n\to\infty} v(\mathrm{M}; n, q)$ *then*

$$v(\mathrm{M}; \infty, q) = G(q;1)^q = \mathrm{e}^{-1}(1 - \tfrac{3}{2}q^{-1} - \tfrac{5}{24}q^{-2} - \tfrac{5}{16}q^{-3} - O(q^{-4})).$$

Moreover, $0 < (-1)^{n+1}(v(\mathrm{M}; \infty, q) - v(\mathrm{M}; n, q)) < \frac{1}{2}16^{q-1}q^{-(n+1)(n+q)/(2(q-1))}$.

REMARK 4.6. We commented in §1 that the behaviour of $v(\mathrm{M}; n, q)$ is similar to that of $p_n(q)$, the probability that a randomly chosen monic polynomial of degree n over F should have no zeros. The fact that $p_n(q) = (1-q^{-1})^q$ if $n \geqslant q$ is an expression of the fact that for $\lambda \in F$ the events 'λ is not a root of $f(t)$' are truly independent. Our first heuristic argument for the fact that $v(\mathrm{M}; n, q)$ should be close to e^{-1} required that the events 'λ is not an eigenvalue of a random $n \times n$ matrix X' should be independent,

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

or nearly so. If these events were genuinely independent then $v(\mathrm{M};n,q)$ would be $\prod_{i=1}^{n}(1-q^{-i})^q$ for all $n \geqslant q$. But then $v(\mathrm{M};n,q)$ would converge monotonically to $v(\mathrm{M};\infty,q)$ as $n \to \infty$, which it does not. We conclude that in fact, as one would expect, they are not independent. On the other hand, the fact that

$$|v(\mathrm{M};\infty,q)-v(\mathrm{M};n,q)| = O(q^{-(n+1)\,(n+q)/(2(q-1))}),$$

which is very small for large n, is an indication that these events are very close to being independent.

5. *The symplectic groups*

Recall that for the symplectic groups the dimension n must be even, and we define $m := \frac{1}{2}n$. Also, $\Theta = \{\pm 1\}$ and $|\Psi| = \frac{1}{2}(q-3)$ if q is odd; $\Theta = \{1\}$, $|\Psi| = \frac{1}{2}(q-2)$ if q is even. Corresponding to Theorem 4.1 we have:

THEOREM 5.1.

$$V(\mathrm{Sp};q;z) = \begin{cases} (1-z)^{-1}\,U(\mathrm{Sp};q;z)^{-2}\,U(\mathrm{GL};q;z)^{-(q-3)/2} & \text{if } q \text{ is odd,} \\ (1-z)^{-1}\,U(\mathrm{Sp};q;z)^{-1}\,U(\mathrm{GL};q;z)^{-(q-2)/2} & \text{if } q \text{ is even.} \end{cases}$$

Proof. In the primary decomposition of V corresponding to a symplectic transformation the spaces V_0, V_θ, being non-singular, must have even dimensions $2m_0$, $2m_\theta$. Let $\mathbf{m}$ be a partition of m into non-negative parts indexed by $\{0\} \cup \Theta \cup \Psi$, and let $\mathbf{n}$ be the family $\{2m_0, (2m_\theta)_{\theta\in\Theta}, (m_\psi)_{\psi\in\Psi}\}$. The symplectic group $\mathrm{Sp}(2m,q)$ is transitive on the set of decompositions

$$V = V_0 \oplus^{\perp} \bigoplus_{\theta\in\Theta}{}^{\perp} V_\theta \oplus^{\perp} \bigoplus_{\psi\in\Psi}{}^{\perp} (W_\psi \oplus W_\psi^*)$$

with dimension partition $\mathbf{n}$, and the stabiliser of one of them is a direct product $\mathrm{Sp}(2m_0,q) \times \prod_\theta \mathrm{Sp}(2m_\theta,q) \times \prod_\psi \mathrm{GL}(m_\psi,q)$. Conducting a census we therefore find that

$$\begin{aligned} |\mathrm{Sp}(2m,q)| = \sum_{\mathbf{m}} & \frac{|\mathrm{Sp}(2m,q)|}{|\mathrm{Sp}(2m_0,q)| \prod |\mathrm{Sp}(2m_\theta,q)| \prod |\mathrm{GL}(m_\psi,q)|} \\ & \times v(\mathrm{Sp};m_0,q)\,|\mathrm{Sp}(2m_0,q)| \times \prod_{\theta\in\Theta} u(\mathrm{Sp};m_\theta,q)\,|\mathrm{Sp}(2m_\theta,q)| \\ & \times \prod_{\psi\in\Psi} u(\mathrm{GL};m_\psi,q)\,|\mathrm{GL}(m_\psi,q)| \end{aligned}$$

for $m \geqslant 1$ (recall that $u(\mathrm{Sp};0,q) = v(\mathrm{Sp};0,q) = u(\mathrm{GL};0,q) = 1$). The orders of the various groups cancel and so

$$1 = \sum_{\mathbf{m}} v(\mathrm{Sp};m_0,q) \prod_{\theta\in\Theta} u(\mathrm{Sp};m_\theta,q) \prod_{\psi\in\Psi} u(\mathrm{GL};m_\psi,q).$$

This equation holds for $m \geqslant 0$, so, multiplying by z^m and summing over m we find that

$$(1-z)^{-1} = V(\mathrm{Sp};q;z)\,U(\mathrm{Sp};q;z)^{|\Theta|}\,U(\mathrm{GL};q;z)^{|\Psi|}.$$

Since $|\Theta| = 2$ and $|\Psi| = \frac{1}{2}(q-3)$ if q is odd, while $|\Theta| = 1$, $|\Psi| = \frac{1}{2}(q-2)$ if q is even, we have the required formula.

THEOREM 5.2. $U(\mathrm{Sp};q;z) = G(q^2;qz)^{-1}$.

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

Proof. We have $|\mathrm{Sp}(2m,q)| = q^{m^2}\prod_{i=1}^{m}(q^{2i}-1)$ and, by a theorem of Steinberg (see [**11**, Theorem 15.1] or Carter [**2**, Theorem 6.6.1])

$$u(\mathrm{Sp};m,q)\,|\mathrm{Sp}(2m,q)| = |\{\text{unipotent members of } \mathrm{Sp}(2m,q)\}| = q^{2m^2}.$$

Therefore

$$U(\mathrm{Sp};q;z) = \sum_{m=0}^{\infty}\frac{q^{2m^2}}{q^{m(2m+1)}\prod_1^m(1-q^{-2i})}z^m = \sum_{m=0}^{\infty}c_m(q^2)\,(z/q)^m$$

and this is $G(q^2;qz)^{-1}$ by Theorem 2.1(2).

