Probability in the Classical Groups over Finite Fields:

Symmetric Functions, Stochastic Algorithms, and Cycle Indices

A thesis presented by

Jason Edward Fulman

to

The Department of Mathematics

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in the subject of

Mathematics

Harvard University

Cambridge, Massachusetts

April, 1997

Acknowledgements

Above all I am grateful to my thesis advisor, Persi Diaconis, for giving me a fantastic thesis problem and area of mathematics to work in. It is impossible to overstate the value of his intuition and advice, or the influence his guidance has had on me. The math in this thesis evolved from discussions with him. He was also immensely helpful in the arduous task of editing this thesis. Equally important was his personal warmth and unique way of making mathematics concrete and unintimidating. To Persi Diaconis: a heartfelt thanks.

Dick Gross has also been a good mentor for me. His enthusiasm and energy continue to be inspiring. He patiently outlined to me the essentials of algebraic groups and encouraged me to think in those terms.

I learned from conversations with Arkady Berenstein, Anatol N. Kirillov, Ken Fan, and Ed Frenkel about mathematics relevant to this thesis. I also want to thank Noam Elkies, Ira Gessel, Barry Mazur, and Richard Stanley for being accessible and suggesting other possible problems. This encouragement meant a lot to me. Tal Kubo was always willing to talk, and Jared Wunsch was helpful with Mathematica.

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 in my final year. These grants freed me from financial constraints and gave me the time to become fully immersed in my work. I am also grateful to Donna D'Fini for on many occasions going far beyond the call of her job in simplifying the administrative aspect of my life.

Finally, I thank my parents for their practical advice and support, infinite devotion and patience, and help in choosing my mentors wisely.

Notation

Here is some notation which will be frequently used throughout this thesis. Precise definitions will come later.

Notation about Finite Fields and Polynomials:

F_q Finite field of size q

$\bar{F}_q$ The algebraic closure of F_q

$\phi(z)$ A polynomial over a finite field

$\Phi(n)$ The number of integers between 1 and n inclusive relatively prime to n

m_ϕ The degree of ϕ

$\tilde{\phi}$ The image of ϕ under the involution $\tilde{}$

$\bar{\phi}$ The image of ϕ under the involution $\bar{}$

$I_{m,q}$ The number of monic, non-constant, degree m irreducible $\phi \neq z$ with coefficients in F_q

$\tilde{I}_{m,q}$ The number of monic, non-constant, degree m irreducible ϕ with non-0 constant term, coefficients in F_q and invariant under $\tilde{}$

$\bar{I}_{m,q^2}$ The number of monic, non-constant, degree m irreducible ϕ with non-0 constant term, coefficients in F_{q^2} and invariant under $\bar{}$

$[u^n]$ The coefficient of u^n in some polynomial expression

Notation about Partitions and Tableaux:

$\lambda \vdash |\lambda|$ A partition of some non-integer $|\lambda|$ into parts $\lambda_1 \geq \lambda_2 \geq \cdots$

λ_ϕ A partition corresponding to a polynomial ϕ in the rational canonical form of some element

$\lambda_\phi^\pm$ A symplectic or orthogonal signed partition

$m_i(\lambda)$ The number of parts of λ of size i

λ' The partition dual to λ in the sense that $\lambda_i' = m_i(\lambda) + m_{i+1}(\lambda) + \cdots$

$n(\lambda)$ The quantity $\sum_{i\geq 1}(i-1)\lambda_i$

$P_\lambda(x; q, t)$ The Macdonald symmetric function corresponding to λ

$P_{x,y,q,t}(\lambda)$ A measure on partitions coming from the Macdonald symmetric functions

T A Young tableau

Notation about q-analogs:

$[n]$ The q analog of n, i.e. $1 + q + \cdots + q^{n-1}$

$[n]\mathbf{!}$ The q-analog of $n!$, i.e. $[1][2]\cdots[n]$

$\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]$ The q-analog of the binomial coefficient, i.e. $\frac{[n]!}{[k]![n-k]!}$

$(x)_i$ This is $(1-x)(1-\frac{x}{q})\cdots(1-\frac{x}{q^{i-1}})$

$(x,q)_\infty$ This is $(1-x)(1-xq)(1-xq^2)\cdots$

Notation about Groups:

W A Weyl group

C A conjugacy class in W

G An algebraic group

$g = g_s g_u$ The Jordan decomposition of g as a product of commuting semisimple and unipotent elements

F A Frobenius map

G^F The fixed points of G under F

T An F-stable maximal torus

$N_{G_1}(G_2)$ The normalizer in G_1 of some group G_2

$C_G(g)$ The centralizer of g in G

Abstract

The basic goal of this thesis is to develop a probabilistic approach for understanding what a typical element α of $GL(n,q), U(n,q), Sp(2n,q)$ or $O(n,q)$ looks like. This thesis aims to answer questions such as "What is the chance that α is semi-simple or regular?" and "What is the average order of α?" Answers to these questions have applications to the theory of random number generation and to testing algorithms for generating random elements of finite groups.

The classical groups over finite fields will be used to define measures on partitions. For the case of $GL(n,q)$ this boils down to rational canonical form. Algebraic conditions such as semi-simplicity are translated into conditions on the shapes of these partitions and this view is used to obtain new results. Our definitions lead to interesting combinatorics, such as q-analogs of the Bell and Stirling numbers and an appearance of the Rogers-Ramanujan identities in the general linear groups.

We relate the measure on partitions coming from the classical groups to the Hall-Littlewood polynomials. The Macdonald symmetric functions are used to define more general measures on partitions, such as a q-analog of Plancharel measure. Probabilistic algorithms are developed for growing partitions (and in the case of GL or U also Young tableaux) according to these measures. These algorithms give probabilistic interpretations to identities from symmetric function theory and lead to proofs of theorems such as Steinberg's count of unipotent elements (which is normally proven by character theory) and results of Rudvalis and Shinoda [51]. Kerov's q-generalization of the hook walk of combinatorics [36] can be obtained from these algorithms as well.

The concept of a cycle index is developed for the unitary, symplectic, and orthogonal groups. These cycle indices all factor. The number of irreducible polynomials ϕ invariant under certain involutions is computed. This leads to results about the number of Jordan blocks and average order of an element of a finite classical group.

Contents

Acknowledgements **i**

Notation **ii**

Abstract **iv**

Introduction **1**

1 Motivation and Background **3**
1.1 The Symmetric Groups S_n . . . 3
1.2 The General Linear Groups $GL(n, q)$ . . . 6
1.3 Some Further Motivation . . . 8
1.4 Review of Algebraic Groups . . . 9

2 Measures on Partitions and Probabilistic Algorithms **11**
2.1 Chapter Overview . . . 11
2.2 History of Partitions and Probabilistic Algorithms . . . 12
2.3 Background on the Macdonald Symmetric Functions . . . 13
2.4 Defining Measures $P_{x,y,q,t}$ from the Macdonald Symmetric Functions . . . 15
2.5 An Algorithm for Picking From $P_{x,y,q,t}$ . . . 16
2.6 Example 1: Hall-Littlewood Polynomials . . . 19
2.7 Young Tableau Algorithm . . . 21
2.8 Weights on the Young Lattice . . . 25
2.9 Example 2: Schur Functions and a q-analog of the Plancharel Measure of the Symmetric Group . . . 29
2.10 Comparison with Kerov's q-analogs of Plancharel Measure and the Hook Walk . . . 33

3 The General Linear Groups **35**
3.1 Chapter Overview . . . 35
3.2 The Kung-Stong Cycle Index for $GL(n, q)$ . . . 35
3.3 Connection with the Hall-Littlewood Measures . . . 38
3.4 The Size of the Partitions . . . 40
3.5 Counting Jordan Blocks . . . 41
3.6 The Number of Parts in the Partitions . . . 42
3.7 The Largest Part of the Partitions . . . 49
3.8 Counting Regular and Regular-Semisimple Matrices . . . 51
3.9 The $q \to \infty$ limit of the Cycle Indices . . . 55

4 The Unitary Groups **58**
4.1 Chapter Overview 58
4.2 Conjugacy Classes in the Unitary Groups 58
4.3 The Cycle Index for the Unitary Groups 60
4.4 Connection with the Hall-Littlewood Measures 62
4.5 The Size of the Partitions 63
4.6 Counting Jordan Blocks 64
4.7 The Number of Parts in the Partitions 65
4.8 Average Order of an Element of $U(n, q)$ 68

5 The Symplectic Groups **70**
5.1 Chapter Overview 70
5.2 Conjugacy Classes in the Symplectic Groups 70
5.3 The Cycle Index for the Symplectic Groups 72
5.4 Size of the Partition Corresponding to $z - 1$ 74
5.5 Counting Jordan Blocks 76
5.6 Number of Parts of the Partition Corresponding to $z - 1$ 77
5.7 Average Order of an Element of $Sp(2n, q)$ 78

6 The Orthogonal Groups **80**
6.1 Chapter Overview 80
6.2 Conjugacy Classes in the Orthogonal Groups 80
6.3 The Cycle Index for the Orthogonal Groups 83
6.4 Size of the Partition Corresponding to $z - 1$ 85
6.5 Counting Jordan Blocks 85
6.6 Number of Parts in the Partition Corresponding to $z - 1$ 86
6.7 Average Order of an Element of $O(n, q)$ 87

Suggestions for Future Research **89**

Introduction

The purpose of this introduction is two-fold: to describe the organization of this thesis and to state which results we believe to be the most important. Although it might make more sense to do this after Chapter 1 which is more motivational, we prefer to highlight the key results as early as possible.

The organization of this thesis is as follows. Chapter 1 begins with an account of some of what is known about probability in the symmetric and general linear groups. For the symmetric groups the Polya cycle index and its probabilistic applications are described. For the general linear groups the Kung/Stong cycle index and some of its uses to date are reviewed. The interesting work of Rudvalis and Shinoda is also discussed. Chapter 1 concludes with some further motivation and a review of algebraic groups. Chapter 2 develops a link between probability and symmetric function theory. The Macdonald symmetric functions are used to define measures on partitions and to give a probabilistic algorithm for growing partitions according to these measures. Some important special cases are considered, for instance a q-analog of Plancharel measure and the hook walk. This chapter can be read with no knowledge of the classical groups. Chapter 3 focuses on the general linear groups. Crucial here is the connection of the conjugacy classes of GL with the Hall-Littlewood polynomials and the probabilistic algorithms of Chapter 2. Some new applications of the cycle index of GL to the $n \to \infty$ asymptotics of $GL(n,q)$ are then given. The group theoretic interpretation of the Rogers-Ramanujan identities may also be of interest. Chapters 4,5, and 6 discuss probability in the finite unitary, symplectic, and orthogonal groups respectively. Cycle indices are found for these groups and are used to read off algebraic information. Some connections are made with the general linear group and the probabilistic algorithms of Chapter 2. Although the unitary, symplectic, and orthogonal groups could have been treated in one chapter, they are sufficiently different and important that they are treated separately. The thesis ends with a list of some questions and possible directions for future research.

Here is what we believe to be six important contributions of this thesis.

1. The definition of measures on partitions from the Macdonald polynomials, as described in Section 2.4.

2. Probabilistic algorithms for growing partitions according to these measures, as described in Sections 2.5, 2.6, 2.7, 2.8, and 2.10.

3. The connection of 1 and 2 with the classical groups, described in Sections 3.3, 4.4, 5.3 and 6.3. Especially interesting is the application of the algorithms to give probabilistic proofs of algebraic results such as Steinberg's count of unipotent elements (Section 3.4) and theorems of Rudvalis and Shinoda on the distribution of fixed vectors of a random element of $GL(n,q)$ (Section 3.6).

4. The appearance of the Rogers-Ramanujan identities in the general linear groups, as described in Section 3.7.

5. Finding the cycle indices for the finite unitary, symplectic, and orthogonal groups, as described in Sections 4.3, 5.3, and 6.3.

6. Reading algebraic information off of the cycle indices, as described in Chapter 3,4,5, and 6.

Chapter 1

Motivation and Background

1.1 The Symmetric Groups S_n

In this section the symmetric groups are used as a model for the sort of study to be undertaken for the classical groups over finite fields. Polya's cycle index for the tower S_n is introduced and probabilistic interpretations of it are discussed. This interpretation will later be generalized to the classical groups over finite fields. Much of the exposition in this section is influenced by talks given by Persi Diaconis and some of his unpublished notes [10].

Here are some typical questions one could ask about a random permutation $\pi \in S_n$:

1. "What is the chance that π has a_1 fixed points?" This is the famous matching problem, dating back to Monmort in 1708. Its solution is one of the earliest results in probability.

2. "How many cycles does π have?" This is a mainstay of the Ewens sampling formula of modern population genetics [17].

3. "What is the order of π?" This is a classical combinatorial problem with applications in finite group theory. For example, when $n = 52$, the permutation with maximal order has order 180,180.

4. "What is L_1, the length of the longest cycle of π?" This is of interest because of its connections with number theory. Knuth and Trabb Pardo [38] show that L_1/n has the same $n \to \infty$ limit distribution as $\frac{log(P_1(x))}{log(n)}$, where x is a uniformly chosen integer between 1 and n, and $P_1(x)$ is the largest prime factor of x.

All of these problems have in fact been solved. To give a flavor of the subject, we state the answers to questions 2-4. The Polya cycle index will then be introduced and given a probabilistic interpretation which will lead to a solution of problem 1.

For question 2, Goncharov [27] proved that the number of cycles in a random permutation is asymptotically normal with mean $log\ n$ and standard deviation $(log\ n)^{\frac{1}{2}}$. For question 3, Goh and Schmutz [23] proved that if μ_n is the average order of an element of S_n, then:

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

where $C = 2.99047....$ For question 4, let L_1 denote the length of the longest cycle of a permutation, and E_n expectation in S_n. Goncharov [27] showed that $\frac{L_1}{n}$ has a limit distribution.

Lloyd and Shepp [42] computed the moments of this limit distribution. For instance the first moment is:

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

A common trait of these questions is that the functions involved do not depend on the labelling of the set $\{1, \cdots, n\}$ being permuted. They depend only on the conjugacy class of π, i.e. on the cycle vector $(a_1(\pi), \cdots, a_n(\pi))$ where $a_i(\pi)$ is the number of i-cycles of π. Namely, a_1 is the number of fixed points of π, $\sum a_i$ is the number of cycles of π, the least common multiple of the a_i is the order of π, and the largest $a_i \neq 0$ is the length of the longest cycle of π. An important ingredient in the solution of these problems is the following so-called Polya Cycle Index, which was initially introduced for the purpose of enumerating certain types of chemical compounds [50]. Write:

$$Z_{S_n}(x_1, \cdots, x_n) = \frac{1}{n!} \sum_{\pi \in S_n} \prod_i x_i^{a_i(\pi)}$$

Then 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 give the following factorization:

$$\sum_{n=0}^\infty u^n Z_{S_n} = \prod_{m=1}^\infty e^{\frac{x_m u^m}{m}}$$

Lloyd and Shepp [42] found a useful probabilistic interpretation for the Polya cycle index. Setting all $x_i = 1$ in the reciprocal of the Polya cycle index shows that $1-u = e^{-\sum_m \frac{u^m}{m}}$. Therefore:

$$\sum_{n=0}^\infty (1-u) u^n Z_{S_n} = \prod_{m=1}^\infty e^{\frac{u^m}{m}(x_m - 1)}$$

Now suppose that $0 < u < 1$. The left-hand side is the probability generating function for cycle structure after first picking the size of the symmetric group with the chance of n equal to $(1-u)u^n$, and then picking uniformly in S_n. For the right hand side, recall the Poisson(λ) distribution which is equal to $j \geq 0$ with probability $\frac{e^{-\lambda}\lambda^j}{j!}$. The Poisson ($\lambda$) distribution has $e^{\lambda(x-1)}$ as its probability generating function in the variable x. So the right hand side is the product of generating functions of Poisson variables with parameters $\frac{u^i}{i}$. These considerations imply the following theorem of Lloyd and Shepp [42].

Theorem 1 *For $0 < u < 1$, choose the size of the symmetric group with probability of n equal to $(1-u)u^n$. Then choose π uniformly in S_n. The random variables $a_i(\pi)$ (defined on the union of all symmetric groups) are independent Poisson($\frac{u^i}{i}$).*

The following lemma 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 1 *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 $[u^n]\frac{f(u)}{1-u} = \sum_{i=0}^{n} a_i$. $\square$

Let P_n be the distribution of fixed points of an element of S_n (i.e. the object of study of problem 1). Theorem 1 and Lemma 1 show that the $n \to \infty$ limit of P_n is Poisson(1). This argument can be used to prove the more general fact that for any $i < \infty$, the joint distribution of $(a_1(\pi), \cdots, a_i(\pi))$ converges to independent (Poisson(1), $\cdots$, Poisson($\frac{1}{i}$)).

A remarkable fact which deserves mention is that the first n moments of P_n are equal to the first n moments of the Poisson(1) distribution. This will be called the moment contact phenomenon. Analogous statements will be proved for the classical groups over finite fields in Sections 3.6, 4.7, 5.6, and 6.6. It will thus be useful to give a proof of the moment contact phenomenon for S_n, arguing as in Diaconis [11]. For this recall Burnside's Lemma.

Lemma 2 *Let a finite group G act on a set X. Let $F(g)$ denote the number of fixed points of $g \in G$ and let $O(X)$ be the set of orbits of this action. Then:*

$$\sum_{g \in G} F(g) = |O(x)|$$

Recall that the lth Bell number B_l is defined as the number of set partitions of a set of size l. For example, $B_3 = 5$ and the 5 set partitions of $\{1,2,3\}$ are:

$$\begin{array}{r} \{1,2,3\} \\ \{1\},\{2,3\} \\ \{2\},\{1,3\} \\ \{3\},\{1,2\} \\ \{1\},\{2\},\{3\} \end{array}$$

Theorem 2 *For $1 \leq l \leq n$, the lth moment of the distribution of fixed points of S_n is equal to B_l.*

PROOF: Apply Lemma 2 to the action of S_n on l-tuples whose coordinates are elements of the set $\{1, \cdots, n\}$. The orbits of this action correspond bijectively to set partitions of $\{1, \cdots, l\}$ by defining the blocks of the partition to consist of coordinates with equal values. $\square$

Note from the interpretation of the moments as counting something (the number of orbits of an action), that they are integers. As a sequence of integers converging to a limit must eventually be equal to the limit, it is clear that the moments stabilize. Theorem 2 is interesting in that it computes the limit and says how quickly the stabilization takes place (in fact, it is not hard to see that the stabilization does not occur for $n < l$).

It is worth remarking that it is possible to give good bounds on how quickly the convergence of P_n to Poisson(1) occurs. Recall the notion of variation distance between two probability distributions P and Q on a set X. The definition, as in Chapter 3 of Diaconis [11], is:

$$|P - Q|_{TV} = \frac{1}{2} \sum_{x \in X} |P(x) - Q(x)|$$

Arratia and Tavare [2] prove that:

$$\frac{2^n}{(n+1)!} \frac{n}{n+2} \leq |P_n - Poisson(1)|_{TV} \leq \frac{2^n}{(n+1)!}$$

A q-analog of this result for the groups $GL(n,q)$ will be given in Section 3.6.

1.2 The General Linear Groups $GL(n,q)$

This section reviews some aspects of probability in the groups $GL(n,q)$. There are a number of ad-hoc results which have been obtained. For instance Fine and Herstein [18] and Gerstenhaber [22] show that there are $q^{n(n-1)}$ nilpotent matrices over a finite field of size q. Hansen and Schmutz [30] studied the characteristic polynomial of a random matrix. They made precise the statement that "Except for factors of small degree, the characteristic polynomial of a random matrix in $GL(n,q)$ is like a random monic degree n polynomial over F_q". Neumann and Praeger [46], [47] obtained good bounds for the chance that an element of $GL(n,q)$ is regular or regular-semisimple (see Section 3.8 for the definitions of these terms and details on their work).

A unified approach to these results emerges from the work of Kung [39] and Stong [56], who developed a cycle index for the groups $GL(n,q)$. Let us review this briefly. First it is necessary to understand the conjugacy classes of $GL(n,q)$. As is explained in Chapter 6 of Herstein [32] (an explanation in terms of algebraic groups will be given in Section 1.4), 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 $|\lambda_\phi|$. Let m_ϕ denote the degree of ϕ. The only restrictions necessary for this data to represent a 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,

1. The characteristic polynomial of $\alpha \in GL(n,q)$ is equal to $\prod_{\phi} \phi^{|\lambda_{\phi}(\alpha)|}$.

2. Let $\lambda_{\phi,1}$ be largest part of a partition λ_{ϕ}. Then the minimal polynomial of α is equal to $\prod_{\phi} \phi^{\lambda_{\phi,1}(\alpha)}$. In particular, α is semisimple (diagonalizable over the algebraic closure of F_q) if and only if $\lambda_{\phi,1}(\alpha) \leq 1$ for all ϕ.

3. An element α of $GL(n,q)$ is "regular" (see Section 3.8) if and only if its characteristic polynomial is equal to its minimal polynomial, thus if and only if all $\lambda_{\phi}(\alpha)$ have at most 1 part.

To define the cycle index for $GL(n,q)$, let $x_{\phi,\lambda}$ be variables corresponding to pairs of polynomials and partitions. Define:

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

Following Kung [39], Stong [56] then proves the factorization:

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

Here $c_{GL,\phi,q}(\lambda)$ is a certain function on partitions which is described in Section 3.2.

Using this cycle index, Stong [56], [57] and Goh and Schmutz [24] studied some properties of random elements of $GL(n,q)$ such as the number of Jordan blocks and average order. Stong 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 proved convergence to the normal distribution. The research done to date using the cycle index for $GL(n,q)$ emphasizes the polynomials in the rational canonical form of α. This thesis attempts to understand the partitions as well. The program of finding the cycle indices and reading information off of them will be carried further for $GL(n,q)$ in Chapter 3 and extended to the other classical groups in Chapters 4-6. Especially important will be the idea of stating algebraic conditions on α in terms of the partitions $\lambda_{\phi}(\alpha)$.

We now review the work of Rudvalis and Shinoda [51]. They studied an analog of the distribution of fixed vectors for the classical groups over finite fields. Let $G = G(n)$ be a classical group (i.e. one of GL,U,Sp, or O) acting on an n dimensional vector space V over a finite field F_q (in the unitary case F_{q^2}) in its natural way. Let $P_{G,n}(k,q)$ be the chance that an element of G fixes a k dimensional subspace and let $P_{G,\infty}(k,q)$ be the $n \to \infty$ limit of $P_{G,n}(k,q)$. Rudvalis and Shinoda [51] found (in a 76 page unpublished work) formulas for $P_{G,\infty}(k,q)$. Their formulas are, setting $x = \frac{1}{q}$:

1. $P_{GL,\infty}(k,q) = [\prod_{r=1}^{\infty}(1-x^r)] \frac{x^{k^2}}{(1-x)^2 \cdots (1-x^k)^2}$

2. $P_{U,\infty}(k,q) = [\prod_{r=1}^{\infty} \frac{1}{1+x^{2r-1}}] \frac{x^{k^2}}{(1-x^2) \cdots (1-x^{2k})}$

3. $P_{Sp,\infty}(k,q) = [\prod_{r=1}^{\infty} \frac{1}{1+x^r}] \frac{x^{\frac{k^2+k}{2}}}{(1-x) \cdots (1-x^k)}$

4. $P_{O,\infty}(k,q) = [\prod_{r=0}^{\infty} \frac{1}{1+x^r}] \frac{x^{\frac{k^2-k}{2}}}{(1-x) \cdots (1-x^k)}$

At first glance it is not even clear that these are probability distributions in k, but as Rudvalis and Shinoda note, this follows from identities of Euler. The proof of these formulas of Rudvalis and Shinoda used Moebius version on the lattice of subspaces and a detailed knowledge of geometry over finite fields. One of the goals of this thesis is to understand these results in terms of cycle indices and probabilistic algorithms (at least for GL and U).

