9 Dec 1997

Cycle Indices for the Finite Classical Groups

By Jason Fulman

Dartmouth College

Jason.E.Fulman@Dartmouth.Edu

Abstract

This paper defines and develops cycle indices for the finite classical groups. These tools are then applied to study properties of a random matrix chosen uniformly from one of these groups. Properties studied by this technique will include semisimplicity, regularity, regular semisimplicity, the characteristic polynomial, number of Jordan blocks, and average order of a matrix.

1 Introduction and Background

Polya [29], in a landmark paper on combinatorics, introduced the cycle index of the symmetric groups. This can be written as follows. Let $a_i(\pi)$ be the number of i-cycles of π. The Taylor expansion of e^z and the fact that there are $\frac{n!}{\prod_i a_i! i^{a_i}}$ elements of S_n with a_i i-cycles, yield the following theorem.

Theorem 1 *(Polya [29])*

$$\sum_{n=0}^{\infty} \frac{u^n}{n!} \sum_{\pi \in S_n} \prod_i x_i^{a_i(\pi)} = \prod_{m=1}^{\infty} e^{\frac{x_m u^m}{m}}.$$

The Polya cycle index has been a key tool in understanding what a typical permutation $\pi \in S_n$ "looks like". It is useful for studying properties of a permutation which depend only on its cycle structure. Here are some examples of theorems which can be proved using the cycle index. Lloyd and Shepp [25] showed that for any $i < \infty$, the joint distribution of $(a_1(\pi), \cdots, a_i(\pi))$ for π chosen uniformly in S_n converges to independent (Poisson(1), $\cdots$, Poisson($\frac{1}{i}$)) as $n \to \infty$. Goncharov [17] proved that the number of cycles in a random permutation is asymptotically normal with mean $log\ n$ and standard deviation $(log\ n)^{\frac{1}{2}}$. Goh and Schmutz [14] proved that if μ_n is the average order of an element of S_n, then:

$$log\ \mu_n = C\sqrt{\frac{n}{log\ n}} + O(\frac{\sqrt{n} log log n}{log n})$$

where $C = 2.99047....$ Letting L_1 denote the length of the longest cycle of a permutation, Goncharov [17] showed that $\frac{L_1}{n}$ has a limit distribution. Lloyd and Shepp [25] computed the moments of this limit distribution. For instance, letting E_n signify expectation in S_n, they proved that:

$$\lim_{n\to\infty} E_n(\frac{L_1}{n}) = \int_0^{\infty} exp[-x - \int_x^{\infty} \frac{e^{-y}}{y} dy]dx = 0.62432997...$$

For more on the Polya cycle index, including a wonderful probabilistic interpretation due to Lloyd and Shepp, see Chapter 1 of Fulman [9].

Kung [22] and Stong [32] developed a cycle index for the finite general linear groups, with an eye toward studying properties of a random element of $GL(n,q)$. Chapter 1 of Fulman [9] gives motivation (for instance from the theory of random number generators) for why one might want to study random matrices. Let us review the Kung/Stong cycle index, as one of the goals of this paper is to carry out a similar undertaking for the other finite classical groups. First it is necessary to understand the conjugacy classes of $GL(n,q)$. As is explained in Chapter 6 of Herstein [20], an element $\alpha \in GL(n,q)$ has its conjugacy class determined by its rational canonical form (this is slightly different from Jordan canonical form, which only works over algebraically closed fields). This form corresponds to the following combinatorial data. To each monic non-constant irreducible polynomial ϕ over F_q, associate a partition (perhaps the trivial partition) λ_ϕ of some non-negative integer $|\lambda_\phi|$ into parts $\lambda_1 \geq \lambda_2 \geq \cdots$. Let m_ϕ denote the degree of ϕ. The only restrictions necessary for this data to represent a conjugacy class are: conjugacy class are:

1. $|\lambda_z| = 0$
2. $\sum_\phi |\lambda_\phi| m_\phi = n$

An explicit representative of this conjugacy class may be given as follows. Define the companion matrix $C(\phi)$ of a polynomial $\phi(z) = z^{m_\phi} + \alpha_{m_\phi - 1} z^{m_\phi - 1} + \cdots + \alpha_1 z + \alpha_0$ to be:

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ -\alpha_0 & -\alpha_1 & \cdots & \cdots & -\alpha_{m_\phi - 1} \end{pmatrix}$$

Let $\phi_1, \cdots, \phi_k$ be the polynomials such that $|\lambda_{\phi_i}| > 0$. Denote the parts of λ_{ϕ_i} by $\lambda_{\phi_i,1} \geq \lambda_{\phi_i,2} \geq \cdots$. Then a matrix corresponding to the above conjugacy class data is:

$$\begin{pmatrix} R_1 & 0 & 0 & 0 \\ 0 & R_2 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & R_k \end{pmatrix}$$

where R_i is the matrix:

$$\begin{pmatrix} C(\phi_i^{\lambda_{\phi_i,1}}) & 0 & 0 \\ 0 & C(\phi_i^{\lambda_{\phi_i,2}}) & 0 \\ 0 & 0 & \cdots \end{pmatrix}$$

For example, the identity matrix has λ_{z-1} equal to (1^n) and an elementary reflection with $a \neq 0$ in the $(1,2)$ position, ones on the diagonal and zeros elsewhere has λ_{z-1} equal to $(2, 1^{n-2})$.

As was true for the symmetric groups, many algebraic properties of a matrix α can be stated in terms of the data parameterizing its conjugacy class. For example, the characteristic polynomial of $\alpha \in GL(n,q)$ is equal to $\prod_\phi \phi^{|\lambda_\phi(\alpha)|}$. Section 3 will give further examples.

Kung [22] and Stong [32] developed a cycle index for the finite general linear groups, analogous to Polya's cycle index for the symmetric groups. It can be described as follows. Let $x_{\phi,\lambda}$ be variables corresponding to pairs of polynomials and partitions. Then the cycle index for $GL(n,q)$ is defined by

$$Z_{GL(n,q)} = \frac{1}{|GL(n,q)|} \sum_{\alpha \in GL(n,q)} \prod_{\phi \neq z} x_{\phi,\lambda_\phi(\alpha)}$$

It is also helpful to define a quantity $c_{GL,\phi,q^{m_\phi}}(\lambda)$. If λ is the empty partition, set $c_{GL,\phi,q^{m_\phi}}(\lambda) = 1$. Using the standard notation for partitions, let λ have m_i parts of size i. Write:

$$d_i = m_1 1 + m_2 2 + \cdots + m_{i-1}(i-1) + (m_i + m_{i+1} + \cdots + m_j)i$$

Then define:

$$c_{GL,\phi,q^{m_\phi}}(\lambda) = \prod_i \prod_{k=1}^{m_i} (q^{m_\phi d_i} - q^{m_\phi(d_i-k)})$$

Following Kung [22], Stong [32] proves the factorization:

$$1 + \sum_{n=1}^{\infty} Z_{GL(n,q)} u^n = \prod_{\phi \neq z} \sum_\lambda x_{\phi,\lambda} \frac{u^{|\lambda| m_\phi}}{c_{GL,\phi,q^{m_\phi}}(\lambda)}$$

The terms $c_{GL,\phi,q^{m_\phi}}$ in the Kung-Stong cycle index appear difficult to work with, and Section 2 will give several useful rewritings. Nevertheless, Stong [32], [33] and Goh and Schmutz [15] have used this cycle index successfully to study properties of random elements of $GL(n,q)$. For instance, Stong [32] showed that the number of Jordan blocks of a random element of $GL(n,q)$ has mean and variance $log(n) + O(1)$, and Goh and Schmutz [15] proved convergence to the normal distribution. Stong [32] also obtained asymptotic (in n and q) estimates for the chance that an element of $GL(n,q)$ is a vector space derangement (i.e. fixes only the origin), the number of elements of $GL(n,q)$ satisfying a fixed polynomial equation, and the chance that all polynomials appearing in the rational canonical form of $\alpha \in GL(n,q)$ are linear. Stong [33] studied the average order of a matrix.

The structure of this paper is as follows. Section 2 gives useful rewritings of the cycle index for the general linear groups. Section 3 applies the Kung/Stong cycle index to obtain exact formulas for the $n \to \infty$ limit of the chance that an element of $GL(n,q)$ or $Mat(n,q)$ is semisimple, regular, or regular semisimple. Section 4 uses work of Wall on the conjugacy classes of the unitary, symplectic, and orthogonal groups to obtain cycle indices for these groups. Section 5 uses the theory of algebraic groups to study the $q \to \infty$ limit of these cycle indices. Finally, Section 6 applies the cycle indices of Section 4 to study the characteristic polynomial, number of Jordan blocks, and average order of an element of a finite classical group. There is much more applied work to be done using these cycle indices; the results of Sections 3 and 6 are meant only as a start. Section 7 gives some suggestions for future research.

The work in this paper is taken from the author's Ph.D. thesis [9], done under the supervision of Persi Diaconis. There are three papers which should be considered companions to this one. Fulman [12] connects the cycle indices with symmetric function theory and exploits this connection to develop probabilistic algorithms with group theoretic meaning. Fulman [11] applies the algorithms of Fulman [12] to prove group theoretic results and can be read with no knowlegde of symmetric functions. Finally, Fulman [10] establishes an appearance of the Rogers-Ramanujan identities in the finite general linear groups; this is relevant to Section 3 of this paper.

2 Cycle Index of the General Linear Group: Useful Rewritings

Although the ultimate purpose of this section is to rewrite the cycle index of the general linear groups in useful ways, we begin with some remarks about the cycle index which were excluded from the brief discussion in the introductory section. First recall from the introduction that:

$$1+\sum_{n=1}^{\infty} \frac{u^n}{|GL(n,q)|} \sum_{\alpha \in GL(n,q)} \prod_{\phi \neq z} x_{\phi,\lambda_\phi(\alpha)} = \prod_{\phi \neq z} \sum_{\lambda} x_{\phi,\lambda} \frac{u^{|\lambda| m_\phi}}{c_{GL,\phi,q^{m_\phi}}(\lambda)}$$

where

$$c_{GL,\phi,q^{m_\phi}}(\lambda) = \prod_i \prod_{k=1}^{m_i} (q^{m_\phi d_i} - q^{m_\phi (d_i - k)})$$

and

$$d_i = m_1 1 + m_2 2 + \cdots + m_{i-1}(i-1) + (m_i + m_{i+1} + \cdots + m_j) i.$$

Remarks

1. The fact that the cycle index factors comes from the fact in Kung [22] that if α has data $\lambda_\phi(\alpha)$, then the conjugacy class of α in $GL(n,q)$ has size:

$$\frac{|GL(n,q)|}{\prod_\phi c_{GL,\phi,q(\lambda_\phi(\alpha))}}$$

The following example should make this formula seem more real. A transvection in $GL(n,q)$ is defined as a determinant 1 linear map whose pointwise fixed space is a hyperplane. For instance the matrix with $a \neq 0$ in the $(1,2)$ position, ones on the diagonal and zeros elsewhere is a transvection. The transvections generate $SL(n,q)$ (e.g. Suzuki [34]) and are useful in proving the simplicity of the projective special linear groups.

Transvections can be counted directly. Let V be an n dimensional vector space over F_q with dual space V^*. It is not hard to see that the action of any transvection τ is of the form:

$$\tau(\vec{x}) = \vec{x} + \vec{a}\psi(\vec{x})$$

where $\vec{a} \in V$ is a non-0 vector and $\psi \in V^*$ is a non-0 linear form on V which vanishes on $\vec{a}$. It readily follows that the number of transvections is:

$$\frac{(q^n - 1)(q^{n-1} - 1)}{q-1}$$

Transvections can also be counted using Kung's class size formula. It is not hard to show that an element $\alpha \in GL(n,q)$ is a transvection if and only if $\lambda_{z-1}(\alpha) = (2, 1^{n-2})$ and $|\lambda_\phi(\alpha)| = 0$ for all $\phi \neq z-1$. This follows from the fact that a transvection has all eigenvalues 1 and from a lemma in Fulman [9], which says that the dimension of the fixed space of α is the number of parts of the partition $\lambda_{z-1}(\alpha)$. Thus all transvections in $GL(n,q)$ are conjugate and Kung's formula shows that the size of the conjugacy class in $GL(n,q)$ corresponding to $\lambda_{z-1} = (2, 1^{n-2})$ is:

$$\frac{|GL(n,q)|}{c_{GL,z-1,q}(2,1^{n-2})} = \frac{(q^n - 1)(q^{n-1} - 1)}{q-1}.$$

2. The orbits of $GL(n,q)$ on $Mat(n,q)$ (all $n*n$ matrices) under conjugation are again parameterized by the data λ_ϕ. However the parition λ_ϕ need not have size zero. This leads to the factorization:

$$1+\sum_{n=1}^{\infty}\frac{u^n}{|Mat(n,q)|}\sum_{\alpha\in Mat(n,q)}\prod_{\phi\neq z} x_{\phi,\lambda_\phi(\alpha)} = \prod_{\phi}\sum_{\lambda} x_{\phi,\lambda}\frac{u^{|\lambda|m_\phi}}{c_{GL,\phi,q^{m_\phi}}(\lambda)}$$

This factorization will be used in Section 3, and shows that any successful application of cycle index theory to $GL(n,q)$ can be carried over to $Mat(n,q)$, and conversely.

3. Many of Stong's applications of the general linear group cycle index made use of the fact that it is possible to count the number of monic, degree m, irreducible polynomials $\phi\neq z$ over a finite field F_q. Letting $I_{m,q}$ denote the number of such polynomials, the following lemma is well-known. Let μ be the usual Moebius function of elementary number theory.

Lemma 1

$$I_{m,q}=\frac{1}{m}\sum_{k|m}\mu(k)(q^{\frac{m}{k}}-1)$$

PROOF: From Hardy and Wright [19], the number of monic, degree m, irreducible polynomials with coefficients in F_q is:

$$\frac{1}{m}\sum_{k|m}\mu(k)q^{\frac{m}{k}}$$

Now use the fact that $\sum_{k|m}\mu(k)$ is 1 if $m=1$ and 0 otherwise. $\square$

Similar counting results, for special types of polynomials relevant to the other finite classical groups, will be obtained in Section 4.

Now, we give two rewritings of the seemingly horrible quantitiy $c_{GL,\phi,q^{m_\phi}}$ which appeared in the Kung/Stong cycle index for the general linear groups. Recall that if λ is a partition of n into parts $\lambda_1\geq\lambda_2\cdots$, that $m_i(\lambda)$ is the number of parts in the partition equal to i. Let $\lambda_i'=m_i(\lambda)+m_{i+1}(\lambda)+\cdots$ be the ith part of the partition dual to λ. Also, $(\frac{1}{q})_r$ will denote $(1-\frac{1}{q})\cdots(1-\frac{1}{q^r})$.