THEOREM 5.3. *Define* $v(\mathrm{Sp};\infty,q) := \lim_{m\to\infty} v(\mathrm{Sp};m,q)$. *Then*

$$v(\mathrm{Sp};\infty,q) = \begin{cases} G(q^2;q)^2\,G(q;1)^{(q-3)/2} & \text{when } q \text{ is odd,}\\ G(q^2;q)\,G(q;1)^{(q-2)/2} & \text{when } q \text{ is even.}\end{cases}$$

Moreover, $|v(\mathrm{Sp};\infty,q)-v(\mathrm{Sp};m,q)| < \frac{1}{3}4^q q^{-(m+1)^2/(q-1)}$ *if* $m \geqslant q-2$.

Proof. Suppose that q is odd: the calculations for even values of q are similar (but a little easier) and will be omitted. From Theorems 5.1, 5.2 and 4.2 we have that $V(\mathrm{Sp};q;z) = (1-z)^{-1}\,G(q^2;qz)^2\,G(q;z)^{(q-3)/2}$. Lemma 2.3 tells us that

$$G(q^2;qz)^2\,G(q;z)^{(q-3)/2} = \sum_{0}^{\infty}(-1)^m a_m z^m$$

where $a_m > 0$. Also, adapting the notation of Theorem 2.4 a little, we can write

$$G(q^2;qz)^2 = \sum_{0}^{\infty}(-1)^m g_{q^2}^{(2)}(m)\,q^m z^m, \quad G(q;z)^{(q-3)/2} = \sum_{0}^{\infty}(-1)^m g_q^{(q-3)/2}(m)\,z^m,$$

where, by that theorem,

$$g_{q^2}^{(2)}(m)\,q^m < (2+3q^{-1})\,c(q^2)^2\,q^{-m^2/2}$$

and (if $q \geqslant 5$)

$$g_q^{(q-3)/2}(m) < (2+3q^{-1/2})^{(q-5)/2}\,c(q)^{(q-3)/2}\,q^{-m(m+(q-3)/2)/(q-3)}.$$

Since $q^{-s^2/2} \leqslant q^{m/2}q^{-s(s+1)/2}$ whenever $0 \leqslant s \leqslant m$, the calculation which provided the inductive step from $r = \frac{1}{2}(q-3)$ to $r = \frac{1}{2}(q-1)$ in the proof of Theorem 2.4 yields that

$$a_m < (2+3q^{-1})\,(2+3q^{-1/2})^{(q-3)/2}\,c(q^2)^2\,c(q)^{(q-3)/2}\,q^{m/2}\,q^{-m(m+(q-1)/2)/(q-1)}.$$

Clearly $2+3q^{-1} < 2+3q^{-1/2}$; also $c(q^2)^2 < c(q)$ by Lemma 2.2(3). It follows that

$$a_m < (2+3q^{-1/2})^{(q-1)/2}\,c(q)^{(q-1)/2}\,q^{-m^2/(q-1)} < 4^{q-1}q^{-m^2/(q-1)}$$

by Lemma 2.2(4). Now $V(\mathrm{Sp};q;z) = (1-z)^{-1}\sum(-1)^m a_m z^m$. Therefore $v(\mathrm{Sp};m,q) = \sum_{i=0}^{m}(-1)^i a_i$ and

$$v(\mathrm{Sp};\infty,q) = \sum_{i=0}^{\infty}(-1)^i a_i = G(q^2;q)^2\,G(q;1)^{(q-3)/2}.$$

Moreover,

$$|v(\mathrm{Sp};\infty,q)-v(\mathrm{Sp};m,q)| < \sum_{i=m+1}^{\infty}a_i < \sum_{i=m+1}^{\infty}4^{q-1}q^{-i^2/(q-1)}.$$

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

Now $\sum_{m+1}^{\infty} q^{-i^2/(q-1)} < q^{-(m+1)^2/(q-1)} \sum_{j=0}^{\infty} q^{-2j(m+1)/(q-1)}$ and so if $m+1 \geqslant q-1$ then

$$\sum_{m+1}^{\infty} q^{-i^2/(q-1)} < (q^2/(q^2-1))\, q^{-(m+1)^2/(q-1)} \leqslant \tfrac{4}{3} q^{-(m+1)^2/(q-1)}.$$

Therefore $|v(\mathrm{Sp}; \infty, q) - v(\mathrm{Sp}; m, q)| < \frac{1}{3} 4^q q^{-(m+1)^2/(q-1)}$ if $m \geqslant q-2$, as the theorem states.

We have not checked that $a_m > a_{m+1}$ for all sufficiently large m though we believe this to be true. This would mean that from some point on $v(\mathrm{Sp}; m, q)$ differs from $v(\mathrm{Sp}; \infty, q)$ by less than a_{m+1}.

THEOREM 5.4.

$$v(\mathrm{Sp}; \infty, q) = \begin{cases} \mathrm{e}^{-1/2}(1 - \frac{5}{4}q^{-1} + \frac{131}{96}q^{-2} - \frac{997}{384}q^{-3} + O(q^{-4})) & \textit{when } q \textit{ is odd}, \\ \mathrm{e}^{-1/2}(1 - \frac{3}{4}q^{-1} + \frac{59}{96}q^{-2} - \frac{459}{384}q^{-3} + O(q^{-4})) & \textit{when } q \textit{ is even}. \end{cases}$$

Proof. This may be proved by the method used for Theorem 4.4. Alternatively, it can be derived from that theorem by the following calculation. Again, we deal only with the case where q is odd. By Theorem 5.3, in this case $v(\mathrm{Sp}; \infty, q) = G(q^2; q)^2 G(q; 1)^{(q-3)/2}$. Squaring:

$$\begin{aligned} (G(q^2; q)^2\, G(q; 1)^{(q-3)/2})^2 &= G(q; 1)^{q-1} \prod_1^{\infty} (1 - q^{-(2i-1)})^4 \prod_1^{\infty} (1 - q^{-i})^{-2} \\ &= G(q; 1)^{q-1} (1 - q^{-1})^2 (1 - q^{-2})^{-2} (1 - q^{-3})^2 (1 - O(q^{-4})) \\ &= G(q; 1)^{q-1} (1 - 2q^{-1} + 3q^{-2} - 6q^{-3} + O(q^{-4})). \end{aligned}$$

By Theorem 4.4 therefore

$$\begin{aligned} &(G(q^2; q)^2\, G(q; 1)^{(q-3)/2})^2 \\ &\quad = \mathrm{e}^{-1}(1 - \tfrac{1}{2}q^{-1} + \tfrac{7}{24}q^{-2} - \tfrac{25}{48}q^{-3} + O(q^{-4}))\,(1 - 2q^{-1} + 3q^{-2} - 6q^{-3} + O(q^{-4})) \\ &\quad = \mathrm{e}^{-1}(1 - \tfrac{5}{2}q^{-1} + \tfrac{103}{24}q^{-2} - \tfrac{413}{48}q^{-3} + O(q^{-4})). \end{aligned}$$

By the Binomial Theorem, $(1-z)^{1/2} = 1 - \frac{1}{2}z - \frac{1}{8}z^2 - \frac{1}{16}z^3 + O(z^4)$, and so

$$\begin{aligned} v(\mathrm{Sp}; \infty, q) &= G(q^2; q)^2\, G(q; 1)^{(q-3)/2} \quad \text{(when } q \text{ is odd)} \\ &= \mathrm{e}^{-1/2}(1 - \tfrac{5}{2}q^{-1} + \tfrac{103}{24}q^{-2} - \tfrac{413}{48}q^{-3} + O(q^{-4}))^{1/2} \\ &= \mathrm{e}^{-1/2}(1 - \tfrac{5}{4}q^{-1} + \tfrac{131}{96}q^{-2} - \tfrac{997}{384}q^{-3} + O(q^{-4})), \end{aligned}$$

as the theorem states (for odd values of q). The proof when q is even can be arranged in a similar way.