1.3 Some Further Motivation

The purpose of this section is to give some further motivation for the work in this thesis. Here it is.

1. As was explained while stating problems 1-4 in Section 1.1, permutation groups relate to many areas of mathematics and science, such as number theory and population genetics. Diaconis and Shahshahani [13] have obtained interesting results about probability in the classical compact groups. In this context conjugacy classes are parameterized by eigenvalues. They showed that a type of moment contact phenomenon occurs and studied how the eigenvalues are spread out on the unit circle. Mehta [45] discusses applications of these eigenvalue distributions. One application is to the spectra of slow neutron scattering. He also describes how the eigenvalues are empirically related to the spacings between the zeros of the zeta function. The problems studied here are the natural analogs of these rich problems for the finite classical groups. There is every reason to believe that their answers will relate to an equally rich set of problems.

2. A lively program in combinatorics is the study of the shapes of partitions of a number n under various measures. Here are three measures which have been actively investigated. One widely studied measure is the uniform measure on partitions. Many results can be found in the works of Andrews [1] and Fristedt [20]. For a second way of putting measures on partitions of n, note that $\pi \in S_n$ defines a partition of n by looking at the lengths of its cycles (i.e. the conjugacy class of π). So picking a uniform $\pi \in S_n$ induces a measure on partitions of n. This measure was discussed in Section 1.1. A third way of putting measures on partitions comes from the irreducible representations of the symmetric group and is called Plancharel measure. For anxious readers the definition of Plancharel measure is $P(\lambda) = \frac{n!}{\prod_{s \in \lambda} h(s)^2}$ where $h(s)$ is the hooklength of s. The Plancharel measure has been studied, for instance, by Kerov and Vershik [37].

   In Chapter 2 the Macdonald symmetric functions are used to define a 2-parameter class of measures on all partitions. For instance, renormalizing the measure coming from the Schur functions to live on partitions of size n leads to a q-analog of Plancharel measure. Our motivation for these definitions in fact came from the finite classical groups. For instance, here is how one can use $GL(n,q)$ to define measures on partitions. Recall the notion of the rational canonical form of $\alpha \in GL(n,q)$. Fix an irreducible polynomial ϕ over F_q and consider the partition $\lambda_\phi(\alpha)$ which corresponds to ϕ in the rational canonical form of α. As with the symmetric group, given $0 < u < 1$, pick n with probability $(1-u)u^n$ and then choose α uniformly in $GL(n,q)$. This induces a measure on the set of all partitions. The $u \to 1$ limit corresponds to the $n \to \infty$ limit of a uniform α chosen in $GL(n,q)$.

3. A third motivation for studying probability in classical groups over finite fields is to be able to analyze random number generators or algorithms for generating random elements in finite groups. A random number generator can be used to generate a supposedly "random" matrix over a finite field (typically one generates thirty-two 32-bit blocks and makes a 32 by 32 matrix over F_2 out of them). Marsaglia and Tsay [44] have used the rank of this matrix as an effective way of screening out bad random number generators. Of course, to apply this test, one needs to know how the rank of a randomly chosen matrix behaves.

   Similarly, an algorithm for generating random elements of finite groups can be applied to the classical groups. The algorithms which seem to work the best (such as those employed in algebra systems like Cayley and Gap) have defied direct mathematical analysis. Therefore, to evaluate how well they work, one uses them to pick from some finite classical group and compares data with the results for an element chosen uniformly from the group. A clear discussion of this is in [9]. The point is that the cycle index machinery developed in this thesis allows one to get a handle on what a random element of a finite classical group looks like.

1.4 Review of Algebraic Groups

One definition of the finite unitary, symplectic, and orthogonal groups is as the subgroups of $GL(n,q)$ (in the unitary case as a subgroup of $GL(n,q^2)$) preserving a special type (Hermitian, skew-symmetric, symmetric) of non-degenerate bilinear form over F_q. The details of these definitions will be given in Chapters 4-6. A superb account of this viewpoint is Chapter 1 of Carter's book on simple groups of Lie type [7].

The purpose of this section is to discuss the finite classical groups from the viewpoint of algebraic groups. This viewpoint will be used later. Good references are Chapter 1 of Carter's book on finite groups of Lie type [8] and Chapter 8 of Humphreys [33].

Let G be a connected, reductive (feel free to ignore these adjectives) algebraic group defined over $\bar{F}_q$, the algebraic closure of F_q. Viewing G as contained in $GL(n,\bar{F}_q)$, a map $F: G \to G$ is called a Frobenius map if some power of it is a standard Frobenius map $F: (a_{ij}) \to (a_{ij}^q)$. Let G^F be the elements of G fixed by F. The groups $GL(n,q), Sp(2n,q)$ and $O(n,q)$ arise as fixed points of the Frobenius map $F: (a_{ij}) \to (a_{ij}^q)$ on the corresponding groups over $\bar{F}_q$. The group $U(n,q)$ arises as the fixed points of the Frobenius map $F: (a_{ij}) \to ((a_{ij}^q)^t)^{-1}$ on $GL(n,q^2)$.

An element of G^F is called semisimple if it is diagonalizable over $\bar{F}_q$. An element of G^F is called unipotent if it has all eigenvalues equal to 1. Letting p be the characteristic of F_q, it is easy to check that semisimple elements have order prime to p and unipotent elements have order a power of p. An important theorem is the Jordan decomposition which says that $g \in G$ may be written uniquely as $g = g_s g_u$ where g_s is semi-simple, g_u is unipotent, and g_s commutes with g_u. If $g \in G^F$, then $g_s, g_u \in G^F$.

In fact, the Jordan decomposition of elements gives a way of "factoring" the conjugacy classes of G^F. We will describe this factorization and then show that in the case of $GL(n,q)$ it gives the rational canonical form of a matrix. The essence of the factorization is the following proposition, which is stated without proof in Chapter 8 of Humphreys [33].

Proposition 1 *The conjugacy classes of G^F correspond bijectively to pairs (A,B) where the A form a set of representatives of conjugacy classes of semisimple elements in G^F and the B form a set of representatives of unipotent classes in the centralizer of A.*

PROOF: Define a map from conjugacy classes of G^F to such pairs (A,B) as follows. Pick g in the class and write it $g = g_s g_u$ as above. Then g_s is conjugate to a unique semisimple representative A. Let h_1 be such that $h_1 g_s h_1^{-1} = A$. Then $h_1 g_u h_1^{-1}$ is a unipotent element in $C_G(A)$ and so defines a unipotent class in $C_G(A)$. This class is well-defined, for if $h_2 g_s h_2^{-1} = A$, then $h_1 g_u h_1^{-1}$ and $h_2 g_u h_2^{-1}$ are conjugate by $h_2 h_1^{-1} \in C_G(A)$.

The map is $1-1$ because if g is conjugate to both AB_1 and AB_2, then, as was just shown, B_1 and B_2 are conjugate by an element of $C_G(A)$. The map is onto because one can take g to be the product of any such pair of elements (A,B). □

We now consider the example of $GL(n,q)$. Here the semi-simple conjugacy classes correspond to the possible characteristic polynomials. Let ϕ be an irreducible polynomial of degree m_ϕ. If the characteristic polynomial of a semisimple α factors as $\prod_{i=1}^r \phi_i^{n_i}$, then the centralizer of α is isomorphic to $\prod_i GL(n_i, q^{m_{\phi_i}})$. The unipotent classes of $GL(n_i, q^r)$ for any r correspond to partitions of n_i. This is the explanation (without proofs) of rational canonical form in terms of algebraic groups.

Wall [61] gives a parameterization of the conjugacy classes of the finite unitary, symplectic and orthogonal groups using combinatorial data such as polynomials and partitions (this will be discussed in Sections 4.2, 5.2, and 6.2). It would be desirable to understand Wall's parameterizations in terms of Proposition 1, as has just been done for the general linear groups.

Although unnecessary for the rest of this thesis, it is worth noting that analogs of the Jordan decomposition and Proposition 1 hold for any finite group. For any prime p, call $g \in G$ p-semisimple if it has order prime to p and p-unipotent if it has order a power of p. Then the Jordan decomposition and Proposition 1 carry over with the words semisimple and unipotent replaced by p-semisimple and p-unipotent.

As an example, take the symmetric group S_n and some prime p. The Jordan decomposition for elements works as follows. Write π as a product of its cycles (which all commute). Given an l-cycle x, write $l = p^a r$, where p and r are relatively prime. Then there are C, D such that $Cp^a + Dr = 1$, so x is a product of $(x^{p^a})^C$ and $(x^r)^D$. This represents an l-cycle as a product of p^a r-cycles and r p^a-cycles, where everything commutes. On the level of conjugacy classes the pairs (A, B) may be described as follows. The A correspond to partitions of n into m_i parts of size i, where $m_i = 0$ if p divides i. The B which are second coordinates of such an A correspond to partitions of each m_i into parts which have size a power of p. This can all be deduced from the fact that the centralizer of $\pi \in S_n$ is a direct product of various wreath products, and from the description of conjugacy classes of wreath products in Chapter 4 of James and Kerber [34]. The details of the proof are omitted as we have already gone far afield.

Chapter 2

Measures on Partitions and Probabilistic Algorithms

2.1 Chapter Overview

Following this overview, a brief history is given of some work of Diaconis and Kemperman [12], Greene, Nijenhuis and Wilf [28], [29], and Kerov [35], [36] on probabilistic algorithms for generating partitions which arise in mathematical problems. In Section 2.4 the Macdonald symmetric functions are used to define measures $P_{x,y,q,t}$ on the set of all partitions λ of all integers. In Section 2.5 a probabilistic algorithm is given for growing partitions according to these measures. The treatment in these sections may seem like abstract symbol-pushing, so the remainder of this chapter focuses on two concrete examples.

The first example, considered in Section 2.6, is the case $q = 0, y_i = t^{i-1}$ and is a specialization of the Hall-Littlewood functions. The further specialization $x_i = ut^i$, where $0 < u < 1$ will be studied in Sections 2.7 and 2.8. As will emerge in Sections 3.3, 4.4, 5.3 and 6.3, this case arises naturally in the finite classical groups. For instance, suppose one sets $t = \frac{1}{q^m}$, where q is the size of a finite field and m is some natural number. Then this measure on partitions turns out to be the same as the measure on partitions obtained by fixing a monic, irreducible polynomial ϕ of degree m, picking the size of a general linear group with probability of size n equal to $(1-u)u^n$, then picking α uniformly in $GL(n,q)$ and taking the partition $\lambda_\phi(\alpha)$ corresponding to ϕ in the rational canonical form of α. Note that this is analogous to the way in which the Poisson distribution arises in the theory of the symmetric groups. In this special case the probabilistic algorithm for generating partitions simplifies. We also give a second, different algorithm which in fact creates a Young tableau. This leads to a natural way of putting weights on the Young lattice. This view will be used later (Sections 3.6 and 4.7) to give probabilistic proofs of the formulas of Rudvalis and Shinoda for the distribution of the dimension of the fixed space of an element of $GL(n,q)$ or $U(n,q)$.

The second example, considered in Sections 2.9 and 2.10 is the case $q = t, x_i = t^i$. This measure, renormalized to live on partitions of size n, is a q-analog of the Plancharel measure $\frac{n!}{\prod_{s \in \lambda} h(s)^2}$ on partitions of n (here $h(x)$ is the hook-length). As the $q = 1$ case is so connected with the representation theory of S_n, it is reasonable to expect this q-analog to be connected with the representation theory of $GL(n,q)$. In fact, this measure leads us to define polynomials $J_n(q)$ with nice combinatorial properties. For instance, these polynomials turn out to be sums of squares of Kostka-Foulkes polynomials, these latter polynomials being special cases of Kazhdan-Lusztig polynomials. The chapter ends by showing that the probabilistic algorithm of Section 2.5 specialized to this second example can be conditioned to give exactly one of Kerov's q-generalizations [36] of the hook walk of Greene, Nijenhuis, and Wilf [28], [29].

2.2 History of Partitions and Probabilistic Algorithms

We begin by reviewing some standard notation about partitions, as on pages 2-5 of Macdonald [43]. Let λ be a partition of some non-negative integer $|\lambda|$ into parts $\lambda_1 \geq \lambda_2 \geq \cdots$. Let $m_i(\lambda)$ be the number of parts of λ of size i, and let λ' be the partition dual to λ in the sense that $\lambda_i' = m_i(\lambda) + m_{i+1}(\lambda) + \cdots$. Let $n(\lambda)$ be the quantity $\sum_{i \geq 1} (i-1)\lambda_i$.

It is also useful to define the diagram associated to λ as the set of points $(i,j) \in Z^2$ such that $1 \leq j \leq \lambda_i$. We use the convention that the row index i increases as one goes downward and the column index j increases as one goes across. So the diagram of the partition (5441) is:

$$\begin{array}{lllll} . & . & . & . & . \\ . & . & . & . & \\ . & . & . & . & \\ . & & & & \end{array}$$

It is sometimes useful to think of these dots as boxes. Given a square s in the diagram of a partition λ, let $l'(s), l(s), a(s), a'(s)$ be the number of squares in the diagram of λ to the north, south, east, and west of s respectively. So the diagram

$$\begin{array}{lllll} . & . & . & . & . \\ . & s & . & . & \\ . & . & . & . & \\ . & & & & \end{array}$$

has $l'(s) = l(s) = a'(s) = 1$ and $a(s) = 2$.

A skew-diagram is the set theoretic difference $\lambda - \mu$ of two diagrams λ and μ, where the diagram of λ contains the diagram of μ. A horizontal strip is a skew-diagram with at most one square in each column. For instance:

$$\begin{array}{lllll} & & & & . \\ & & & & \\ & & . & . & \\ . & & & & \end{array}$$

There are many ways of putting measures on partitions of a given size n. Perhaps the most natural measure is the uniform measure. This has been studied extensively by Erdos and Szalay [15] and Fristedt [20], for instance. Andrews [1] gives many more references.

Some measures on partitions can be built up stochastically. As a first example, recall the measure on partitions of n induced by the conjugacy classes of S_n. The chance of λ, a partition of n with a_i i-cycles, is equal to $\frac{1}{\prod_i a_i! i^{a_i}}$. Diaconis and Kemperman [12] give a stochastic procedure, which they call the Chinese restaurant process, for building up these partitions. They relate this process to the theory of Dirichlet priors. The Chinese restaurant process is equivalent to a procedure of Kingman in the theory of population genetics (see page 154 of Kerov [35]).

As a second example, consider the Plancharel measure on partitions of n. Let $h(s) = a(s) + l(s) + 1$ be the hook length of $s \in \lambda$. Then the formula $\frac{n!}{\prod_{s \in \lambda} h(s)^2}$ defines a measure on partitions of n. Greene, Nijenhaus, and Wilf [28] give a stochastic way of building up these partitions, called the hook walk. Kerov [35] relates the hook-walk to the Markov moment problem of probability theory and gives a q-generalization of the hook walk [36].

The measures introduced in Section 2.4 using the Macdonald symmetric functions differ from the measures in this section in that they are defined on all partitions of all integers, and not on partitions of a fixed size. In this sense, they are finer measures since they can always be renormalized to live on partitions of size n. It will be demonstrated in Section 2.10 that conditioning a specialization of the algorithm of Section 2.5 gives one of Kerov's q-generalizations of the hook walk.

2.3 Background on the Macdonald Symmetric Functions

The Macdonald symmetric functions $P_\lambda(x_i;q,t)$ are the most general class of symmetric functions known at present. A good account of these symmetric functions is Chapter 6 of Macdonald's book [43].

To define the Macdonald symmetric functions, recall the power sum and monomial symmetric functions. The rth power sum p_r is defined as $\sum x_i^r$ and the p_λ are defined as $p_{\lambda_1}p_{\lambda_2}\cdots$. The monomial symmetric functions are the symmetric functions whose restriction to the variables $x_1,\cdots,x_n$ is $\sum x^\alpha$ where the sum is over all distinct permutations α of $\lambda=(\lambda_1,\cdots,\lambda_n)$.

The Macdonald symmetric functions are defined as follows. Let $0<q,t<1$ be real parameters. Put the following scalar product on the ring of symmetric functions in the variables x_i:

$$<p_\lambda,p_\mu>=\delta_{\lambda,\mu}z_\lambda\prod_{i=1}^{\lambda_1'}\frac{1-q^{\lambda_i}}{1-t^{\lambda_i}}$$

where $z_\lambda=\prod_{i\geq 1} i^{m_i(\lambda)}m_i(\lambda)!$ and $\delta_{\lambda,\mu}$ is 1 if $\lambda=\mu$ and 0 otherwise.

Now fix n. The partitions of n can be put in lexicographic order. This is a total ordering such that $\lambda=(\lambda_1,\cdots,\lambda_n)$ is greater than $\mu=(\mu_1,\cdots,\mu_n)$ iff the first non-vanishing difference $\lambda_i-\mu_i$ is positive. So the partitions of 5 in lexicographic order from smallest to largest are $(1^5),(21^3),(2^21),(31^2),(32),(41),(5)$. The Macdonald symmetric functions (for λ a partition of n) are the basis of the ring of degree n symmetric functions obtained by applying the Gram-Schmidt orthogonalization process to the monomial symmetric functions, where one orthogonalizes in lexicographic order.

As is explained on pages 305-6 of Macdonald [43], various specializations of the Macdonald symmetric functions give the Hall-Littlewood polynomials, Schur functions, zonal polynomials, and Jack symmetric functions. In many ways the Macdonald symmetric functions are quite elusive. For instance, in this generality, they do not have any known group theoretic interpretation.

Here is some more notation of Macdonald's which will be needed.

1. Recall from Section 2.2 that if s is a square in the diagram of a partition λ, then $l_\lambda'(s),l_\lambda(s)$, $a_\lambda(s),a_\lambda'(s)$ denote the number of squares in the diagram of λ to the north, south, east, and west of s respectively. The subscript λ will sometimes be omitted if the partition λ is clear from context.

   Given a partition λ and a square s, set $b_\lambda(s)=1$ if $s\notin\lambda$. Otherwise set:

$$b_\lambda(s)=\frac{1-q^{a_\lambda(s)}t^{l_\lambda(s)+1}}{1-q^{a_\lambda(s)+1}t^{l_\lambda(s)}}$$

   Let $b_\lambda(q,t)=\prod_{s\in\lambda}b_\lambda(s)$.

2. Define

$$\phi_{\lambda/\mu}(q,t) = \prod_{s \in C_{\lambda/\mu}} \frac{b_\lambda(s)}{b_\mu(s)}$$

where $C_{\lambda/\mu}$ is the union of the columns intersecting $\lambda - \mu$.

3. The skew Macdonald polynomials (in one variable) are defined as:

$$P_{\lambda/\mu}(x;q,t) = \frac{b_\mu(q,t)}{b_\lambda(q,t)} \phi_{\lambda/\mu}(q,t) x^{|\lambda|-|\mu|}$$

if $\lambda - \mu$ is a horizontal strip, and 0 otherwise.

4. Let $(x,q)_\infty$ denote $\prod_{i=1}^{\infty}(1-xq^{i-1})$. Then define $\prod(x,y;q,t)$ by:

$$\prod(x,y;q,t) = \prod_{i,j=1}^{\infty} \frac{(tx_iy_j,q)_\infty}{(x_iy_j,q)_\infty}$$

Also define $g_n(y;q,t)$ as the coefficient of x^n in $\prod_j \frac{(txy_j,q)_\infty}{(xy_j,q)_\infty}$.

Using this notation, we write down five identities of Macdonald which will be needed in this chapter. It is convenient to name them (the Pieri Formula is already named).

1. Measure Identity:

$$\sum_\lambda P_\lambda(x;q,t)P_\lambda(y;q,t)b_\lambda(q,t) = \prod(x,y;q,t)$$

This is proved on page 324 of Macdonald [43].

2. Factorization Theorem:

$$\prod(x,y;q,t) = \prod_{n\geq 1} e^{\frac{1}{n}\frac{1-t^n}{1-q^n}p_n(x)p_n(y)}$$

This is proved on page 310 of [43].

3. Principal Specialization Formula:

$$P_\lambda(1,t,\cdots,t^{N-1};q,t) = t^{n(\lambda)} \prod_{s\in\lambda} \frac{1-q^{a'(s)}t^{N-l'(s)}}{1-q^{a(s)}t^{l(s)+1}}$$

This is proved on page 337 of [43].

4. Skew Expansion:

$$P_\lambda(x_1,\cdots,x_N;q,t) = \sum_\mu P_\mu(x_1,\cdots,x_{N-1};q,t)P_{\lambda/\mu}(x_N;q,t)$$

This is discussed on pages 343-7 of [43].

5. Pieri Formula:

$$P_\mu(y;q,t)g_r(y;q,t) = \sum_{\substack{\lambda:|\lambda-\mu|=r \\ \lambda-\mu \text{ horiz. strip}}} \phi_{\lambda/\mu}(q,t)P_\lambda(y;q,t)$$

This on page 340 of [43]. Although this is not mentioned in Macdonald, it is worth remarking that the Pieri Formula has its history in the work of the great Italian algebraic geometer Pieri, who found rules for multiplying classes of Schubert varieties in the cohomology ring of Grassmanians (see page 24 of Fulton [21]). In this special case, which corresponds to $q = t$, the Pieri formula becomes:

$$s_\mu s_{(r)} = \sum_{\substack{\lambda:|\lambda-\mu|=r \\ \lambda-\mu \text{ horiz. strip}}} s_\lambda$$

where s_λ is the Schur function corresponding to a partition λ.

2.4 Defining Measures $P_{x,y,q,t}$ from the Macdonald Symmetric Functions

In this section the Macdonald symmetric functions are used to define families of probability measures on the set of all partitions of all numbers. It is assumed throughout this chapter that x, y, q, t satisfy the following conditions:

1. $0 \leq t, q < 1$
2. $x_i, y_i \geq 0$
3. $\sum_{i,j} \frac{x_i y_j}{1-x_i y_j} < \infty$

The following formula defines a probability measure $P_{x,y,q,t}$ on the set of all partitions of all numbers:

$$P_{x,y,q,t}(\lambda) = \frac{P_\lambda(x;q,t)P_\lambda(y;q,t)b_\lambda(q,t)}{\prod(x,y;q,t)}$$

Lemma 3 *$P_{x,y,q,t}$ is a measure.*

Proof: By the Measure Identity and the fact that there are countably many partitions, it suffices to check that $0 \leq P_{x,y,q,t}(\lambda) < \infty$ for all λ. For this it is sufficient to show (again by the Measure Identity) that $P_\lambda(x;q,t), b_\lambda(q,t) \geq 0$ for all λ and that $0 \leq \prod(x,y;q,t) < \infty$.

Condition 1 implies that $b_\lambda(q,t) \geq 0$ for all λ. We claim that $x_i \geq 0$ implies that $P_\lambda(x;q,t) \geq 0$. To see this, note that when $P_\lambda(x;q,t)$ is expanded in monomials in the x variables, all coefficients are non-negative. For any particular monomial, this follows by repeated use of the Skew Expansion.

By the Factorization Theorem, showing that $0 \leq \prod(x,y;q,t) < \infty$ is equivalent to showing that:

$$0 \leq \sum_{n\geq 1} \frac{1}{n}\frac{1-t^n}{1-q^n} p_n(x)p_n(y) < \infty$$

Conditions 1 and 2 imply that this expression is non-negative. To see that it is finite, use Condition 3 as follows:

$$\begin{aligned}\sum_{n\geq 1}\frac{1}{n}\frac{1-t^n}{1-q^n}p_n(x)p_n(y) &\leq \frac{1}{1-q}\sum_{n\geq 1}p_n(x)p_n(y)\\ &= \frac{1}{1-q}\sum_{i,j\geq 1}\frac{x_iy_j}{1-x_iy_j}\\ &< \infty\end{aligned}$$

□

Define truncated measures $P^N_{x,y,q,t}(\lambda)$ to be 0 if λ has more than N parts, and otherwise:

$$P^N_{x,y,q,t}(\lambda) = \frac{P_\lambda(x_1,\cdots,x_N,0,\cdots;q,t)P_\lambda(y;q,t)b_\lambda(q,t)}{\prod(x_1,\cdots,x_N,0,\cdots,y;q,t)}$$

Let $P^0(x,y,q,t)$ be 1 on the empty partition and 0 elsewhere. The following remarks are useful.