Theorem 2

$$\begin{aligned} c_{GL,\phi,q^{m_\phi}}(\lambda) &= q^{2m_\phi[\sum_{h<i}hm_h(\lambda)m_i(\lambda)+\frac{1}{2}\sum_i(i-1)m_i(\lambda)^2]}\prod_i|GL(m_i(\lambda),q^{m_\phi})| \\ &= q^{m_\phi[\sum_i(\lambda_i')^2]}\prod_i(\frac{1}{q^{m_\phi}})_{m_i(\lambda)} \end{aligned}$$

PROOF: For both equalities assume that $m_\phi=1$, since the result will be proved for all q and one could then substitute q^{m_ϕ} for q.

For the first equality, it's easy to see that the factors of the form q^r-1 are the same on both sides, so it suffices to look at the powers of q on both sides. The power of q on the left-hand side is $\sum_i[d_im_i(\lambda)-\binom{m_i(\lambda)}{2}]$ and the power of q on the right-hand side is $\sum_i[im_i(\lambda)^2-\binom{m_i(\lambda)}{2}+\sum_{h<i}hm_h(\lambda)m_i(\lambda)]$. Thus it is enough to show that:

$$\sum_i d_i = \sum_i [im_i(\lambda) + 2\sum_{h<i} hm_h(\lambda)]$$

This equality follows from the observation that:

$$d_i = [\sum_{h<i} hm_h(\lambda)] + im_i(\lambda) + [\sum_{i<k} im_k(\lambda)]$$

For the second equality of the theorem, write $(\frac{1}{q})_{m_i(\lambda)}$ as $\frac{|GL(m_i(\lambda),q)|}{q^{m_i(\lambda)^2}}$. Comparing powers of q reduces us to proving that:

$$\sum_i (\lambda_i')^2 = \sum_i [im_i(\lambda) + 2\sum_{h<i} hm_h(\lambda)]m_i(\lambda)$$

This last equation follows quickly after substituting $\lambda_i' = m_i(\lambda) + m_{i+1}(\lambda) + \cdots$. $\square$

In fact, there is a third (and extremely useful) rewriting of $c_{GL,\phi,q^{m_\phi}}(\lambda)$ in terms of $P_\lambda(x_i;t)$, the Hall-Littlewood symmetric functions. Let $n(\lambda) = \sum_i (i-1)\lambda_i = \sum_i \binom{\lambda_i'}{2}$. Theorem 3 of Fulman [9] shows that:

$$c_{GL,\phi,q^{m_\phi}}(\lambda) = \frac{q^{m_\phi n(\lambda)}}{P_\lambda(\frac{1}{q^{m_\phi}}, \frac{1}{q^{2m_\phi}}, \cdots; \frac{1}{q^{m_\phi}})}$$

The proof is omitted in the present treatment, as this article will not make use of the connections with symmetric function theory developed in Fulman [9].

Lemma 2 is due to Stong [32] and will be useful in future sections. It was proved using an identity of Goldman and Rota and the fact that the number of unipotent (all eigenvalues equal to 1) elements of $GL(n,q)$ is $q^{n(n-1)}$. Fulman [11] gives a probabilstic proof.

Lemma 2

$$\sum_\lambda \frac{1}{c_{GL,\phi,q^{m_\phi}}(\lambda)} = \prod_{r=1}^{\infty} (\frac{1}{1-\frac{u^{m_\phi}}{q^{rm_\phi}}})$$

3 Application: Counting Semisimple, Regular, and Regular Semisimple Matrices

This section will use the cycle index of the general linear groups to obtain asymptotic formulas for the chance that an element of $GL(n,q)$ or $Mat(n,q)$ is semisimple, regular, or regular semisimple. The strategy for applying the cycle index to studying a property of a matrix which depends only on its conjugacy class will always be the same: first translate the property into a statement about the partitions λ_ϕ parameterizing the conjugacy class, then manipulate the cycle index accordingly.

The following three lemmas will prove useful for working with the cycle index. Lemma 3 allows one to gain insight into $n \to \infty$ asymptotics. (An alternate approach uses the method of moments). We use the notation that $[u^n]g(u)$ is the coefficient of u^n in the Taylor expansion of $g(u)$ around 0.

Lemma 3 *If $f(1) < \infty$ and f has a Taylor series around 0, then:*

$$lim_{n\to\infty}[u^n]\frac{f(u)}{1-u} = f(1)$$

PROOF: Write the Taylor expansion $f(u) = \sum_{n=0}^{\infty} a_n u^n$. Then observe that $[u^n]\frac{f(u)}{1-u} = \sum_{i=0}^{n} a_i$. $\Box$

Lemmas 4 and 5 will be useful for manipulating products which appear in the cycle index. Recall that m_ϕ is the degree of a monic, polynomial ϕ which is irreducible over F_q, the finite field of size q.

Lemma 4

$$\prod_{\phi}(1 - \frac{u^{m_\phi}}{q^{m_\phi t}}) = 1 - \frac{u}{q^{t-1}}$$

PROOF: Assume that $t = 1$, the general case following by replacing u by $\frac{u}{q^{t-1}}$. Expanding $\frac{1}{1-\frac{u^{m_\phi}}{q^{m_\phi}}}$ as a geometric series and using unique factorization in $F_q[x]$, one sees that the coefficient of u^d in the reciprocal of the left hand side is $\frac{1}{q^d}$ times the number of monic polynomials of degree d, hence 1. Comparing with the reciprocal of the right hand side completes the proof. $\Box$

Lemma 5

$$\prod_{\phi \neq z} \prod_{r=1}^{\infty}(1 - \frac{u^{m_\phi}}{q^{r m_\phi}}) = 1 - u$$

PROOF: Lemma 4 implies that:

$$\prod_{\phi} \prod_{r \geq 1}(1 - \frac{u^{m_\phi}}{q^{r m_\phi}}) = \prod_{r \geq 1}(1 - \frac{u}{q^{r-1}})$$

The result follows by cancelling the terms corresponding to $\phi = z$. Alternatively, this result can be deduced from Lemma 2. $\Box$

Application 1: Semisimplicity

Recall that an element of $Mat(n,q)$ is said to be semisimple if it is diagonalizable over $\bar{F}_q$, the algebraic closure of F_q. This application uses the cycle index to study the $n \to \infty$ limit of the chance that an element of $GL(n,q)$ or $Mat(n,q)$ is semisimple. The first step is to express this condition in terms of rational canonical form.

Recall the Jordan canonical form of a matrix (Chapter 6 of Herstein [20]), which parameterizes the conjugacy classes of GL over an algebraically closed field, such as $\bar{F}_q$. This is the same as the rational canonical form of a matrix (Section 1), except that now the companion matrix $C(\phi_i^A)$ is conjugate to:

$$\begin{pmatrix} D(\beta) & 0 & 0 & 0 \\ 0 & D(\beta^q) & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & D(\beta^{q^{m_\phi - 1}}) \end{pmatrix}$$

where $\beta, \cdots, \beta^{q^{m_\phi - 1}}$ are the roots of ϕ and $D(\gamma)$ is the $A * A$ matrix:

$$\begin{pmatrix} \gamma & 1 & 0 & 0 & 0 \\ 0 & \gamma & 1 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \gamma & 1 \\ 0 & 0 & 0 & 0 & \gamma \end{pmatrix}$$

Lemma 6 *An element $\alpha \in Mat(n,q)$ is semisimple if and only if $\lambda_\phi(\alpha)'_2 = 0$ (i.e. all parts in all partitions in the rational canonical form of α have size at most one).*

PROOF: The explicit description of Jordan canonical form just given implies that α is diagonalizable over $\bar{F}_q$ if and only if there are no companion matrices $C(\phi_i^A)$ where $A \geq 2$. □

Another tool we will use in applying the cycle index to semisimplicity is Gordon's generalization of the Rogers-Ramanujan identities. It is worth remarking that this gives what seems to be the first appearance of these identities in finite group theory (see Fulman [10] for more on this). Lemma 7 is a statement of Gordon's generalization of the Rogers-Ramanujan identities. It is taken directly from page 111 of Andrews [1].

Lemma 7 *For $1 \leq i \leq k, k \geq 2$, and $|x| < 1$*

$$\sum_{n_1,\cdots,n_{k-1}\geq 0} \frac{x^{N_1^2+\cdots+N_{k-1}^2+N_i+\cdots+N_{k-1}}}{(x)_{n_1}\cdots(x)_{n_{k-1}}} = \prod_{\substack{r=1 \\ r\neq 0,\pm i (mod\ 2k+1)}}^{\infty} \frac{1}{1-x^r}$$

where $N_j = n_j + \cdots n_{k-1}$.

Lemma 7 yields the following corollary.

Corollary 1

$$\prod_{r=1}^{\infty}(1-\frac{1}{q^{rm_\phi}}) \sum_{\lambda:\lambda_1<k} \frac{1}{c_{GL,\phi,q^{m_\phi}}(\lambda)} = \prod_{\substack{r=1 \\ r=0,\pm k (mod\ 2k+1)}}^{\infty} (1-\frac{1}{q^{m_\phi r}})$$

PROOF: Assume without loss of generality that $\phi = z-1$. By the second equality in Theorem 2, this probability is equal to:

$$\begin{aligned}
\prod_{r=1}^{\infty}(1-\frac{1}{q^r}) \sum_{\lambda:\lambda_1<k} \frac{1}{c_{GL,\phi,q^{m_\phi}}(\lambda)} &= \prod_{r=1}^{\infty}(1-\frac{1}{q^r}) \sum_{\lambda:\lambda_1<k} \frac{1}{q^{\sum_i (\lambda_i')^2} \prod_i (\frac{1}{q})_{m_i(\lambda)}} \\
&= \prod_{r=1}^{\infty}(1-\frac{1}{q^r}) \sum_{m_1(\lambda),\cdots,m_{k-1}(\lambda)\geq 0} \frac{1}{q^{\sum_i (\lambda_i')^2} \prod_i (\frac{1}{q})_{m_i(\lambda)}}
\end{aligned}$$

The result now follows from Lemma 7 by setting $n_i = m_i(\lambda)$, $i = k$, and $x = \frac{1}{q}$. □

With these tools in hand, the main results of this application can now be obtained.

Theorem 3 *The $n \to \infty$ limiting probability that an element of $Mat(n,q)$ is semisimple is:*

$$\prod_{\substack{r=1 \\ r=0,\pm 2 (mod\ 5)}}^{\infty} (1-\frac{1}{q^{r-1}})$$

PROOF: By the cycle index for $Mat(n,q)$, Lemmas 3, 4, 5, 6 and Corollary 1, the $n \to \infty$ limit of the chance that an element of $Mat(n,q)$ is semisimple is:

$$
\begin{aligned}
& lim_{n\to\infty}\frac{|GL(n,q)|}{q^{n^2}}[u^n]\prod_{\phi}\sum_{\lambda:\lambda_1<2}\frac{u^{m_\phi|\lambda|}}{c_{GL,\phi,q^{m_\phi}}(\lambda)}\\
= & lim_{n\to\infty}\frac{|GL(n,q)|}{q^{n^2}}[u^n]\frac{1}{1-u}\frac{1}{\prod_{r=1}^{\infty}(1-\frac{u}{q^r})}\prod_{\phi}[\prod_{r=1}^{\infty}(1-\frac{u^{m_\phi}}{q^{rm_\phi}})\sum_{\lambda:\lambda_1<2}\frac{u^{m_\phi|\lambda|}}{c_{GL,\phi,q^{m_\phi}}(\lambda)}]\\
= & \prod_{\phi}[\prod_{r=1}^{\infty}(1-\frac{1}{q^{rm_\phi}})\sum_{\lambda:\lambda_1<2}\frac{1}{c_{GL,\phi,q^{m_\phi}}(\lambda)}]\\
= & \prod_{\substack{r=1\\ r=0,\pm 2(mod\ 5)}}^{\infty}(1-\frac{1}{q^{r-1}})
\end{aligned}
$$

□

Theorem 4 *The $n\to\infty$ limiting probability that an element of $GL(n,q)$ is semisimple is:*

$$\prod_{\substack{r=1\\ r=0,\pm 2(mod\ 5)}}^{\infty}\frac{(1-\frac{1}{q^{r-1}})}{(1-\frac{1}{q^r})}$$

PROOF: Arguing as in Theorem 3 the chance is:

$$
\begin{aligned}
& lim_{n\to\infty}[u^n]\prod_{\phi\neq z}\sum_{\lambda:\lambda_1<2}\frac{u^{m_\phi|\lambda|}}{c_{GL,\phi,q^{m_\phi}}(\lambda)}\\
= & lim_{n\to\infty}[u^n]\frac{1}{1-u}\prod_{\phi\neq z}\prod_{r=1}^{\infty}(1-\frac{u^{m_\phi}}{q^{rm_\phi}})\sum_{\lambda:\lambda_1<2}\frac{u^{m_\phi|\lambda|}}{c_{GL,\phi,q^{m_\phi}}(\lambda)}\\
= & \prod_{\phi\neq z}\prod_{r=1}^{\infty}(1-\frac{1}{q^{rm_\phi}})\sum_{\lambda:\lambda_2'=0}\frac{1}{c_{GL,\phi,q^{m_\phi}}(\lambda)}]\\
= & \prod_{\phi\neq z}\prod_{\substack{r=1\\ r=0,\pm 2(mod\ 5)}}^{\infty}(1-\frac{1}{q^r})\\
= & \prod_{\substack{r=1\\ r=0,\pm 2(mod\ 5)}}^{\infty}(\frac{1}{1-\frac{1}{q^r}})\prod_{\phi}\prod_{\substack{r=1\\ r=0,\pm 2(mod\ 5)}}^{\infty}(1-\frac{1}{q^r})\\
= & \prod_{\substack{r=1\\ r=0,\pm 2(mod\ 5)}}^{\infty}\frac{(1-\frac{1}{q^{r-1}})}{(1-\frac{1}{q^r})}
\end{aligned}
$$

□

Application 2: Regularity and Regular-Semisimplicity

An element of an algebraic group G (usually taken to be connected and reductive) is called regular if the dimension of its centralizer is as small as possible (this minimal dimension turns out to be equal to the rank of G, i.e. the dimension of a maximal torus of G). Regular elements are very important in the representation theory of finite groups of Lie type. This application will give formulas for the $n \to \infty$ limit of the chance that an element of $GL(n,q)$ or $Mat(n,q)$ is regular or regular-semisimple.

The first step is to translate the conditions of regularity and regular semisimplicity into conditions on the paritions λ_ϕ. Let $\bar{F_q}$ denote an algebraic closure of the field of q elements.