6. *The unitary groups*

The unitary group $\mathrm{U}(n, q)$ is a subgroup of $\mathrm{GL}(n, F)$ where the field F is now $\mathbb{F}_{q^2}$. In this case $\Theta = \{\theta \in F^\times \mid \theta^{q+1} = 1\}$ and so $|\Theta| = q+1$ since $F^\times$ is a cyclic group of order q^2-1. Therefore $|\Psi| = \frac{1}{2}(q^2 - q - 2)$.

THEOREM 6.1. $V(\mathrm{U}; q; z) = (1-z)^{-1}\, U(\mathrm{U}; q; z)^{-(q+1)}\, U(\mathrm{GL}; q^2; z)^{-(q^2-q-2)/2}$.

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

The proof is similar to that for the symplectic groups and we leave the details to the reader.

THEOREM 6.2. $U(\mathrm{U};q;z) = G(-q;-z)^{-1}$.

Proof. Since $|\mathrm{U}(n,q)| = q^{n(n-1)/2}\prod_{i=1}^{n}(q^i-(-1)^i)$ and since from Steinberg's theorem we have that $u(\mathrm{U};n,q)\,|\mathrm{U}(n,q)| = q^{n(n-1)}$,

$$U(\mathrm{U};q;z) = \sum_{n=0}^{\infty} \frac{q^{n(n-1)}}{q^{n^2}\prod_1^n(1-(-1)^i q^{-i})} z^n = \sum_{n=0}^{\infty} ((-q)^{-n}\, c_n(-q))\,(-z)^n.$$

Thus $U(\mathrm{U};q,z) = G(-q;-z)^{-1}$ by Theorem 2.1(2).

THEOREM 6.3. *If* $v(\mathrm{U};\infty,q) := \lim_{n\to\infty} v(\mathrm{U};n,q)$ *then*

$$v(\mathrm{U};\infty,q) = G(-q;-1)^{q+1}\, G(q^2;1)^{(q^2-q-2)/2}.$$

Moreover,

$$|v(\mathrm{U};\infty,q) - v(\mathrm{U};n,q)| < 4^{q^2+q+1} q^{-n(4n+q^2+3q+2)/2(q^2+3q+2)}$$

for all $n > q^2$.

Proof. It follows from Theorems 6.1, 6.2 and 4.2 that

$$V(\mathrm{U};q;z) = (1-z)^{-1}\, G(-q;-z)^{q+1}\, G(q^2;z)^{(q^2-q-2)/2}$$

and therefore that $v(\mathrm{U};\infty,q) = G(-q;-1)^{q+1}\, G(q^2;1)^{(q^2-q-2)/2}$ (the argument is the same as for the GL and Sp cases).

To find the rate of convergence of $v(\mathrm{U};n,q)$ to $G(-q;-1)^{q+1}\, G(q^2;1)^{(q^2-q-2)/2}$ we proceed as follows. Although the coefficients $(-1)^{n(n+3)/2}\, c_n(-q)\, q^{-n(n+1)/2} z^n$ of the power series for $G(-q;-z)$ do not alternate in sign we can nevertheless apply the argument that proved Theorem 2.4. For, certainly $0 < c_n(-q) < c_n(q)$ and so, applying that argument to the absolute values of the coefficients, we find that if $G(-q;-z)^{q+1} = \sum_0^\infty b_n z^n$ then

$$|b_n| < (2+3q^{-1/2})^q\, c(q)^{q+1}\, q^{-n(n+q+1)/(2(q+1))}.$$

By Theorem 2.4 itself we have that $G(q^2;z)^{(q^2-q-2)/2} = \sum b'_n z^n$ where

$$|b'_n| < (2+3q^{-1})^{(q^2-q-4)/2}\, c(q^2)^{(q^2-q-2)/2}\, q^{-2\frac{n(n+(q^2-q-2)/2)}{q^2-q-2}}.$$

Therefore $G(-q;-z)^{q+1}\, G(q^2,z)^{(q^2-q-2)/2} = \sum_0^\infty a_n z^n$, where

$$|a_n| < (2+3q^{-1/2})^q\, c(q)^{q+1}\, (2+3q^{-1})^{(q^2-q-4)/2}\, c(q^2)^{(q^2-q-2)/2} \times \sum_{s=0}^{n} q^{-\frac{s(s+q+1)}{2(q+1)} - 2\frac{(n-s)(n-s+(q^2-q-2)/2)}{q^2-q-2}}.$$

The first part of the upper bound for $|a_n|$ can be treated as follows: since $2+3q^{-1} < 2+3q^{-1/2}$ and $c(q^2) < c(q)$, and since $(2+3q^{-1/2})\, c(q) < 16$ by Lemma 2.2(4), we have that

$$\begin{aligned}(2+3q^{-1/2})^q\, c(q)^{q+1}\, (2+3q^{-1})^{(q^2-q-4)/2}\, c(q^2)^{(q^2-q-2)/2} &< (2+3q^{-1/2})^{(q^2+q+4)/2}\, c(q)^{(q^2+q)/2} \\ &< 4^{q^2+q}(2+3q^{-1/2})^{-2} \\ &< 4^{q^2+q-1}.\end{aligned}$$

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

To treat the second part, that is the sum, since

$$\begin{aligned}\frac{s(s+q+1)}{2(q+1)}+\frac{2(n-s)\,(n-s+\frac{1}{2}(q^2-q-2))}{q^2-q-2}&\\ =\frac{(q-2)\,s(s+q+1)+4(n-s)\,(n-s+\frac{1}{2}(q^2-q-2))}{2(q+1)\,(q-2)}&\\ =\frac{q+2}{2(q+1)\,(q-2)}\left(s-\frac{4n}{q+2}\right)^2+\frac{n(4n+(q+1)\,(q+2))}{2(q+1)\,(q+2)}+\tfrac{1}{2}(n-s)&\\ >\frac{n(4n+(q+1)\,(q+2))}{2(q+1)\,(q+2)}+\tfrac{1}{2}(n-s),&\end{aligned}$$

we have that

$$\begin{aligned}\sum_{s=0}^{n} q^{-\frac{s(s+q+1)}{2(q+1)}-2\frac{(n-s)\,(n-s+(q^2-q-2)/2)}{q^2-q-2}}&<q^{-\frac{n(4n+(q+1)\,(q+2))}{2(q+1)\,(q+2)}}\sum_{s=0}^{n} q^{-(n-s)/2}\\ &<q^{-\frac{n(4n+(q+1)\,(q+2))}{2(q+1)\,(q+2)}}\times\frac{q^{1/2}}{q^{1/2}-1}.\end{aligned}$$