1. Arguing as in Lemma 3 shows that the $P^N_{x,y,q,t}$ are probability measures. It is also clear that $lim_{N\to\infty}P^N_{x,y,q,t} = P_{x,y,q,t}$. There are other possible definitions of $P^N_{x,y,q,t}$ which converge to $P_{x,y,q,t}$ in the $N\to\infty$ limit (for instance one can truncate both the x and y variables). These deserve further investigation.

2. If one sets $y_i = t^{i-1}$, then $\frac{1}{\prod(x,y;q,t)}$ simplifies to $\prod_i(x_i,q)_\infty$. The Principal Specialization Formula then gives the simpler formula:

$$P_{x,y,q,t}(\lambda) = [\prod_i(x_i,q)_\infty]\frac{t^{n(\lambda)}P_\lambda(x;q,t)}{\prod_{s\in\lambda}1-q^{a(s)+1}t^{l(s)}}$$

   Further simplifications will be discussed as Examples 1 and 2 of this chapter.

2.5 An Algorithm for Picking From $P_{x,y,q,t}$

This section gives a stochastic method for picking from $P_{x,y,q,t}$ under conditions 1-3 of Section 2.4.

Algorithm for Picking from $P_{x,y,q,t}$

Step 0 Start with λ the empty partition and N (which we call the interval number) equal to 1.

Step 1 Pick an integer n_N so that $n_N = k$ with probability $\prod_j\frac{(x_Ny_j,q)_\infty}{(tx_Ny_j,q)_\infty}g_k(y;q,t)x_N^k$. (These probabilities sum to 1 by the definition of g_k).

Step 2 Let Λ be a partition containing λ such that the difference $\Lambda-\lambda$ is a horizontal strip of size n_N. There are at most a finite number of such Λ. Change λ to Λ with probability:

$$\frac{\phi_{\Lambda/\lambda}(q,t)}{g_{n_N}(y;q,t)}\frac{P_\Lambda(y;q,t)}{P_\lambda(y;q,t)}$$

(These probabilities sum to 1 by the Pieri Formula). Then set $N=N+1$ and go to Step 1.

It will be proved in Lemma 4 that this algorithm terminates with probability 1. It will be seen in Section 2.10 that a conditioned version of this algorithm is exactly one of Kerov's q-generalizations of the well studied hook walk of combinatorics.

As an example of the algorithm, suppose we are at Step 1 with $N = 3$ and the partition λ:

$$\begin{array}{ll} \cdot & \cdot \\ \cdot & \end{array}$$

We then pick n_3 according to the rule in Step 1. Suppose that $n_3 = 2$. We thus add a horizontal strip of size 2 to λ, giving Λ equal to one the following four partitions with probability given by the rule in Step 2:

$$\begin{array}{ll} \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \end{array}$$

$$\begin{array}{lll} \cdot & \cdot & \cdot \\ \cdot & & \\ \cdot & & \end{array}$$

$$\begin{array}{lll} \cdot & \cdot & \cdot \\ \cdot & \cdot & \end{array}$$

$$\begin{array}{llll} \cdot & \cdot & \cdot & \cdot \\ \cdot & & & \end{array}$$

We then set $N = 4$ and return to Step 1.

Lemma 4 *The algorithm terminates with probability 1.*

PROOF: Recall the Borel-Cantelli lemmas of probability theory, which say that if A_N are events with probability $P(A_N)$ and $\sum_N P(A_N) < \infty$, then with probability 1 only finitely many A_N occur. Let A_N be the event that at least one box is added to the partition during interval N. To prove the lemma it is sufficient to show that only finitely many A_N occur.

The Factorization Theorem implies that $g_0 = 1$. Again using the Factorization Theorem and the fact that $1 - e^{-x} \leq x$ for $x \geq 0$ shows that:

$$\begin{aligned} \sum_{N \geq 1} P(A_N) &= \sum_{N \geq 1} [1 - (\prod_j \frac{(x_N y_j; q)_\infty}{(t x_N y_j; q)_\infty}) g_0] \\ &= \sum_{N \geq 1} [1 - e^{-\sum_{n \geq 1} \frac{1}{n} \frac{1-t^n}{1-q^n} (x_N)^n p_n(y)}] \\ &\leq \sum_{N \geq 1} \sum_{n \geq 1} [\frac{1}{n} \frac{1-t^n}{1-q^n} (x_N)^n p_n(y)] \end{aligned}$$

$$
\begin{aligned}
&= \sum_{n\geq 1} \frac{1}{n}\frac{1-t^n}{1-q^n} p_n(x)p_n(y) \\
&\leq \frac{1}{1-q}\sum_{n\geq 1} p_n(x)p_n(y) \\
&= \frac{1}{1-q}\sum_{i,j\geq 1} \frac{x_iy_j}{1-x_iy_j} \\
&< \infty
\end{aligned}
$$

□

Theorem 3 is the main result of this section. Since q and t are fixed, the notation in the proof of Theorem 3 will be abbreviated somewhat by omitting the explicit dependence on these variables.

Theorem 3 *The chance that the algorithm yields the partition λ at the end of interval N is $P^N_{x,y,q,t}(\lambda)$. Consequently, the algorithm for picking from $P_{x,y,q,t}$ works.*

PROOF: Since the algorithm proceeds by adding horizontal strips, it is clear that the partition produced at the end of interval N has at most N parts.

The base case $N = 0$ is clear since the algorithm starts with the empty partition and $P^0_{x,y,q,t}$ is 1 on the empty partition and 0 elsewhere.

For the induction step, the Skew Expansion gives:

$$
\begin{aligned}
P^N_{x,y,q,t}(\Lambda) &= [\prod_{i=1}^N \prod_j \frac{(x_iy_j,q)_\infty}{(tx_iy_j,q)_\infty}] P_\Lambda(x_1,\cdots,x_N)P_\Lambda(y)b_\Lambda \\
&= [\prod_{i=1}^N \prod_j \frac{(x_iy_j,q)_\infty}{(tx_iy_j,q)_\infty}] P_\Lambda(y)b_\Lambda \sum_{\lambda\subset\Lambda} P_\lambda(x_1,\cdots,x_{N-1})P_{\Lambda/\lambda}(x_N) \\
&= [\prod_{i=1}^N \prod_j \frac{(x_iy_j,q)_\infty}{(tx_iy_j,q)_\infty}] P_\Lambda(y)b_\Lambda \sum_{\substack{\lambda\subset\Lambda \\ \Lambda-\lambda \ horiz.\ strip}} P_\lambda(x_1,\cdots,x_{N-1})x_N^{|\Lambda|-|\lambda|}\frac{b_\lambda}{b_\Lambda}\phi_{\Lambda/\lambda} \\
&= \sum_{\substack{\lambda\subset\Lambda \\ \Lambda-\lambda \ horiz.\ strip}} [(\prod_{i=1}^{N-1} \prod_j \frac{(x_iy_j,q)_\infty}{(tx_iy_j,q)_\infty}) P_\lambda(x_1,\cdots,x_{N-1})P_\lambda(y)b_\lambda] \\
&\quad [\prod_j \frac{(x_Ny_j,q)_\infty}{(tx_Ny_j,q)_\infty} g_{|\Lambda|-|\lambda|}(y)x_N^{|\Lambda|-|\lambda|}][\frac{\phi_{\Lambda/\lambda}}{g_{|\Lambda|-|\lambda|}(y)}\frac{P_\Lambda(y)}{P_\lambda(y)}] \\
&= \sum_{\substack{\lambda\subset\Lambda \\ \Lambda-\lambda \ horiz.\ strip}} [P^{N-1}_{x,y,q,t}(\lambda)][\prod_j \frac{(x_Ny_j,q)_\infty}{(tx_Ny_j,q)_\infty} g_{|\Lambda|-|\lambda|}(y)x_N^{|\Lambda|-|\lambda|}] \\
&\quad [\frac{\phi_{\Lambda/\lambda}}{g_{|\Lambda|-|\lambda|}(y)}\frac{P_\Lambda(y)}{P_\lambda(y)}]
\end{aligned}
$$

Probabilistically, this equality says that the chance that the algorithm gives Λ at the end of interval N is equal to the sum over all λ such that Λ/λ is a horizontal strip of the chance that the algorithm gives λ at the end of interval $N-1$ and that λ then grows to Λ in interval N. This proves the theorem. □

Corollary 1 *The distribution of the size of a partition λ chosen from $P_{x,y,q,t}$ has as its probability generating function in the variable z:*

$$\frac{\prod(xz, y; q, t)}{\prod(x, y; q, t)}$$

PROOF: By the way the algorithm works, the growth of λ during different intervals is independent. So it suffices to show that the chance λ grows by k in interval N is:

$$\prod_j \frac{(x_N y_j, q)_\infty}{(tx_N y_j, q)_\infty} [z^k] \prod_j \frac{(tx_N z y_j, q)_\infty}{(x_N z y_j, q)_\infty}$$

This is clear from Step 1 of the algorithm and the definition of g_k. □

As will be seen in Section 3.4, in the specialization $q = 0, x_i = t^i, y_i = t^{i-1}$ and $t = \frac{1}{q}$ (this q, different from the previous, is the order of a finite field), Corollary 1 proves Steinberg's theorem that the number of unipotent elements in $GL(n, q)$ is $q^{n(n-1)}$.

This section closes by noting that in the case $y_i = t^{i-1}$, there is a nice expression for g_n. For this and future use, recall the following lemma of Stong [56], which has an analytic proof.

Lemma 5 *For $|q| > 1$ and $0 < u < 1$,*

1. $\prod_{r=1}^{\infty} (\frac{1}{1-\frac{u}{q^r}}) = \sum_{n=0}^{\infty} \frac{u^n q^{\binom{n}{2}}}{(q^n-1)\cdots(q-1)}$
2. $\prod_{r=1}^{\infty} (1 - \frac{u}{q^r}) = \sum_{n=0}^{\infty} \frac{(-u)^n}{(q^n-1)\cdots(q-1)}$

Corollary 2 *If $0 < t, q < 1$, then $g_n(t^{i-1}; q, t) = \frac{1}{(1-q^n)\cdots(1-q)}$*

PROOF: By Lemma 5,

$$\begin{aligned} g_n(t^{i-1}; q, t) &= [u^n] \prod_{i=1}^{\infty} (\frac{1}{1 - uq^{i-1}}) \\ &= \frac{1}{q^n} [u^n] \prod_{i=1}^{\infty} (\frac{1}{1 - uq^i}) \\ &= \frac{1}{q^n} \frac{1}{q^{\binom{n}{2}} (\frac{1}{q^n} - 1) \cdots (\frac{1}{q} - 1)} \\ &= \frac{1}{(1 - q^n) \cdots (1 - q)} \end{aligned}$$

□

2.6 Example 1: Hall-Littlewood Polynomials

In this section the measure $P_{x,y,q,t}$ is studied under the specialization $y^i = t^{i-1}, q = 0$. As one motivation for these choices, note that setting $q = 0$ in the Macdonald polynomials gives the Hall-Littlewood polynomials. The Hall-Littlewood polynomials arise in many settings. To name three, they arise in enumerative problems in the theory of abelian p-groups, in the representation theory of $GL(n,q)$, and in the Hecke ring of GL over a local field. A good account of this is in Chapters 3-5 of Macdonald [43].

The further specialization $x_i = ut^i$ will be considered in Section 2.7. This further specialization is the case relevant to the finite classical groups. Nevertheless, in this section it will be seen that the probabilistic algorithm of Section 2.5 simplifies without having to assume that $x_i = ut^i$.

There is an explicit formula (which will not be used but is included for completeness) for the Hall-Littlewood polynomials. Let the permutation w act on the x-variables by sending x_i to $x_{w(i)}$. There is also a coordinate-wise action of w on $\lambda = (\lambda_1, \cdots, \lambda_n)$ and S_n^λ is defined as the subgroup of S_n stabilizing λ in this action. Recall that $m_i(\lambda)$ is the number of parts of λ of size i. For a partition $\lambda = (\lambda_1, \cdots, \lambda_n)$ of length $\leq n$, two formulas for the Hall-Littlewood polynomial are (page 208 of Macdonald [43]):

$$
\begin{aligned}
P_\lambda(x_1, \cdots, x_n; t) &= \left[\frac{1}{\prod_{i \geq 0} \prod_{r=1}^{m_i(\lambda)} \frac{1-t^r}{1-t}}\right] \sum_{w \in S_n} w\left(x_1^{\lambda_1} \cdots x_n^{\lambda_n} \prod_{i<j} \frac{x_i - tx_j}{x_i - x_j}\right) \\
&= \sum_{w \in S_n / S_n^\lambda} w\left(x_1^{\lambda_1} \cdots x_n^{\lambda_n} \prod_{\lambda_i > \lambda_j} \frac{x_i - tx_j}{x_i - x_j}\right)
\end{aligned}
$$

Here w acts on the x-variables. At first glance it is not obvious that these are polynomials, but the denominators cancel out after the symmetrization. The Hall-Littlewood polynomials interpolate between the Schur functions ($t = 0$) and the monomial symmetric functions ($t = 1$).

Supposing that $0 < t, x_i < 1, \sum_i x_i < 1$, we give a simplified algorithm which allows one to grow the partition λ by adding 1 box at a time. Using the Borel-Cantelli lemmas it is straightforward to check that this algorithm always halts.

Simplified Algorithm for Picking from $P_{x,t^{i-1},0,t}$

Step 0 Start with λ the empty partition and $N = 1$. Also start with a collection of coins indexed by the natural numbers such that coin i has probability x_i of heads and probability $1 - x_i$ of tails.

Step 1 Flip coin N.

Step 2a If coin N comes up tails, leave λ unchanged, set $N = N + 1$ and go to Step 1.

Step 2b If coin N comes up heads, let j be the number of the last column of λ whose size was increased during a toss of coin N (on the first toss of coin N which comes up heads, set $j = 0$). Pick an integer $S > j$ according to the rule that $S = j + 1$ with probability $t^{\lambda'_{j+1}}$ and $S = s > j + 1$ with probability $t^{\lambda'_s} - t^{\lambda'_{s-1}}$ otherwise. Then increase the size of column S of λ by 1 and go to Step 1.

For example, suppose we are at Step 1 with λ equal to the following partition:

$$
\begin{array}{llll}
. & . & . & . \\
. & . & & \\
. & & &
\end{array}
$$

Suppose also that $N = 4$ and that coin 4 had already come up heads once, at which time we added to column 1, giving λ. Now we flip coin 4 again and get heads, going to Step 2b. We have that $j = 1$. Thus we add a dot to column 1 with probability 0, to column 2 with probability t^2, to column 3 with probability $t - t^2$, to column 4 with probability 0, and to column 5 with probability $1 - t$. We then return to Step 1.

Note that the dots added during the tosses of a given coin form a horizontal strip.

Theorem 4 shows that the simplified algorithm works.

Theorem 4 *The simplified algorithm for picking from $P_{x,t^{i-1},0,t}$ refines the general algorithm.*

PROOF: Let interval N denote the time between the first and last tosses of coin N. To prove the theorem, it will be shown that the two algorithms add horizontal strips in the same way during interval N.

For this observe that the size of the strips added in interval N is the same for the two algorithms. Since $q = 0$ the integer n_N in Step 1 of the general algorithm is equal to k with probability $(1 - x_N)x_N^k$. This is equal to the chance of k heads of coin N in the simplified algorithm.

Given that a strip of size k is added during interval N, the general algorithm then increases λ to Λ with probability:

$$\frac{\phi_{\Lambda/\lambda}(0,t)}{g_k(t^{i-1};0,t)} \frac{P_\Lambda(1,t,t^2,\cdots;0,t)}{P_\lambda(1,t,t^2,\cdots;0,t)}$$

This probability can be simplified. Lemma 2 shows that $g_k(t^{i-1};0,t) = 1$. The definition of $\phi_{\Lambda/\lambda}(0,t)$ and the Principal Specialization Formula show that the probability can be rewritten as:

$$\Big(\prod_{s \in C_{\Lambda/\lambda}} \frac{b_\Lambda(s)}{b_\lambda(s)}\Big) \frac{t^{n(\Lambda)} \prod_{s \in \Lambda} \frac{1}{1-0^{a_\Lambda(s)}t^{l_\Lambda(s)+1}}}{t^{n(\lambda)} \prod_{s \in \lambda} \frac{1}{1-0^{a_\lambda(s)}t^{l_\lambda(s)+1}}}$$

where $0^0 = 1$. Let A be the set of column numbers $a > 1$ such that $\Lambda - \lambda$ intersects column a but not column $a - 1$. Let A' be the set of column numbers a such that either $a = 1$ or $a > 1$ and $\Lambda - \lambda$ intersects both columns a and $a - 1$. Most of the terms in the above expression cancel, giving:

$$\frac{t^{n(\Lambda)}}{t^{n(\lambda)}} \prod_{a \in A} (1 - t^{\lambda'_{a-1} - \lambda'_a}) = \prod_{a \in A'} t^{\lambda'_a} \prod_{a \in A} (t^{\lambda'_a} - t^{\lambda'_{a-1}})$$

It is easily seen that the simplified algorithm can go from λ to Λ in exactly 1 way, and this also happens with probability equal to:

$$\prod_{a \in A'} t^{\lambda'_a} \prod_{a \in A} (t^{\lambda'_a} - t^{\lambda'_{a-1}})$$

□

2.7 Young Tableau Algorithm

In this section it is assumed as in Section 2.6 that $q = 0, y_i = t^{i-1}$. It is further assumed that $x = ut^i$. We also set $t = \frac{1}{q}$ where q, different from the q above, is the size of a finite field. This is the case relevant to the finite classical groups.

As will emerge, the algorithm in this section is quite different from the simplified algorithm, which works by adding horizontal strips. A tantalizing question is to understand if there is some algebraic analog of the skew Macdonald polynomials which explains why this algorithm works.

Recall that a Young tableau T of size n is a partition of n with each box containing one of $\{1, \cdots, n\}$ such that each of $\{1, \cdots, n\}$ appears exactly once and the numbers increase in each row and column of T. For instance,

$$\begin{array}{llll} 1 & 3 & 5 & 6 \\ 2 & 4 & 7 & \\ 8 & 9 & & \end{array}$$

is a Young tableau. We call the algorithm in this section the Young Tableau Algorithm because numbering the boxes in the order in which they are created gives a Young tableau. It is assumed that $0 < u < 1$ and $q > 1$.

The Young Tableau Algorithm

Step 0 Start with $N = 1$ and λ the empty partition. Also start with a collection of coins indexed by the natural numbers, such that coin i has probability $\frac{u}{q^i}$ of heads and probability $1 - \frac{u}{q^i}$ of tails.

Step 1 Flip coin N.

Step 2a If coin N comes up tails, leave λ unchanged, set $N = N + 1$ and go to Step 1.

Step 2b If coin N comes up heads, choose an integer $S > 0$ according to the following rule. Set $S = 1$ with probability $\frac{q^{N-\lambda'_1}-1}{q^N-1}$. Set $S = s > 1$ with probability $\frac{q^{N-\lambda'_s}-q^{N-\lambda'_{s-1}}}{q^N-1}$. Then increase the size of column s of λ by 1 and go to Step 1.

Note that as with the previous algorithms, this algorithm halts by the Borel-Cantelli lemmas.

Let us now look at the same example as in Section 2.6, so as to see that the Young Tableau Algorithm is quite different from the simplified algorithm for the Hall-Littlewood polynomials.

So suppose we are at Step 1 with λ equal to the following partition:

$$\begin{array}{llll} . & . & . & . \\ . & . & & \\ . & & & \end{array}$$

Suppose also that $N = 4$ and that coin 4 had already come up heads once, at which time we added to column 1, giving λ. Now we flip coin 4 again and get heads, going to Step 2b. We add to column 1 with probability $\frac{q-1}{q^4-1}$, to column 2 with probability $\frac{q^2-q}{q^4-1}$, to column 3 with probability $\frac{q^3-q^2}{q^4-1}$, to column 4 with probability 0, and to column 5 with probability $\frac{q^4-q^3}{q^4-1}$. We then return to Step 1.

Note that there is a non-0 probability of adding to column 1, and that the dots added during the toss of a given coin need not form a horizontal strip. This contrasts sharply with the algorithm in Section 2.6.

We use the notation that $(x)_N = (1-x)(1-\frac{x}{q}) \cdots (1-\frac{x}{q^{N-1}})$. Recall from Section 2.2 that $m_i(\lambda)$ is the number of parts of λ of size i, that $n(\lambda) = \sum_i (i-1)\lambda_i$, that $a(s)$ is the number of squares in λ to the east of s, and that $l(s)$ is the number of squares in λ to the south of s. Lemma 6 gives a formula for the truncated measure $P^N_{\frac{u}{q^i}, \frac{1}{q^{i-1}}, 0, \frac{1}{q}}$ in terms of this notation.

Lemma 6 $P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda)=0$ *if* λ *has more than* N *parts. Otherwise:*

$$P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda)=\frac{u^{|\lambda|}(\frac{u}{q})_N(\frac{1}{q})_N}{(\frac{1}{q})_{N-\lambda_1'}}\prod_{i\geq 1}\frac{1}{q^{(\lambda_i')^2}(\frac{1}{q})_{m_i(\lambda)}}$$

PROOF: The first statement is clear from the definition of the measure $P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}$ in Section 2.4. The second equality can be deduced from the definition of $P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}$ and the Principal Specialization Formula as follows:

$$\begin{aligned}
P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda) &= \frac{P_\lambda(\frac{u}{q},\cdots,\frac{u}{q^N},0,\cdots;0,\frac{1}{q})P_\lambda(\frac{1}{q^{i-1}};0,\frac{1}{q})b_\lambda(0,t)}{\prod(\frac{u}{q},\cdots,\frac{u}{q^N},0,\cdots,\frac{1}{q^{i-1}};0,\frac{1}{q})}\\
&= [\prod_{i=1}^N(1-\frac{u}{q^i})]P_\lambda(\frac{u}{q},\cdots,\frac{u}{q^N},0,\cdots;0,\frac{1}{q})P_\lambda(\frac{1}{q^{i-1}};0,\frac{1}{q})b_\lambda(0,t)\\
&= \frac{\prod_{i=1}^N(1-\frac{u}{q^i})(1-\frac{1}{q^i})}{\prod_{i=1}^{N-\lambda_1'}(1-\frac{1}{q^i})}\frac{P_\lambda(\frac{u}{q},\cdots,\frac{u}{q^N},0,\cdots;0,\frac{1}{q})}{q^{n(\lambda)}}\\
&= \frac{u^{|\lambda|}(\frac{u}{q})_N(\frac{1}{q})_N}{(\frac{1}{q})_{N-\lambda_1'}}\frac{P_\lambda(\frac{1}{q},\cdots,\frac{1}{q^N},0,\cdots;0,\frac{1}{q})}{q^{n(\lambda)}}\\
&= \frac{u^{|\lambda|}(\frac{u}{q})_N(\frac{1}{q})_N}{(\frac{1}{q})_{N-\lambda_1'}}\frac{1}{q^{|\lambda|+2n(\lambda)}}\prod_{s\in\lambda:a(s)=0}\frac{1}{1-\frac{1}{q^{l(s)+1}}}\\
&= \frac{u^{|\lambda|}(\frac{u}{q})_N(\frac{1}{q})_N}{(\frac{1}{q})_{N-\lambda_1'}}\prod_{i\geq 1}\frac{1}{q^{(\lambda_i')^2}(\frac{1}{q})_{m_i(\lambda)}}
\end{aligned}$$

where the last equality uses the fact that $n(\lambda)=\sum_i\binom{\lambda_i'}{2}$. □

Theorem 5 *The chance that the Young Tableau algorithm yields* λ *at the end of interval* N *is* $P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda)$.