Lemma 8 *An element $\alpha \in GL(n,q) \subset GL(n,\bar{F_q})$ is regular if and only if all $\lambda_\phi(\alpha)$ have at most one part.*

PROOF: Let β be an eigenvalue of α over $\bar{F_q}$ and let V_β be the eigenspace associated to β. The dimension of V_β is $|\lambda_\phi(\alpha)|$. Let $\alpha|_{V_\beta}$ be the restriction of α to V_β. It is not hard to see that:

$$C_{GL(n,\bar{F_q})}(\alpha) = \prod_\phi \prod_{\beta\ root\ of\ \phi} C_{GL(|\lambda_\phi(\alpha)|,\bar{F_q})}(\alpha|_{V_\beta})$$

One can prove from Jordan canonical form, described before Lemma 6 in the previous application, that $C_{GL(|\lambda_\phi(\alpha)|,\bar{F_q})}(\alpha|_{V_\beta})$ has dimension $\sum_i (\lambda'_{\phi,i}(\alpha))^2$. Thus the centralizer of $\alpha \in GL(n,\bar{F_q})$ has dimension $\sum_\phi m_\phi \sum_i (\lambda'_{\phi,i}(\alpha))^2$. Given the value $|\lambda_\phi(\alpha)|$, Lagrange multipliers show that $\sum_i (\lambda'_{\phi,i}(\alpha))^2$ is minimized when $\lambda_\phi(\alpha)$ has at most 1 part. The result follows since $\sum_\phi m_\phi \sum_i \lambda'_{\phi,i}(\alpha) = n$. $\square$

Corollary 2 *An element of $GL(n,q)$ is regular-semisimple if and only if $|\lambda_\phi| = 0, 1$ for all ϕ.*

PROOF: This is immediate from Lemmas 6 and 8. $\square$

It is worth remarking that the condition of Lemma 8, and hence the condition of regularity in $GL(n,q)$, is equivalent to the condition that the minimum polynomial of α is equal to the characteristic polynomial of α.

Lemma 8 leads us to call an element $\alpha \in Mat(d,q)$ regular if all $\lambda_\phi(\alpha)$ have at most one part. Neumann and Praeger [27], [28] studied the chance that a matrix is regular or regular-semisimple (they called these conditions "cyclic" and "separable"). They were interested in these probabilities because they give a way to test random number generators and computer algorithms for generating random elements from a finite group (see Chapter 1 of Fulman [9] for further motivation). Volkmann and Fleischmann [8] and Lehrer [23] studied this problem as well.

Some theorems of Neumann and Praeger are:

1. For $n \geq 2$, the chance that an $n*n$ matrix is not regular semi-simple is at least $q^{-1} - q^{-2} - q^{-3}$ and at most $q^{-1} + O(q^{-2})$.
2. For $n \geq 2$, the chance that an $n*n$ matrix is not regular is at least $\frac{1}{q^2(q+1)}$ and at most $\frac{1}{(q^2-1)(q-1)}$.

In the next four theorems, the cycle index machinery is used to find $n \to \infty$ formulas for the chance that a $n*n$ matrix or an element of $GL(n,q)$ is regular or regular-semisimple. These are good examples of results which seem hard to prove by other methods. Throughout, Lemma 3 is used freely.

Theorem 5 *The $n \to \infty$ chance that an $n*n$ matrix in $Mat(n,q)$ is regular-semisimple is equal to:*

$$\prod_{r=1}^{\infty}(1-\frac{1}{q^r})$$

PROOF: Corollary 2 says that an element of $Mat(n,q)$ is regular semisimple iff all λ_ϕ have size at most 1. So the cycle index for $Mat(n,q)$ and Lemma 4 imply that the probability of regular-semisimplicity is:

$$\begin{aligned}
& \lim_{n\to\infty}\frac{|GL(n,q)|}{q^{n^2}}[u^n]\prod_{\phi}(1+\frac{u^{m_\phi}}{q^{m_\phi}-1}) \\
= & \lim_{n\to\infty}\frac{|GL(n,q)|}{q^{n^2}}[u^n]\frac{\prod_\phi(1+\frac{u^{m_\phi}}{q^{m_\phi}-1})(1-\frac{u^{m_\phi}}{q^{m_\phi}})}{1-u} \\
= & \prod_{r=1}^{\infty}(1-\frac{1}{q^r})\prod_{\phi}(1+\frac{1}{q^{m_\phi}-1})(1-\frac{1}{q^{m_\phi}}) \\
= & \prod_{r=1}^{\infty}(1-\frac{1}{q^r})
\end{aligned}$$

□

Theorem 6 *The $n \to \infty$ chance that an $n*n$ matrix in $Mat(n,q)$ is regular is equal to:*

$$(1-\frac{1}{q^5})\prod_{r=3}^{\infty}(1-\frac{1}{q^r})$$

PROOF: Lemma 8 shows that regularity is equivalent to all λ_ϕ having at most 1 part. The cycle index for $Mat(n,q)$ and Lemma 4 give that the probability is:

$$\begin{aligned}
& \lim_{n\to\infty}\frac{|GL(n,q)|}{q^{n^2}}[u^n]\prod_{\phi}(1+\sum_{j=1}^{\infty}\frac{u^{jm_\phi}}{q^{jm_\phi-m_\phi}(q^{m_\phi}-1)}) \\
= & \prod_{r=1}^{\infty}(1-\frac{1}{q^r})\lim_{n\to\infty}[u^n]\frac{\prod_\phi(1-\frac{u^{m_\phi}}{q^{m_\phi}})(1+\sum_{j=1}^{\infty}\frac{u^{jm_\phi}}{q^{jm_\phi-m_\phi}(q^{m_\phi}-1)})}{1-u} \\
= & \prod_{r=1}^{\infty}(1-\frac{1}{q^r})\lim_{n\to\infty}[u^n]\frac{\prod_\phi(1+\frac{u^{m_\phi}}{q^{m_\phi}(q^{m_\phi}-1)})}{1-u} \\
= & \prod_{r=1}^{\infty}(1-\frac{1}{q^r})\prod_{\phi}(1+\frac{1}{q^{m_\phi}(q^{m_\phi}-1)}) \\
= & \prod_{r=3}^{\infty}(1-\frac{1}{q^r})\prod_{\phi}(1+\frac{1}{q^{m_\phi}(q^{m_\phi}-1)})(1-\frac{1}{q^{2m_\phi}})(1-\frac{1}{q^{3m_\phi}}) \\
= & \prod_{r=3}^{\infty}(1-\frac{1}{q^r})\prod_{\phi}(1-\frac{1}{q^{6m_\phi}}) \\
= & (1-\frac{1}{q^5})\prod_{r=3}^{\infty}(1-\frac{1}{q^r})
\end{aligned}$$

□

Theorem 7 *The $n \to \infty$ chance that an element of $GL(n,q)$ is regular-semisimple is equal to:*

$$1 - \frac{1}{q}$$

PROOF: By the cycle index for GL, the probability is:

$$\begin{aligned}
& \lim_{n\to\infty} [u^n] \prod_{\phi \neq z} \left(1 + \frac{u^{m_\phi}}{q^{m_\phi}-1}\right) \\
= & \lim_{n\to\infty} [u^n] \frac{(1-\frac{u}{q}) \prod_{\phi\neq z} [(1+\frac{u^{m_\phi}}{q^{m_\phi}-1})(1-\frac{u^{m_\phi}}{q^{m_\phi}})]}{1-u} \\
= & 1 - \frac{1}{q}
\end{aligned}$$

□

Theorem 8 *The $n \to \infty$ chance that an element of $GL(n,q)$ is regular is equal to:*

$$\frac{1-\frac{1}{q^5}}{1+\frac{1}{q^3}}$$

PROOF: By the cycle index for GL, the probability is:

$$\begin{aligned}
& \lim_{n\to\infty} [u^n] \prod_{\phi\neq z} \left(1 + \sum_{j=1}^{\infty} \frac{u^{jm_\phi}}{q^{jm_\phi - m_\phi}(q^{m_\phi}-1)}\right) \\
= & \lim_{n\to\infty} [u^n] \frac{(1-\frac{u}{q}) \prod_{\phi\neq z} (1+\frac{u^{m_\phi}}{(q^{m_\phi}-1)(1-\frac{u^{m_\phi}}{q^{m_\phi}})})(1-\frac{u^{m_\phi}}{q^{m_\phi}})}{1-u} \\
= & (1-\frac{1}{q}) \prod_{\phi\neq z}^{\infty} \left(1+\frac{1}{q^{m_\phi}(q^{m_\phi}-1)}\right) \\
= & \frac{1-\frac{1}{q}}{1+\frac{1}{q(q-1)}} \prod_{\phi} \left(\frac{1-\frac{1}{q^{6m_\phi}}}{(1-\frac{1}{q^{2m_\phi}})(1-\frac{1}{q^{3m_\phi}})}\right) \\
= & \frac{1-\frac{1}{q}}{1+\frac{1}{q(q-1)}} \frac{1-\frac{1}{q^5}}{(1-\frac{1}{q})(1-\frac{1}{q^2})} \\
= & \frac{1-\frac{1}{q^5}}{1+\frac{1}{q^3}}
\end{aligned}$$

□

It is worth remarking, along the lines of Neumann and Praeger [27], that these results are intuitively reasonable. Namely, Steinberg [31] proved that the set of non-regular elements in an algebraic group has codimension 3. Suppose this set to be a non-singular (which it is not) high dimensional (which it is for large n) variety. Then the chance of non-regularity would be about $\frac{1}{q^3}$, so the chance of regularity would be about $1-\frac{1}{q^3}$ which is consistent with Theorems 6 and 8.

Similarly, Neumann and Praeger [27] noted that a matrix is regular semisimple if and only if the discriminant of its characteristic polynomial is non-zero. As this restriction is defined by one equation, the chance of being regular semisimple should be about $1-\frac{1}{q}$, which is consistent with Theorems 5 and 7.

Finally, the chance of being semi-simple is greater than the chance of being regular semi-simple, which is consistent with Theorem 4.

4 Cycle Indices of the Finite Unitary, Symplectic, and Orthogonal Groups

This section develops cycle indices for the finite unitary, symplectic, and orthogonal groups, and in that order. For the symplectic and orthogonal groups, it will be assumed that the characteristic is not equal to 2. The main ingredient is work of Wall [35] on the conjugacy classes of these groups. The rewritings of $c_{GL,\phi,q^{m_\phi}}$ from Section 2 will be used to relate these cycle indices to the cycle index of the general linear groups.

The Unitary Groups

The unitary group $U(n,q)$ (we allow characteristic 2) can be defined as the subgroup of $GL(n,q^2)$ preserving a non-degenerate skew-linear form. Recall that a skew-linear form on an n dimensional vector space V over F_{q^2} is a bilinear map $<,>: V \times V \rightarrow F_{q^2}$ such that $<\vec{x},\vec{y}>=<\vec{y},\vec{x}>^q$ (raising to the qth power is an involution in a field of order q^2). One such form is given by $<\vec{x},\vec{y}>=\sum_{i=1}^n x_i y_i^q$. It is known (page 7 of Carter [4]) that any two non-degenerate skew-linear forms are equivalent, so that $U(n,q)$ is unique up to isomorphism. The order of $U(n,q)$ is $q^{\binom{n}{2}}\prod_{i=1}^n (q^i-(-1)^i)$.

To define a cycle index for the finite unitary groups, it is first necessary to understand their conjugacy classes. Given a polynomial ϕ with coefficients in F_{q^2} and non vanishing constant term, define a polynomial $\tilde{\phi}$ by:

$$\tilde{\phi} = \frac{z^{m_\phi}\phi^q(\frac{1}{z})}{[\phi(0)]^q}$$

where ϕ^q raises each coefficient of ϕ to the qth power. Writing this out, a polynomial $\phi(z) = z^{m_\phi}+\alpha_{m_\phi-1}z^{m_\phi-1}+\cdots+\alpha_1 z+\alpha_0$ with $\alpha_0 \neq 0$ is sent to $\tilde{\phi}(z) = z^{m_\phi}+(\frac{\alpha_1}{\alpha_0})^q z^{m_\phi-1}+\cdots+(\frac{\alpha_{m_\phi-1}}{\alpha_0})^q z+(\frac{1}{\alpha_0})^q$.

Wall [35] proves that the conjugacy classes of the unitary group correspond to the following combinatorial data. As was the case with $GL(n,q^2)$, an element $\alpha \in U(n,q)$ associates to each monic, non-constant, irreducible polynomial ϕ over F_{q^2} a partition λ_ϕ of some non-negative integer $|\lambda_\phi|$ by means of rational canonical form. The restrictions necessary for the data λ_ϕ to represent a conjugacy class are:

1. $|\lambda_z| = 0$
2. $\lambda_\phi = \lambda_{\tilde{\phi}}$
3. $\sum_\phi |\lambda_\phi| m_\phi = n$

Recall that $m_i(\lambda)$ denotes the number of parts of λ of size i. Wall computed the size of a conjugacy class corresponding to the data λ_ϕ as:

$$\frac{|U(n,q)|}{\prod_\phi B(\phi)}$$

where

$$\begin{aligned} A(\phi^i) &= |U(m_i(\lambda_\phi), q^{m_\lambda})| \ if \ \phi = \tilde{\phi} \\ &= |GL(m_i(\lambda_\phi), q^{2m_\lambda})|^{\frac{1}{2}} \ if \ \phi \neq \tilde{\phi} \end{aligned}$$

and

$$B(\phi) = q^{2m_\phi [\sum_{h<i} hm_h(\lambda_\phi) m_i(\lambda_\phi) + \frac{1}{2} \sum_i (i-1) m_i(\lambda_\phi)^2]} \prod_i A(\phi^i).$$

As an example of this formula, consider the set of unitary transvections, namely determinant 1 elements of $U(n,q)$ whose pointwise fixed space is $n-1$ dimensional. Fulman [9] counts unitary transvections directly, showing that the number of them is:

$$\frac{(q^n - (-1)^n)(q^{n-1} - (-1)^{n-1})}{q+1}$$

This checks with the class size formula. The fact that the dimension of the fixed space of $\alpha \in U(n,q)$ is the number of parts of $\lambda_{z-1}(\alpha)$ implies that $\alpha \in U(n,q)$ is a unitary transvection exactly when $\lambda_{z-1}(\alpha) = (2, 1^{n-2})$ and $|\lambda_\phi(\alpha)| = 0$ for $\phi \neq z-1$. Thus Wall's work implies that the unitary transvections form a single conjugacy class of size:

$$\frac{|U(n,q)|}{q^{2n-3}|U(n-2,q)||U(1,q)|} = \frac{(q^n - (-1)^n)(q^{n-1} - (-1)^{n-1})}{q+1}.$$

In analogy with the general linear groups, define a cycle index for the unitary groups by:

$$1 + \sum_{n=1}^{\infty} \frac{u^n}{|U(n,q)|} \sum_{\alpha \in U(n,q)} \prod_{\phi \neq z} x_{\phi, \lambda_\phi(\alpha)}$$

Theorem 10 will give a factorization theorem for this cycle index in terms of quantities for GL (so that some of the results obtained for the general linear groups can be carried over for free). For this and future use in the applications of Section 6, it is desirable to count the number of ϕ of a given degree invariant under $\tilde{}$.