Therefore

$$|a_n|<\frac{q^{1/2}}{q^{1/2}-1}4^{q^2+q-1}\,q^{-\frac{n(4n+(q+1)\,(q+2))}{2(q+1)\,(q+2)}}<4^{q^2+q}q^{-\frac{n(4n+(q+1)\,(q+2))}{2(q+1)\,(q+2)}}.$$

It follows that $\sum_{n+1}^{\infty}|a_i|<4|a_{n+1}|$ as soon as n is large enough ($n>q^2$ certainly suffices) and therefore that

$$|v\,(\mathrm{U};\infty,q)-v\,(\mathrm{U};n,q)|<4^{q^2+q+1}q^{-\frac{n(4n+q^2+3q+2)}{2(q^2+3q+2)}}$$

for all $n>q^2$.

Although, as we have already observed, the coefficients of the power series for $G(-q;-z)$ do not alternate in sign, it is a curious fact that those for $G(-q;-z)^{q+1}G(q^2;z)^{-(q^2-q-2)/2}$ do if $q\geqslant 4$. For, $G(-q;-z)=\prod_1^{\infty}(1-(-1)^{i-1}q^{-i}z)$ and $G(q^2;z)=\prod_1^{\infty}(1-q^{-2i}z)$. Therefore

$$G(-q;-z)\,G(q^2;z)=\prod_1^{\infty}(1-q^{-2j+1}z)\prod_1^{\infty}(1-q^{-4i}z^2)=G(q^2;qz)\,G(q^4;z^2)$$

and so

$$G(-q;-z)^{q+1}\,G(q^2;z)^{-(q^2-q-2)/2}=G(q^2;qz)^{q+1}\,G(q^4;z^2)^{q+1}\,G(q^2;z)^{(q^2-3q-4)/2}.$$

Therefore, by Theorem 2.1 and Lemma 2.3, if $q\geqslant 4$ then the series for $v(\mathrm{U};\infty,q)$ is an alternating series.

THEOREM 6.4. $v(\mathrm{U};\infty,q)=\mathrm{e}^{-3/2}(1-\frac{7}{12}q^{-2}-\frac{1}{3}q^{-3}+O(q^{-4}))$.

Proof. Since $v(\mathrm{U};\infty,q)=G(-q;-1)^{q+1}\,G(q^2;1)^{(q^2-q-2)/2}$, taking logarithms we have that

$$\begin{aligned}\log v(\mathrm{U};\infty,q)&=(q+1)\log G(-q;-1)+\tfrac{1}{2}(q^2-q-2)\log G(q^2;1)\\ &=(q+1)\sum_{i=1}^{\infty}\log(1-(-1)^{i-1}q^{-i})+\tfrac{1}{2}(q^2-q-2)\sum_{i=1}^{\infty}\log(1-q^{-2i}).\end{aligned}$$

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

Expand the logarithmic summands as $-\sum_{j=1}^{\infty}(-1)^{(i-1)j}j^{-1}q^{-ij}$ and $-\sum_{j=1}^{\infty}j^{-1}q^{-2ij}$ respectively. Then

$$\begin{aligned}\log v(\mathrm{U};\infty,q) &= -(q+1)\sum_{i=1}^{\infty}(-1)^{i-1}q^{-i} + -\tfrac{1}{2}(q^2-q-2)\sum_{i=1}^{\infty}q^{-2i} - E\\ &= -1-\frac{q^2-q-2}{2(q^2-1)} - E\\ &= -\tfrac{3}{2}+\frac{1}{2(q-1)} - E,\end{aligned}$$

where

$$E := (q+1)\sum_{i=1}^{\infty}\sum_{j=2}^{\infty}(-1)^{(i-1)j}j^{-1}q^{-ij} + \tfrac{1}{2}(q^2-q-2)\sum_{i=1}^{\infty}\sum_{j=2}^{\infty}j^{-1}q^{-2ij}.$$

Modulo q^{-4} we find that

$$\begin{aligned}E &= (q+1)(\tfrac{1}{2}q^{-2}+\tfrac{1}{3}q^{-3}+\tfrac{3}{4}q^{-4}+O(q^{-5}))+\tfrac{1}{2}(q^2-q-2)(\tfrac{1}{2}q^{-4}+O(q^{-6}))\\ &= \tfrac{1}{2}q^{-1}+\tfrac{13}{12}q^{-2}+\tfrac{5}{6}q^{-3}+O(q^{-4}),\end{aligned}$$

and so

$$\begin{aligned}\log v(\mathrm{U};\infty,q) &= -\tfrac{3}{2}+\tfrac{1}{2}(q^{-1}+q^{-2}+q^{-3}+O(q^{-4}))-(\tfrac{1}{2}q^{-1}+\tfrac{13}{12}q^{-2}+\tfrac{5}{6}q^{-3}+O(q^{-4}))\\ &= -\tfrac{3}{2}-\tfrac{7}{12}q^{-2}-\tfrac{1}{3}q^{-3}+O(q^{-4}).\end{aligned}$$

Consequently

$$\begin{aligned}v(\mathrm{U};\infty,q) &= \mathrm{e}^{-3/2}\exp(-\tfrac{7}{12}q^{-2}-\tfrac{1}{3}q^{-3}+O(q^{-4}))\\ &= \mathrm{e}^{-3/2}(1-\tfrac{7}{12}q^{-2}-\tfrac{1}{3}q^{-3}+O(q^{-4})),\end{aligned}$$

as the theorem states.

7. *The orthogonal groups*

As indicated in §3, our treatment of the orthogonal groups has to differ somewhat from the other cases. We recalled in §1 the familiar fact that if both q and n are odd then every member of $\mathrm{SO}(n,q)$ has 1 as an eigenvalue. In fact, it is nearly as well known that if q is odd and $X\in\mathrm{O}(n,q)\setminus\mathrm{SO}(n,q)$ then X has -1 as an eigenvalue, whatever the value of n. The reason is as follows. Suppose that $X\in\mathrm{O}(n,q)\setminus\mathrm{SO}(n,q)$, so that $\det X=-1$. Let $c_X(t)$ be the characteristic polynomial $\det(tI-X)$ of X. We can write $c_X(t)=(t-1)^{m_1}(t+1)^{m_{-1}}g(t)$, where neither 1 nor -1 is a root of g and $m_1\geqslant 0$, $m_{-1}\geqslant 0$. Since X is orthogonal it is similar to $(X^{\mathrm{tr}})^{-1}$ and so elements λ,λ^{-1} of the algebraic closure of $\mathbb{F}_q$ occur with the same multiplicity as roots of $c_X(t)$. Therefore $\det X=(-1)^{m_{-1}}$ and so m_{-1} must be odd. In particular, $m_{-1}\geqslant 1$, that is, -1 is an eigenvalue of X.