PROOF: The theorem is clear if $N<\lambda_1'$ for then $P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda)=0$, and Step 2b does not permit the number of parts of the partition to exceed the number of the coin being tossed at any stage in the algorithm.

For the case $N\geq\lambda_1'$, use induction on $|\lambda|+N$. The base case is that λ is the empty partition. This means that coins $1,2,\cdots,N$ all came up tails on their first tosses, which occurs with probability $(\frac{u}{q})_N$. So the base case checks.

Let $s_1\leq s_2\leq\cdots\leq s_k$ be the columns of λ with the property that changing λ by decreasing the size of one of these columns by 1 gives a partition λ^{s_i}. It then suffices to check that the claimed formula for $P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda)$ satisfies the equation:

$$\begin{aligned}
P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda) &= (1-\frac{u}{q^N})P^{N-1}_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda)+\frac{u}{q^N}\frac{q^{N-\lambda_1'}-1}{q^N-1}P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda^1)\\
&\quad+\sum_{s_i>1}\frac{u}{q^N}\frac{q^{N-\lambda_{s_i}'+1}-q^{N-\lambda_{s_i-1}'}}{q^N-1}P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda^{s_i})
\end{aligned}$$

This equation is based on the following logic. Suppose that when coin N came up tails, the algorithm gave the partition λ. If coin N came up tails on its first toss, then we must have had λ when coin $N-1$ came up tails. Otherwise, for each s_i we add the probability that "The algorithm gave the partition λ^{s_i} on the penultimate toss of coin N and the partition λ on the last toss of coin N". It is not hard to see that this probability is equal to the probability of getting λ^{s_i} on the final toss of coin N, multiplied by the chance of a heads on coin N which then gives the partition λ from λ^{s_i}.

We divide both sides of this equation by $P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda)$ and show that the terms on the right-hand side sum to 1. First consider the terms with $s_i > 1$. Induction gives that:

$$\begin{aligned}
&\sum_{s_i>1} \frac{u}{q^N}\frac{q^{N-\lambda'_{s_i}+1}-q^{N-\lambda'_{s_{i-1}}}}{q^N-1}\frac{P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda^{s_i})}{P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda)} \\
= &\sum_{s_i>1} \frac{q^{-\lambda'_{s_i}+1}-q^{-\lambda'_{s_{i-1}}}}{q^N-1}\frac{q^{\binom{\lambda'_{s_i}}{2}}(\frac{1}{q})_{\lambda'_{s_{i-1}}-\lambda'_{s_i}}(\frac{1}{q})_{\lambda'_{s_i}-\lambda'_{s_{i+1}}}}{q^{\binom{\lambda'_{s_i}-1}{2}}(\frac{1}{q})_{\lambda'_{s_{i-1}}-\lambda'_{s_i}+1}(\frac{1}{q})_{\lambda'_{s_i}-\lambda'_{s_{i+1}}-1}} \\
= &\sum_{s_i>1} \frac{q^{-\lambda'_{s_i}+1}-q^{-\lambda'_{s_{i-1}}}}{q^N-1}q^{2\lambda'_{s_i}-1}\frac{(1-\frac{1}{q^{\lambda'_{s_i}-\lambda'_{s_{i+1}}}})}{(1-\frac{1}{q^{\lambda'_{s_{i-1}}-\lambda'_{s_i}+1}})} \\
= &\sum_{s_i>1} \frac{q^{\lambda'_{s_i}}-q^{\lambda'_{s_{i+1}}}}{q^N-1} \\
= &\frac{q^{\lambda'_2}-1}{q^N-1}
\end{aligned}$$

Next consider the term coming from $P^{N-1}_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda)$. If $N=\lambda'_1$, then $\lambda'_1 > N-1$, so $P^{N-1}_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda)$ is 0 by what we have proven. Otherwise,

$$\begin{aligned}
(1-\frac{u}{q^N})\frac{P^{N-1}_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda)}{P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda)} &= (1-\frac{u}{q^N})\frac{(\frac{u}{q})_{N-1}(\frac{1}{q})_{N-1}(\frac{1}{q})_{N-\lambda'_1}}{(\frac{u}{q})_N(\frac{1}{q})_N(\frac{1}{q})_{N-\lambda'_1-1}} \\
&= \frac{(1-\frac{1}{q^{N-\lambda'_1}})}{(1-\frac{1}{q^N})} \\
&= \frac{q^N-q^{\lambda'_1}}{q^N-1}
\end{aligned}$$

So this term always contributes $\frac{q^N-q^{\lambda'_1}}{q^N-1}$.

Finally, consider the term coming from $P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda^1)$. This vanishes if $\lambda_1=\lambda_2$ since then λ^1 is not a partition. Otherwise,

$$\frac{u}{q^N}\frac{q^{N-\lambda'_{s_1}+1}-1}{q^N-1}\frac{P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda^{s_1})}{P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda)} = \frac{q^{-\lambda'_{s_1}+1}-q^{-N}}{q^N-1}\frac{(\frac{1}{q})_{N-\lambda'_1}}{(\frac{1}{q})_{N-\lambda'_1+1}}\frac{q^{\binom{\lambda'_{s_1}}{2}}(\frac{1}{q})_{\lambda'_1-\lambda'_2}}{q^{\binom{\lambda'_1-1}{2}}(\frac{1}{q})_{\lambda'_1-\lambda'_2-1}}$$

$$= \frac{q^{-\lambda_1'+1} - q^{-N}}{q^N - 1} \frac{1}{(1 - \frac{1}{q^{N-\lambda_1'+1}})} q^{2\lambda_1'-1}(1 - \frac{1}{q^{\lambda_1'-\lambda_2'}})$$

$$= \frac{q^{\lambda_1'} - q^{\lambda_2'}}{q^N - 1}$$

So in all cases this term contributes $\frac{q^{\lambda_1'} - q^{\lambda_2'}}{q^N - 1}$.
Adding up the three terms completes the proof. □

As an example of Lemma 6 and Theorem 5, suppose that $N = 4$ and λ is the partition:

$$\begin{array}{ll} \cdot & \cdot \\ \cdot & \\ \cdot & \end{array}$$

Then the chance that the Young Tableau Algorithm gives the partition λ when coin 4 comes up tails is:

$$\frac{u^4(1 - \frac{u}{q})(1 - \frac{u}{q^2})(1 - \frac{u}{q^3})(1 - \frac{u}{q^4})(1 - \frac{1}{q^3})(1 - \frac{1}{q^4})}{q^{10}(1 - \frac{1}{q})^2}$$

2.8 Weights on the Young Lattice

In this section T denotes a Young tableau and λ denotes the partition corresponding to T. Let $|T|$ be the size of T. As explained in Section 2.7, the Young Tableau algorithm constructs a Young tableau, and thus defines a measure on the set of all Young tableaux.

Let $P_{\frac{u}{q^i}, \frac{1}{q^{i-1}}, 0, \frac{1}{q}}(T)$ be the chance that the Young Tableau algorithm of Section 2.7 outputs T, and let $P^N_{\frac{u}{q^i}, \frac{1}{q^{i-1}}, 0, \frac{1}{q}}(T)$ be the chance that it outputs T when coin N comes up tails.

We also introduce the following notation. Let $T_{(i,j)}$ be the entry in the (i, j) position of T (recall that i is the row number and j the column number). For $j \geq 2$, let $A_{(i,j)}$ be the number of entries $(i', j-1)$ such that $T_{(i',j-1)} < T_{(i,j)}$. Let $B_{(i,j)}$ be the number of entries $(i', 1)$ such that $T_{(i',1)} < T_{(i,j)}$. For instance the tableau:

$$\begin{array}{cccc} 1 & 3 & 5 & 6 \\ 2 & 4 & 7 & \\ 8 & 9 & & \end{array}$$

has $T_{(1,3)} = 5$. Also $A_{(1,3)} = 2$ because there are 2 entries in column $3 - 1 = 2$ which are less than 5 (namely 3 and 4). Finally, $B_{(1,3)} = 2$ because there are 2 entries in column 1 which are less than 5 (namely 1 and 2).

There is a simple formula for $P^N_{\frac{u}{q^i}, \frac{1}{q^{i-1}}, 0, \frac{1}{q}}(T)$ in terms of this notation.

Theorem 6 $P^N_{\frac{u}{q^i}, \frac{1}{q^{i-1}}, 0, \frac{1}{q}}(T) = 0$ *if T has greater than N parts. Otherwise:*

$$P^N_{\frac{u}{q^i}, \frac{1}{q^{i-1}}, 0, \frac{1}{q}}(T) = \frac{u^{|T|}}{|GL(\lambda_1', q)|} \frac{\prod_{r=1}^{N}(1 - \frac{u}{q^r})(1 - \frac{1}{q^r})}{\prod_{r=1}^{N-\lambda_1'}(1 - \frac{1}{q^r})} \prod_{\substack{(i,j)\in\lambda \\ j \geq 2}} \frac{q^{1-i} - q^{-A_{(i,j)}}}{q^{B_{(i,j)}} - 1}$$

PROOF: The case where T has more than N parts is proven as in Theorem 5.

The case $\lambda'_1 \leq N$ is proven by induction on $|T|+N$. If $|T|+N = 1$, then T is the empty tableau and $N = 1$. This means that coin 1 in the Tableau algorithm came up tails on the first toss, which happens with probability $1 - \frac{u}{q}$. So the base case checks.

For the induction step, there are two cases. The first case is that the largest entry in T occurs in column $s > 1$. Removing the largest entry from T gives a tableaux T^s. We have the equation:

$$P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(T) = (1 - \frac{u}{q^N})P^{N-1}_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(T) + \frac{u}{q^N}\frac{q^{N-\lambda'_s+1} - q^{N-\lambda'_{s-1}}}{q^N - 1}P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(T^s)$$

The two terms in this equation correspond to the whether or not T was completed at time N. We divide both sides of the equation by $P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(T)$, substitute in the conjectured formula, and show that it satisfies this recurrence. The two terms on the right hand side then give:

$$\frac{q^N - q^{\lambda'_1}}{q^N - 1} + \frac{q^{-\lambda'_s+1} - q^{-\lambda'_{s-1}}}{q^N - 1}\frac{1}{\frac{q^{-\lambda'_s+1} - q^{-\lambda'_{s-1}}}{q^{\lambda'_1} - 1}} = 1$$

The other case is that the largest entry of T occurs in column 1. We then have the equation:

$$P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(T) = (1 - \frac{u}{q^N})P^{N-1}_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(T) + \frac{u}{q^N}\frac{q^{N-\lambda'_1} - 1}{q^N - 1}P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(T^1)$$

As in the previous case, we divide both sides of the equation by $P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(T)$, substitute in the conjectured formula, and show that it satisfies this recurrence. The two terms on the right hand side then give:

$$\frac{q^N - q^{\lambda'_1}}{q^N - 1} + \frac{1}{q^N}\frac{q^{N-\lambda'_1+1} - 1}{q^N - 1}\frac{1}{(1 - \frac{1}{q^{N-\lambda'_1+1}})}\frac{|GL(\lambda'_1, q)|}{|GL(\lambda'_1 - 1, q)|} = 1$$

This completes the induction, and the proof of the theorem. □

For instance, Theorem 6 says that if

$$S = \frac{u^4(1 - \frac{u}{q})(1 - \frac{u}{q^2})(1 - \frac{u}{q^3})(1 - \frac{u}{q^4})(1 - \frac{1}{q^2})(1 - \frac{1}{q^3})(1 - \frac{1}{q^4})}{|GL(3, q)|}$$

then the chances that the Young Tableau Algorithm gives the following tableaux:

$$\begin{matrix} 1 & 2 \\ 3 & \\ 4 & \end{matrix}$$

$$\begin{matrix} 1 & 3 \\ 2 & \\ 4 & \end{matrix}$$

$$\begin{matrix} 1 & 4 \\ 2 & \\ 3 & \end{matrix}$$

when coin 4 comes up tails are $\frac{S}{q}$, $\frac{S}{q^2}$, and $\frac{S}{q^3}$ respectively. Note that the sum of these probabilities is:

$$\frac{u^4(1-\frac{u}{q})(1-\frac{u}{q^2})(1-\frac{u}{q^3})(1-\frac{u}{q^4})(1-\frac{1}{q^3})(1-\frac{1}{q^4})}{q^{10}(1-\frac{1}{q})^2}$$

As must be the case and as was proved at the end of Section 2.7, this quantity is also equal to the chance that the Young Tableau Algorithm gives the partition:

$$\begin{array}{ll} \cdot & \cdot \\ \cdot & \\ \cdot & \end{array}$$

An interesting object in combinatorics is the Young lattice. The elements of this lattice are all partitions of all numbers. An edge is drawn between partitions λ and Λ if Λ is obtained from λ by adding one box. Note that a Young tableau T of shape λ is equivalent to a path in the Young lattice from the empty partition to λ. This equivalence is given by growing the partition λ by adding boxes in the order $1, \cdots, n$ in the positions determined by T. For instance the tableau:

$$\begin{array}{lll} 1 & 3 & 4 \\ 2 & & \end{array}$$

corresponds to the path:

$$\emptyset \rightarrow \begin{array}{l} \cdot \\ \end{array} \rightarrow \begin{array}{l} \cdot \\ \cdot \end{array} \rightarrow \begin{array}{ll} \cdot & \cdot \\ \cdot & \end{array} \rightarrow \begin{array}{lll} \cdot & \cdot & \cdot \\ \cdot & & \end{array}$$

One reason that the Young lattice is interesting is its connection with representation theory. For instance, it is well known (e.g. page 73 of Sagan [52]) that the dimension of the irreducible representation of S_n corresponding to the partition λ is the number of tableaux of shape λ, and hence the number of paths in the Young lattice from the empty partition to λ.

The measure $P_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(T)$ on Young tableaux has the following description in terms of weights on the Young lattice.

Corollary 3 *Put weights $m_{\lambda,\Lambda}$ on the Young lattice according to the rules:*

1. $m_{\lambda,\Lambda} = \frac{u}{q^{\lambda'_1}(q^{\lambda'_1+1}-1)}$ *if Λ is obtained from λ by adding a box to column 1*

2. $m_{\lambda,\Lambda} = \frac{u(q^{-\lambda'_s}-q^{-\lambda'_{s-1}})}{q^{\lambda'_1}-1}$ *if Λ is obtained from λ by adding a box to column $s > 1$*

Then the chance that the Tableau algorithm produces T is equal to:

$$\prod_{r=1}^{\infty}(1-\frac{u}{q^r})\prod_{i=0}^{|T|-1} m_{\gamma_i,\gamma_{i+1}}$$

where the γ_i are the partitions in the path along the Young lattice which corresponds to the tableau T.

PROOF: This follows by letting $N \to \infty$ in Theorem 6 and the fact that T corresponds to a unique path in the Young lattice. $\square$

Note that the total weight out of the empty partition is $\frac{u}{q-1}$ and that the total weight out of any other partition λ is:

$$\begin{aligned} \frac{u}{q^{\lambda'_1}(q^{\lambda'_1+1}-1)} + \sum_{i\geq 2} \frac{u(q^{-\lambda'_s} - q^{-\lambda'_{s-1}})}{q^{\lambda'_1}-1} &= \frac{u}{q^{\lambda'_1}(q^{\lambda'_1+1}-1)} + \frac{u}{q^{\lambda'_1}} \\ &= \frac{uq}{q^{\lambda'_1+1}-1} \\ &< 1 \end{aligned}$$

Since the sum of the weights out of a partition λ to a larger partition Λ is less than 1, the weights can also be viewed as transition probabilities, provided that one allows for halting.

As an application of Corollary 3, we derive the generating function for the size of a partition having k parts. As will be seen in Sections 3.6 and 4.7, this proves the formulas of Rudvalis and Shinoda for the chance that an element of $GL(n,q)$ or $U(n,q)$ has a k-dimensional fixed space and gives a probabilistic interpretation to the products in these formulas.

For this some more notation is needed. Let T be a Young tableau with k parts. We define numbers $h_1(T), \cdots, h_k(T)$ associated with T. Let $h_m(T) = T_{(m+1,1)} - T_{(m,1)} - 1$ for $1 \leq m \leq k-1$ and let $h_k(T) = |T| - T_{(k,1)}$. So if $k = 3$ and T is the tableau

$$\begin{matrix} 1 & 3 & 5 & 6 \\ 2 & 4 & 7 & \\ 8 & 9 & & \end{matrix}$$

then $h_1(T) = 2-1-1 = 0$, $h_2(T) = 8-2-1 = 5$, and $h_3(T) = 9-8 = 1$. View T as being created by the Young Tableau algorithm. Then for $1 \leq m \leq k-1$, $h_m(T)$ is the number of boxes added to T after it becomes a tableau with m parts and before it becomes a tableau with $m+1$ parts. $h_k(T)$ is the number of boxes added to T after it becomes a tableau with k parts. The proof of Theorem 7 will show that if one conditions T chosen from the measure $P_{\frac{u}{q^i}, \frac{1}{q^i-1}, 0, \frac{1}{q}}$ on having k parts, then the random variables $h_1(T), \cdots, h_k(T)$ are independent geometrics with parameters $\frac{u}{q}, \cdots, \frac{u}{q^k}$. This will explain the factorization on the right-hand side of the formula in Theorem 7.

Theorem 7

$$\sum_{\lambda:\lambda'_1=k} x^{|\lambda|} P_{\frac{u}{q^i}, \frac{1}{q^i-1}, 0, \frac{1}{q}}(\lambda) = \frac{(ux)^k}{|GL(k,q)|} \frac{\prod_{r=1}^{\infty}(1-\frac{u}{q^r})}{\prod_{r=1}^{k}(1-\frac{ux}{q^r})}$$

PROOF: We sum over all Young tableaux T with k parts "$x^{|T|}$ times the chance that the Tableau algorithm outputs T''. The point is that one can easily compute the probability that the Tableau algorithm produces a tableau T with given values $h_1, \cdots, h_k$.

Suppose that one takes a step up along the Young lattice from a partition with m parts. Corollary 3 implies that the weight for adding to column 1 is $\frac{u}{q^m(q^{m+1}-1)}$, and that the sum of the weights for adding to any other column is $\frac{u}{q^m}$. Thus $x^{|T|}$ times the chance that the Tableau algorithm yields a tableau with given values $h_1, \cdots, h_k$ is:

$$\prod_{r=1}^{\infty}(1-\frac{u}{q^r})\frac{(xu)^k}{|GL(k,q)|}\prod_{m=1}^{k}(\frac{ux}{q^m})^{h_m}$$

Summing over all possible values of $h_m \geq 0$ gives:

$$\begin{aligned}\sum_{\lambda:\sum \lambda_1'=k} x^{|\lambda|}P_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda) &= \prod_{r=1}^{\infty}(1-\frac{u}{q^r})\frac{(ux)^k}{|GL(k,q)|}\prod_{m=1}^{k}[\sum_{h_m=0}^{\infty}(\frac{ux}{q^m})^{h_m}] \\ &= \prod_{r=1}^{\infty}(1-\frac{u}{q^r})\frac{(ux)^k}{|GL(k,q)|}\prod_{m=1}^{k}\frac{1}{(1-\frac{ux}{q^m})} \\ &= \frac{(ux)^k}{|GL(k,q)|}\frac{\prod_{r=1}^{\infty}(1-\frac{u}{q^r})}{\prod_{r=1}^{k}(1-\frac{ux}{q^r})}\end{aligned}$$

□

2.9 Example 2: Schur Functions and a q-analog of the Plancharel Measure of the Symmetric Group

This section studies the measure $P_{x,y,q,t}(\lambda)$ under the specialization $x_i = t^i, y_i = t^{i-1}, q = t$. We then set $t = \frac{1}{q}$, where this q is the size of a finite field. As motivation for these choices, it is known (page 306 of Macdonald [43]) that setting $q = t$ in the Macdonald symmetric functions gives the Schur functions. Since the Schur functions have numerous applications in the theory of the symmetric and general linear groups, it is natural to set $q = t$. The specializations $x_i = t^i$ and $y_i = t^{i-1}$ lead to nice simplifications because the Principal Specialization Formula can be applied.

A q-analog of Plancharel measure arises in a natural way in this section. This q-analog will be compared and contrasted with Kerov's q-analog [36] in Section 2.10. Let us recall the definition of Plancharel measure and its connection with the representation theory of the symmetric groups. Letting $h(s) = a(s) + l(s) + 1$ be the hook-length of $s \in \lambda$, the Plancharel measure on partitions of size n assigns to λ the probability $\frac{n!}{\prod_{s\in\lambda} h(s)^2}$. The connection with the representation theory of the symmetric group is that the irreducible representations of S_n can be parameterized by partitions λ of n such that the representation corresponding to λ has dimension $\frac{n!}{\prod_{s\in\lambda} h(s)}$ (pages 53-96 of Sagan [52]). The Plancharel measure is a measure because the sum of the squares of the dimensions of the irreducible representations of a group is equal to the order of a group.

Lemma 7 gives a formula for the measure $P^N_{\frac{u}{q^i},\frac{1}{q^{i-1}},\frac{1}{q},\frac{1}{q}}$. We use the notation that $(x)_N = (1-x)(1-\frac{x}{q})\cdots(1-\frac{x}{q^{N-1}})$. Let $h(s) = a(s) + l(s) + 1$ and $c(s) = a'(s) - l'(s)$ denote the hook length and content of $s \in \lambda$ (here $l'(s), l(s), a(s)$, and $a'(s)$ are the number of squares in λ to the north, south, east, and west of s respectively).

Lemma 7

$$P^N_{\frac{1}{q^i},\frac{1}{q^{i-1}},\frac{1}{q},\frac{1}{q}}(\lambda) = [\prod_{r=1}^{N}\prod_{t=0}^{\infty}(1-\frac{1}{q^{r+t}})]\frac{1}{q^{2n(\lambda)+|\lambda|}}\prod_{s\in\lambda}\frac{1-\frac{1}{q^{N+c(s)}}}{(1-\frac{1}{q^{h(s)}})^2}$$

PROOF: This can be deduced from the definition of the measure $P^N_{\frac{1}{q^i},\frac{1}{q^{i-1}},\frac{1}{q},\frac{1}{q}}$ and the Principal Specialization Formula as follows:

$$\begin{aligned}
P^N_{\frac{1}{q^i},\frac{1}{q^{i-1}},\frac{1}{q},\frac{1}{q}}(\lambda) &= \frac{P_\lambda(\frac{1}{q},\cdots,\frac{1}{q^N},0,\cdots;\frac{1}{q},\frac{1}{q})P_\lambda(\frac{1}{q^{i-1}};\frac{1}{q},\frac{1}{q})b_\lambda(\frac{1}{q},\frac{1}{q})}{\prod(\frac{1}{q},\cdots,\frac{1}{q^i},0,\cdots,\frac{1}{q^{i-1}})} \\
&= [\prod_{r=1}^{N}\prod_{t=0}^{\infty}(1-\frac{1}{q^{r+t}})]\frac{1}{q^{n(\lambda)}}\prod_{s\in\lambda}\frac{1}{(1-\frac{1}{q^{h(s)}})}P_\lambda(\frac{1}{q},\cdots,\frac{1}{q^N},0,\cdots;\frac{1}{q},\frac{1}{q}) \\
&= [\prod_{r=1}^{N}\prod_{t=0}^{\infty}(1-\frac{1}{q^{r+t}})]\frac{1}{q^{2n(\lambda)+|\lambda|}}\prod_{s\in\lambda}\frac{1-\frac{1}{q^{N+c(s)}}}{(1-\frac{1}{q^{h(s)}})^2}
\end{aligned}$$

□

Renormalizing the measure $P_{\frac{1}{q^i},\frac{1}{q^{i-1}},\frac{1}{q},\frac{1}{q}}$ to live on partitions of size n will give a q-analog of the Plancharel measure. To this end, we introduce polynomials $J_n(q)$. First define $J_\lambda(q)$ by:

$$J_\lambda(q) = \frac{q^{|\lambda|^2-|\lambda|-2n(\lambda)}[(\frac{1}{q})_{|\lambda|}]^2}{\prod_{s\in\lambda}(1-\frac{1}{q^{h(s)}})^2}$$

The measure $P_{\frac{1}{q^i},\frac{1}{q^{i-1}},\frac{1}{q},\frac{1}{q}}$ can then be written as:

$$P_{\frac{1}{q^i},\frac{1}{q^{i-1}},\frac{1}{q},\frac{1}{q}}(\lambda) = [\prod_{r=1}^{\infty}\prod_{t=0}^{\infty}(1-\frac{1}{q^{r+t}})]\frac{J_\lambda(q)}{q^{|\lambda|^2}(1-\frac{1}{q})^2\cdots(1-\frac{1}{q^{|\lambda|}})^2}$$

It is not apriori clear that the $J_\lambda(q)$ are polynomials in q, but this will turn out to be true. Define $J_n(q) = \sum_{\lambda:|\lambda|=n} J_\lambda(q)$ and $J_0(q) = 1$. The $J_n(q)$ have interesting properties. The first 5 polynomials $J_n(q)$ are:

$$\begin{aligned}
J_1(q) &= 1 \\
J_2(q) &= 1+q^2 \\
J_3(q) &= 1+q^2+2q^3+q^4+1 \\
J_4(q) &= 1+q^2+2q^3+4q^4+2q^5+4q^6+2q^7+4q^8+2q^9+q^{10}+q^{12} \\
J_5(q) &= 1+q^2+2q^3+4q^4+6q^5+7q^6+8q^7+12q^8+12q^9+14q^{10} \\
&\quad +12q^{11}+12q^{12}+8q^{13}+7q^{14}+6q^{15}+4q^{16}+2q^{17}+q^{18}+q^{20}
\end{aligned}$$

Proposition 2, which follows immediately from the definitions in this section, explains why one might be interested in the polynomials $J_\lambda(q)$ and $J_n(q)$.