Lemma 9 $\widetilde{\phi_1 \phi_2} = \tilde{\phi}_1 \tilde{\phi}_2$.

PROOF: From the definition of the involution $\tilde{}$, the lemma reduces to the observation that $(\phi_1 \phi_2)^q = (\phi_1^q)(\phi_2^q)$, where ^{q} is the map which raises each coefficient of a polynomial to the qth power. $\square$

Let $\tilde{I}_{m,q^2}$ be the number of monic, irreducible polynomials ϕ of degree m over F_{q^2} such that $\phi = \tilde{\phi}$.

Theorem 9 *$\tilde{I}_{m,q^2} = 0$ if m is even and $\tilde{I}_{m,q^2} = \frac{1}{m}\sum_{d|m}\mu(d)(q^{\frac{m}{d}}+1)$ if m is odd.*

PROOF: Let M_m be the number of monic degree m polynomials (not necessarily irreducible) and let $\tilde{M}_m$ be the number of monic degree m polynomials ϕ (not necessarily irreducible) such that $\phi(0) \neq 0$ and $\phi = \tilde{\phi}$. Define $A(t) = 1 + \sum_{m=1}^{\infty} M_m t^m$ and $B(t) = 1 + \sum_{m=1}^{\infty} \tilde{M}_m t^m$. Note that $A(t) = \frac{1}{1-q^2 t}$ because $M_m = q^{2m}$. Wall [35] observes that $B(t) = \frac{1+t}{1-qt}$ (this follows from the fact that $\tilde{M}_m = q^m + q^{m-1}$, which is clear from the explicit description of the definition of $\tilde{\phi}$ given above).

The fact that the involution $\tilde{}$ preserves degree gives the following equation (where as usual all polynomials in the products are irreducible):

$$A(t) = \frac{1}{1-t} \prod_{\phi \neq z, \phi = \tilde{\phi}} (1 + \sum_{n=1}^{\infty} t^{nm_\phi}) \prod_{\{\phi, \tilde{\phi}\}, \phi \neq \tilde{\phi}} (1 + \sum_{n=1}^{\infty} t^{nm_\phi})^2$$

Lemma 9 implies that a polynomial invariant under $\tilde{}$ is a product of terms ϕ where $\phi = \tilde{\phi}$ and $\phi\tilde{\phi}$ where $\phi \neq \tilde{\phi}$. This gives the equation:

$$B(t) = \prod_{\phi \neq z, \phi = \tilde{\phi}} (1 + \sum_{n=1}^{\infty} t^{nm_\phi}) \prod_{\{\phi, \tilde{\phi}\}, \phi \neq \tilde{\phi}} (1 + \sum_{n=1}^{\infty} t^{2nm_\phi})$$

These equations give:

$$\begin{aligned}
\frac{B(t)^2}{A(t^2)} &= (1-t^2) \frac{\prod_{m=0}^{\infty} (1 + \sum_{n=1}^{\infty} t^{mn})^{2\tilde{I}_{m,q^2}}}{\prod_{m=0}^{\infty} (1 + \sum_{n=1}^{\infty} t^{2mn})^{\tilde{I}_{m,q^2}}} \\
&= (1-t^2) \prod_{m=0}^{\infty} \frac{(1-t^{2m})^{\tilde{I}_{m,q^2}}}{(1-t^m)^{2\tilde{I}_{m,q^2}}} \\
&= (1-t^2) \prod_{m=0}^{\infty} (\frac{1+t^m}{1-t^m})^{\tilde{I}_{m,q^2}}
\end{aligned}$$

Combining this with the explicit expressions for $A(t)$ and $B(t)$ given above shows that:

$$\prod_{m=0}^{\infty} (\frac{1+t^m}{1-t^m})^{\tilde{I}_{m,q^2}} = (\frac{1+t}{1-t})(\frac{1+qt}{1-qt})$$

Take logarithms of both sides of this equation, using the expansions $log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + \cdots$ and $log(1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} + \cdots$.

The left-hand side becomes:

$$\sum_{m=0}^{\infty} 2\tilde{I}_{m,q^2} (t^m + \frac{t^{3m}}{3} + \frac{t^{5m}}{5} + \cdots)$$

The right-hand becomes:

$$\sum_{m \ odd} 2(\frac{1+q^m}{m}) t^m$$

Comparing coefficients of t^m shows that $\tilde{I}_{m,q^2}=0$ for m even and that $\sum_{d|m} 2\tilde{I}_{d,q^2}\frac{d}{m}=2(\frac{1+q^m}{m})$ for m odd. Moebius inversion proves that $\tilde{I}_{m,q^2}=\frac{1}{m}\sum_{d|m}\mu(d)(1+q^{\frac{m}{d}})$ if m is odd. $\Box$

Next, it will be proved that the cycle index of the unitary groups factors. (One can prove a factorization theorem without Theorem 9, but Theorem 9 is necessary to get an expression in terms of quantities related to GL). The quantities $c_{GL,\phi,q^{m_\phi}}$ and their various rewritings were considered in Section 2.

Theorem 10

$$\begin{aligned}1+\sum_{n=1}^{\infty}\frac{u^n}{|U(n,q)|}\sum_{\alpha\in U(n,q)}\prod_{\phi\neq z}x_{\phi,\lambda_\phi(\alpha)} &= \prod_{\phi\neq z,\phi=\tilde{\phi}}[\sum_\lambda x_{\phi,\lambda}\frac{(-u)^{|\lambda|m_\phi}}{c_{GL,z-1,-(q^{m_\phi})}(\lambda)}]\\ &\quad \prod_{\{\phi,\tilde{\phi}\},\phi\neq\tilde{\phi}}[\sum_\lambda x_{\phi,\lambda}x_{\tilde{\phi},\lambda}\frac{u^{2|\lambda|m_\phi}}{c_{GL,z-1,q^{2m_\phi}}(\lambda)}]\end{aligned}$$

Proof: The theorem follows from Wall's description and formula for conjugacy class sizes in the unitary group, provided that one can prove that for all $\phi=\tilde{\phi}$,

$$\begin{aligned}&\frac{u^{|\lambda_\phi|}}{q^{2m_\phi[\sum_{h<i}hm_h(\lambda_\phi)m_i(\lambda_\phi)+\frac{1}{2}\sum_i(i-1)m_i(\lambda_\phi)^2]}\prod_i|U(m_i(\lambda_\phi),q^{m_\phi})|}\\ =&\frac{(-u)^{|\lambda_\phi|}}{(-q)^{2m_\phi[\sum_{h<i}hm_h(\lambda_\phi)m_i(\lambda_\phi)+\frac{1}{2}\sum_i(i-1)m_i(\lambda_\phi)^2]}\prod_i|GL(m_i(\lambda_\phi),(-q)^{m_\phi})|}\end{aligned}$$

The formulas for $|GL(n,q)|$ and $|U(n,q)|$ show that $|GL(n,-q)|=(-1)^n|U(n,q)|$.

The proof of the desired equation boils down to keeping track of powers of -1 and using the fact from Theorem 9 that if $\phi=\tilde{\phi}$, then ϕ has odd degree. With a little more detail,

$$\begin{aligned}|\lambda_\phi|+m_\phi[\sum_i(i-1)m_i(\lambda_\phi)^2]+m_\phi[\sum_i m_i(\lambda_\phi)] &= |\lambda_\phi|+\sum_i(i-1)m_i(\lambda_\phi)^2+m_i(\lambda_\phi)\ (mod\ 2)\\ &= |\lambda_\phi|+\sum_i im_i(\lambda_\phi)\ (mod\ 2)\\ &= 2|\lambda_\phi|\ (mod\ 2)\\ &= 0\ (mod\ 2)\end{aligned}$$

$\Box$

The Symplectic Groups

This paper assumes for simplicity that the characteristic of F_q is not equal to 2. The symplectic group $Sp(2n,q)$ can be defined as the subgroup of $GL(2n,q)$ preserving a non-degenerate alternating form on F_q. Recall that an alternating form on a $2n$ dimensional vector space V over F_q is a bilinear map $<,>: V\times V\rightarrow F_q$ such that $<\vec{x},\vec{y}>=-<\vec{y},\vec{x}>$ (alternating forms do not exist in odd dimension). One such form is given by $<\vec{x},\vec{y}>=\sum_{i=1}^n(x_{2i-1}y_{2i}-x_{2i}y_{2i-1})$. As is explained in Chapter 1 of Carter [4], there is only one such form up to equivalence, so $Sp(2n,q)$ is unique up to isomorphism. The order of $Sp(2n,q)$ is $q^{n^2}\prod_{i=1}^n(q^{2i}-1)$.

With the aim of finding a cycle index for the symplectic groups, let us first understand their conjugacy classes. Given a a polynomial ϕ with coefficients in F_q and non vanishing constant term, define a polynomial $\bar{\phi}$ by:

$$\bar{\phi} = \frac{z^{m_\phi} \phi^q(\frac{1}{z})}{[\phi(0)]^q}$$

where ϕ^q raises each coefficient of ϕ to the qth power. Explicitly, a polynomial $\phi(z) = z^{m_\phi} + \alpha_{m_\phi-1} z^{m_\phi-1} + \cdots + \alpha_1 z + \alpha_0$ with $\alpha_0 \neq 0$ is sent to $\bar{\phi}(z) = z^{m_\phi} + (\frac{\alpha_1}{\alpha_0})^q z^{m_\phi-1} + \cdots + (\frac{\alpha_{m_\phi-1}}{\alpha_0})^q z + (\frac{1}{\alpha_0})^q$. The notation $\bar{\phi}$ breaks from Wall [35], in which $\tilde{\phi}$ was used, but these maps are different. Namely $\tilde{}$ is defined on polynomials with coefficients in F_q, but $\bar{}$ is defined on polynomials with coefficients in F_{q^2}. The distinction between the maps $\tilde{}$ and $\bar{}$ will be evident in the different statements of Theorems 9 and 11.

Wall [35] showed that a conjugacy class of $Sp(2n,q)$ corresponds to the following data. To each monic, non-constant, irreducible polynomial $\phi \neq z \pm 1$ associate a partition λ_ϕ of some non-negative integer $|\lambda_\phi|$. To ϕ equal to $z-1$ or $z+1$ associate a symplectic signed partition $\lambda_\phi^{\pm}$, by which is meant a partition of some natural number $|\lambda_\phi^{\pm}|$ such that the odd parts have even multiplicity, together with a choice of sign for the set of parts of size i for each even $i > 0$.

Example of a Symplectic Signed Partition

$$\begin{array}{cccccc}
 & \cdot & \cdot & \cdot & \cdot & \cdot \\
 & \cdot & \cdot & \cdot & \cdot & \cdot \\
+ & \cdot & \cdot & \cdot & \cdot & \\
 & \cdot & \cdot & \cdot & & \\
 & \cdot & \cdot & \cdot & & \\
- & \cdot & \cdot & & & \\
 & \cdot & \cdot & & &
\end{array}$$

Here the $+$ corresponds to the parts of size 4 and the $-$ corresponds to the parts of size 2. This data represents a conjugacy class of $Sp(2n,q)$ if and only if:

1. $|\lambda_z| = 0$
2. $\lambda_\phi = \lambda_{\bar{\phi}}$
3. $\sum_{\phi = z \pm 1} |\lambda_\phi^{\pm}| + \sum_{\phi \neq z \pm 1} |\lambda_\phi| m_\phi = 2n$

Wall computed the size of a conjugacy class corresponding to this data as:

$$\frac{|Sp(2n,q)|}{\prod_\phi B(\phi)}$$

where

$$B(\phi) = q^{[\sum_{h<i} h m_h(\lambda_\phi^{\pm}) m_i(\lambda_\phi^{\pm}) + \frac{1}{2}\sum_i (i-1) m_i(\lambda_\phi^{\pm})^2]} \prod_i A(\phi^{\pm,i}) \ if\ \phi = z \pm 1$$
$$B(\phi) = q^{m_\phi [\sum_{h<i} h m_h(\lambda_\phi) m_i(\lambda_\phi) + \frac{1}{2}\sum_i (i-1) m_i(\lambda_\phi)^2]} \prod_i A(\phi^i) \ if\ \phi \neq z \pm 1$$

and

$$
\begin{aligned}
A(\phi^{\pm,i}) &= |Sp(m_i(\lambda^{\pm}_{\phi}),q)| \ if \ i=1 \ (mod \ 2)\\
&= q^{\frac{m_i(\lambda^{\pm}_{\phi})}{2}}|O(m_i(\lambda^{\pm}_{\phi}),q)| \ if \ i=0 \ (mod \ 2)\\
A(\phi^{i}) &= |U(m_i(\lambda_{\phi}),q^{\frac{m_\lambda}{2}})| \ if \ \phi=\bar{\phi}\\
&= |GL(m_i(\lambda_{\phi}),q^{m_\lambda})|^{\frac{1}{2}} \ if \ \phi\neq\bar{\phi}.
\end{aligned}
$$

Here $O(m_i(\lambda_{\phi}),q)$ is the orthogonal group with the same sign as the sign associated to the parts of size i (see the upcoming treatment of the orthogonal groups in this section for more background on them). The quantity $B(\phi)$ will also be denoted by $c_{Sp,\phi,q^{m_\phi}}(\lambda^{\pm})$.

As an example, consider the set of symplectic transvections, i.e. determinant 1 elements of $Sp(2n,q)$ whose pointwise fixed space is $n-1$ dimensional. Fulman [9] uses direct counting arguments to show that there are a total of $q^{2n}-1$ symplectic transvections.

These symplectic transvections split into two conjugacy classes of size $\frac{q^{2n}-1}{2}$. Using the fact that the dimension of the fixed space of α is the number of parts of $\lambda^{\pm}_{z-1}(\alpha)$, one concludes that an element of $Sp(2n,q)$ is a symplectic transvection if and only if $\lambda_{z-1}(\alpha)$ is $(+2,1^{n-2})$ or $(-2,1^{n-2})$ and $|\lambda_{\phi}|=0$ for $\phi\neq z-1$. By Wall's class size formula, the sizes of these conjugacy classes are:

$$\frac{|Sp(2n,q)|}{q^{2n-\frac{3}{2}}|Sp(2n-2,q)|q^{\frac{1}{2}}|O^{\pm}(1,q)|}=\frac{q^{2n}-1}{2}$$

for both conjugacy classes. This confirms that there are $q^{2n}-1$ symplectic transvections.