From now on the dimension n is taken to be even, that is, $n=2m$. We shall need Dye's charming observation [**4**] that the map $D: X\mapsto \dim\mathrm{Im}(I-X) \pmod 2$ is a homomorphism from an orthogonal group to the additive group of integers modulo 2. Given that n is even this map is the same as $X\mapsto\dim\mathrm{Ker}(I-X) \pmod 2$. When q is odd $\mathrm{Ker}\,D=\mathrm{SO}^{\varepsilon}(2m,q)$; when q is a power of 2 the kernel is $\Omega^{\varepsilon}(2m,q)$. Following Carter [**2**, p. 26] and Taylor [**13**, p. 160] we follow the convention:

$$\mathrm{SO}^{\varepsilon}(2m,q) := \mathrm{Ker}\,D.$$

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

Thus when q is a power of 2 we use the names $\Omega^\varepsilon(2m,q)$, $\mathrm{SO}^\varepsilon(2m,q)$ interchangeably. The point is that, with this convention, by Dye's theorem, all elements of $\mathrm{O}^\varepsilon(2m,q)\setminus \mathrm{SO}^\varepsilon(2m,q)$ have 1 as an eigenvalue and so:

THEOREM 7.1. *All eigenvalue-free matrices in* $O^\varepsilon(2m,q)$ *lie in* $\mathrm{SO}^\varepsilon(2m,q)$.

Because Steinberg's theorem counts the unipotent elements in $\mathrm{SO}^\varepsilon(2m,q)$ (and not those in $\mathrm{O}^\varepsilon(2m,q)$ when q is a power of 2), we find that to prove our theorems we have to conduct a census of $\mathrm{SO}^\varepsilon(2m,q)$ rather than of $\mathrm{O}^\varepsilon(2m,q)$. For the orthogonal groups the sets Θ, Ψ introduced in §3 are the same as for the symplectic groups: that is, Θ consists of ± 1 if q is odd and it is the singleton $\{1\}$ if q is a power of 2; correspondingly, $|\Psi|$ is $\frac{1}{2}(q-3)$ or $\frac{1}{2}(q-2)$. Consider now the primary decomposition

$$V = V_0 \oplus^\perp \bigoplus_{\theta\in\Theta}{}^\perp V_\theta \oplus^\perp \bigoplus_{\psi\in\Psi}{}^\perp V_\psi,$$

where $V_\psi = W_\psi \oplus W_\psi^*$, and

$$X = X_0 \oplus \bigoplus_{\theta\in\Theta} X_\theta \oplus \bigoplus_{\psi\in\Psi} (X_\psi \oplus X_\psi^*)$$

of an element X of $\mathrm{SO}^\varepsilon(2m,q)$. In this decomposition V_0, V_θ, are non-singular subspaces of V. If q is even this automatically means that $\dim V_0$, $\dim V_\theta$ have to be even. If q is odd then as the argument preceding Theorem 7.1 shows, $\dim V_{-1}$ and $\dim V_1$ have to be even, and so $\dim V_0$ also is even. (That $\dim V_0$ is even can also be seen from the fact that the eigenvalues of X_0 in the algebraic closure of $\mathbb{F}_q$ come in inverse pairs.) Thus m is partitioned as $m_0 + \sum m_\theta + \sum m_\psi$, where $2m_0 = \dim V_0$, $2m_\theta = \dim V_\theta$, and (as in §3) $m_\psi = \dim W_\psi = \dim W_\psi^*$. Because it has totally isotropic subspaces of half its dimension, the space V_ψ has to be of Witt type $+$. Since the type of an orthogonal direct sum is the product of the types of the summands, the types ε_0, ε_θ, of V_0, V_θ are then restricted only by the condition that $\varepsilon_0 \prod \varepsilon_\theta = \varepsilon$. For a given partition $\mathbf{m}$ of m and for a given tuple (triple if q is odd, pair if q is even) $\mathbf{e}$ of types ε_0, ε_θ, the group $\mathrm{O}^\varepsilon(2m,q)$ is transitive on the set of orthogonal decompositions of V described above, and the stabiliser of one of them is $\mathrm{O}^{\varepsilon_0}(2m_0,q)\times\prod \mathrm{O}^{\varepsilon_\theta}(2m_\theta,q) \times\prod \mathrm{GL}(m_\psi,q)$. Conducting a census of $\mathrm{SO}^\varepsilon(2m,q)$ for $m\geqslant 1$ we therefore find that

$$\tfrac{1}{2} = \sum_{\mathbf{m},\mathbf{e}} v(\mathrm{O}^{\varepsilon_0};m_0,q)\prod_{\theta\in\Theta} u(\mathrm{O}^{\varepsilon_\theta};m_\theta,q)\prod_{\psi\in\Psi} u(\mathrm{GL};m_\psi,q), \tag{1ε}$$

where the sum is over all partitions $\mathbf{m}$ of m into $1+|\Theta|+|\Psi|$ non-negative parts and all tuples $\mathbf{e} = (\varepsilon_0,\varepsilon_\theta)$ such that $\varepsilon_0\prod\varepsilon_\theta = \varepsilon$. It was in order that the census here should work correctly that we defined $u(\mathrm{O}^+;0,q) := v(\mathrm{O}^+;0,q) := 1$ and $u(\mathrm{O}^-;0,q) := v(\mathrm{O}^-;0,q) := 0$ in §3. In §3 we also defined

$$u^+(\mathrm{O};m,q) := u(\mathrm{O}^+;m,q)+u(\mathrm{O}^-;m,q),\quad u^-(\mathrm{O};m,q) := u(\mathrm{O}^+;m,q)-u(\mathrm{O}^-;m,q),$$
$$v^+(\mathrm{O};m,q) := v(\mathrm{O}^+;m,q)+v(\mathrm{O}^-;m,q),\quad v^-(\mathrm{O};m,q) := v(\mathrm{O}^+;m,q)-v(\mathrm{O}^-;m,q).$$

Adding and subtracting equations $(1+)$ and $(1-)$ we get

$$\sum_{\mathbf{m}} v^+(\mathrm{O};m_0,q)\prod_{\theta\in\Theta} u^+(\mathrm{O};m_\theta,q)\prod_{\psi\in\Psi} u(\mathrm{GL};m_\psi,q) = 1 \quad \text{for } m\geqslant 0$$

and

$$\sum_{\mathbf{m}} v^-(\mathrm{O};m_0,q)\prod_{\theta\in\Theta} u^-(\mathrm{O};m_\theta,q)\prod_{\psi\in\Psi} u(\mathrm{GL};m_\psi,q) = \begin{cases} 0 & \text{if } m\geqslant 1,\\ 1 & \text{if } m = 0.\end{cases}$$