Proposition 2 *Under the measure $P_{\frac{1}{q^i},\frac{1}{q^{i-1}},\frac{1}{q},\frac{1}{q}}$, the conditional probability of λ given that $|\lambda| = n$ is equal to $\frac{J_\lambda(q)}{J_n(q)}$.*

We begin our study of $J_\lambda(q)$ and $J_n(q)$ with a fact from page 11 of Macdonald [43], which we prove as the proof is omitted there.

Lemma 8 *Let $h(s) = a(s) + l(s) + 1$ by the hooklength of $s \in \lambda$, and let $n(\lambda) = \sum_{i \geq 1}(i-1)\lambda_i$. Then:*

$$\sum_{s \in \lambda} h(s) = n(\lambda) + n(\lambda') + |\lambda|$$

PROOF: One way to compute the sum of the hook lengths is to count the number of hooks containing a given $s = (i,j) \in \lambda$. There are clearly $i + j - 1$ such hooks. Therefore,

$$\begin{aligned}
\sum_{s \in \lambda} h(s) &= \sum_{s \in \lambda}(i + j - 1) \\
&= \sum_{s \in \lambda}(i-1) + \sum_{s \in \lambda}(j-1) + \sum_{s \in \lambda} 1 \\
&= n(\lambda) + n(\lambda') + |\lambda|
\end{aligned}$$

□

It is possible to relate the polynomials $J_\lambda(q)$ to the Kostka-Foulkes polynomials $K_\lambda(q)$ (sometimes denoted $K_{\lambda(1^n)}(q)$). The Kostka-Foulkes polynomials are discussed on pages 242-3 of Macdonald [43] and are also studied in Pak and Stoyanovskii [49]. They are defined as:

$$K_\lambda(q) = \frac{q^{n(\lambda)}[|\lambda|]!}{\prod_{s \in \lambda}[h(s)]}$$

where $[n] = 1 + q + \cdots + q^{i-1}$, the q-analog of the number n. The Kostka-Foulkes polynomials are special cases of Kazhdan-Lusztig polynomials. One can also check from Chapter 4 of Macdonald [43] that $K_{\lambda'}(q)$ is the degree of the unipotent representation of $GL(n,q)$ corresponding to the partition λ'.

Proposition 3 connects the $J_\lambda(q)$ to the Kostka-Foulkes polynomials.

Proposition 3 $J_\lambda(q) = [K_{\lambda'}(q)]^2$

PROOF: Using Lemma 8, observe that:

$$\begin{aligned}
J_\lambda(q) &= \frac{q^{|\lambda|^2 - |\lambda| - 2n(\lambda)}[(\frac{1}{q})_{|\lambda|}]^2}{\prod_{s \in \lambda}(1 - \frac{1}{q^{h(s)}})^2} \\
&= q^{|\lambda|^2 - |\lambda| - 2n(\lambda)} \frac{q^{2\sum_{s \in \lambda} h(s)}}{\prod_{s \in \lambda}(q^{h(s)} - 1)^2} \frac{\prod_{i=1}^{|\lambda|}(q^i - 1)^2}{q^{|\lambda|^2 + |\lambda|}} \\
&= q^{2\sum_{s \in \lambda} h(s) - 2|\lambda| - 2n(\lambda)} \left(\frac{[|\lambda|]!}{\prod_{s \in \lambda}[h(s)]}\right)^2 \\
&= q^{2n(\lambda')} \left(\frac{[|\lambda'|]!}{\prod_{s \in \lambda'}[h(s)]}\right)^2 \\
&= K_{\lambda'}(q)^2
\end{aligned}$$

□

Theorem 8 gives some properties of the $J_n(q)$. By the remark before Proposition 3, $J_n(q)$ is the sum of the squares of the degrees of the irreducible unipotent representations of $GL(n,q)$. Recall that $[u^n]f(u)$ means the coefficient of u^n in $f(u)$.

Theorem 8 *1. $J_n(q)$ is a symmetric polynomial of degree $2\binom{n}{2}$ which has non-negative integer coefficients and satisfies $J_n(1) = n!$.*

2. $\frac{J_n(q)}{q^{n^2}(1-\frac{1}{q})^2\cdots(1-\frac{1}{q^n})^2} = [u^n]\frac{1}{\prod_{r=1}^{\infty}\prod_{s=0}^{\infty}(1-\frac{u}{q^{r+s}})}$

3. $J_n(q)$ satisfies the recurrence:

$$\frac{J_n(q)}{q^{n^2}(1-\frac{1}{q})^2\cdots(1-\frac{1}{q^n})^2} = \frac{q^n}{q^n-1}\sum_{i=1}^{n}\frac{q^{\binom{i}{2}}}{(q^i-1)\cdots(q-1)}\frac{J_{n-i}}{q^{(n-i)(n-i+1)}(1-\frac{1}{q})^2\cdots(1-\frac{1}{q^{n-i}})^2}$$

PROOF: Proposition 3 shows that $J_n(q)$ is a polynomial with non-negative integer coefficients. Note by Lemma 8 that:

$$\begin{aligned} deg(J_\lambda) &= 2deg(K_{\lambda'}) \\ &= 2[n(\lambda') + \binom{|\lambda|+1}{2} - \sum_{s\in\lambda'} h(s)] \\ &= 2\binom{|\lambda|}{2} - 2n(\lambda) \end{aligned}$$

Thus J_λ has degree $2\binom{|\lambda|}{2}$ for $\lambda = (|\lambda|)$ and smaller degree for all other λ. So $J_n(q)$ has degree $2\binom{n}{2}$.

Symmetry means that $J_n(q) = q^{2\binom{n}{2}}J_n(\frac{1}{q})$. In fact $J_\lambda(q) + J_{\lambda'}(q)$ satisfies this property, by Lemma 8.

To see that $J_n(1) = n!$, observe that:

$$\begin{aligned} J_n(1) &= \sum_{\lambda\vdash n}[K_{\lambda'}(1)]^2 \\ &= \sum_{\lambda\vdash n}[K_{\lambda}(1)]^2 \\ &= \sum_{\lambda\vdash n}[\frac{n!}{\prod_{s\in\lambda} h(x)}]^2 \\ &= n! \end{aligned}$$

where the last step follows since the irreducible representation of S_n parameterized by λ has dimension $\frac{n!}{\prod_{x\in\lambda} h(x)}$, and the sum of the squares of the dimensions of the irreducible representations of a group is equal to the order of a group. A simpler proof follows from the recurrence which is part 3 of this theorem and the easy to check fact that all terms coming from $i > 1$ in the recurrence vanish upon setting $q = 1$.

For the second part of the theorem, it is useful to consider the measure $P_{\frac{u}{q^i},\frac{1}{q^{i-1}},\frac{1}{q},\frac{1}{q}}$. Arguing as in Lemma 7 shows that:

$$P_{\frac{u}{q^i},\frac{1}{q^{i-1}},\frac{1}{q},\frac{1}{q}}(\lambda) = [\prod_{r=1}^{\infty}\prod_{t=0}^{\infty}(1-\frac{u}{q^{r+t}})]\frac{u^{|\lambda|}J_\lambda(q)}{q^{|\lambda|^2}(1-\frac{1}{q})^2\cdots(1-\frac{1}{q^{|\lambda|}})^2}$$

The fact that this is a measure means that:

$$\sum_{n=1}^{\infty} \frac{u^n J_n(q)}{q^{n^2}(1-\frac{1}{q^2})\cdots(1-\frac{1}{q^n})^2} = \frac{1}{[\prod_{r=0}^{\infty}\prod_{s=1}^{\infty}(1-\frac{u}{q^{r+s}})]}$$

Taking coefficients of u^n on both sides proves the second part.

For the third part, induction and Lemma 5 give that:

$$\begin{aligned}
\frac{J_n(q)}{q^{n^2}(1-\frac{1}{q})^2\cdots(1-\frac{1}{q^n})^2} &= [u^n]\frac{1}{\prod_{r=0}^{\infty}\prod_{s=1}^{\infty}(1-\frac{u}{q^{r+s}})} \\
&= [u^n](\frac{1}{\prod_{t=1}^{\infty}(1-\frac{u}{q^t})})(\frac{1}{\prod_{r=0}^{\infty}\prod_{s=2}^{\infty}(1-\frac{u}{q^{r+s}})}) \\
&= [u^n](\frac{1}{\prod_{t=1}^{\infty}(1-\frac{u}{q^t})})(\frac{1}{\prod_{r=0}^{\infty}\prod_{s=1}^{\infty}(1-\frac{u}{q^{r+s+1}})}) \\
&= \sum_{i=0}^{n}(\frac{q^{\binom{i}{2}}}{(q^i-1)\cdots(q-1)})(\frac{J_{n-i}}{q^{n-i}q^{(n-i)^2}(1-\frac{1}{q})^2\cdots(1-\frac{1}{q^{n-i}})^2})
\end{aligned}$$

□

Corollary 4 of Theorem 8 shows that conditioning the measure $P_{\frac{1}{q^i},\frac{1}{q^{i-1}},\frac{1}{q},\frac{1}{q}}$ on $|\lambda| = n$ gives a q-analog of the Plancharel measure on partitions of size n. This measure will be further explored in Section 2.10.

Corollary 4 *The conditional probability of λ given that $|\lambda| = n$ under the measure $P_{\frac{1}{q^i},\frac{1}{q^{i-1}},\frac{1}{q},\frac{1}{q}}$ is a q-analog of Plancharel measure.*

Proof: Proposition 2 shows that the conditional probability is $\frac{J_\lambda(q)}{J_n(q)}$. The result follows from the definition of $J_\lambda(q)$, and the fact that $J_n(1) = n!$, which is part of the first statement of Theorem 8.
□

2.10 Comparison with Kerov's q-analogs of Plancharel Measure and the Hook Walk

Recall from Section 2.9 the Plancharel measure on partitions of n which assigns to λ mass $\frac{n!}{\prod_{s\in\lambda}h(s)^2}$, where $h(s)$ is the hook length of s. In Section 2.9 a q-analog of Plancharel measure was defined by the formula $\frac{J_\lambda(q)}{J_n q}$ where:

$$\begin{aligned}
J_\lambda(q) &= \frac{q^{|\lambda|^2-|\lambda|-2n(\lambda)}[(\frac{1}{q})_{|\lambda|}]^2}{\prod_{s\in\lambda}(1-\frac{1}{q^{h(s)}})^2} \\
J_n(q) &= q^{n^2}(1-\frac{1}{q})^2\cdots(1-\frac{1}{q^n})^2[u^n]\frac{1}{\prod_{r=1}^{\infty}\prod_{s=0}^{\infty}(1-\frac{u}{q^{r+s}})}
\end{aligned}$$

and $[u^n]$ means the coefficient of u^n.

Kerov [36] has some q-analogs of Plancharel measure. Let us consider his q-analog which comes from the Schur functions. It is related to Hecke algebras and knot invariants (see the references in his paper). Unfortunately, no explicit formula is given for his measure (although it will soon be clear that it is different from our q-analog).

Kerov's q-analog of Plancharel measure is defined implicitly by means of a probabilistic algorithm called the q hook walk. This walk starts with the empty partition, and adds a box at a time. The partition λ grows to Λ (here $|\Lambda| = |\lambda| + 1$) with probability:

$$\frac{q^{n(\Lambda)} \prod_{s \in \lambda} [h(s)]}{q^{n(\lambda)} \prod_{s \in \Lambda} [h(s)]}$$

It can now be seen that Kerov's q-analog of Plancharel measure is different from the q-analog introduced in Section 2.9, because the partition

$$\cdot \quad \cdot$$

has mass $\frac{1}{q+1}$ under Kerov's q-analog of Plancharel measure and mass $\frac{q^2}{q^2+1}$ under our q-analog of Plancharel measure.

Proposition 4 relates Kerov's q hook walk to the algorithm of Section 2.5.

Proposition 4 *Suppose that n_N is equal to 1 for all N in Step 1 of the algorithm of Section* 2.5 *for picking from $P_{\frac{1}{q^i}, \frac{1}{q^{i-1}}, \frac{1}{q}, \frac{1}{q}}$. The growth process on partitions this defines is exactly Kerov's q hook walk.*

PROOF: Step 2 in the algorithm of Section 2.5 changes λ to Λ with probability:

$$\frac{\phi_{\Lambda/\lambda}(\frac{1}{q}, \frac{1}{q})}{g_1(\frac{1}{q^{i-1}})} \frac{P_\Lambda(\frac{1}{q^{i-1}}; \frac{1}{q}, \frac{1}{q})}{P_\lambda(\frac{1}{q^{i-1}}; \frac{1}{q}, \frac{1}{q})}$$

The definition of $\phi_{\Lambda/\lambda}$ shows that $\phi_{\Lambda/\lambda}(\frac{1}{q}, \frac{1}{q}) = 1$. Corollary 2 shows that $g_1 = \frac{1}{1-\frac{1}{q}}$. The Principal Specialization Formula shows that $P_\lambda(\frac{1}{q^{i-1}}; \frac{1}{q}, \frac{1}{q})$ is equal to $\frac{1}{q^{n(\lambda)}} \prod_{s \in \lambda} \frac{1}{1-q^{h(s)}}$. Combining these facts proves that:

$$\frac{\phi_{\Lambda/\lambda}(\frac{1}{q}, \frac{1}{q})}{g_1(\frac{1}{q^{i-1}})} \frac{P_\Lambda(\frac{1}{q^{i-1}}; \frac{1}{q}, \frac{1}{q})}{P_\lambda(\frac{1}{q^{i-1}}; \frac{1}{q}, \frac{1}{q})} = \frac{q^{n(\Lambda)} \prod_{s \in \lambda} [h(s)]}{q^{n(\lambda)} \prod_{s \in \Lambda} [h(s)]}$$

as desired. □

Chapter 3

The General Linear Groups

3.1 Chapter Overview

This chapter begins in Section 3.2 with a description of the Kung-Stong cycle index and Stong's applications of it. In Section 3.3 several useful rewritings of the cycle index are given. The general linear groups are then used to define measures λ_ϕ on partitions. These measures turn out to be a special case of the measures defined in Chapter 2. In Sections 3.4, 3.6 and 3.7, the shapes of the random partitions λ_ϕ are studied and results are obtained about the distribution of the size, number of parts, and largest part of these partitions. These theorems are closely related to the probabilistic algorithms of Chapter 2 and to interesting combinatorics such as q-analogs of the Stirling and Bell numbers and the Rogers-Ramanujan identities. In Sections 3.5, 3.7 and 3.8, the cycle index for GL is used to obtain exact formulas for the $n \to \infty$ limit of the chance that an element of $GL(n,q)$ is regular, semisimple, or regular semisimple. Section 3.9 uses algebraic groups to study the $q \to \infty$ limit of the cycle index.

3.2 The Kung-Stong Cycle Index for $GL(n,q)$

To start let us describe the Kung-Stong cycle index for the general linear groups [39], [56]. This was discussed to some extent in Section 1.2. The notation used differs from Stong's but is more consistent with the theory of partitions. In any case, the concepts are the same.

Let α be an element of $GL(n,q)$. Then, as was explained in Section 1.2, α has its conjugacy class determined by its rational canonical form. This form corresponds to the following combinatorial data. To each monic irreducible polynomial ϕ over F_q, α associates a partition (perhaps the trivial partition) λ_ϕ of some non-negative integer $|\lambda_\phi|$. For example, the identity matrix has λ_{z-1} equal to (1^n) and an elementary matrix with $a \neq 0$ in the $(1,2)$ position, ones on the diagonal and zeros elsewhere has λ_{z-1} equal to $(2, 1^{n-2})$. In what follows λ_ϕ will be viewed as a function from the union of the general linear groups $GL(n,q)$ to the set of partitions. Recall that m_ϕ denotes the degree of ϕ. The only restrictions necessary for the data λ_ϕ to represent a conjugacy class are:

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

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 polynomial z may appear with non-zero multiplicity, so only the second restriction remains.

Let $x_{\phi,\lambda}$ be variables corresponding to pairs of polynomials and partitions. Define cycle indices for $GL(n,q)$ and $Mat(n,q)$ by:

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

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

It is also helpful to define a quantity $c_{GL,\phi,q}(\lambda)$. If λ is the empty partition, set $c_{GL,\phi,q}(\lambda) = 1$. 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:

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

Following Kung [39], Stong [56] proves the factorizations:

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

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

The factorization for the general linear groups is equivalent to the fact 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 [58]) and are useful in proving the simplicity of the projective special linear groups. We will count transvections directly and then check this with the class size formula.

Let V be an n dimensional vector space over F_q with some 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 $\vec{a}$. So the number of transvections is:

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

The numerator comes from the fact that there are $q^n - 1$ non-0 vectors $\vec{a}$ and $q^{n-1} - 1$ non-0 linear forms on V which vanish on $\vec{a}$. The denominator comes from the fact that sending $\vec{a}, \psi$ to $\lambda \vec{a}, \frac{1}{\lambda}\psi$ where $\lambda \in F_q$ is non-0 gives the same transvection.

This computation can also be done using the class size formula. Observe 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 the upcoming Lemma 11, 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. The Kung-Stong formula shows that the size of the conjugacy class in $GL(n,q)$ corresponding to $\lambda_{z-1} = (2, 1^{n-2})$ is:

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

The terms $c_{GL,\phi,q}$ in the Kung-Stong cycle indices appear difficult to work with, and in Section 3.3 several rewritings of them will be given. Nevertheless, Stong [56] was able to apply these formulas to obtain nice results. Stong obtained asymptotic (in n and q) estimates for the following quantities:

1. the number of conjugacy classes of $GL(n,q)$
2. the chance that an element of $GL(n,q)$ is a vector space derangement (i.e. fixes only the origin)
3. the mean and variance of the number of Jordan blocks of an element of $GL(n,q)$
4. the number of elements of $GL(n,q)$ satisfying a fixed polynomial equation
5. the chance that all polynomials appearing in the rational canonical form of $\alpha \in GL(n,q)$ are linear

Stong developed the heuristic that a degree m polynomial should be thought of as an m-cycle and studied the distribution of the degree of the rth highest degree polynomial occurring in the rational canonical form of α. Finally, he found a sense in which the $q \to \infty$ limit of the cycle index of $GL(n,q)$ converges to the cycle index of the symmetric group (see Section 3.9 for an interpretation and generalization of this result using the theory of algebraic groups). In [57], Stong obtained some results about the average order of a matrix (see Sections 4.8, 5.7 and 6.7 for a partial extension of these to the other classical groups).

The results in this chapter have a more probabilistic and less analytic flavor than Stong's work, which made use of asymptotic tools such as Laplace's method and Tauberian theorems. Some exact limit formulas will be obtained. The emphasis in this thesis is on understanding the partitions in the rational canonical form of α. To date, little seems to be known about these partitions.

More, however, is known about the polynomials in the rational canonical form of α. Lemma 9, for instance, counts irreducible polynomials of a given degree and will be used later. Let $I_{m,q}$ be the number of monic, degree m, irreducible $\phi \neq z$ with coefficients in F_q. Let μ be the usual Moebius function of elementary number theory.

Lemma 9

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

PROOF: From Hardy and Wright [31], 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. □

An analog of Lemma 9 will be proved for the other classical groups in Sections 4.3 and 5.3.

As the theory is basically equivalent for $GL(n,q)$ and $Mat(n,q)$, most of this chapter will focus on $GL(n,q)$.

3.3 Connection with the Hall-Littlewood Measures

This section begins with several useful rewritings of the expression $c_{GL,\phi,q}$ which appeared in the cycle index for $GL(n,q)$. Recall that:

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

where

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

and $m_i(\lambda)$ is the number of parts of λ of size i.

We use the notation of Section 2.3. Thus $l(s)$ and $a(s)$ are the number of squares to the south and east of s respectively. Also, $n(\lambda)=\sum_i(i-1)\lambda_i=\sum_i\binom{\lambda_i'}{2}$. Let $(\frac{1}{q})_i=(1-\frac{1}{q})(1-\frac{1}{q^2})\cdots(1-\frac{1}{q^i})$ and let $P_\lambda(x_1,x_2,\cdots;t)$ be the Hall-Littlewood polynomial corresponding to the partition λ, as defined in Section 2.6.

Theorem 9

$$\begin{aligned}c_{GL,\phi,q}(\lambda) &= q^{2m_\phi[\sum_{h<i}hm_h(\lambda)m_i(\lambda)+\frac{1}{2}\sum_i(i-1)m_i(\lambda)^2]}\prod_i|GL(m_i(\lambda),q^{m_\phi})|\\ &= q^{m_\phi[\sum_i(\lambda_i')^2]}\prod_i(\frac{1}{q^{m_\phi}})_{m_i(\lambda)}\\ &= \frac{q^{m_\phi n(\lambda)}}{P_\lambda(\frac{1}{q^{m_\phi}},\frac{1}{q^{2m_\phi}},\cdots;0,\frac{1}{q^{m_\phi}})}\end{aligned}$$

PROOF: For all three 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 $\lambda_i' = m_i(\lambda) + m_{i+1}(\lambda) + \cdots$.

For the third equality, the Principal Specialization Formula of Section 2.3 gives:

$$\begin{aligned} \frac{q^{m_\phi n(\lambda)}}{P_\lambda(\frac{1}{q^{m_\phi}}, \frac{1}{q^{2m_\phi}}, \cdots; 0, \frac{1}{q^{m_\phi}})} &= q^{|\lambda|+2n(\lambda)} \prod_{s\in\lambda: a(s)=0} (1 - \frac{1}{q^{l(s)+1}}) \\ &= q^{\sum_i (\lambda_i')^2} \prod_i (\frac{1}{q})_{m_i(\lambda)} \end{aligned}$$

For the third equality, the Principal Specialization Formula of Section 2.3 gives:

$$\begin{aligned} \frac{q^{m_\phi n(\lambda)}}{P_\lambda(\frac{1}{q^{m_\phi}}, \frac{1}{q^{2m_\phi}}, \cdots; 0, \frac{1}{q^{m_\phi}})} &= q^{|\lambda|+2n(\lambda)} \prod_{s\in\lambda: a(s)=0} (1 - \frac{1}{q^{l(s)+1}}) \\ &= q^{\sum_i (\lambda_i')^2} \prod_i (\frac{1}{q})_{m_i(\lambda)} \end{aligned}$$

□

Recall the measures $P_{\frac{u}{q^i}, \frac{1}{q^{i-1}}, 0, \frac{1}{q}}$ defined in Section 2.6 and studied as Example 1 of Chapter 2. Theorem 10 connects these with the cycle index of $GL(n,q)$ (see the remark after the theorem for a probabilistic interpretation).