As with the general linear and unitary groups define a cycle index for the symplectic groups by

$$1+\sum_{n=1}^{\infty}\frac{u^{2n}}{|Sp(2n,q)|}\sum_{\alpha\in Sp(2n,q)}\prod_{\phi=z\pm1}x_{\phi,\lambda^{\pm}_{\phi}(\alpha)}\prod_{\phi\neq z,z\pm1}x_{\phi,\lambda_{\phi}(\alpha)}$$

Theorem 12 will prove that this cycle index factors. For this Theorem 11, which counts polynomials invariant under the involution $\bar{}$, is essential. Let $\bar{I}_{m,q}$ be the number of monic irreducible polynomials ϕ of degree m with coefficients in F_q such that $\phi=\bar{\phi}$.

Lemma 10 $\overline{\phi_1\phi_2}=\bar{\phi}_1\bar{\phi}_2$.

Proof: From the definition of the involution $\bar{}$, the lemma reduces to the observation that $(\phi_1\phi_2)^q=(\phi_1^q)(\phi_2^q)$, where ^{q} is the map which raises each coefficient of a polynomial to the qth power. □

Theorem 11 *1. $\bar{I}_{1,q}=2$ and the two degree 1 polynomials such that $\phi=\bar{\phi}$ are $z\pm1$.*

2. If $m\neq1$ is odd, then $\bar{I}_{m,q}=0$.

3. If $m=2^r m_0$ is even, with m_0 odd, then $\bar{I}_{m,q}=\frac{1}{m}\sum_{d|m_0}\mu(d)(q^{\frac{m}{2d}}-1)$.

Proof: The method of proof is essentially the same as that used for the unitary groups in Theorem 9. Let M_m be the number of monic degree m polynomials (not necessarily irreducible) over F_q and let $\bar{M}_m$ be the number of monic degree m polynomials ϕ (not necessarily irreducible) over F_q such that $\phi(0)\neq0$ and $\phi=\bar{\phi}$. Define $A(t)=1+\sum_{m=1}^{\infty}M_m t^m$ and $B(t)=1+\sum_{m=1}^{\infty}\bar{M}_m t^m$. Note that

$A(t) = \frac{1}{1-qt}$ because $M_m = q^m$. On page 37 of Wall [35] it is noted that $B(t) = \frac{(1+t)^2}{1-qt^2}$ (this follows from the explicit description of the definition of $\bar{\phi}$.

Arguing exactly as for the unitary group in Theorem 9 gives:

$$\frac{B(t)^2}{A(t^2)} = (1-t^2)\prod_{m=0}^{\infty}(\frac{1+t^m}{1-t^m})^{\bar{I}_{m,q}}$$

Combining this with the explicit expressions for $A(t)$ and $B(t)$ given above yields:

$$\prod_{m=0}^{\infty}(\frac{1+t^m}{1-t^m})^{\bar{I}_{m,q}} = \frac{(1+t)^3}{(1-t)(1-qt^2)}$$

Take logarithms of both sides of this equation, using the expansions $log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + \cdots$ and $log(1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} + \cdots$.

The left-hand side becomes:

$$\sum_{m=0}^{\infty} 2\bar{I}_{m,q}(t^m + \frac{t^{3m}}{3} + \frac{t^{5m}}{5} + \cdots)$$

The right-hand side becomes:

$$4\sum_{m\ odd}\frac{t^m}{m} + 2\sum_{m\ even}\frac{t^m}{m}(q^{\frac{m}{2}}-1)$$

Comparing coefficients of t shows that $\bar{I}_{1,q} = 2$. Since $z-1$ and $z+1$ satisfy $\phi = \bar{\phi}$, these are the two degree 1 polynomials satisfying $\phi = \bar{\phi}$. The $\bar{I}_{m,q}$ are all non-negative and the odd degree terms on the right-hand side have been accounted for. Thus $\bar{I}_{m,q} = 0$ if $m \neq 1$ is odd.

Now suppose that m is even and write $m = 2^r m_0$ where m_0 is odd. The coefficient of t^m on the right-hand side is $\frac{2}{m}(q^{\frac{m}{2}}-1)$. The coefficient of t^m in the left-hand side is $\sum_{k|m_0} 2\frac{k}{m_0}\bar{I}_{2^r k,q}$. This gives the relation:

$$\sum_{k|m_0} k\bar{I}_{2^r k,q} = \frac{q^{2^{r-1}m_0}-1}{2^r}$$

It is straightforward to check that on the lattice of odd integers with divisibility as the inclusion relation, Moebius inversion holds in the sense that if $F(n) = \sum_{d|n} f(d)$ for all odd n, then $f(n) = \sum_{d|n}\mu(d)F(\frac{n}{d})$ for all odd n. Fix r and define functions on the lattice of odd integers by $F_r(n) = \frac{q^{2^{r-1}n}-1}{2^r}$ and $f_r(n) = n\bar{I}_{2^r n,q}$. The theorem follows by Moebius inversion. $\square$

It can now be seen that the cycle index for the symplectic groups factors.

Theorem 12

$$\begin{aligned}
&1 + \sum_{n=1}^{\infty}\frac{u^{2n}}{|Sp(2n,q)|}\sum_{\alpha\in Sp(2n,q)}\prod_{\phi=z\pm 1} x_{\phi,\lambda_{\phi}^{\pm}(\alpha)}\prod_{\phi\neq z,z\pm 1} x_{\phi,\lambda_\phi(\alpha)}\\
= &\prod_{\phi=z\pm 1}\sum_{\lambda^{\pm}} x_{\phi,\lambda^{\pm}}\frac{u^{|\lambda^{\pm}|}}{c_{Sp,\phi,q^{m_\phi}}(\lambda^{\pm})}\prod_{\substack{\phi=\bar{\phi}\\ \phi\neq z\pm 1}}\sum_{\lambda} x_{\phi,\lambda}\frac{(-(u^{m_\phi}))^{|\lambda|}}{c_{GL,z-1,-\sqrt{q^{m_\phi}}}(\lambda)}\\
&\prod_{\{\phi,\bar{\phi}\},\phi\neq\bar{\phi}}\sum_{\lambda} x_{\phi,\lambda}x_{\bar{\phi},\lambda}\frac{u^{2|\lambda|m_\phi}}{c_{GL,z-1,q^{m_\phi}}(\lambda)}
\end{aligned}$$

PROOF: Consider the coefficients of u^n on both sides when n is even. Their equality follows from Wall's formulas for conjugacy class sizes for the symplectic groups. We have also made use of the following elementary fact:

$$\frac{u^{|\lambda_\phi| m_\phi}}{q^{\frac{m_\phi}{2}[2\sum_{h<i} h m_h(\lambda_\phi) m_i(\lambda_\phi) + \sum_i (i-1) m_i(\lambda_\phi)^2]} \prod_i |U(m_i(\lambda_\phi), q^{\frac{m_\phi}{2}})|}$$
$$= \frac{(-(u^{m_\phi}))^{|\lambda_\phi|}}{(-(q^{\frac{m_\phi}{2}}))^{[2\sum_{h<i} h m_h(\lambda_\phi) m_i(\lambda_\phi) + \sum_i (i-1) m_i(\lambda_\phi)^2]} \prod_i |GL(m_i(\lambda_\phi), -(q^{\frac{m_\phi}{2}}))|}$$

which is true because $|U(n,q)| = (-1)^n |GL(n,-q)|$.

Consider the coefficients of u^n on both sides when n is odd. The coefficient on the left-hand side is 0. It thus suffices to show that only even powers of u appear in each term of the product on the right-hand side of the factorization. This is clear for polynomials ϕ such that $\phi \neq \bar{\phi}$. It is true for the polynomials $z \pm 1$ because all odd parts in the associated signed partitions have even multiplicity. Finally, Theorem 11 implies that all polynomials $\phi \neq z \pm 1$ such that $\phi = \bar{\phi}$ have even degree. So these polynomials contribute only even powers of u as well. □

The Orthogonal Groups

This article assumes for simplicity that the characteristic of F_q is not equal to 2. The orthogonal groups can be defined as subgroups of $GL(n,q)$ preserving a non-degenerate symmetric bilinear form (see Chapter 1 of Carter [4]). For $n = 2l+1$ odd, there are two such forms up to isomorphism, with inner product matrices A and δA, where δ is a non-square in F_q and A is equal to:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0_l & I_l \\ 0 & I_l & 0_l \end{pmatrix}$$

Denote the corresponding orthogonal groups by $O^+(2l+1,q)$ and $O^-(2l+1,q)$. This distinction will be useful, even though these groups are isomorphic. Their common order is:

$$2q^{l^2} \prod_{i=1}^{l} (q^{2i} - 1)$$

For $n = 2l$ even, there are again two non-degenerate symmetric bilinear forms up to isomorphism with inner product matrices:

$$\begin{pmatrix} 0_l & I_l \\ I_l & 0_l \end{pmatrix}$$

$$\begin{pmatrix} 0_{l-1} & I_{l-1} & 0 & 0 \\ I_{l-1} & 0_{l-1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -\delta \end{pmatrix}$$

where δ is a non-square in F_q. Denote the corresponding orthogonal groups by $O^+(2l,q)$ and $O^-(2l,q)$. They are not isomorphic and have orders:

$$2q^{l^2-l}(q^l \mp 1)\prod_{i=1}^{l-1}(q^{2i}-1)$$

To describe the conjugacy classes of the finite orthogonal groups, it is necessary to use the notion of the Witt type of a non-degenerate quadratic form, as in Chapter 9 of Bourbaki [3]. Call a non-degenerate form N null if the vector space V on which it acts can be written as a direct sum of 2 totally isotropic subspaces (a totally isotropic space is one on which the inner product vanishes identically). Define two non-degenerate quadratic forms Q' and Q to be equivalent if Q' is isomorphic to the direct sum of Q and a null N. The Witt type of Q is the equivalence class of Q under this equivalence relation. There are 4 Witt types over F_q, which Wall denotes by $\mathbf{0}, \mathbf{1}, \delta, \omega$, corresponding to the forms $0, x^2, \delta x^2, x^2 - \delta y^2$ where δ is a fixed non-square of F_q. These 4 Witt types form a ring, but only the additive structure is relevant here. The sum of two Witt types with representatives Q_1, Q_2 on V_1, V_2 is the equivalence class of $Q_1 + Q_2$ on $V_1 + V_2$.

Proposition 1 *The four orthogonal groups $O^+(2n+1,q), O^-(2n+1,q), O^+(2n,q), O^-(2n,q)$ arise from forms Q of Witt types $\mathbf{1}, \delta, \mathbf{0}, \omega$ respectively.*

PROOF: This follows from the explicit description above of the inner product matrices which give rise to the various orthogonal groups. □

Consider the following combinatorial data. To each monic, non-constant, irreducible polynomial $\phi \neq z \pm 1$ associate a partition λ_ϕ of some non-negative integer $|\lambda_\phi|$. To ϕ equal to $z-1$ or $z+1$ associate an orthogonal signed partition $\lambda_\phi^\pm$, by which is meant a partition of some natural number $|\lambda_\phi^\pm|$ such that all even parts have even multiplicity, and all odd $i > 0$ have a choice of sign. For $\phi = z-1$ or $\phi = z+1$ and odd $i > 0$, we denote by $\Theta_i(\lambda_\phi^\pm)$ the Witt type of the orthogonal group on a vector space of dimension $m_i(\lambda_\phi^\pm)$ and sign the choice of sign for i.

Example of an Orthogonal Signed Partition

$$\begin{array}{lllll} & \cdot & \cdot & \cdot & \cdot \\ & \cdot & \cdot & \cdot & \cdot \\ - & \cdot & \cdot & \cdot & \\ & \cdot & \cdot & & \\ & \cdot & \cdot & & \\ + & \cdot & & & \\ & \cdot & & & \end{array}$$

Here the $-$ corresponds to the part of size 3 and the $+$ corresponds to the parts of size 1.

Theorem 13, though not explicitly stated by Wall [35], is implicit in the discussion on pages 38-40 of his article. His statements seem different because he fixes an $\alpha \in GL(n,q)$ and asks which orthogonal groups contain a conjugate of α. Here we want to fix the group and parameterize its conjugacy classes. The polynomial $\bar{\phi}$ is defined as in the symplectic case.

Theorem 13 *The data $\lambda_{z-1}^\pm, \lambda_{z+1}^\pm, \lambda_\phi$ represents a conjugacy class of some orthogonal group if:*

1. $|\lambda_z| = 0$

2. $\lambda_\phi = \lambda_{\bar\phi}$

3. $\sum_{\phi=z\pm1} |\lambda_\phi^\pm| + \sum_{\phi\neq z\pm1} |\lambda_\phi| m_\phi = n$

In this case, the data represents the conjugacy class of exactly 1 orthogonal group $O(n,q)$, with sign determined by the condition that the group arises as the stabilizer of a form of Witt type:

$$\sum_{\phi=z\pm1}\sum_{i\ odd}\Theta_i(\lambda_\phi^\pm) + \sum_{\phi\neq z\pm1}\sum_{i\geq1} im_i(\lambda_\phi)\omega$$

The conjugacy class has size:

$$\frac{|O(n,q)|}{\prod_\phi B(\phi)}$$

where

$$\begin{aligned}
B(\phi) &= q^{[\sum_{h<i} hm_h(\lambda_\phi^\pm)m_i(\lambda_\phi^\pm)+\frac{1}{2}\sum_i(i-1)m_i(\lambda_\phi^\pm)^2]}\prod_i A(\phi^{\pm,i})\ if\ \phi = z\pm1\\
B(\phi) &= q^{m_\phi[\sum_{h<i} hm_h(\lambda_\phi)m_i(\lambda_\phi)+\frac{1}{2}\sum_i(i-1)m_i(\lambda_\phi)^2]}\prod_i A(\phi^{i})\ if\ \phi \neq z\pm1
\end{aligned}$$

and

$$\begin{aligned}
A(\phi^{\pm,i}) &= |O(m_i(\lambda_\phi^\pm),q)|\ if\ i=1\ (mod\ 2)\\
&= q^{-\frac{m_i(\lambda_\phi^\pm)}{2}}|Sp(m_i(\lambda_\phi^\pm),q)|\ if\ i=0\ (mod\ 2)\\
A(\phi^i) &= |U(m_i(\lambda_\phi),q^{\frac{m_\lambda}{2}})|\ if\ \phi=\bar\phi\\
&= |GL(m_i(\lambda_\phi),q^{m_\lambda})|^{\frac{1}{2}}\ if\ \phi\neq\bar\phi.
\end{aligned}$$

Here $O(m_i(\lambda_\phi),q)$ is the orthogonal group with the same sign as the sign associated to the parts of size i.