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

For the generating functions $U^\varepsilon(\mathrm{O};q;z)$ and $V^\varepsilon(\mathrm{O};q;z)$ we therefore have that

$$V^+(\mathrm{O};q;z)\,U^+(\mathrm{O};q;z)^{|\Theta|}\,U(\mathrm{GL};q,z)^{|\Psi|}=(1-z)^{-1},$$
$$V^-(\mathrm{O};q;z)\,U^-(\mathrm{O};q;z)^{|\Theta|}\,U(\mathrm{GL};q,z)^{|\Psi|}=1.$$

The number of unipotent elements that lie in $\mathrm{SO}^\varepsilon(2m,q)$ is $q^{2m(m-1)}$ (see [**10**, Theorem 15.1]) and $|\mathrm{O}^\varepsilon(2m,q)|=2q^{m^2-m}(q^m-\varepsilon 1)\prod_{i=1}^{m-1}(q^{2i}-1)$ (see [**12**, p. 141]). Then $u(\mathrm{O}^\varepsilon;m,q)$ works out to be $\frac{1}{2}q^{-2m}(q^m+\varepsilon 1)\prod_{i=1}^{m}(1-q^{-2i})^{-1}$. Adding and subtracting we find that

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

$$u^-(\mathrm{O};m,q)=q^{-2m}\prod_{i=1}^{m}(1-q^{-2i})^{-1}=q^{-2m}c_m(q^2)$$

for $m\geqslant 1$. It follows from Theorem 2.1(2) that $U^+(\mathrm{O};q;z)=G(q^2;qz)^{-1}$ and $U^-(\mathrm{O};q;z)=G(q^2;z)^{-1}$. Thus:

THEOREM 7.2. (1) *$U^+(\mathrm{O};q;z)=G(q^2;qz)^{-1}$ and $U^-(\mathrm{O};q;z)=G(q^2;z)^{-1}$;*

(2) $$V^+(\mathrm{O};q;z)=\begin{cases}(1-z)^{-1}\,G(q^2;qz)^2\,G(q;z)^{(q-3)/2} & \text{if } q \text{ is odd},\\ (1-z)^{-1}\,G(q^2;qz)\,G(q;z)^{(q-2)/2} & \text{if } q \text{ is even};\end{cases}$$

(3) $$V^-(\mathrm{O};q;z)=\begin{cases}G(q^2;z)^2\,G(q;z)^{(q-3)/2} & \text{if } q \text{ is odd},\\ G(q^2;z)\,G(q;z)^{(q-2)/2} & \text{if } q \text{ is even}.\end{cases}$$

THEOREM 7.3. *Define $v(\mathrm{O}^\varepsilon;\infty,q):=\lim_{m\to\infty}v(\mathrm{O}^\varepsilon;m,q)$. Then*

$$v(\mathrm{O}^+;\infty,q)=v(\mathrm{O}^-;\infty,q)=\begin{cases}\frac{1}{2}G(q^2;q)^2\,G(q;1)^{(q-3)/2} & \text{if } q \text{ is odd},\\ \frac{1}{2}G(q^2;q)\,G(q;1)^{(q-2)/2} & \text{if } q \text{ is even}.\end{cases}$$

Moreover, if $m\geqslant q-2$ then

$$|v(\mathrm{O}^\varepsilon;\infty,q)-v(\mathrm{O}^\varepsilon;m,q)|<\begin{cases}\frac{1}{2}4^q\,q^{-m(m+(q-1)/2)/(q-1)} & \text{if } q \text{ is odd},\\ \frac{1}{2}4^q\,q^{-m(m+(q/2))/(q-1)} & \text{if } q \text{ is even}.\end{cases}$$

Sketch proof. It follows easily from Theorem 7.2 that $v^+(\mathrm{O};m,q)\to G(q^2;q)^{|\Theta|}\,G(q;1)^{|\Psi|}$ and $v^-(\mathrm{O};m,q)\to 0$ as $m\to\infty$. Now $v(\mathrm{O}^+;m,q)=\frac{1}{2}(v^+(\mathrm{O};m,q)+v^-(\mathrm{O};m,q))$ and $v(\mathrm{O}^-;m,q)=\frac{1}{2}(v^+(\mathrm{O};m,q)-v^-(\mathrm{O};m,q))$, and so

$$\lim_{m\to\infty}v(\mathrm{O}^+;m,q)=\lim_{m\to\infty}v(\mathrm{O}^-;m,q)=\tfrac{1}{2}G(q^2;q)^{|\Theta|}\,G(q;1)^{|\Psi|},$$

and the first assertion follows from the fact that $|\Theta|=2$, $|\Psi|=\frac{1}{2}(q-3)$ when q is odd, and $|\Theta|=1$, $|\Psi|=\frac{1}{2}(q-2)$ when q is even. The rate of convergence may be treated as follows. Write $G(q^2;qz)^{|\Theta|}\,G(q;z)^{|\Psi|}$ as $\sum_0^\infty(-1)^m a_m z^m$ and $G(q^2;z)^{|\Theta|}\,G(q;z)^{|\Psi|}$ as $\sum_0^\infty(-1)^m b_m z^m$, where, by Lemma 2.3, a_m and b_m are positive. Then

$$\begin{aligned}v(\mathrm{O}^+;\infty,q)-v(\mathrm{O}^+;m,q)&=\tfrac{1}{2}(v^+(\mathrm{O};\infty,q)-v(\mathrm{O}^+;m,q)+v^-(\mathrm{O};\infty,q)-v^-(\mathrm{O};m,q))\\ &=\tfrac{1}{2}(-1)^{m+1}(\varepsilon_m+b_m),\end{aligned}$$

where $\varepsilon_m:=\sum_{i=0}^\infty(-1)^i a_{m+1+i}$. The calculations that proved the last part of Theorem 5.3 tell us that $|\varepsilon_m|<\frac{1}{3}4^q q^{-(m+1)^2/(q-1)}$. Very similar calculations yield that

$$b_m<(2+3q^{-1/2})^{(q-1)/2}\,c(q)^{(q-1)/2}\,q^{-m(m+(q-1)/2)/(q-1)}<4^{q-1}q^{-m(m+(q-1)/2)/(q-1)}.$$

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

It is easy to see that

$$\tfrac{1}{3}4^q q^{-(m+1)^2/(q-1)} < 4^{q-1}q^{-m(m+(q-1)/2)/(q-1)}$$

when $m \geqslant 1$. Therefore certainly $|v(\mathrm{O}^+;\infty,q)-v(\mathrm{O}^+;m,q)| < \tfrac{1}{2}4^q q^{-m(m+(q-1)/2)/(q-1)}$. This proves our assertion in the case when q is odd; the case when q is a power of 2 is similar.