Theorem 10

$$\begin{aligned} 1 + \sum_{n=1}^{\infty} Z_{GL(n,q)} u^n &= \prod_{\phi \neq z} \sum_\lambda x_{\phi,\lambda} \frac{P_\lambda(\frac{u}{q^{m_\lambda}}, \frac{u}{q^{2m_\lambda}}, \cdots; \frac{1}{q^{m_\lambda}})}{q^{m_\phi n(\lambda)}} \\ (1-u)[1 + \sum_{n=1}^{\infty} Z_{GL(n,q)} u^n] &= \prod_{\phi \neq z} \sum_\lambda x_{\phi,\lambda} P_{\frac{u^{m_\phi}}{q^{im_\phi}}, \frac{1}{q^{(i-1)m_\phi}}, 0, \frac{1}{q^{m_\phi}}}(\lambda) \end{aligned}$$

Proof: The first equation is the cycle index for GL combined with the third equality in Theorem 9.

The definition of the measure $P_{\frac{u^{m_\phi}}{q^{im_\phi}}, \frac{1}{q^{(i-1)m_\phi}}, 0, \frac{1}{q^{m_\phi}}}$ gives that:

$$P_{\frac{u^{m_\phi}}{q^{im_\phi}}, \frac{1}{q^{(i-1)m_\phi}}, 0, \frac{1}{q^{m_\phi}}}(\lambda) = \prod_{r=1}^{\infty} (1 - \frac{u^{m_\phi}}{q^{rm_\phi}}) \frac{P_\lambda(\frac{u}{q^{m_\lambda}}, \frac{u}{q^{2m_\lambda}}, \cdots; \frac{1}{q^{m_\lambda}})}{q^{m_\phi n(\lambda)}}$$

Therefore,

$$1+\sum_{n=1}^{\infty} Z_{GL(n,q)}u^n = \prod_{\phi\neq z}\sum_{\lambda} x_{\phi,\lambda}\frac{P_{\frac{u^{m_\phi}}{q^{im_\phi}},\frac{1}{q^{(i-1)m_\phi}},0,\frac{1}{q^{m_\phi}}}(\lambda)}{\prod_{r=1}^{\infty}(1-\frac{u^{m_\phi}}{q^{rm_\phi}})}$$

Setting all $x_{\phi,\lambda}$ to 1 in this equation gives:

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

Combining these last two equations proves the second equality of the theorem. □

An important remark is that Theorem 10 has the following probabilistic interpretation. For $0<u<1$, pick an integer randomly so that the chance of getting n is $(1-u)u^n$. Then choose an element of $GL(n,q)$ uniformly. The random variables λ_ϕ (defined on the union of all the groups GL) are independent with distribution $P_{\frac{u^{m_\phi}}{q^{im_\phi}},\frac{1}{q^{(i-1)m_\phi}},0,\frac{1}{q^{m_\phi}}}$. This observation will enable us to apply the probabilistic methods of Chapter 2.

Theorem 10 gives the following corollary which will be useful for studying $n\to\infty$ asymptotics.

Corollary 5 *The $n\to\infty$ limit of the random variables λ_ϕ with the uniform distribution on $GL(n,q)$ is $P_{\frac{1}{q^{im_\phi}},\frac{1}{q^{(i-1)m_\phi}},0,\frac{1}{q^{m_\phi}}}$.*

PROOF: Use the second equality in Theorem 10 and Lemma 1. □

3.4 The Size of the Partitions

The following theorem of Steinberg is normally proven using the Steinberg character, as on page 156 of Humphreys [33]. Recall that $\alpha\in GL(n,q)$ is called unipotent if all of its eigenvalues are equal to 1.

Theorem 11 *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 purpose of this section is to show that the GL case of Theorem 11 follows from the cycle index for GL and the probabilistic approach of Chapter 2. Related ideas will be useful for the other classical groups.

Theorem 12 *The number of unipotent elements of $GL(n,q)$ is $q^{n(n-1)}$.*

PROOF: Any unipotent α has $|\lambda_\phi(\alpha)|=0$ for $\phi\neq z-1$. Recall the following equation from the proof of Theorem 10:

$$1+\sum_{n=1}^{\infty} Z_{GL(n,q)}u^n = \prod_{\phi\neq z}[\sum_{\lambda} x_{\phi,\lambda}\frac{P_{\frac{u^{m_\phi}}{q^{im_\phi}},\frac{1}{q^{(i-1)m_\phi}},0,\frac{1}{q^{m_\phi}}}(\lambda)}{\prod_{r=1}^{\infty}(1-\frac{u^{m_\phi}}{q^{rm_\phi}})}]$$

In this equation, set $x_{z-1,\lambda} = 1$ for all λ and $x_{\phi,\lambda} = 0$ for $\phi \neq z-1$. Lemma 5 shows that the number of unipotent elements of $GL(n,q)$ is:

$$\begin{aligned} |GL(n,q)|[u^n] \sum_{\lambda} \frac{P_{\frac{u}{q^i},\frac{1}{q(i-1)},0,\frac{1}{q}}(\lambda)}{\prod_{r=1}^{\infty}(1-\frac{u}{q^r})} &= |GL(n,q)|[u^n] \prod_{r=1}^{\infty}(\frac{1}{1-\frac{u}{q^r}}) \\ &= q^{n(n-1)} \end{aligned}$$

□

Although this may not be transparent from the proof, Theorem 12 essentially used the generating function in the variable u of the size of a partition chosen from the measure $P_{\frac{1}{q^i},\frac{1}{q(i-1)},0,\frac{1}{q}}$ (Corollary 1 in Section 2.5). Using the cycle index in a similar fashion gives the following result of Gerstenhaber [22].

Theorem 13 *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:*

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

3.5 Counting 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. Stong [56] proves that the random variable X_n has mean and variance $log(n) + O(1)$. Goh and Schmutz [24] prove that X_n is asymptotically normal.

Lemma 10 gives a generating function for $X_n(\alpha)$ which simplifies somewhat Stong's computation of the mean of X_n. We perform this computation both to illustrate the elegance of the cycle index approach, and because the same technique will be used later for the other classical groups.

Lemma 10

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

Proof: Set $x_{\phi,\lambda} = x^{|\lambda|}$ for all polynomials ϕ. The result now follows from the second equality in Theorem 10 and from the generating function in the variable x of the size of a partition chosen from the measure $P_{\frac{u}{q^i},\frac{1}{q(i-1)},0,\frac{1}{q}}$ (Corollary 1 in Section 2.5). □

The mean of X_n is now easily computed.

Theorem 14 $EX_n = log(n) + O(1)$, *where the expectation is taken over the group $GL(n,q)$ with q fixed.*

Proof: Differentiating both sides of the generating function of Lemma 10 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:

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

□

Presumably it is possible to compute the variance and prove the asymptotic normality of X_n using the generating function of Lemma 10.

3.6 The Number of Parts in the Partitions

Let $P_{GL,n}(k,q)$ be the probability that an element of $GL(n,q)$ has a k dimensional fixed space, and let $P_{GL,\infty}(k,q)$ be the $n \to \infty$ limit of $P_{GL,n}(k,q)$. As noted in the introduction, Rudvalis and Shinoda obtained formulas for these quantities. This section begins with probabilistic proofs of these formulas using the Young Tableau Algorithm. The first step is to connect the theorems of Rudvalis and Shinoda with the partitions in the rational canonical form of α.

Lemma 11 *The dimension of the fixed space of an element α in $GL(n,q)$ is equal to $\lambda_{z-1}(\alpha)'_1$ (i.e. the number of parts of the partition corresponding to the polynomial $z-1$ in the rational canonical form of α).*

PROOF: It must be shown that the kernel of $\alpha - I$, where I is the identity map, has dimension $\lambda_{z-1}(\alpha)'_1$. By the explicit description of the rational canonical form of a matrix in Section 1.2, it is enough to prove that the kernel of the linear map with matrix $M = C((z-1)^i) - I$ is 1 dimensional for all i (as in Section 1.2, $C(\phi)$ is the companion matrix of a polynomial ϕ).

Each of the first $i-1$ rows of M sums to 0, and they are linearly independent. So it needs to be shown that the last row of M has sum 0. This follows from the fact that the coefficients of $(z-1)^i$ sum to 0. □

The Rudvalis/Shinoda formulas for $P_{GL,n}(k,q)$ and $P_{GL,\infty}(k,q)$ can now be deduced from Theorem 7 (which followed from the Young Tableau Algorithm).

Theorem 15 *1.* $P_{GL,n}(k,q) = \frac{1}{|GL(k,q)|}\sum_{i=0}^{n-k}\frac{(-1)^i q^{\binom{i}{2}}}{q^{ki}|GL(i,q)|}$

2. $P_{GL,\infty}(k,q) = \prod_{r=1}^{\infty}(1-\frac{1}{q^r})[\frac{(\frac{1}{q})^{k^2}}{(1-\frac{1}{q})^2\cdots(1-\frac{1}{q^k})^2}]$

PROOF: Using Lemma 11, Theorem 7 with $x=1$, Theorem 10, and Lemma 5 with u replaced by uq^{-k}, the chance that an element of $GL(n,q)$ has a k dimensional fix space is:

$$\begin{aligned}
[u^n]\frac{1}{1-u}\sum_{\lambda:\lambda_1'=k} P_{\frac{u}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda) &= [u^n]\frac{u^k\prod_{r=1}^{\infty}(1-\frac{u}{q^{k+r}})}{(1-u)|GL(k,q)|}\\
&= \frac{1}{|GL(k,q)|}[u^{n-k}]\frac{1}{1-u}\sum_{i=0}^{\infty}\frac{(-1)^i(uq^{-k})^i}{(q^i-1)\cdots(q-1)}\\
&= \frac{1}{|GL(k,q)|}\sum_{i=0}^{n-k}\frac{(-1)^i q^{-ki}}{(q^i-1)\cdots(q-1)}
\end{aligned}$$

For the second part of the theorem use Corollary 5 and Theorem 7 with $x=1$ and $u=1$ to conclude that:

$$\begin{aligned}
P_{GL,\infty}(k,q) &= \sum_{\lambda:\lambda_1'=k} P_{\frac{1}{q^i},\frac{1}{q^{i-1}},0,\frac{1}{q}}(\lambda)\\
&= \frac{\prod_{r=k+1}^{\infty}(1-\frac{1}{q^r})}{|GL(k,q)|}\\
&= \prod_{r=1}^{\infty}(1-\frac{1}{q^r})[\frac{(\frac{1}{q})^{k^2}}{(1-\frac{1}{q})^2\cdots(1-\frac{1}{q^k})^2}]
\end{aligned}$$

□

Some more group theoretic information can be read off of Theorem 7. This requires the following identity from page 280 of Hardy and Wright [31].

Lemma 12

$$\frac{1}{(1-ax)\cdots(1-ax^k)} = 1 + ax\frac{1-x^k}{1-x} + a^2x^2\frac{(1-x^k)(1-x^{k+1})}{(1-x)(1-x^2)} + \cdots$$

Theorem 16 *Fix an irreducible polynomial ϕ of degree m_ϕ.*

1. *The chance that $\alpha \in GL(n,q)$ has $\lambda_\phi(\alpha)$ with k parts and size j is:*

$$\frac{1}{|GL(k,q^{m_\phi})|}\frac{(\frac{1}{q^{m_\phi}})_{j-1}}{q^{(j-k)m_\phi}(\frac{1}{q^{m_\phi}})_{k-1}(\frac{1}{q^{m_\phi}})_{j-k}}\sum_{i=0}^{n-j}\frac{(-1)^i}{(q^{im_\phi}-1)\cdots(q^{m_\phi}-1)}$$

2. *The $n\to\infty$ limit of the chance that $\alpha \in GL(n,q)$ has $\lambda_\phi(\alpha)$ with k parts and size j is:*

$$\frac{\prod_{r=1}^{\infty}(1-\frac{1}{q^{rm_\phi}})}{|GL(k,q^{m_\phi})|}\frac{(\frac{1}{q^{m_\phi}})_{j-1}}{q^{(j-k)m_\phi}(\frac{1}{q^{m_\phi}})_{k-1}(\frac{1}{q^{m_\phi}})_{j-k}}$$

PROOF: As usual, assume without loss of generality that $\phi = z-1$. From the cycle index, Theorem 7, and Lemma 12, the probability is:

$$\begin{aligned}
[u^n x^j]\frac{1}{1-u}\frac{(ux)^k}{|GL(k,q)|}\frac{\prod_{r=1}^{\infty}(1-\frac{u}{q^r})}{\prod_{r=1}^{k}(1-\frac{ux}{q^r})} &= \frac{1}{|GL(k,q)|}\sum_{i=k}^{n}[u^{i-k}x^{j-k}]\frac{\prod_{r=1}^{\infty}(1-\frac{u}{q^r})}{\prod_{r=1}^{k}(1-\frac{ux}{q^r})} \\
&= \frac{1}{|GL(k,q)|}[(ux)^{j-k}]\frac{1}{\prod_{r=1}^{k}(1-\frac{ux}{q^r})}\sum_{i=k}^{n}[u^{i-j}]\prod_{r=1}^{\infty}(1-\frac{u}{q^r}) \\
&= \frac{1}{|GL(k,q)|}\frac{(\frac{1}{q})_{j-1}}{q^{j-k}(\frac{1}{q})_{k-1}(\frac{1}{q})_{j-k}}\sum_{i=j}^{n}[u^{i-j}]\prod_{r=1}^{\infty}(1-\frac{u}{q^r}) \\
&= \frac{1}{|GL(k,q)|}\frac{(\frac{1}{q})_{j-1}}{q^{j-k}(\frac{1}{q})_{k-1}(\frac{1}{q})_{j-k}}\sum_{i=0}^{n-j}\frac{(-1)^i}{(q^i-1)\cdots(q-1)}
\end{aligned}$$

The second part follows from the first part and the second assertion of Lemma 5.
□

Theorem 16 suggests that for large q, given that the partition λ_ϕ has size j, it will mostly likely consist of 1 part of length j. Section 3.8 will give a more precise formulation. Theorem 16 has the following consequence.

Corollary 6 *The number of rank $n-k$ nilpotent $n*n$ matrices is:*

$$\frac{|GL(n,q)|}{|GL(k,q)|}\frac{(\frac{1}{q})_{n-1}}{q^{n-k}(\frac{1}{q})_{k-1}(\frac{1}{q})_{n-k}}$$

PROOF: Add the identity matrix, then use Lemma 11 and part 1 of Theorem 16 with $j=n$. □

The remainder of this section examines the convergence of the distributions $P_{GL,n}$ to $P_{GL,\infty}$ and related combinatorics. Recall from Section 1.1 that for $n \geq l$, the lth moment of the distribution of fixed vectors in S_n is equal to the lth moment of its Poisson(1) limit. The following theorem is the analogous result for $GL(n,q)$.

Theorem 17 *For $n \geq l$, the lth moment of the distribution of fixed vectors in the natural action of $GL(n,q)$ is equal to the number of subspaces of an l dimensional vector space over F_q.*

PROOF: Apply Lemma 2 (Burnside) to the setting $G = GL(n,q)$, X is the product of l copies of V, and G acts separately on each coordinate of this l-tuple. This shows that the lth moment of the distribution of fixed vectors is the number of orbits of $GL(n,q)$ on the product of l copies of V.

So it suffices to show that the number of orbits of $GL(n,q)$ on the product of l copies of V is equal to the number of subspaces of an l dimensional vector space over F_q. To each orbit assign an invariant k called the number of parts of the orbit. Define k of the orbit by taking any element $(v_1,\cdots,v_l)$ in the orbit, and letting k be the dimension of the span of $\{v_1,\cdots,v_l\}$.

We prove more that what we need for the theorem, namely that the total number of orbits with k parts is the q-binomial coefficient $\begin{bmatrix} l \\ k \end{bmatrix}$, the number of k dimensional subspaces of an l dimensional space. This is done bijectively. Given an orbit, let $i_1,\cdots,i_k$ be the positions such that the dimension of the span of $\{v_1,\cdots,v_i\}$ is one more than the dimension of the span of $\{v_1,\cdots,v_{i-1}\}$. Let $v=(v_1,\cdots,v_l)$ be the unique element of the orbit such that $v_{i_1},\cdots,v_{i_k}$ are the standard basis vectors $e_1, \cdots, e_k$. Let M be the $n * l$ matrix whose columns are the vectors $v_1, \cdots, v_l$. Let M' be M with the last $n-k$ rows chopped off, so that M' is a $k * l$ matrix. Note that M' is in reduced row-echelon form, and hence by basic linear algebra corresponds to a unique k dimensional subspace of an l dimensional space. □

The number of subspaces of an l dimensional vector space was studied by Goldman and Rota [25], who termed them Galois numbers and found a recurrence for them. Although logically unnecessary, since it is fun and because a similar technique works for the other classical groups, we give a pictorial proof, which is probably new, of their theorem.

Theorem 18 *The limit moments M_l of the distribution of fixed vectors satisfy the recurrence $M_0 = 1$, $M_1 = 2$, $M_l = 2M_{l-1} + q^{l-1}M_{l-2}$.*

PROOF: Substituting $x = \frac{1}{q}$ in Theorem 6, it suffices to show that $M_l(x)$ satisfies the recurrence of the theorem, where $M_l(x)$ is defined so that:

$$M_l(x) \prod_{r=1}^{\infty} \frac{1}{1-x^r} = \sum_{k=0}^{\infty} \frac{x^{k^2}}{x^{kl}(1-x)^2 \cdots (1-x^k)^2}$$

Recall the concept of the Durfee square of a partition, used in the chapter on partitions in Hardy and Wright [31]. This is the largest square which fits in the diagram of a partition. Note that the coefficient of x^r in the kth term on the right hand side is $|S_k|$, where S_k is the set of partitions of $r + lk$ dots such that the Durfee square is of size $k * k$. Let A_k be the subset of S_k whose $k+1$st row also has size k, and let B_k be the subset of S_k whose $k+1$st column has size k. As can be seen by deleting a row or column respectively, both $|A_k|$ and $|B_k|$ are equal to the number of partitions of $r + (l-1)k$ dots such that the Durfee square is of size $k * k$. Thus $\sum_k (|A_k| + |B_k|) = 2[x^r]M_{l-1} \prod_{r=1}^{\infty} \frac{1}{1-x^r}$. Similarly, $\sum_k |A_k \cap B_k| = [x^r]M_{l-2} \prod_{r=1}^{\infty} \frac{1}{1-x^r}$. Finally, it is not to hard to see that:

$$\begin{aligned}
\sum_k |A_k \cup B_k|^c &= [x^r](\prod_{r=1}^{\infty} \frac{1}{1-x^r}) \sum_{k=1}^{\infty} \frac{x^{k^2}}{x^{lk}(1-x)^2 \cdots (1-x^{k-1})^2} \\
&= [x^r](\prod_{r=1}^{\infty} \frac{1}{1-x^r}) \sum_{k=1}^{\infty} \frac{x^{k^2-lk}}{(1-x)^2 \cdots (1-x^{k-1})^2} \\
&= [x^r](\prod_{r=1}^{\infty} \frac{1}{1-x^r}) \sum_{k=0}^{\infty} \frac{x^{k^2}}{x^{l-1}x^{(l-2)k}(1-x)^2 \cdots (1-x^k)^2} \\
&= [x^r](\prod_{r=1}^{\infty} \frac{1}{1-x^r}) \frac{M_{l-2}}{x^{l-1}}
\end{aligned}$$

where ^{c} denotes set complementation. The result now follows from the fact that $|S_k| = |A_k| + |B_k| - |A_k \cap B_k| + |A_k \cup B_k|^c$ for all k. □

Theorem 17 showed that the $n \to \infty$ limit of the distribution of fixed vectors of $GL(n,q)$ is reminiscent of the Poisson(1) distribution. Theorem 19 will show that the $n \to \infty$ limit distribution of fixed lines of V under the action of $GL(n,q)$ is a true q-analog of the Poisson distribution.

Recall that $S(l,k)$, the Stirling numbers of the second kind, are defined as the number of partitions of a set of size l into k parts. For example, $S(4,2) = 7$ because the seven partitions of $\{1,2,3,4\}$ into 2 parts are:

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

We define a q-analog $S_q(l,k)$ of the Stirling numbers of the second kind (an equivalent definition is in [5]). Pick $n \geq l$, let V be an n-dimensional vector space over F_q, and let $P^1(V)$ be the set of lines in V. Let $GL(n,q)$ act on the product of l copies of $P^1(V)$ by acting on each coordinate separately. Given an orbit of this action, define the number of parts of the orbit to be the dimension of the span of the l lines which are the coordinates of some representative of the orbit. Define $S_q(l,k)$ to be the number of orbits of this action with k parts. (It is not hard to see that this number is independent of $n \geq l$). Define $B_q(l) = \sum_{k=1}^{l} S_q(l,k)$. Conceptually, one may think of an orbit of $GL(n,q)$ on the l-fold copy of $P^1(V)$ as a q-analog of a set partition. In fact in [5], it was shown that there is a natural lattice structure one can put on these orbits which is a q-analog of the partition lattice. However, no connection was made with probability theory or representation theory.

Theorem 19 establishes some properties of these q-analogs. Recall that $[i]$ is equal to $1 + q + \cdots + q^{i-1}$, the q-analog of the integer i. The $q = 1$ cases of parts 3 and 4 in the following theorem are known (see page 34 of Stanley [54]).

Theorem 19 *1. $B_q(l)$ is the lth moment of the $n \to \infty$ limit of the distribution of fixed lines of an n dimensional vector space V under the action of $GL(n,q)$.*

2. $B_q(l)$ is the multiplicity of the trivial representation in the l fold tensor product of the permutation representation of $GL(n,q)$ on $P^1(V)$.

3. $S_q(l,k)$ satisfies the recurrence $S_q(l,k) = [k]S_q(l-1,k) + S_q(l-1,k-1)$, with initial conditions $S_q(l,0) = 0$, $S_q(l,1) = 1$.

4. $\sum_{l \geq k} S_q(l,k)x^l = \frac{x^k}{(1-x)(1-[2]x)\cdots(1-[k]x)}$

PROOF: The first assertion follows from Burnside's Lemma (Lemma 2) applied to the setting $G = GL(n,q)$, X is the product of l copies of $P^1(V)$, and G acts separately on each coordinate of this l-tuple.

For the second assertion, note that the lth moment is equal to $\frac{1}{|G|}\sum_{g \in G} F(g)^l$, where $F(g)$ is the number of fixed lines of $g \in G = GL(n,q)$. By character theory, this is the inner product of the character of the trivial representation with the l-fold tensor product of the permutation representation of $GL(n,q)$ on $P^1(V)$.

For the third part, recall that $S_q(l,k)$ is the number of orbits of $GL(l,q)$ on the l-fold copy of $P^1(V)$ with k parts. Consider the first $l-1$ coordinates of a representative of an orbit. If they span a k dimensional space, then the last coordinate must be one of the $[k]$ lines in their span, which accounts for the term $[k]S_q(l-1,k)$. If they span a $k-1$ dimensional space, then all possible choices of the last coordinate lead to the same orbit, which accounts for the term $S_q(l-1,k-1)$.