In the case $\phi = z\pm1$, $B(\phi)$ will also be denoted by $c_{O,\phi,q^{m_\phi}}(\lambda^\pm)$.

As an example of this formula, consider the set of orthogonal symmetries in $O^+(n,q)$ where n is odd (considerations for the other orthogonal groups are analogous). An orthogonal symmetry is a determinant -1 orthogonal map with an $n-1$ dimensional fixed space. Orthogonal symmetries are important because they generate the orthogonal group containing them (page 129 of Artin [2]). It is worth remarking that orthogonal transvections exist only in the characteristic 2 case, which is excluded here.

Fulman [9] counts the orthogonal symmetries in $O^+(n,q)$ directly, showing that there are q^{n-1} of them. The orthogonal symmetries in $O^+(n,q)$ fall into two conjugacy classes. These may be described in terms of Wall's combinatorial data. One conjugacy class corresponds to the data $\lambda_{z-1} = (+1^{n-1}), \lambda_{z+1} = (+1)$. The other conjugacy class corresponds to the data $\lambda_{z-1} = (-1^{n-1}), \lambda_{z+1} = (-1)$. This follows from Theorem 13 and the fact that the dimension of the fixed space of α is the number of parts of $\lambda_{z-1}^\pm(\alpha)$. So the class size formulas of Wall imply that the total number of orthogonal symmetries in $O^+(n,q)$ for n odd is:

$$\frac{|O^+(n,q)|}{q^{\frac{1}{2}(n-2)}|O^+(n-1,q)|q^{\frac{1}{2}}|O^+(1,q)|}+\frac{|O^+(n,q)|}{q^{\frac{1}{2}(n-2)}|O^-(n-1,q)|q^{\frac{1}{2}}|O^-(1,q)|}=q^{n-1}$$

In analogy with the general linear, unitary, and symplectic groups, define a cycle index for the orthogonal groups by:

$$\sum_{n=1}^{\infty}[\frac{u^n}{|O^+(n,q)|}\sum_{\alpha\in O^+(n,q)}\prod_{\phi=z\pm1}x_{\phi,\lambda_\phi^\pm(\alpha)}\prod_{\phi\neq z,z\pm1}x_{\phi,\lambda_\phi(\alpha)}]$$
$$+[\frac{u^n}{|O^-(n,q)|}\sum_{\alpha\in O^-(n,q)}\prod_{\phi=z\pm1}x_{\phi,\lambda_\phi^\pm(\alpha)}\prod_{\phi\neq z,z\pm1}x_{\phi,\lambda_\phi(\alpha)}]$$

Theorem 14 shows that the cycle index of the finite orthogonal groups factors.

Theorem 14

$$\sum_{n=1}^{\infty}[\frac{u^n}{|O^+(n,q)|}\sum_{\alpha\in O^+(n,q)}\prod_{\phi=z\pm1}x_{\phi,\lambda_\phi^\pm(\alpha)}\prod_{\phi\neq z,z\pm1}x_{\phi,\lambda_\phi(\alpha)}]$$
$$+[\frac{u^n}{|O^-(n,q)|}\sum_{\alpha\in O^-(n,q)}\prod_{\phi=z\pm1}x_{\phi,\lambda_\phi^\pm(\alpha)}\prod_{\phi\neq z,z\pm1}x_{\phi,\lambda_\phi(\alpha)}]$$
$$=\prod_{\phi=z\pm1}\sum_{\lambda^\pm}x_{\phi,\lambda^\pm}\frac{u^{|\lambda^\pm|}}{c_{O,\phi,q^{m_\phi}}(\lambda^\pm)}\prod_{\substack{\phi=\bar{\phi}\\ \phi\neq z\pm1}}\sum_{\lambda}x_{\phi,\lambda}\frac{(-(u^{m_\phi}))^{|\lambda|}}{c_{GL,z-1,-\sqrt{q^{m_\phi}}}(\lambda)}$$
$$\prod_{\{\phi,\bar{\phi}\},\phi\neq\bar{\phi}}\sum_{\lambda}x_{\phi,\lambda}x_{\bar{\phi},\lambda}\frac{u^{2|\lambda|m_\phi}}{c_{GL,z-1,q^{m_\phi}}(\lambda)}$$

Proof: The first equation follows from Theorem 13 since every term in the product on the right hand side corresponds to a conjugacy class in exactly one of the orthogonal groups, and the class sizes check. □

5 The $q\to\infty$ Limit of the Cycle Indices

At the end of his paper, Stong [32] stated that if one sets $x_{\phi,\lambda}=(x_{m_\phi})^{|\lambda|}$ in the cycle index of the general linear groups and lets $q\to\infty$, then one obtains the cycle index of the symmetric groups. Indeed, Lemma 2 from Section 2 shows that for fixed q the cycle index for GL becomes:

$$\prod_{m=1}^{\infty}\prod_{r=1}^{\infty}(\frac{1}{1-(\frac{u}{q^r})^m x_m})^{I_{m,q}}$$

where $I_{m,q}$ is the number of monic, degree m, irreducible $\phi\neq z$ defined over a field of q elements. Letting $q\to\infty$ and using the formula for $I_{m,q}$ (Lemma 1) gives:

$$lim_{q\to\infty}\prod_{m=1}^{\infty}\prod_{r=1}^{\infty}(\frac{1}{1-(\frac{u}{q^r})^m x})^{I_{m,q}}=\prod_{m=1}^{\infty}e^{\frac{x_m u^m}{m}}$$

This fact may also be stated as follows. Fix n. Then the $q \to \infty$ limit of the probability that the characteristic polynomial of a uniformly chosen element of $GL(n,q)$ factors into a_m irreducible polynomials of degree m is equal to the chance that a randomly chosen element of S_n has a_m m-cycles.

We now use algebraic groups to give a conceptual statement and proof of Stong's observation which generalizes to other groups. Dick Gross suggested that such an interpretation should exist and was kind enough to explain the basics of algebraic groups.

The necessary background about maximal tori in algebraic groups can all be found in Chapter 3 of Carter [5]. Let us review some of these facts. Take G to be a connected, reductive algebraic group over $\bar{F}_q$ which is Chevalley (this means that the Frobenius map giving rise to G^F is $x \to x^q$ where q is a prime power) such that G' is simply connected. Recall that a torus of G is a subgroup of G which is isomorphic to a product of copies of the multiplicative group of $\bar{F}_q$, and that a maximal torus of G is a maximal such subgroup. Any two maximal tori of G are conjugate in G.

A maximal torus of G^F is defined to be a group T^F where T is a maximal torus of G. As is discussed on pages 32-33 of Carter, the Lang-Steinberg theorem of algebraic groups implies that G^F has a maximal torus T^F which is diagonalizable over F_q (such a maximal torus is called maximally split). While it is true that all maximally split maximal tori T^F are conjugate in G^F, the maximal tori of G^F may fall into many conjugacy classes.

Proposition 3.3.3 of Carter says that under these conditions, there is a bijection Φ between G^F conjugacy classes of F-stable maximal tori in G and conjugacy classes of the Weyl group W. We recall the definition of Φ (the proof that it is a bijection is harder). Let T_0 be a fixed F-stable maximally split maximal torus of G (this exists by the Lang-Steinberg theorem). Since all maximal tori in G are conjugate to T_0, one can write $T =^g T_0$ for some $g \in G$ (the symbol ^{g} denotes conjugation by g). Clearly $g^{-1}F(g) \in N(T_0)$. Since $W = N(T_0)/T$, this associates to T an element of W, which turns out to be well defined up to conjugacy in W.

Next, one can define a map ω (similar to that in Lehrer [23]) from G^F to conjugacy classes of W. Given $\alpha \in G^F$, let α_s be the semi-simple part of α. Theorem 3.5.6 of Carter says that G' simply connected implies that $C_G(\alpha_s)$ is connected. Take T to be an F-stable maximal torus in $C_G(\alpha_s)$ such that T^F is maximally split. By what has been said before, all such T are conjugate in $C_G(\alpha_s)^F$ and hence in G^F. Define $\omega(\alpha) = \Phi(T)$.

In the case of $GL(n,q)$, the map ω sends an element α whose characteristic polynomial factors into a_m irreducible polynomials of degree m to the conjugacy class of S_n corresponding to permutations with a_m m-cycles.

Proposition 3.6.6 of Carter implies that for q sufficiently large, all maximal tori T^F of G^F lie in exactly 1 maximal torus of G (this condition is called non-degeneracy). For such q one can then define a a bijection Φ' between G^F conjugacy classes of maximal tori T^F of G^F and conjugacy classes of W by $\Phi'(T^F) = \Phi(T)$, where T is the unique maximal torus of G containing T^F.

We now prove the following theorem.

Theorem 15 *Let G be a connected, reductive Chevalley group which is defined over F_q, such that G' is simply connected. Suppose that as $q \to \infty$, the chance that an element of G^F is regular, semi-simple approaches 1. Then for all conjugacy classes c in W,*

$$\lim_{q \to \infty} P_{G^F}(\omega(\alpha) \in c) = P_W(w \in c)$$

where both probabilities are with respect to the uniform distribution.

PROOF: Take q large enough that all maximal tori of G^F are non-degenerate, so that the construction of Φ' works. From page 29 of Carter [5], a regular semi-simple element α of G lies in a unique maximal torus, which implies by non-degeneracy that α lies in a unique T^F. This also implies that $\omega(\alpha) = \Phi'(T^F)$. Therefore:

$$\begin{aligned}
\lim_{q\to\infty} P_{G^F}(\omega(\alpha)=c) &= \lim_{q\to\infty} \frac{|\{\alpha \ \mathit{regular\ semisimple} : \omega(\alpha)=c\}|}{|G^F|} \\
&= \lim_{q\to\infty} \sum_{T^F:\Phi'(T^F)=c} \frac{|\{\alpha \ \mathit{regular\ semisimple}, \alpha \in T^F\}|}{|G^F|} \\
&= \lim_{q\to\infty} \frac{|\{\alpha \ \mathit{regular\ semisimple}, \alpha \in T\}|}{|N_{G^F}(T^F)|}
\end{aligned}$$

Proposition 3.3.6 and Corollary 3.6.5 of Carter give that $N_{G^F}(T^F)/T^F$ is isomorphic to $C_W(w)$, so that:

$$|N_{G^F}(T^F)|/|T^F| = \frac{|W|}{|c|}$$

Therefore,

$$\lim_{q\to\infty} P_{G^F}(\omega(\alpha)=c) = \frac{|c|}{|W|} \lim_{q\to\infty} \frac{|\{\alpha \ \mathit{regular\ semisimple}, \alpha \in T^F\}|}{|T^F|}$$

Summing over the finitely many conjugacy classes c on both sides of this equation gives 1. Thus,

$$\lim_{q\to\infty} \frac{|\{\alpha \ \mathit{regular\ semisimple}, \alpha \in T^F\}|}{|T^F|} = 1$$

for all T^F, which proves the theorem. □

The heuristics at the end of Section 3 suggest that as $q \to \infty$, the chance that an element is regular semi-simple approaches 1. This should be directly checkable for the classical groups using the cycle indices (although the unitary group is not Chevalley so Theorem 15 does not apply). Some recent work of Lehrer [24] using l-adic cohomology gives involved expressions for the chance that an element of a finite group of Lie type is regular semisimple. It may be possible to read the $q \to \infty$ limit off of his results.

6 Application: The Characteristic Polynomial, Number of Jordan Blocks, and Average Order of an Element in a Finite Classical Group

This section applies the cycle indices of Section 4 to carry over work of Stong [32],[33] on the general linear groups to the unitary, symplectic, and orthogonal groups. In particular, we will study the characteristic polynomial, the number of Jordan blocks, and the average order of an element in a finite classical group. Other authors, notably Hansen [18] and Goh and Schmutz [15], have obtained interesting results about random matrices. The results of this section are an indication that the analogs of their theorems carry over to the other classical groups.

Application 1: The Characteristic Polynomial

This application will make use of the following theorem of Steinberg, which counts the number of unipotent elements (i.e. all eigenvalues equal to one) α in a finite classical group. Clearly α is unipotent if and only if its characteristic polynomial is a power of $z-1$. Steinberg's count is normally proven using the Steinberg character, as on page 156 of Humphreys [21]. Fulman [11] gives a probabilistic proof, at least for the general linear and unitary cases.

Theorem 16 *The number of unipotent elements in a finite group of Lie type G^F is the square of the order of a p-Sylow of G^F, where p is the prime used in the construction of G^F (in the case of the classical groups, p is the characteristic of F_q).*

The General Linear Groups Reiner [30] and Gerstenhaber [13] proved the following theorem counting elements of $GL(n,q)$ wight a given characteristic polynomial. Presumably Stong [32] knew how to do this using the cycle index, but we include a proof as one did not appear there.

Recall that if $f(u)$ is a polynomial in u^n, then the notation $[u^n]f(u)$ means the coefficient of u^n in $f(u)$.

Theorem 17 *Let ϕ be a monic polynomial of degree n which factors into irreducibles as $\phi = \prod_{i=1}^r \phi_i^{j_i}$. Then the number of elements of $GL(n,q)$ with characteristic polynomial ϕ is:*

$$|GL(n,q)| \prod_{i=1}^r \frac{q^{m_\phi j_i(j_i-1)}}{|GL(j_i, q^{m_\phi})|}$$

PROOF: In the cycle index for the general linear groups, set $x_{\phi,\lambda} = 1$ if $\phi = \phi_i$ and $|\lambda| = j_i$. Otherwise, set $x_{\phi,\lambda} = 0$. Taking coefficients of u^n shows that the number of elements of $GL(n,q)$ with characteristic polynomial ϕ is:

$$\begin{aligned} & |GL(n,q)|[u^n] \prod_{i=1}^r \sum_{\lambda:|\lambda|=j_i} \frac{u^{j_i(m_{\phi_i})}}{c_{GL,\phi,q^{m_\phi}}} \\ = & |GL(n,q)| \prod_{i=1}^r \sum_{\lambda:|\lambda|=j_i} \frac{1}{c_{GL,\phi,q^{m_\phi}}} \\ = & |GL(n,q)| \prod_{i=1}^r \frac{q^{m_\phi j_i(j_i-1)}}{|GL(j_i, q^{m_\phi})|} \end{aligned}$$

where the last equality uses the cycle index and Steinberg's count of unipotents (Theorem 16) which says that there are $q^{n(n-1)}$ unipotent elements in $GL(n,q)$. $\square$

The Unitary Groups Arguing as in the general linear case, but using the cycle index for the unitary groups leads to the following count of elements of $U(n,q)$ given a given characteristic polynomial.