The calculation to prove Theorem 5.4 yields:

THEOREM 7.4.

$$v(\mathrm{O}^+;\infty,q) = v(\mathrm{O}^-;\infty,q) = \begin{cases} \tfrac{1}{2}\mathrm{e}^{-1/2}(1-\tfrac{5}{4}q^{-1}+\tfrac{131}{96}q^{-2}-\tfrac{997}{384}q^{-3}+O(q^{-4})) & \textit{if } q \textit{ is odd,} \\ \tfrac{1}{2}\mathrm{e}^{-1/2}(1-\tfrac{3}{4}q^{-1}+\tfrac{59}{96}q^{-2}-\tfrac{459}{384}q^{-3}+O(q^{-4})) & \textit{if } q \textit{ is even.} \end{cases}$$

The special case of our theorems for orthogonal groups over $\mathbb{F}_2$ is of particular interest. It is needed for our study of cyclic matrices in [**8**] and was the starting point for the whole of this work.

THEOREM 7.5. *When $q = 2$ we have*

$$v(\mathrm{O}^+;\infty,2) = v(\mathrm{O}^-;\infty,2) = \tfrac{1}{2}G(4;2) = \tfrac{1}{2}\prod_{i=1}^{\infty}(1-2^{-(2i-1)}) = 0.2097\ldots$$

and $|v(\mathrm{O}^\varepsilon;m,2)-\tfrac{1}{2}G(4,2)| < \tfrac{10}{11}2^{-m(m+1)}$ for all $m \geqslant 1$.

Proof. All that needs justification is the error estimate. From the generating function equations $V^+(\mathrm{O};2;z) = (1-z)^{-1}G(4;2z)$ and $V^-(\mathrm{O};2;z) = G(4;z)$, we have that

$$v^+(\mathrm{O};m,2) = G(4;2)+(-1)^{m+1}\eta \quad \text{where } 0 < \eta < c_{m+1}(4)\,2^{-m(m+1)-(m+1)}$$

and

$$v^-(\mathrm{O};m,2) = (-1)^m c_m(4)\,2^{-m(m-1)-2m}.$$

Now $c_m(4) < \tfrac{16}{11}$ by Lemma 2.2(2), and

$$v(\mathrm{O}^+;m,2) = \tfrac{1}{2}(v^+(\mathrm{O};m,2)+v^-(\mathrm{O};m,2)), \quad v(\mathrm{O}^-;m,2) = \tfrac{1}{2}(v^+(\mathrm{O};m,2)-v^-(\mathrm{O};m,2)).$$

Therefore

$$\begin{aligned} |v(\mathrm{O}^\varepsilon;m,2)-\tfrac{1}{2}G(4,2)| &< \tfrac{1}{2}(c_{m+1}(4)\,2^{-(m+1)^2}+c_m(4)\,2^{-m(m+1)}) \\ &< \tfrac{8}{11}2^{-m(m+1)}(2^{-(m+1)}+1) \\ &\leqslant \tfrac{10}{11}2^{-m(m+1)} \end{aligned}$$

if $m \geqslant 1$, as stated in the theorem.

8. *Concluding observations*

For $\lambda \in F$, a matrix will be said to be *λ-free* if λ does not occur as an eigenvalue. Thus, for example, the 1-free invertible matrices are precisely the derangements of $\mathrm{GL}(n,F)$ acting on the set $V^\#$ of non-zero vectors of F^n. For a given value of λ, and for a given matrix group G, what is the probability that a matrix X chosen at random from G is λ-free? Although this question seems intrinsically a little less interesting than

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

the one treated in the main body of this paper, we sketch an answer here because it is of great use in our work on cyclic matrices. It can be obtained relatively easily by our methods.

In §3 we defined on $F^\times$ a pairing $\lambda \mapsto \lambda^*$ associated with a classical group other than GL. It is convenient to define such a 'pairing' also in the case of GL, namely, the identity mapping. Recall that Θ was defined to be the set of self-paired members of $F^\times$ and Ψ was chosen to be a set of representatives of the pairs of non-self-paired members: thus for GL we have $\Theta = F^\times$ and $\Psi = \varnothing$. For a classical group G of type X and for $\lambda \in F^\times$ define

$$w(\mathrm{X}, \lambda; m, q) := \frac{|\{\lambda\text{-free elements of } G\}|}{|G|},$$

where m is the parameter described in the second paragraph of §3. Then define the generating function

$$W(\mathrm{X}, \lambda; q, z) := \sum_{m=0}^{\infty} w(\mathrm{X}, \lambda; m, q)\, z^m.$$

For the orthogonal groups (for which, recall, we restrict attention to the even-dimensional case) we need to combine the generating functions by defining

$$W^{\pm}(\mathrm{O}, \lambda; q, z) := W(\mathrm{O}^+, \lambda; q, z) \pm W(\mathrm{O}^-, \lambda; q, z).$$

Consider first elements θ of Θ, that is, self-paired eigenvalues. Using primary decomposition of matrices in the same way as in §§4–7 we find that

$$W(\mathrm{X}, \theta; q, z)\, U(\mathrm{X}; q, z) = (1-z)^{-1} \quad \text{for } \mathrm{X} \in \{\mathrm{GL}, \mathrm{Sp}, \mathrm{U}\},$$

$$W^{\varepsilon}(\mathrm{O}, \theta; q, z)\, U^{\varepsilon}(\mathrm{O}; q, z) = \begin{cases} (1-z)^{-1} & \text{if } \varepsilon = +, \\ 1 & \text{if } \varepsilon = -. \end{cases}$$

From Theorems 4.2, 5.2 and 6.2 it follows that

$$W(\mathrm{X}, \theta; q, z) = \begin{cases} (1-z)^{-1} G(q; z) & \text{if } \mathrm{X} = \mathrm{GL}, \\ (1-z)^{-1} G(q^2; qz) & \text{if } \mathrm{X} = \mathrm{Sp}, \\ (1-z)^{-1} G(-q; -z) & \text{if } \mathrm{X} = \mathrm{U}. \end{cases}$$

And from Theorem 7.2(1) we have that

$$W^{\varepsilon}(\mathrm{O}, \theta; q, z) = \begin{cases} (1-z)^{-1} G(q^2; qz) & \text{if } \varepsilon = +, \\ G(q^2; z) & \text{if } \varepsilon = -. \end{cases}$$

Then we find that

$$w(\mathrm{GL}, \theta; n, q) = \sum_{k=0}^{n} (-1)^k c_k(q)\, q^{-k(k+1)/2},$$

$$w(\mathrm{Sp}, \theta; m, q) = \sum_{k=0}^{m} (-1)^k c_k(q^2)\, q^{-k^2},$$

$$w(\mathrm{U}, \theta; n, q) = \sum_{k=0}^{n} (-1)^{k(k+1)/2} c_k(-q)\, q^{-k(k+1)/2},$$

and

$$w(\mathrm{O}^{\varepsilon}, \theta; m, q) = \tfrac{1}{2}\left(\sum_{k=0}^{m} (-1)^k c_k(q^2)\, q^{-k^2} \right) + \varepsilon \tfrac{1}{2} (-1)^m c_m(q^2)\, q^{-m(m+1)}.$$

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

The finite sum can be approximated by the sum to infinity and so we have the following theorem.