For the fourth part, let $(v_1, \cdots, v_l)$ be the representative of an orbit with k parts. Define a dimension sequence $d_1, \cdots, d_l$ by letting d_i be the dimension of the span of $\{v_1, \cdots, v_i\}$. Since the number of orbits with a given dimension sequence is $\frac{\prod_{i=1}^{l}[d_i]}{[k]!}$, summing over all possible dimension sequences gives:

$$\begin{aligned} S_q(l,k) &= \sum_{\substack{\vec{d}: d_1=1, d_l=k \\ d_{i+1} \leq d_i+1}} \frac{\prod_{i=1}^{l}[d_i]}{[k]!} \\ &= \sum_{1 \leq d_1, \cdots, d_{l-k} \leq k} [d_1] \cdots [d_{l-k}] \\ &= [x^l] \frac{x^k}{(1-x)(1-[2]x)\cdots(1-[k]x)} \end{aligned}$$

□

It is possible to place these results in a more general context. Let $n, l, k, r \geq 1$ be integers. Define $S_q(n,l,k,r)$ as the number of orbits of $GL(n,q)$ on the l fold product of k dimensional subspaces such that r is the dimension of the space spanned by the coordinates of some representative of the orbit. Let $B_q(n,l,k) = \sum_{r=1}^{n} S_q(n,l,k,r)$. Similarly, define $S(n,l,k,r)$ as the number of orbits of S_n on the l fold product of size k subsets of $\{1, \cdots, n\}$ such that r is the cardinality of the union of the coordinates of some representative of the orbit. Let $B(n,l,k) = \sum_{r=1}^{n} S(n,l,k,r)$.

Given Theorem 19, the following conjecture in plausible.

Conjecture $S_1(n,l,k,r) = S(n,l,k,r)$ for all $n, l, k, r \geq 1$.

A direct combinatorial proof seems challenging. Perhaps the concept of Schubert cells, which assigns a size k subset of $\{1, \cdots, n\}$ to every k dimensional subspace of an n dimensional vector space over F_q, will be helpful. If the conjecture is correct, it should be possible, along the lines of part 2 of Theorem 19, to give a representation theoretic proof of the weaker assertion that $B_1(n,l,k) = B(n,l,k)$.

This section ends by considering how quickly the distributions $P_{GL,n}$ converge to $P_{GL,\infty}$. Recall the notion of total variation distance between two probability distributions P and Q on a set X (this notion was also used in Section 1.1). Total variation distance is defined as:

$$|P - Q|_{TV} = \frac{1}{2} \sum_{x \in X} |P(x) - Q(x)|$$

The following bound from Neumann and Praeger [46] is useful.

Lemma 13 *For all* $n \geq 2$,

$$\prod_{r=1}^{n} (1 - \frac{1}{q^r}) > (1 - \frac{1}{q})^2$$

Theorem 20 combines Theorem 15 with a technique of Arratia and Tavare [2] for bounding the total variation distance between the distribution of fixed points in S_n and its Poisson(1) limit.

Theorem 20 $\frac{C(q)}{q^{\frac{n^2+3n}{2}}} \leq |P_{GL,n} - P_{GL,\infty}|_{TV} \leq \frac{C'(q)}{q^{\frac{n^2+3n}{2}}}$ *where* $C(q), C'(q)$ *depend on* q *but not* n.

PROOF: Part 1 of Theorem 15 says that:

$$P_{GL,n}(k) = \frac{1}{|GL(k,q)|} \sum_{i=0}^{n-k} \frac{(-1)^i q^{\binom{i}{2}}}{q^{ik}|GL(i,q)|}$$

The fact that this sum is an alternating series whose summands decrease in magnitude implies that:

$$\begin{aligned}
& \frac{1}{|GL(k,q)|}\left[\frac{q^{\binom{n-k+1}{2}}}{q^{(n-k+1)k}|GL(n-k+1,q)|} - \frac{q^{\binom{n-k+2}{2}}}{q^{(n-k+2)k}|GL(n-k+2,q)|}\right] \\
\leq \; & |P_{GL,n}(k) - P_{GL,\infty}(k)| \\
\leq \; & \frac{1}{|GL(k,q)|} \frac{q^{\binom{n-k+1}{2}}}{q^{(n-k+1)k}|GL(n-k+1,q)|}
\end{aligned}$$

Let's look at the lower bound and upper bound after summing over k ranging from 0 to n. For the lower bound:

$$\begin{aligned}
& \sum_{k=0}^{n} \frac{1}{|GL(k,q)|}\left[\frac{q^{\binom{n-k+1}{2}}}{q^{(n-k+1)k}|GL(n-k+1,q)|} - \frac{q^{\binom{n-k+2}{2}}}{q^{(n-k+2)k}|GL(n-k+2,q)|}\right] \\
= \; & \sum_{k=0}^{n} \frac{1}{|GL(k,q)|} \frac{q^{n+2} - q^k - 1}{q^{(n-k+2)(\frac{n+k+3}{2})}(1-\frac{1}{q})\cdots(1-\frac{1}{q^{n-k+2}})} \\
\geq \; & \frac{q^{n+2} - q^{n+1}}{q^{\frac{n^2+5n+6}{2}}} \sum_{k=0}^{n} \frac{1}{q^{\frac{k^2-k}{2}}} \\
= \; & \frac{C_1(q)}{q^{\frac{n^2+3n}{2}}}
\end{aligned}$$

For the upper bound:

$$\sum_{k=0}^{n} \frac{1}{|GL(k,q)|} \frac{q^{\binom{n-k+1}{2}}}{q^{(n-k+1)k}|GL(n-k+1,q)|} \leq \frac{1}{q(1-\frac{1}{q})^4} \frac{1}{q^{\frac{n^2+3n}{2}}} \sum_{k=0}^{n} \frac{1}{q^{\frac{k^2-k}{2}}} = \frac{C_2(q)}{q^{\frac{n^2+3n}{2}}}$$

These give:

$$\frac{C_1(q)}{q^{\frac{n^2+3n}{2}}} \leq \sum_{k=0}^{n} |P_{GL,n}(k) - P_{GL,\infty}(k)| \leq \frac{C_2(q)}{q^{\frac{n^2+3n}{2}}}$$

Part 2 of Proposition 15 says that:

$$P_{GL,\infty}(k) = \left[\prod_{r=1}^{\infty}(1-\frac{1}{q^r})\right] \frac{(\frac{1}{q})^{k^2}}{[(1-\frac{1}{q})\cdots(1-\frac{1}{q^k})]^2}$$

Therefore:

$$\sum_{k=n+1}^{\infty} P_{GL,\infty}(k) = \frac{C_3(q)}{q^{(n+1)^2}}$$

The theorem now follows from the triangle inequality and the fact that:

$$\sum_{k=n+1}^{\infty} P_{GL,n}(k) = 0$$

$\square$

3.7 The Largest Part of the Partitions

This section examines the distribution of the largest part of the partition λ_ϕ in the $n \to \infty$ limit for $GL(n,q)$. Gordon's generalization of the Rogers-Ramanujan identities arises naturally in this context and leads to formulas for the $n \to \infty$ limit of the chance that an element of $GL(n,q)$ or $Mat(n,q)$ is semisimple (i.e. diagonalizable over $\bar{F}_q$, the algebraic closure on F_q).

Lemma 14 is a statement of Gordon's generalization of the Rogers-Ramanujan identities. It is taken directly from page 111 of Andrews [1].

Lemma 14 *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 14 can be applied as follows, giving what seems to be the first appearance of the Rogers-Ramanujan identities in finite group theory.

Theorem 21 *For a fixed irreducible polynomial ϕ of degree m_ϕ and fixed $k \geq 2$, the $n \to \infty$ limit of the chance that α in $GL(n,q)$ has the largest part of the partition $\lambda_\phi(\alpha)$ less than k is:*

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

PROOF: Assume without loss of generality that $\phi = z - 1$. By Corollary 5 and the second equality in Theorem 9, this probability is equal to:

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

The result now follows from Lemma 14 by setting $n_i = m_i(\lambda)$, $i = k$, and $x = \frac{1}{q}$. $\square$

The following problem seems natural. For motivation, recall that in the proof of Theorem 15, Theorem 7 was used to give a probabilistic interpretation to the products in the Rudvalis/Shinoda formulas for $P_{GL,\infty}(k,q)$.

Problem Use Theorem 21 and the algorithms from Chapter 2 (or develop new algorithms) to give a probabilistic interpretation to the products in the Gordon identities, and hence a new proof of these identities. Attempt a similar undertaking for the other classical groups.

Recall that a matrix is said to be semisimple if it is diagonalizable over $\bar{F}_q$, the algebraic closure of F_q. The remainder of this section considers the chance that an element of $GL(n,q)$ 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 [32]), 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 1.2), 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 15 *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 $A \geq 2$. $\square$

Lemma 16 will be useful for manipulating the cycle index.

Lemma 16

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

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, 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. $\square$

Theorem 22 *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 1, 15, 16 and Theorem 21, the chance that an element of $Mat(n,q)$ is semisimple is:

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

□

Theorem 23 *The $n\rightarrow\infty$ 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 22 the chance is:

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

□

3.8 Counting Regular and Regular-Semisimple Matrices

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.

Consider $GL(n,q)$ as contained in $GL(n,\bar{F_q})$. The condition of regularity of $\alpha \in GL(n,q)$ can be stated in terms of the shapes of the partitions $\lambda_\phi(\alpha)$.

Lemma 17 *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 in Section 3.7 (otherwise see page 13 of Humphreys [33]) 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 $\sum_\phi m_\phi \sum_i \lambda'_{\phi,i}(\alpha) = n$. $\square$

It is worth remarking that the condition of Lemma 17, and hence the condition of regularity, is equivalent to the condition that the minimum polynomial of α is equal to the characteristic polynomial of α.

Lemma 17 leads us to call an element $\alpha \in Mat(d,q)$ regular if all $\lambda_\phi(\alpha)$ have at most 1 part. Neumann and Praeger [46], [47] 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 Section 1.3 for further details on this). Volkmann and Fleischmann [19] and Lehrer [40] 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 $n \rightarrow \infty$ 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 1 is used freely.

Theorem 24 *The $n \rightarrow \infty$ 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: Lemmas 15 and 22 show 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 16 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 25 *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 17 shows that regularity is equivalent to all λ_ϕ having at most 1 part. The cycle index for $Mat(n,q)$ and Lemma 16 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 26 *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:

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

□

Theorem 27 *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:

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

□

It is worth remarking, along the lines of Neumann and Praeger [46], that these results are intuitively reasonable. Namely, Steinberg [55] 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 25 and 27.

Similarly, Neumann and Praeger [46] noted that a matrix is regular semisimple iff 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 24 and 26.

Finally, the chance of being semi-simple is greater than the chance of being regular semi-simple, which is consistent with Theorem 23.

3.9 The $q \to \infty$ limit of the Cycle Indices

At the end of his paper, Stong [56] stated that if one sets $x_{\phi,\lambda} = (x_{m_\phi})^{|\lambda|}$ in the cycle index and lets $q \to \infty$, then one obtains the cycle index of the symmetric group. Indeed, Section 3.4 shows that for fixed q the cycle index for GL becomes:

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

Letting $q \to \infty$ and using the formula for $I_{m,q}$ (Lemma 9) gives:

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

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 [8]. 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 [40]) 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 28 *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 [8], 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:

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

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,

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

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

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

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

The heuristics at the end of Section 3.8 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 in this thesis (although the unitary group is not Chevalley so Theorem 28 does not apply). Some recent work of Lehrer [41] 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.

Chapter 4

The Unitary Groups

4.1 Chapter Overview

Section 4.2 describes Wall's work on the conjugacy classes of the finite unitary groups [61]. Section 4.3 studies polynomials invariant under an involution $\tilde{}$. This leads to a cycle index for the unitary groups. Section 4.4 uses the unitary groups to define measures on partitions and shows that these measures are a special case of measures defined in Chapter 2. Sections 4.5 and 4.7 examine some aspects of the shapes of partitions under these measures, such as the distribution of the size and number of parts. Sections 4.6 and 4.8 use the cycle index of Section 4.3 to study the number of Jordan blocks and average order of an element of $U(n,q)$ respectively. The results of these sections are an indication that the analogs of the theorems of Stong, Hansen, Goh, Schmutz, and their co-workers described in Sections 1.2 and 3.2 carry over to the other classical groups.

4.2 Conjugacy Classes in the Unitary Groups

The unitary group $U(n,q)$ (characteristic 2 is allowed in this chapter) 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 [7]) that any two non-degenerate skew-linear forms are equivalent, so that $U(n,q)$ is unique up to isomorphism. From Wall [61], the order of $U(n,q)$ is:

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

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 [61] 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. We will count unitary transvections directly and then check the answer with the class size formula. Let V be the vector space over the field F_{q^2} on which $U(n,q)$ acts. As is explained on page 69 of Dieudonne [14], a unitary transvection τ has the form:

$$\tau(\vec{x}) = \vec{x} + \lambda < \vec{x}, \vec{a} > \vec{a}$$

where $\lambda \in F_{q^2}$ is non-0, satisfying $\lambda^q = -\lambda$ and $\vec{a} \in V$ is a non-0 isotropic vector (i.e. $< \vec{a}, \vec{a} >= 0$). Arguing as on page 145 of Artin [3] (which counts isotropic vectors for the orthogonal case), one can prove inductively that the number of isotropic vectors in V is $(q^n-1)(q^{n-1}+1)+1$ if n is even and $(q^n+1)(q^{n-1}-1)+1$ if n is odd. The number of isotropic directions in V (i.e. a non-0 isotropic vector in V up to scaling) is $\frac{1}{q^2-1}$ times the number of non-0 isotropic vectors in V. One checks that there are $q-1$ unitary transvections in each isotropic direction and hence that the number of unitary transvections in $U(n,q)$ is:

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

This checks with the class size formula. To see this, note that Lemma 11 (which says that the dimension of the fixed space of α 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 the unitary transvections form a single conjugacy class of size:

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

4.3 The Cycle Index for the Unitary Groups

This section develops a cycle index for the finite unitary groups. In analogy with the general linear groups define a cycle index for the unitary groups by:

$$1 + \sum_{n=1}^{\infty} Z_{U(n,q)} u^n$$

where

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

Theorem 30 gives a factorization theorem for this cycle index in terms of quantities for GL (so that some of the results obtained in Chapter 2 can be carried over for free). For this and future use throughout this chapter, it is desirable to count the number of ϕ of a given degree invariant under $\tilde{}$.

Lemma 18 $\widetilde{\phi_1\phi_2} = \tilde{\phi}_1\tilde{\phi}_2$.

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 29 *$\tilde{I}_{m,q^2} = 0$ 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 $A(t) = \frac{1}{1-q^2t}$ because $M_m = q^{2m}$. Wall [61] 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 in Section 4.2).

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 18 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. □

Next, it will be proved that the cycle index of the unitary groups factors. (One can prove a factorization theorem without Theorem 29, but Theorem 29 is necessary to get an expression in terms of quantities related to GL). The quantities $c_{GL,\phi,q}$ and their various rewritings were considered in Section 3.3.

Theorem 30 *Let:*

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

Then:

$$1+\sum_{n=1}^{\infty} Z_{U(n,q)}u^n = \prod_{\phi\neq z,\phi=\tilde{\phi}}[\sum_{\lambda} x_{\phi,\lambda}\frac{(-u)^{|\lambda|m_\phi}}{c_{GL,z-1,-(q^{m_\phi})}(\lambda)}]\prod_{\{\phi,\tilde{\phi}\},\phi\neq\tilde{\phi}}[\sum_{\lambda} x_{\phi,\lambda}x_{\tilde{\phi},\lambda}\frac{u^{2|\lambda|m_\phi}}{c_{GL,z-1,q^{2m_\phi}}(\lambda)}]$$

PROOF: The theorem follows from Wall's description and formula for conjugacy class sizes in the unitary group (Section 4.2), provided that one can prove that for all $\phi = \tilde{\phi}$,

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

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

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 29 that if $\phi = \tilde{\phi}$, then ϕ has odd degree. With a little more detail,

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

□

The corresponding result for the groups GL in Section 3.9 and Theorem 30 show that setting $x_{\phi,\lambda} = x_{m_\phi}^{|\lambda|}$ in the cycle index for the unitary groups gives the factorization:

$$\prod_{\substack{m=1 \\ m\ odd}}^{\infty} \prod_{i=1}^{\infty} \left(\frac{1}{1+(-1)^i(\frac{u^m}{q^{im}})x_m}\right)^{\tilde{I}_{m,q^2}} \prod_{m=1}^{\infty}\prod_{i=1}^{\infty}\left(\frac{1}{1-(\frac{u^{2m}}{q^{2im}})x_m^2}\right)^{\frac{I_{m,q^2}-\tilde{I}_{m,q^2}}{2}}$$

This implies the following fact.

Corollary 7 *Regard all polynomials of the same degree m as equivalent (i.e. set $x_{\phi,\lambda} = x_{m_\phi}^{|\lambda|}$ in the cycle index of the unitary groups). Then letting $q \to \infty$ gives:*

$$\prod_{m\ odd} e^{\frac{x_m u^m}{m}} \prod_{m=1}^{\infty} e^{\frac{(x_m)^2 u^{2m}}{2m}}$$

It would be interesting to interpret Corollary 7 using the cycle index of the hyperoctahedral group B_n, which is the Weyl group of $U(n,q)$. Note that Theorem 28 does not apply since the unitary groups are not Chevalley.

4.4 Connection with the Hall-Littlewood Measures

Theorem 31 connects the finite unitary groups with the measures of Chapter 2.

Theorem 31

$$\begin{aligned}
1+\sum_{n=1}^{\infty} Z_{U(n,q)}u^n &= \prod_{\phi \neq z, \phi=\tilde{\phi}} \frac{\sum_\lambda x_{\phi,\lambda} P_{\frac{(-u)^{m_\phi}}{(-q)^{im_\phi}},\frac{1}{(-q)^{(i-1)m_\phi}},0,\frac{1}{(-q)^{m_\phi}}}(\lambda)}{\prod_{r=1}^{\infty}(1-\frac{(-u)^{m_\phi}}{q^{rm_\phi}})} \\
&\quad \prod_{\{\phi,\tilde{\phi}\},\phi\neq\tilde{\phi}} \frac{\sum_\lambda x_{\phi,\lambda}x_{\tilde{\phi},\lambda} P_{\frac{u^{2m_\phi}}{q^{2im_\phi}},\frac{1}{q^{2(i-1)m_\phi}},0,\frac{1}{q^{2m_\phi}}}(\lambda)}{\prod_{r=1}^{\infty}(1-\frac{u^{2m_\phi}}{q^{2rm_\phi}})}
\end{aligned}$$

$$
\begin{aligned}
(1-u)[1+\sum_{n=1}^{\infty} Z_{U(n,q)} u^n] &= \prod_{\phi \neq z, \phi=\tilde{\phi}} \sum_{\lambda} x_{\phi,\lambda} P_{\frac{(-u)^{m_\phi}}{(-q)^{im_\phi}}, \frac{1}{(-q)^{(i-1)m_\phi}}, 0, \frac{1}{(-q)^{m_\phi}}}(\lambda) \\
&\quad \prod_{\{\phi,\tilde{\phi}\}, \phi \neq \tilde{\phi}} \sum_{\lambda} x_{\phi,\lambda} x_{\tilde{\phi},\lambda} P_{\frac{u^{2m_\phi}}{q^{2im_\phi}}, \frac{1}{q^{2(i-1)m_\phi}}, 0, \frac{1}{q^{2m_\phi}}}(\lambda)
\end{aligned}
$$

PROOF: This follows by arguing as in Theorem 10 for the unitary groups. □

The following remarks are important.

1. There is a probabilistic interpretation for the tower $U(n,q)$ as there was for the tower $GL(n,q)$. For $0 < u < 1$, pick an integer randomly so that the chance of getting n is $(1-u)u^n$. Then choose an element of $U(n,q)$ uniformly. If $\phi = \tilde{\phi}$, then the random variable λ_ϕ has distribution $P_{\frac{(-u)^{m_\phi}}{(-q)^{im_\phi}}, \frac{1}{(-q)^{(i-1)m_\phi}}, 0, \frac{1}{(-q)^{m_\phi}}}$. If $\phi \neq \tilde{\phi}$, then $\lambda_\phi = \lambda_{\tilde{\phi}}$ have distribution $P_{\frac{u^{2m_\phi}}{q^{2im_\phi}}, \frac{1}{q^{2(i-1)m_\phi}}, 0, \frac{1}{q^{2m_\phi}}}$. These random variables are independent and as with GL, the case $u = 1$ corresponds to the $n \to \infty$ limit.

2. The Young Tableau Algorithm of Section 2.7 does not carry over to unitary case if $\phi = \tilde{\phi}$, since then some of the "probabilities" involved are negative. The description in terms of weights on the Young lattice in Corollary 3 of Section 2.8, however, does extend to the unitary groups. The weight formula should be altered as follows. In the case $\phi = \tilde{\phi}$ one replaces the variables (u,q) by $(-u,-q)$, and in the case $\phi \neq \tilde{\phi}$ one replaces the variables (u,q) by (u^2,q^2).

4.5 The Size of the Partitions

This section proves Steinberg's count of unipotent elements in $U(n,q)$ using the cycle index for the unitary groups and the probabilistic algorithms of Chapter 2. Recall that Steinberg's theorem says that the number of unipotent elements is the square of the order of a p-Sylow. The order of $U(n,q)$ is $q^{\binom{n}{2}} \prod_{i=1}^n (q^i - (-1)^i)$ and its p-Sylow has size $q^{\binom{n}{2}}$.

Theorem 32 *The number of unipotent elements of $U(n,q)$ is $q^{n(n-1)}$.*

PROOF: Any unipotent α has $|\lambda_\phi(\alpha)| = 0$ if $\phi \neq z-1$. Setting $x_{\phi,\lambda} = 1$ for $\phi = z-1$, and $x_{\phi,\lambda} = 0$ for all other ϕ in the first equation of Theorem 31 and using Lemma 5 shows that the number of unipotent elements in $U(n,q)$ is:

$$
\begin{aligned}
|U(n,q)|[u^n] \sum_{\lambda} \frac{P_{\frac{-u}{(-q)^i}, \frac{1}{(-q)^{(i-1)}}, 0, \frac{1}{-q}}(\lambda)}{\prod_{r=1}^{\infty}(1 - \frac{-u}{(-q)^r})} &= |U(n,q)|[u^n] \prod_{r=1}^{\infty} (\frac{1}{1 - \frac{(-u)}{(-q)^r}}) \\
&= q^{n(n-1)}
\end{aligned}
$$

□

A similar argument using the cycle index and the remark after Theorem 31 proves the following more general assertion.

Theorem 33 *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:*

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

4.6 Counting Jordan Blocks

As in Section 3.5, let $X_n(\alpha)$ be the number of irreducible polynomials counted with multiplicity occurring in the Jordan canonical form of $\alpha \in U(n,q)$. Lemma 19 gives a generating function for $X_n(\alpha)$.

Lemma 19

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

PROOF: The proof is as in Lemma 10 of Section 3.5. □

With Lemma 19, the mean of X_n is easy to compute.

Theorem 34 $EX_n = \frac{3}{2} log(n) + O(1)$, *where the expectation is taken over the group $U(n,q)$ with q fixed.*

PROOF: Differentiating both sides of the generating function of Lemma 19 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 29 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,

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

□

It should be possible to use the generating function of Theorem 19 to find the variance of the random variable X_n and prove that it is asymptotically normal in the $n \to \infty$ limit.

4.7 The Number of Parts in the Partitions

Let $P_{U,n}(k,q)$ be the probability that an element of $U(n,q)$ has a k dimensional fixed space, and let $P_{U,\infty}(k,q)$ be the $n \to \infty$ limit of $P_{U,n}(k,q)$. A probabilistic proof is now given for the Rudvalis/Shinoda formulas for $P_{U,n}(k,q)$ and $P_{U,\infty}(k,q)$ [51]. It is worth remarking that the crucial ingredient in this proof is the Young Tableau Algorithm of Section 2.7.