Theorem 18 *Let ϕ be a monic polynomial of degree n which factors into irreducibles as $\phi = \prod_i \phi_i^{j_i} \prod_{i'} [\phi_{i'} \tilde{\phi}_{i'}]^{j_{i'}}$, where $\phi_i = \tilde{\phi}_i$ and $\phi_{i'} \neq \tilde{\phi}_{i'}$. Then the number of elements of $U(n,q)$ with characteristic polynomial ϕ is:*

$$|U(n,q)| \prod_i \frac{q^{m_{\phi_i} j_i(j_i-1)}}{|U(j_i, q^{m_{\phi_i}})|} \prod_{i'} \frac{q^{2m_{\phi_{i'}} j_{i'}(j_{i'}-1)}}{|GL(j_{i'}, q^{2m_{\phi_{i'}}})|}$$

The Symplectic Groups The statement for the symplectic groups, proved by the same technique as for the general linear and unitary groups, is as follows.

Theorem 19 *Let ϕ be a polynomial of degree 2n which factors into irreducibles as $(z-1)^{2a}(z+1)^{2b}\prod_i \phi_i^{j_i}\prod_{i'}[\phi_{i'}\bar{\phi_{i'}}]^{j_{i'}}$ where $\phi_{i'} \neq \bar{\phi_{i'}}$. Then the number of elements of $Sp(2n,q)$ with characteristic polynomial ϕ is:*

$$|Sp(2n,q)|\frac{q^{2a^2}}{|Sp(2a,q)|}\frac{q^{2b^2}}{|Sp(2b,q)|}\prod_i \frac{q^{\frac{m_{\phi_i}j_i(j_i-1)}{2}}}{|U(j_i,q^{\frac{m_{\phi_i}}{2}})|}\prod_{i'}\frac{q^{m_{\phi_{i'}}j_i(j_i-1)}}{|GL(j_i,q^{m_{\phi_{i'}}})|}$$

The Orthogonal Groups The corresponding statement for the orthogonal groups is somewhat more complicated, because the cycle index involved averaging over $O^+(n,q)$ and $O^-(n,q)$.

Theorem 20 *Let ϕ be a polynomial of degree n which factors into irreducibles as $(z-1)^a(z+1)^b\prod_i \phi_i^{j_i}\prod_{i'}[\phi_{i'}\bar{\phi_{i'}}]^{j_{i'}}$ where $\phi_{i'} \neq \bar{\phi_{i'}}$. Then $\frac{1}{2}$ of the sum of the proportion of elements in $O^+(n,q)$ and $O^-(n,q)$ with characteristic polynomial ϕ is:*

$$\frac{F(a)F(b)}{2}\prod_i \frac{q^{\frac{m_{\phi_i}j_i(j_i-1)}{2}}}{|U(j_i,q^{\frac{m_{\phi_i}}{2}})|}\prod_{i'}\frac{q^{m_{\phi_{i'}}j_i(j_i-1)}}{|GL(j_i,q^{m_{\phi_{i'}}})|}$$

where:

$$\begin{aligned} F(n) &= \frac{q^{\frac{n^2}{2}}}{|Sp(n,q)|} \ if \ n=0 \ (mod\ 2) \\ &= \frac{q^{\frac{(n-1)^2}{2}}}{|Sp(n-1,q)|} \ if \ n=1 \ (mod\ 2) \end{aligned}$$

Application 2: Number of Jordan Blocks

For $\alpha \in Mat(n,q)$, let $X_n(\alpha)$ be the number of irreducible polynomials counted with multiplicity occurring in the rational canonical form of α. (This is not quite the number of Jordan blocks, but is in the limit that $q \to \infty$). This application uses the cycle index to study $X_n(\alpha)$ where α is an element of a finite classical group. In fact only the mean of X_n will be computed, but the more analytically inclined should be able to compute the variance and prove asymptotic normality using the cycle index.

General Linear Groups The work has been done already in this case. Stong [32] proves that the random variable X_n has mean and variance $log(n)+O(1)$. Goh and Schmutz [15] prove that X_n is asymptotically normal.

We give a somewhat simpler computation of the mean, both to illustrate the elegance of the cycle index approach, and because the same technique works for the other classical groups.

Lemma 11

$$\sum_{n=0}^{\infty}(1-u)u^n\sum_{\alpha\in GL(n,q)}x^{X_n(\alpha)} = \prod_{m=1}^{\infty}\prod_{i=1}^{\infty}\left(\frac{1-(\frac{u}{q^i})^m}{1-(\frac{u}{q^i})^m x}\right)^{I_{m,q}}$$

PROOF: Set $x_{\phi,\lambda} = x^{|\lambda|}$ for all polynomials ϕ. The result follows from Lemma 2 in Section 2. □

The mean of X_n is now easily computed.

Theorem 21 *$EX_n = log(n) + O(1)$, where the expectation is taken over the group $GL(n,q)$ with q fixed.*

PROOF: Differentiating both sides of the generating function of Lemma 11 with respect to x and then setting $x = 1$ gives:

$$\begin{aligned} EX_n &= [u^n]\frac{1}{1-u}\sum_{m=1}^{\infty} I_{m,q}\sum_{i=1}^{\infty}\sum_{l=1}^{\infty}\frac{u^{ml}}{q^{iml}} \\ &= \sum_{r=1}^{n}(\sum_{m|r} I_{m,q})(\sum_{i=1}^{\infty}\frac{1}{q^{ri}}) \end{aligned}$$

It is well known that $I_{m,q} = \frac{q^m}{m} + O(q^{\frac{m}{2}})$, from which it follows that $\sum_{m|r} I_{m,q} = \frac{q^r}{r} + O(q^{\frac{r}{2}})$. Therefore:

$$\begin{aligned} EX_n &= \sum_{r=1}^{n}\sum_{i=1}^{\infty}\frac{1}{q^{ri}}(\frac{q^r}{r} + O(q^{\frac{r}{2}})) \\ &= \sum_{r=1}^{n}\frac{1}{r} + O(q^{-\frac{r}{2}}) \\ &= (\sum_{r=1}^{n}\frac{1}{r}) + O(1) \\ &= log(n) + O(1) \end{aligned}$$

□

The Unitary Groups The same technique works for the unitary groups.

Lemma 12

$$\sum_{n=0}^{\infty}(1-u)u^n \sum_{\alpha \in U(n,q)} x^{X_n(\alpha)} = \prod_{\substack{m=1 \\ m\ odd}}^{\infty}\prod_{i=1}^{\infty}(\frac{1+(-1)^i(\frac{u^m}{q^{im}})}{1+(-1)^i(\frac{u^m}{q^{im}})x})^{\tilde{I}_{m,q^2}} \prod_{m=1}^{\infty}\prod_{i=1}^{\infty}(\frac{1-(\frac{u^{2m}}{q^{2im}})}{1-(\frac{u^{2m}}{q^{2im}})x^2})^{\frac{I_{m,q^2}-\tilde{I}_{m,q^2}}{2}}$$

PROOF: Proceed as in Lemma 11. □

Theorem 22 *$EX_n = \frac{3}{2}log(n) + O(1)$, where the expectation is taken over the group $U(n,q)$ with q fixed.*

PROOF: Differentiating both sides of the generating function of Lemma 12 with respect to x and setting $x = 1$ gives:

$$\begin{aligned} EX_n &= [u^n]\frac{1}{1-u}[\sum_{\substack{m=1 \\ m\ odd}}^{\infty} \tilde{I}_{m,q^2}\sum_{i=1}^{\infty}\sum_{l=1}^{\infty}(-1)^{(i+1)(l+1)}\frac{u^{ml}}{q^{iml}}] + [\sum_{m=1}^{\infty}(I_{m,q^2} - \tilde{I}_{m,q^2})\sum_{i=1}^{\infty}\sum_{l=1}^{\infty}\frac{u^{2ml}}{q^{2iml}}] \\ &= [\sum_{r=1}^{n}\sum_{\substack{m|r \\ m\ odd}} \tilde{I}_{m,q^2}\sum_{i=1}^{\infty}(-1)^{(i+1)(\frac{r}{m}+1)}\frac{1}{q^{ri}}] + [\sum_{\substack{r=1 \\ r\ even}}^{n}\sum_{m|\frac{r}{2}}(I_{m,q^2} - \tilde{I}_{m,q^2})\sum_{i=1}^{\infty}\frac{1}{q^{ri}}] \end{aligned}$$

Recall from Theorem 9 that $\tilde{I}_{m,q^2} = \frac{q^m}{m} + O(q^{\frac{m}{2}})$ for m odd. We also know that $I_{m,q^2} = \frac{q^{2m}}{m} + O(q^m)$. Thus the dominant contribution from the first bracketed term comes from $m = r, i = 1, l = 1$, and the dominant contribution from the second bracketed term comes from $m = \frac{r}{2}, i = 1, l = 1$. Therefore,

$$\begin{aligned} EX_n &= [\sum_{\substack{r=1 \\ r\ odd}}^{n} \frac{1}{r} + O(1)] + [\sum_{\substack{r=1 \\ r\ even}}^{n} \frac{1}{\frac{r}{2}} + O(1)] \\ &= \sum_{r=1}^{n} \frac{1}{r} + \frac{1}{2}\sum_{r=1}^{\frac{n}{2}} \frac{1}{r} + O(1) \\ &= \frac{3}{2} log(n) + O(1) \end{aligned}$$

□

The Symplectic Groups As with the general linear and unitary groups, let $X_{2n}(\alpha)$ be the number of irreducible polynomials counted with multiplicity in the Jordan canonical form of $\alpha \in Sp(2n, q)$. Lemma 13 gives a generating function for $X_{2n}(\alpha)$.

Lemma 13

$$\begin{aligned} \sum_{n=0}^{\infty}(1-u)u^{2n}\frac{1}{|Sp(2n,q)|}\sum_{\alpha \in Sp(2n,q)} x^{X_{2n}(\alpha)} &= \prod_{i=1}^{\infty}(\frac{1-\frac{u^2}{q^{2i-1}}}{1-\frac{(ux)^2}{q^{2i-1}}})^2 \prod_{\substack{m=1 \\ m\ even}}^{\infty}\prod_{i=1}^{\infty}(\frac{1+(-1)^i(\frac{u^m}{q^{\frac{im}{2}}})}{1+(-1)^i(\frac{(ux)^m}{q^{\frac{im}{2}}})})^{\bar{I}_{m,q}} \\ & \prod_{m=1}^{\infty}\prod_{i=1}^{\infty}(\frac{1-\frac{u^{2m}}{q^{im}}}{1-\frac{(ux)^{2m}}{q^{im}}})^{\frac{I_{m,q}-\bar{I}_{m,q}}{2}} \end{aligned}$$

PROOF: This follows immediately from the cycle index for the symplectic groups. □

With Lemma 13, the mean of X_{2n} over $Sp(2n, q)$ is straightforward to compute.

Theorem 23 $EX_{2n} = \frac{3}{2} logn + O(1)$

PROOF: Differentiating both sides of the generating function of Lemma 13 with respect to x and then setting $x = 1$ gives:

$$\begin{aligned} EX_{2n} &= \sum_{r=1}^{n}[u^{2r}]((2\sum_{i=1}^{\infty}\frac{\frac{2u}{q^{2i-1}}}{1-\frac{u^i}{q^{2i-1}}}) + (\sum_{\substack{m=1 \\ m\ even}}^{\infty}\bar{I}_{m,q}\sum_{i=1}^{\infty}\sum_{l=1}^{\infty}(-1)^{(i+1)(l+1)}\frac{u^{ml}}{q^{\frac{iml}{2}}}) \\ &= \qquad +(\sum_{m=1}^{\infty}(I_{m,q}-\bar{I}_{m,q})\sum_{i=1}^{\infty}\sum_{l=1}^{\infty}\frac{u^{2ml}}{q^{iml}})) \end{aligned}$$

The term coming from the first sum is $O(1)$. By Theorem 11, $\bar{I}_{m,q} = \frac{q^{\frac{m}{2}}}{m} + O(q^{\frac{m}{4}})$ for m even. We also know that $I_{m,q} = \frac{q^m}{m} + O(q^{\frac{m}{2}})$. The dominant contribution to $[u^{2r}]$ from the second and third sums comes from $m = 2r, i = 1, l = 1$ and $m = r, i = 1, l = 1$ respectively. Thus,

$$\begin{aligned} EX_{2n} &= [\sum_{r=1}^{n} \frac{1}{2r}] + [\sum_{r=1}^{n} \frac{1}{r}] + O(1) \\ &= \frac{3}{2} logn + O(1) \end{aligned}$$

□

The Orthogonal Groups As with the other classical groups, let $X_n(\alpha)$ be the number of irreducible polynomials counted with multiplicity in the Jordan canonical form of $\alpha \in O(n,q)$.

Lemma 14

$$\begin{aligned} \sum_{n=0}^{\infty} (\frac{1-u}{1+u}) u^n [\sum_{\alpha \in O^+(n,q)} \frac{x^{X_n(\alpha)}}{|O^+(n,q)|} + \sum_{\alpha \in O^-(n,q)} \frac{x^{X_n(\alpha)}}{|O^-(n,q)|}] &= (\frac{1+ux}{1+u} \prod_{i=1}^{\infty} \frac{1-\frac{u^2}{q^{2i-1}}}{1-\frac{(ux)^2}{q^{2i-1}}})^2 \\ & \prod_{\substack{m=1 \\ m\ even}}^{\infty} \prod_{i=1}^{\infty} (\frac{1+(-1)^i \frac{u^m}{q^{\frac{im}{2}}}}{1+(-1)^i \frac{(ux)^m}{q^{\frac{im}{2}}}})^{\bar{I}_{m,q}} \\ & \prod_{m=1}^{\infty} \prod_{i=1}^{\infty} (\frac{1-\frac{u^{2m}}{q^{im}}}{1-\frac{(ux)^{2m}}{q^{im}}})^{\frac{I_{m,q}-\bar{I}_{m,q}}{2}} \end{aligned}$$

PROOF: This follows from the cycle index for the orthogonal groups. □

Let EX_n be $\frac{1}{2}$ of the sum of the averages of X_n over $O^+(n,q)$ and $O^-(n,q)$.