THEOREM 8.1. *If* $\theta \in \Theta$, *that is, if* $\theta \in F^\times$ *for* $\mathrm{GL}(n,q)$, $\theta = \pm 1$ *for* $\mathrm{Sp}(2m,q)$, $\theta^{q+1} = 1$ *for* $\mathrm{U}(n,q)$ *and* $\theta = \pm 1$ *for* $\mathrm{O}^\varepsilon(2m,q)$, *then*

$$\begin{aligned}
w(\mathrm{GL},\theta;n,q) &= G(q,1)+(-1)^{n+1}\eta_n && \text{where } 0<\eta_n<c(q)\,q^{-(n+1)(n+2)/2},\\
w(\mathrm{Sp},\theta;m,q) &= G(q^2,q)+(-1)^{m+1}\eta_m && \text{where } 0<\eta_m<c(q^2)\,q^{-(m+1)^2},\\
w(\mathrm{U},\theta;n,q) &= G(-q,-1)+\eta_n && \text{where } |\eta_n|<2c(-q)\,q^{-(n+1)(n+2)/2},\\
w(\mathrm{O}^\varepsilon,\theta;m,q) &= \tfrac{1}{2}G(q^2,q)+\eta^\varepsilon_m && \text{where } |\eta^\varepsilon_m|<2c(q^2)\,q^{-m(m+1)}.
\end{aligned}$$

Suppose now that $\psi \in F^\times \setminus \Theta$. Then from primary decomposition we derive the formula

$$W(\mathrm{X},\psi;q,z)\,U(\mathrm{GL};q,z) = (1-z)^{-1} \quad \text{for } \mathrm{X}\in\{\mathrm{Sp},\mathrm{U},\mathrm{O}^\varepsilon\},$$

and so

$$W(\mathrm{X},\psi;q,z) = (1-z)^{-1}\,G(q;z) \quad \text{for } \mathrm{X}\in\{\mathrm{Sp},\mathrm{U},\mathrm{O}^\varepsilon\}.$$

This leads to

THEOREM 8.2. *If* $\mathrm{X}\in\{\mathrm{Sp},\mathrm{U},\mathrm{O}^\varepsilon\}$ *and* $\psi\in F^\times\setminus\Theta$ *then*

$$w(\mathrm{X},\psi;m,q) = G(q;1)+(-1)^{m+1}\eta_m \quad \text{where } 0<\eta_m<c(q)\,q^{-(m+1)(m+2)/2}.$$

Except in the case where $\mathrm{X}=\mathrm{O}^\varepsilon$ and $\lambda=\pm1$ the limiting probabilities $G(q;1)$, $G(q^2;q)$ and $G(-q;-1)$ that occur in these two theorems are $\prod_1^\infty(1-q^{-i})$, $\prod_1^\infty(1-q^{-(2i-1)})$ and $\prod_1^\infty(1+(-1)^i q^{-i})$ respectively. Each of these can be expressed in the form $1-q^{-1}-O(q^{-2})$. Thus, with the exception mentioned, the probability that a given element λ of $F^\times$ is an eigenvalue of a matrix X chosen randomly from one of the classical groups G can be expressed in the form $q^{-1}+O(q^{-2})$. This is consistent with the fact that matrices X with eigenvalue λ constitute the codimension-1 algebraic subvariety of G defined by the single polynomial equation $\det(\lambda I-X)=0$.

For $\mathrm{O}^\varepsilon(2m,q)$ and $\lambda=\pm1$ the probability that λ is an eigenvalue is $\frac{1}{2}+\frac{1}{2}q^{-1}$. The geometric interpretation depends on the fact that $\mathrm{O}^\varepsilon(2m,q)$ is disconnected. The connected component containing I is $\mathrm{SO}^\varepsilon(2m,q)$. All elements of $\mathrm{O}^\varepsilon(2m,q)\setminus\mathrm{SO}^\varepsilon(2m,q)$ have λ as an eigenvalue; the probability that λ is an eigenvalue of an element of $\mathrm{SO}^\varepsilon(2m,q)$ is $q^{-1}+O(q^{-2})$, as one would expect.

References

1. GEORGE E. ANDREWS, *The theory of partitions* (Addison-Wesley, Reading, MA, 1976).
2. ROGER W. CARTER, *Finite groups of Lie type: conjugacy classes and complex characters* (Wiley, Chichester, 1985).
3. E. T. COPSON, *An introduction to the theory of functions of a complex variable* (Clarendon Press, Oxford, 1935) (reprinted 1970).
4. R. H. DYE, 'A geometric characterization of the special orthogonal groups and the Dickson invariant', *J. London Math. Soc.* (2) 15 (1977) 472–476.
5. LEONHARD EULER, *Introductio in analysin infinitorum* (2 vols; Lausanne, 1748). Translated into English by John D. Blanton, *Introduction to analysis of the infinite* (Springer, New York, 1988).
6. N. J. FINE and I. N. HERSTEIN, 'The probability that a matrix be nilpotent', *Illinois J. Math.* 2 (1958) 499–504.
7. JENNIE C. HANSEN and ERIC SCHMUTZ, 'How random is the characteristic polynomial of a random matrix?', *Math. Proc. Cambridge Philos. Soc.* 114 (1993) 507–515.
8. PETER M. NEUMANN and CHERYL E. PRAEGER, 'Cyclic matrices in classical groups over finite fields', in preparation, 1996.

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press

9. IRVING REINER, 'On the number of matrices with given characteristic polynomial', *Illinois J. Math.* 5 (1961) 324–329.
10. W. W. ROUSE-BALL, *Mathematical recreations and essays* (11th ed., revised by H. S. M. Coxeter, Macmillan, London, 1939).
11. R. STEINBERG, 'Endomorphisms of linear algebraic groups', *Mem. Amer. Math. Soc.* 80 (1968).
12. DAVID STIRZAKER, *Elementary probability* (Cambridge University Press, Cambridge, 1994).
13. DONALD E. TAYLOR, *The geometry of the classical groups* (Heldermann Verlag, Berlin, 1992).
14. K. ZSIGMONDY, 'Ueber die Anzahl derjenigen ganzen ganzzahligen Functionen *n*ten Grades von *x*, welche in Bezug auf einen gegebenen Primzahlmodul eine vorgeschriebene Anzahl von Wurzeln besitzen', *Sitzungsber. Wien Abt. II* 103 (1894) 135–144.

The Queen's College
Oxford OX1 4AW

Department of Mathematics
University of Western Australia
Perth
WA 6907
Australia

https://doi.org/10.1112/S0024610798006772 Published online by Cambridge University Press