Theorem 24 $EX_n = \frac{3}{2} log(n) + O(1)$

PROOF: To compute EX_n differentiate both sides and set $x=1$ in:

$$[u^n] \frac{1+u}{2(1-u)} (\frac{1+ux}{1+u} \prod_{i=1}^{\infty} \frac{1-\frac{u^2}{q^{2i-1}}}{1-\frac{(ux)^2}{q^{2i-1}}})^2 \prod_{\substack{m=1 \\ m\ even}}^{\infty} \prod_{i=1}^{\infty} (\frac{1+(-1)^i \frac{u^m}{q^{\frac{im}{2}}}}{1+(-1)^i \frac{(ux)^m}{q^{\frac{im}{2}}}})^{\bar{I}_{m,q}} \prod_{m=1}^{\infty} \prod_{i=1}^{\infty} (\frac{1-\frac{u^{2m}}{q^{im}}}{1-\frac{(ux)^{2m}}{q^{im}}})^{\frac{I_{m,q}-\bar{I}_{m,q}}{2}}$$

The first product contributes $O(1)$, so that:

$$EX_n = \sum_{r=1}^{n} \frac{[u^r]+[u^{r-1}]}{2} ((\sum_{\substack{m=1 \\ m\ even}}^{\infty} \bar{I}_{m,q} \sum_{i=1}^{\infty} \sum_{l=1}^{\infty} (-1)^{(i+1)(l+1)} \frac{u^{ml}}{q^{\frac{iml}{2}}}) + (\sum_{m=1}^{\infty} (I_{m,q} - \bar{I}_{m,q}) \sum_{i=1}^{\infty} \sum_{l=1}^{\infty} \frac{u^{2ml}}{q^{iml}}))$$

This proves the theorem by the same logic as in Theorem 23. □

Application 3: The Average Order

Let $v_{GL,n}$ be the average over $GL(n,q)$ of the order of an element of $GL(n,q)$. Stong [33] shows that for fixed q and growing n, $log(v_{GL,n}) = nlog(q) - log(n) + o(log(n))$. The lower bound in the equality was not difficult; the upper bound was hard.

In what follows we compute lower bounds for the other classical groups. Presumably these bounds give the correct answer, as in the general linear case. The involutions $\tilde{}$ and $\bar{}$ on polynomials are defined as in Section 4. We also use the notation that $\Phi(n)$ is the number of i between 1 and n inclusive, which are relatively prime to n.

The Unitary Groups Let $v_{U,n}$ be the average over $U(n,q)$ of the order of an element of $U(n,q)$. It will be shown that for fixed q and growing n, $log(v_{U,n}) \geq nlog(q) - log(n) + o(log(n))$.

From basic field theory the roots of an irreducible polynomial ϕ of degree n over F_{q^2} are an orbit of some β in a degree n extension over F_{q^2} under the Frobenius map $x \rightarrow x^{q^2}$. The next two lemmas are useful.

Lemma 15 *Let L be a degree n extension of F_{q^2}, where n is odd. Then an element β of order q^n+1 in the multiplicative group of L corresponds to an irreducible polynomial ϕ of degree n such that $\phi = \tilde{\phi}$.*

PROOF: First note that the irreducible polynomial ϕ which β gives rise to has degree n. Indeed, suppose that β lies in some proper subfield K of L. Let c be the extension degree of K over F_{q^2}. Then $q^n+1|q^{2c}-1$ and $c<n$. However $c|n$, since L contains K. This is a contradiction.

Next, we show that $\phi = \tilde{\phi}$. Lemma 9 implies that the roots of $\tilde{\phi}$ are $(\frac{1}{\beta})^{q^{2i+1}}$ where $0 \leq i \leq n-1$. Taking $i = \frac{n-1}{2}$ shows that β is a root of $\tilde{\phi}$, so that $\phi = \tilde{\phi}$. □

Lemma 16 *Let L be a degree n extension of F_{q^2}, where n is even. Then an element β of order q^n-1 in the multiplicative group of L corresponds to an irreducible polynomial ϕ of degree $\frac{n}{2}$ such that $\phi \neq \tilde{\phi}$.*

PROOF: Since the order of β is q^n-1, the smallest extension of F_{q^2} containing β is of degree $\frac{n}{2}$. Thus the irreducible polynomial ϕ which β gives rise to has degree $\frac{n}{2}$.

Suppose to the contrary that $\phi = \tilde{\phi}$. Then $\beta = (\frac{1}{\beta})^{q^{2i+1}}$ for some i between 0 and $\frac{n}{2}-1$. Thus the order of β divides q^c+1 for some c between 1 and $n-1$. This is a contradiction, so that $\phi \neq \tilde{\phi}$. □

Theorem 25 *For fixed q and growing n, $log(v_{U,n}) \geq nlog(q) - log(n) + o(log(n))$.*

PROOF: If n is odd, then there are $\frac{\Phi(q^n+1)}{n}$ irreducible polynomials ϕ of degree n such that $\phi = \tilde{\phi}$ and the associated β has order q^n+1. This follows from Lemma 15 and the fact that the elements of order q^n+1 in L are precisely the $\Phi(q^n+1)$ generators of the unique order q^n+1 cyclic subgroup of the multiplicative group of L.

Any α with such a ϕ as its characteristic polynomial has order q^n+1 and by Theorem 18, the number of unitary matrices with such a characteristic polynomial ϕ is:

$$\frac{|U(n,q)|}{q^n+1}$$

Thus for n odd, $v_n \geq \frac{\Phi(q^n+1)}{n}$. From Stong [33] $log(\Phi(N)) = log(N) + O(log(log(N)))$, so that $log(v_n) \geq nlog(q) - log(n) + O(log(log(n)))$.

Suppose that n is even. By Lemma 16 there are $\frac{\Phi(q^n-1)}{\frac{n}{2}}$ polynomials ϕ of degree $\frac{n}{2}$ such that $\phi \neq \tilde{\phi}$ and the associated β has order q^n-1. Thus there are $\frac{\Phi(q^n-1)}{n}$ such pairs $\phi\tilde{\phi}$. Any α with $\phi\tilde{\phi}$ as its characteristic polynomial has order q^n-1 and by Theorem 18, the number of unitary matrices with such a characteristic polynomial is:

$$\frac{|U(n,q)|}{q^n-1}$$

So the result follows as in the case of n odd. $\Box$

The Symplectic Groups Let $v_{Sp,2n}$ be the average over $Sp(2n,q)$ of the order of an element of $Sp(2n,q)$. It will be shown that for fixed q and growing n, $log(v_{Sp,2n}) \geq nlog(q) - log(n) + o(log(n))$. The approach is similar to that used for the unitary groups.

Recall from field theory that an irreducible polynomial of degree n over F_q corresponds to the orbit of some β in a degree n extension over F_q under the Frobenius map $x \rightarrow x^q$.

Lemma 17 *Let L be a degree $2n$ extension of F_q. Then an element β of order q^n+1 in the multiplicative group of L corresponds to an irreducible polynomial ϕ of degree $2n$ such that $\phi = \bar{\phi}$.*

PROOF: Note that the irreducible polynomial ϕ which β gives rise to has degree $2n$. Suppose to the contrary that β lied in K, a proper subfield of L. Letting c denote the extension degree of K over F_q, we have that $q^n+1|q^c-1$, where $c|2n$ and $c<2n$. This is a contradiction.

By Lemma 10, the roots of $\bar{\phi}$ are $(\frac{1}{\beta})^{q^i}$ where $1 \leq i \leq 2n$. Taking $i=n$ shows that β is a root of $\bar{\phi}$. Thus $\phi = \bar{\phi}$. $\Box$

Let $\Phi(n)$ be the number of i between 1 and n inclusive which are relatively prime to n.

Theorem 26 *For fixed q and growing n, $log(v_{Sp,2n}) \geq nlog(q) - log(n) + o(log(n))$.*

PROOF: From Lemma 17, there are $\frac{\Phi(q^n+1)}{2n}$ irreducible polynomials ϕ of degree $2n$ such that the associated β has order q^n+1. This is because the elements of order q^n+1 in L are the $\Phi(q^n+1)$ generators of the order q^n+1 cyclic subgroup of the multiplicative group of L.

By Theorem 19, the number of elements of $Sp(2n,q)$ with characteristic polynomial ϕ is:

$$\frac{|Sp(2n,q)|}{q^n+1}$$

So considering only such α gives the lower bound $v_{Sp,2n} \geq \frac{\Phi(q^n+1)}{2n}$. Using the fact from Stong [33] that $log(\Phi(N)) = log(N) + O(log(log(N)))$ proves the theorem. $\Box$

The Orthogonal Groups

Let $v_{O,n}$ be one half of the sum of the average orders of elements of $O^+(n,q)$ and $O^-(n,q)$.

Theorem 27 *For fixed q and growing n, $log(v_{O,n}) \geq \frac{n}{2}log(q) - log(n) + o(log(n))$.*

PROOF: Assume that n is even (the case of n odd being similar), and consider only orthogonal matrices α whose characteristic polynomial comes from a β of order $q^{\frac{n}{2}}+1$ in a degree n extension of F_q. Then use Lemma 17 and Theorem 20 and argue as in Theorem 26. $\Box$

7 Suggestions for Future Research

1. Read information off of the cycle indices for the classical groups. For instance extend Goh and Schmutz's [15] theorem that the number of Jordan blocks is asymptotically normal to the other classical groups. Give upper bounds for the average order of an element of a unitary, symplectic, or orthogonal matrix. Carry over the asymptotic work on semisimple, regular, and regular-semisimple elements in the general linear groups.

2. Study the cycle indices for the characteristic 2 cases for the symplectic and orthogonal groups. One can deduce from Wall [35] that these also factor and that results analogous to Theorem 11 go through.

3. Find Lie Algebra cycle indices. For instance Stong's cycle index for $Mat(n,q)$ (see Section 2) encodes the orbits of the adjoint action of $GL(n,q)$ on its Lie Algebra. Are there factorizations for the other classical groups as well?

8 Acknowledgements

This work is taken from the author's Ph.D. thesis, done under the supervision of Persi Diaconis at Harvard University. The author is deeply indebted to him for emphasizing the importance of cycle indices and much helpful advice. The author also thanks Dick Gross for patiently explaining the basics of algebraic groups. This research was done under the generous 3-year support of the National Defense Science and Engineering Graduate Fellowship (grant no. DAAH04-93-G-0270) and the support of the Alfred P. Sloan Foundation Dissertation Fellowship.

References

[1] Andrews, G., The theory of partitions. Encyclopedia of Mathematics and its Applications, Vol. 2. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1976.

[2] Artin, E., Geometric algebra. Interscience Publishers, 1957.

[3] Bourbaki, N., Formes sesqulineaires et formes quadratiques (Elements de Mathematique I, livre II), Hermann (Paris), 1959.

[4] Carter, R., Simple groups of lie type. John Wiley and Sons, 1972.

[5] Carter, R., Finite groups of lie type: Conjugacy classes and characters. John Wiley and Sons, 1975.

[6] Dieudonne, J., Sur les groupes classiques. Hermann, Paris 1967.

[7] Fine, N.J. and Herstein, I. N., The probability that a matrix is nilpotent, Illinois J. Math. 2 (1958), 499-504.

[8] Fleischmann, P. and Janiszczak, I., The number of regular semisimple elements for Chevalley groups of classical type. J. Algebra, 155 (1993), no. 2, 482-528.

[9] Fulman, J., Probability in the classical groups over finite fields: symmetric functions, stochastic algorithms, and cycle indices, Ph.D. Thesis, Harvard University, 1997.

[10] Fulman, J., The Rogers-Ramanujan identities, the finite general linear groups, and the Hall-Littlewood polynomials, preprint.

[11] Fulman, J., A probabilistic approach toward the finite general linear and unitary groups, preprint.

[12] Fulman, J., Probabilistic measures and algorithms arising from the Macdonald symmetric functions, preprint.

[13] Gerstenhaber, M., On the number of nilpotent matrices with coefficients in a finite field, Illinois J. Math. 5 (1961), 330-333.

[14] Goh, W. and Schmutz, E., The expected order of a random permutation, Bulletin London Math. Soc. 23 (1991), no. 1, 34-42.

[15] Goh, W. and Schmutz, E., A central limit theorem on $GL_n(F_q)$, Preprint. Department of Math. Drexel University.

[16] Goldman, J. and Rota,G-C., On the foundations of combinatorial theory IV: Finite vector spaces and eulerian generating functions. Studies in Applied Mathematics. Vol. XLIX No. 3. September 1970.

[17] Goncharov, V., Du domaine d'analyse combinatoire, Bull. Acad. Sci. URSS Ser. Math 8 (1944), 3-48; Amer. Math. Soc. Transl. 19 (1950).

[18] Hansen, J. and Schmutz, E., How random is the characteristic polynomial of a random matrix? Math. Proc. Cambridge Philos. Soc. 114 (1993), no. 3, 507-515.

[19] Hardy, G.H. and Wright, E.M., An introduction to the theory of numbers. Fifth edition. Oxford Science Publications, 1979.

[20] Herstein, I.N., Topics in algebra. Second edition. Xerox College Publishing, Lexington, Mass.-Toronto, Ont., 1975.

[21] Humphreys, J., Conjugacy classes in semisimple algebraic groups. Mathematical Surveys and Monographs, 43. American Mathematical Society, Providence, RI 1995.

[22] Kung, J., The cycle structure of a linear transformation over a finite field, Linear Algebra Appl. 36 (1981), 141-155.

[23] Lehrer, G., Rational tori, semisimple orbits and the topology of hyperplane complements. Comment. Math. Helvetici 67 (1992), 226-251.

[24] Lehrer, G., The cohomology of the regular semisimple variety, Preprint.

[25] Lloyd, S.P. and Shepp, L.A., Ordered cycle lengths in a random permutation, Trans. Amer. Math. Soc. 121, 1966, 340-357.

[26] Macdonald, I.G., Symmetric functions and Hall polynomials, Second Edition. Claredon Press, Oxford. 1995.

[27] Neumann, P.M. and Praeger, C.E. Cyclic matrices over finite fields. J. London Math. Soc. (2) 52 (1995) 263-284.

[28] Neumann, P.M. and Praeger, C.E. Cyclic matrices in classical groups over finite fields, preprint, 11/1995.

[29] Polya, G. and Read, R.C., Combinatorial enumeration of groups, graphs, and chemical compounds. Springer-Verlag, New York-Berlin, 1987.

[30] Reiner, I., On the number of matrices with given characteristic polynomial. Illinois J. Math. 5, 1961, 324-329.

[31] Steinberg, R., Regular elements of semisimple algebraic groups. R. Publ. Math. Inst. Hautes Etudes Sci. 25 (1965) 49-80.

[32] Stong, R., Some asymptotic results on finite vector spaces, Advances in Applied Mathematics 9, 167-199 (1988).

[33] Stong, R., The average order of a matrix. Journal of Combinatorial Theory, Series A. Vol. 64, No. 2, November 1993.

[34] Suzuki, M. Group Theory I. Springer-Verlag, 1982.

[35] Wall, G.E., On conjugacy classes in the unitary, symplectic, and orthogonal groups, Journal of the Australian Mathematical Society 3 (1963), 1-63.