Theorem 35 *1.* $P_{U,n}(k,q) = \frac{1}{|U(k,q)|} \sum_{i=0}^{n-k} \frac{(-1)^i (-q)^{\binom{i}{2}}}{(-q)^{ki} |U(i,q)|}$

2. $P_{U,\infty}(k,q) = [\prod_{r=0}^{\infty} (\frac{1}{1+\frac{1}{q^{2r+1}}})] \frac{(\frac{1}{q})^{k^2}}{(1-\frac{1}{q^2}) \cdots (1-\frac{1}{q^{2k}})}$

Proof: Using Lemma 11, Theorem 7 with $x=1$, Theorem 31, and Lemma 5 with u replaced by $-u(-q)^{-k}$, the chance that an element of $U(n,q)$ has a k dimensional fix space is:

$$\begin{aligned}
[u^n] \frac{1}{1-u} \sum_{\lambda:\lambda_1'=k} P_{\frac{-u}{(-q)^i}, \frac{1}{(-q)^{i-1}}, 0, \frac{1}{-q}}(\lambda) &= [u^n] \frac{(-u)^k \prod_{r=1}^{\infty} (1 - \frac{-u}{(-q)^{k+r}})}{(1-u)|GL(k,-q)|} \\
&= \frac{1}{|U(k,q)|} [u^{n-k}] \frac{1}{1-u} \sum_{i=0}^{\infty} \frac{(-1)^i (-u(-q)^{-k})^i}{((-q)^i - 1) \cdots (-q-1)} \\
&= \frac{1}{|U(k,q)|} \sum_{i=0}^{n-k} \frac{(-1)^i (-q)^{\binom{i}{2}}}{(-q)^{ki} |U(i,q)|}
\end{aligned}$$

For the second part of the theorem use Corollary 5 of Chapter 3 and Theorem 7 of Chapter 2 with $x=1$ and $u=-1$ to conclude that:

$$\begin{aligned}
P_{U,\infty}(k,q) &= \sum_{\lambda:\lambda_1'=k} P_{\frac{1}{(-q)^i}, \frac{1}{(-q)^{i-1}}, 0, \frac{1}{-q}}(\lambda) \\
&= \frac{\prod_{r=k+1}^{\infty} (1 - \frac{-1}{(-q)^r})}{|U(k,q)|} \\
&= [\prod_{r=1}^{\infty} (1 - \frac{1}{(-q)^r})] \frac{(\frac{1}{q})^{k^2}}{\prod_{s=1}^{k} (1 + \frac{1}{(-q)^s})(1 - \frac{1}{(-q)^s})} \\
&= [\prod_{r=1}^{\infty} (1 - \frac{1}{(-q)^r})] \frac{(\frac{1}{q})^{k^2}}{(1 - \frac{1}{q^2}) \cdots (1 - \frac{1}{q^{2k}})} \\
&= [\prod_{r=0}^{\infty} (\frac{1}{1 + \frac{1}{q^{2r+1}}})] \frac{(\frac{1}{q})^{k^2}}{(1 - \frac{1}{q^2}) \cdots (1 - \frac{1}{q^{2k}})}
\end{aligned}$$

(the last equality follows from the well known fact–e.g. page 277 of Hardy and Wright [31]–that the number of partitions of n into distinct parts is the same as the number of partitions of n into odd parts). □

The next result is analogous to Theorem 16. Only the unipotent case is discussed, although other polynomials can be treated by the remark after Theorem 31.

Theorem 36 *1. The chance that $\alpha \in U(n,q)$ has $\lambda_{z-1}(\alpha)$ with k parts and size j is:*

$$\frac{1}{|U(k,q)|} \frac{\prod_{i=1}^{j-1}(1-\frac{1}{(-q)^i})}{q^{(j-k)}\prod_{i=1}^{k-1}(1-\frac{1}{(-q)^i})\prod_{i=1}^{j-k}(1-\frac{1}{(-q)^i})} \sum_{i=0}^{n-j} \frac{(-1)^i}{(q^i-(-1)^i)\cdots(q+1)}$$

2. The $n \to \infty$ limit of the chance that $\alpha \in U(n,q)$ has $\lambda_{z-1}(\alpha)$ with k parts and size j is:

$$\frac{\prod_{r=1}^{\infty}(1-\frac{-1}{(-q)^r})}{|U(k,q)|} \frac{\prod_{i=1}^{j-1}(1-\frac{1}{(-q)^i})}{q^{(j-k)}\prod_{i=1}^{k-1}(1-\frac{1}{(-q)^i})\prod_{i=1}^{j-k}(1-\frac{1}{(-q)^i})}$$

PROOF: The cycle index for the unitary groups, Theorem 7, and Lemma 12 show that the probability of part 1 is equal to:

$$\begin{aligned}
& [u^n x^j] \frac{1}{1-u} \frac{(-ux)^k}{|GL(k,-q)|} \frac{\prod_{r=1}^{\infty}(1-\frac{-u}{(-q)^r})}{\prod_{r=1}^{k}(1-\frac{-ux}{(-q)^r})} \\
= \quad & \frac{1}{|U(k,q)|} \sum_{i=k}^{n} [u^{i-k}x^{j-k}] \frac{\prod_{r=1}^{\infty}(1-\frac{-u}{(-q)^r})}{\prod_{r=1}^{k}(1-\frac{-ux}{(-q)^r})} \\
= \quad & \frac{1}{|U(k,q)|} [(ux)^{j-k}] \frac{1}{\prod_{r=1}^{k}(1-\frac{-ux}{(-q)^r})} \sum_{i=k}^{n} [u^{i-j}] \prod_{r=1}^{\infty}(1-\frac{-u}{(-q)^r}) \\
= \quad & \frac{1}{|U(k,q)|} \frac{\prod_{i=1}^{j-1}(1-\frac{1}{(-q)^i})}{q^{(j-k)}\prod_{i=1}^{k-1}(1-\frac{1}{(-q)^i})\prod_{i=1}^{j-k}(1-\frac{1}{(-q)^i})} \sum_{i=j}^{n} [u^{i-j}] \prod_{r=1}^{\infty}(1-\frac{-u}{(-q)^r}) \\
= \quad & \frac{1}{|U(k,q)|} \frac{\prod_{i=1}^{j-1}(1-\frac{1}{(-q)^i})}{q^{(j-k)}\prod_{i=1}^{k-1}(1-\frac{1}{(-q)^i})\prod_{i=1}^{j-k}(1-\frac{1}{(-q)^i})} \sum_{i=0}^{n-j} \frac{(-1)^i}{(q^i-(-1)^i)\cdots(q+1)}
\end{aligned}$$

Part 2 follows from part 1 and Lemma 5.
□

Theorem 36 gives an interpretable consequence.

Corollary 8 *The number of unipotent elements of $U(n,q)$ with a k dimensional fixed space is:*

$$\frac{|U(n,q)|}{|U(k,q)|} \frac{\prod_{i=1}^{n-1}(1-\frac{1}{(-q)^i})}{q^{(n-k)}\prod_{i=1}^{k-1}(1-\frac{1}{(-q)^i})\prod_{i=1}^{n-k}(1-\frac{1}{(-q)^i})}$$

PROOF: Use Lemma 11 and Theorem 36 with $j=n$. □

We now consider the moments of the distribution of fixed vectors in the natural action of $U(n,q)$ on an n dimensional vector space V over F_{q^2}. This will make use of Witt's Lemma, on page 81 of Aschbacher [4].

Lemma 20 *Let V be a unitary, symplectic, or orthogonal space. Let U and W be subspaces of V and suppose that $\alpha : U \to W$ is an isometry. Then α extends to an isometry of V.*

Theorem 37 *For $n \geq 2l$, the lth moment of the distribution of fixed vectors in the natural action of $U(n,q)$ is equal to:*

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

PROOF: It will first be shown that for $n \geq 2l$, these moments are independent of n. By Lemma 2 (Burnside), the lth moment of the distribution of fixed vectors in the natural action of $U(n,q)$ is equal to the number of orbits of the action of $U(n,q)$ on the product of l copies of V, an n dimensional vector space over F_{q^2}. Let $(v_1, \cdots, v_l)$ be a representative of an orbit, and let d_i be the dimension of the span of $\{v_1, \cdots, v_i\}$. It is clear that two invariants of an orbit are the sequence $d_1, \cdots, d_l$ and the $l*l$ inner product matrix $(< v_i, v_j >)$. Lemma 20 (Witt) implies that two orbits with the same invariants are equal.

We claim that for $n \geq 2l$, all sequences $d_1, \cdots, d_l$ such that $d_{i+1} \leq d_i + 1$ arise, and that all matrices $(M_{i,j})$ satisfying $M_{i,j} \in F_{q^2}$ and $M_{i,j} = M_{j,i}^q$ (also called Hermitian matrices) are possible inner product matrices. We prove this claim for the hardest case $n = 2l$ (the $n > 2l$ case follows by adding an identity block to the matrix M' to be constructed). Note that this claim implies that the lth moments of the distribution of fixed vectors in the natural action of $U(n,q)$ are independent of n for $n \geq 2l$. To prove the claim, it suffices to show that given an $l*l$ Hermitian inner product matrix M, there exists a set of linearly independent vectors $v_1, \cdots, v_l$ in V with inner product matrix M. So on a vector space W with the same dimension as V define a Hermitian inner product matrix M' which in block form is:

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

Clearly $det(M') \neq 0$. It is known from Chapter 1 of Carter [7] that there is essentially one non-degenerate Hermitian scalar product on an n dimensional vector space, which implies that there is an isometry between V and W. This proves that the lth moment is independent of n provided that $n \geq 2l$.

It thus suffices to compute the moments for the $n \to \infty$ limit. By part 2 of Theorem 35 the lth moment is $M_l(x)$ where:

$$M_l(x)\prod_{i=0}^{\infty}(1+x^{2i+1}) = \sum_{k=0}^{\infty}\frac{x^{k^2}}{x^{2kl}(1-x^2)\cdots(1-x^{2k})}$$

and $x = \frac{1}{q}$. So the theorem will be proved when it is shown that $M_l(x)$ satisfies $M_0 = 1$, $M_l = M_{l-1}(1+\frac{1}{x^{2l-1}})$. $M_0 = 1$ since it is the sum of the probabilities of a measure.

The coefficient of x^r in the kth summand on right hand side is $|S_k|$, where S_k is the set of symmetric partitions of $r + 2lk$ such that the Durfee square (the largest square contained in the diagram of the partition) is of size $k*k$. This is because a term $(1-x^{2k})$ in the denominator can be viewed as contributing multiples of k to each side of the Durfee square. Let A_k be the subset of S_k whose $k+1$ row has size k. As is seen by deleting the $k+1$st rows and columns in a partition in S, $|A_k|$ is equal to the number of symmetric partitions of $r+2(l-1)k$ whose Durfee square is of size $k*k$. Thus $\sum_k |A_k| = [x^r]M_{l-1}\prod_{i=0}^{\infty}(1+x^{2i+1})$.

Let $B_k = S_k - A_k$. Then:

$$\sum_k |B_k| \;=\; \sum_{k=1}^{\infty}[x^{r+2lk}]\frac{x^{k^2}}{(1-x^2)\cdots(1-x^{2k-2})}$$

$$
\begin{aligned}
&= \sum_{k=1}^{\infty}[x^r]\frac{1}{x^{2l-1}}\frac{x^{(k-1)^2}}{x^{2(k-1)(l-1)}(1-x^2)\cdots(1-x^{2k-2})} \\
&= \sum_{k=0}^{\infty}[x^r]\frac{1}{x^{2l-1}}\frac{x^{k^2}}{x^{2k(l-1)}(1-x^2)\cdots(1-x^{2k})} \\
&= [x^r]\frac{1}{x^{2l-1}}M_{l-1}\prod_{i=0}^{\infty}(1+x^{2i+1})
\end{aligned}
$$

The result follows since $|S_k| = |A_k| + |B_k|$ for all k. □

There is more work to be done here. It should be easy to give total variation bounds between the distributions of $P_{U,n}(k,q)$ and $P_{U,\infty}(k,q)$ by the same technique as in Theorem 20. It would also be desirable to have a representation theoretic proof of Theorem 37 (see Theorem 19 for a discussion of why this is plausible).

4.8 Average Order of an Element of $U(n,q)$

Let $v_{GL,n}$ be the average over $GL(n,q)$ of the order of an element of $GL(n,q)$ (recall that the order of g in a group G is the smallest n such that g^n is the identity). Stong [57] shows that for fixed q and growing n, $log(v_{GL,n}) = nlog(q) - log(n) + o(log(n))$. Let $v_{U,n}$ be the average over $U(n,q)$ of the order of an element of $U(n,q)$. In this section it is shown that for fixed q and growing n, $log(v_{U,n}) \geq nlog(q) - log(n) + o(log(n))$. Presumably Stong's techniques carry over to prove that this lower bound is an upper bound as well.

Let $\Phi(n)$ denote the number of i between 1 and n inclusive, which are relatively prime to 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 $x \to x^{q^2}$. The next two lemmas are useful.

Lemma 21 *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 18 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 22 *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 38 *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 21 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 33, 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 [57] $log(\Phi(N)) = log(N) + O(log(log(N)))$, so that $log(v_n) \geq nlog(q) - log(n) + O(log(log(n)))$.

Suppose that n is even. By Lemma 22 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 33, 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. $\square$

Chapter 5

The Symplectic Groups

5.1 Chapter Overview

Section 5.2 describes Wall's results on the conjugacy classes of the finite symplectic groups [61]. Section 5.3 studies polynomials invariant under an involution $^{-}$. From this a cycle index for the symplectic groups emerges. Section 5.3 also uses the symplectic groups to define measures on partitions, and for all polynomials other than $\phi = z \pm 1$ relates these measures to the measures of Chapter 2. Sections 5.4 and 5.6 focus on the more elusive case $\phi = z \pm 1$ and study the size and number of parts of the corresponding random symplectic signed partitions. Sections 5.5 and 5.7 use the cycle index of Section 5.3 to obtain results on the number of Jordan blocks and average order of an element of $Sp(2n, q)$.

5.2 Conjugacy Classes in the Symplectic Groups

In this chapter it is assumed 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 $<,>: V \times V \to F_q$ 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 [7], there is only one such form up to equivalence, so $Sp(2n, q)$ is unique up to isomorphism. From Wall [61], the order of $Sp(2n, q)$ is:

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

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 [61], in which $\tilde{\phi}$ was used, but these maps are different. Namely $\tilde{}$ is defined on polynomials with coefficients in F_q, but $^{-}$ is defined on polynomials with coefficients in F_{q^2}. The distinction between the maps $\tilde{}$ and $\bar{}$ is evident in the different statements of Theorems 29 and 39.

Wall [61] 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

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

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

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

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 (see Chapter 6 for background on the orthogonal groups). The quantity $B(\phi)$ will also be denoted by $c_{Sp,\phi,q}(\lambda^{\pm})$.

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. It is known (page 139 of Artin [3]) that the symplectic transvections generate $Sp(2n, q)$. We will count symplectic transvections directly and then check the answer with Wall's formula. Let V be the vector space over the field F_{q^2} on which $Sp(2n, q)$ acts. As is explained on pages 9-10 of Dieudonne [14], a symplectic transvection τ has the form:

$$\tau(\vec{x}) = \vec{x} + \lambda < \vec{x}, \vec{a} > \vec{a}$$

where $\lambda \in F_q$ is non-0 and $\vec{a} \neq 0$. There are $\frac{q^{2n}-1}{q-1}$ lines in V. For any $\mu \in F_q$ with $\mu \neq 0$, replacing $\vec{a}$ by $\mu\vec{a}$ and λ by $\frac{\lambda}{\mu^2}$ gives the same transvection τ. Thus there are $q-1$ symplectic transvections along each line and hence a total of $q^{2n}-1$ symplectic transvections.

These symplectic transvections split into two conjugacy classes of size $\frac{q^{2n}-1}{2}$. To see this, note that Lemma 11 (which says that the dimension of the fixed space of α is the number of parts of $\lambda_{z-1}^{\pm}(\alpha)$) implies 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.

5.3 The Cycle Index for the Symplectic Groups

As with the general linear and unitary groups define:

$$Z_{Sp(2n,q)} = \frac{1}{|Sp(2n, q)|} \sum_{\alpha \in Sp(2n,q)} \prod_{\phi = z \pm 1} x_{\phi, \lambda_\phi^{\pm}(\alpha)} \prod_{\phi \neq z, z \pm 1} x_{\phi, \lambda_\phi(\alpha)}$$

Theorem 40 will prove that this cycle index factors. For this Theorem 39, 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 23 $\overline{\phi_1 \phi_2} = \bar{\phi}_1 \bar{\phi}_2$.

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

2. If $m \neq 1$ 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 29. 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 $\phi(0) \neq 0$ 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 [61] it is noted that $B(t) = \frac{(1+t)^2}{1-qt^2}$ (this follows from the explicit description of the definition of $\bar{\phi}$ given in Section 5.2).

Arguing exactly as for the unitary group in Theorem 29 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 40

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

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 given in Section 5.2. 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 39 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 symplectic groups can be used to define measures on partitions λ_ϕ and symplectic signed partitions $\lambda_{z\pm1}^{\pm}$ as follows. Fix u so that $0 < u < 1$ and pick the dimension with probability of dimension $2n$ equal to $(1-u^2)u^{2n}$. Then pick α uniformly in $Sp(2n,q)$ and let λ_ϕ and $\lambda_{z\pm1}^{\pm}$ be the data corresponding to the conjugacy class of α.

The cycle index for the symplectic groups and the remarks in Section 3.3 give an understanding of the partitions corresponding to the polynomials $\phi \neq z \pm 1$. If $\phi \neq z \pm 1$ and $\phi = \bar{\phi}$, the random variable λ_ϕ has distribution $P_{\frac{(-1)^{i-1} u^{m_\phi}}{q^{\frac{i m_\phi}{2}}}, \frac{(-1)^{i-1}}{q^{\frac{(i-1) m_\phi}{2}}}, 0, \frac{-1}{q^{\frac{m_\phi}{2}}}}$. If $\phi \neq \bar{\phi}$, then $\lambda_\phi = \lambda_{\bar{\phi}}$ have distribution $P_{\frac{u^{2m_\phi}}{q^{i m_\phi}}, \frac{1}{q^{(i-1) m_\phi}}, 0, \frac{1}{q^{m_\phi}}}$. The distribution of the symplectic signed partitions $\lambda_{z\pm1}^{\pm}$ is more elusive and future research should be focused here. The following two problems seem natural.

Problem Find a probabilistic algorithm for growing partitions (signed or dropping the signs) corresponding to the polynomial $z-1$ in the symplectic groups. This algorithm must be consistent with the distributions of the size and number of parts of λ_{z-1} (see Sections 5.4 and 5.6). Presumably, the algorithm proceeds by adding tiles which are 1 by 2 rectangles or 2 by 1 rectangles, but the rules seem hard to find.

Problem Find the correct analog of the Hall-Littlewood polynomials for the symplectic groups, and understand their relationship, if any, to the probabilistic algorithm of the preceding problem.

5.4 Size of the Partition Corresponding to $z - 1$

This section uses Steinberg's count of unipotent elements (Theorem 11) and the cycle index for the symplectic groups to study the size of the partition corresponding to the polynomial $z-1$ under the measure defined in Section 5.3. Theorem 41 gives a generating function for the random variable $|\lambda_{z-1}^{\pm}|$, proving that as in the case of the general linear groups, it is an infinite convolution of geometrics.

Theorem 41 *For $0 < u < 1$, pick an even integer with the probability of getting $2n$ equal to $(1-u^2)u^{2n}$. Then pick a uniform element α from $Sp(2n,q)$. The probability generating function in the variable x for the random variable $|\lambda^{\pm}_{z-1}(\alpha)|$ is:*

$$\prod_{r=1}^{\infty} \frac{(1-\frac{u^2}{q^{2r-1}})}{(1-\frac{(ux)^2}{q^{2r-1}})}$$

PROOF: First observe that:

$$\sum_{\lambda^{\pm}} \frac{(ux)^{|\lambda^{\pm}|}}{c_{Sp,z-1,q}(\lambda^{\pm})} = 1 + \sum_{j=1}^{\infty} \frac{(ux)^j q^{2j^2}}{|Sp(2j,q)|}$$

To prove this, count the number of unipotent elements in the group $Sp(2j,q)$ in two ways. The first way, using the cycle index for the symplectic groups gives:

$$|Sp(2j,q)|[(ux)^{2j}] \sum_{\lambda^{\pm}} \frac{(ux)^{|\lambda^{\pm}|}}{c_{Sp,z-1,q}(\lambda^{\pm})}$$

The second way is to use Theorem 11 (Steinberg) which says that the number of unipotent elements in $Sp(2j,q)$ is q^{2j^2}. This proves the claim.

Rewriting using Lemma 5 gives:

$$\begin{aligned}
\sum_{\lambda^{\pm}} \frac{(ux)^{|\lambda^{\pm}|}}{c_{Sp,z-1,q}(\lambda^{\pm})} &= 1 + \sum_{j=1}^{\infty} \frac{(ux)^j q^{2j^2}}{|Sp(2j,q)|} \\
&= 1 + \sum_{j=1}^{\infty} \frac{(u^2x^2q)^j (q^2)^{\binom{j}{2}}}{(q^{2j}-1)\cdots(q^2-1)} \\
&= \prod_{r=1}^{\infty} \frac{1}{(1-\frac{(ux)^2}{q^{2r-1}})}
\end{aligned}$$

Taking the reciprocal of the cycle index and setting all the x variables equal to 1 gives:

$$1-u = \prod_{\phi=z\pm 1} \prod_{r=1}^{\infty} (1-\frac{u^2}{q^{2r-1}}) \prod_{\substack{\phi=\bar{\phi} \\ \phi \neq z\pm 1}} \prod_{r=1}^{\infty} (1-\frac{u^{rm_{\phi}}}{q^{\frac{rm_{\phi}}{2}}}) \prod_{\{\phi,\bar{\phi}\},\phi\neq\bar{\phi}} \prod_{r=1}^{\infty} (1-\frac{u^{2rm_{\phi}}}{q^{rm_{\phi}}})$$

The theorem follows by multiplying this last equation by the equation in the statement of Theorem 40 and then setting $x_{z-1,\lambda^{\pm}} = x^{|\lambda^{\pm}|}$, $x_{z+1,\lambda^{\pm}} = 1$, and $x_{\phi,\lambda} = 1$ for $\phi \neq z \pm 1$. □

The corresponding result for the groups GL in Section 3.9, Theorem 40, and Theorem 41 show that setting $x_{\phi,\lambda^{\pm}} = x_1^{|\lambda^{\pm}|}$ and $x_{\phi,\lambda} = x_{m_{\phi}}^{|\lambda|}$ in the cycle index of Theorem 40 for the symplectic groups gives the factorization:

$$\prod_{r=1}^{\infty} (\frac{1}{1-\frac{(ux_1)^2}{q^{2r-1}}})^2 \prod_{\substack{m=1 \\ m\ even}}^{\infty} \prod_{r=1}^{\infty} (\frac{1}{1-\frac{(ux_m)^m}{q^{\frac{rm}{2}}}})^{\bar{I}_{m,q}} \prod_{m=1}^{\infty} \prod_{r=1}^{\infty} (\frac{1}{1-\frac{(ux_m)^{2m}}{q^{rm}}})^{\frac{I_{m,q}-\bar{I}_{m,q}}{2}}$$

This implies the following corollary.

Corollary 9 *Regard all polynomials of the same degree m as equivalent (i.e. set $x_{z\pm 1,\lambda^{\pm}} = x_1^{|\lambda^{\pm}|}$ and $x_{\phi,\lambda_{\phi}} = x_{m_{\phi}}^{|\lambda_{\phi}|}$ in the cycle index of Theorem 40). Then letting $q \to \infty$ gives:*

$$\prod_{m\ even} e^{\frac{x_m u^m}{m}} \prod_{m=1}^{\infty} e^{\frac{(x_m)^2 u^{2m}}{2m}}$$

Recall from Section 3.4 that the generating function for $|\lambda_{z-1}|$ for the general linear groups is:

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

A comparison of this expression with the statement of Theorem 41 and some calculations for small values of n suggest that the following problem has a nice solution.

Problem Find a clumping map CL from all symplectic signed partitions $\lambda^{\pm}$ (unipotent conjugacy classes of the groups $Sp(2n,q)$ for all n) to all partitions λ (unipotent conjugacy classes of the groups $GL(n,q)$ for all n) such that:

1. $|CL(\lambda^{\pm})| = \frac{|\lambda^{\pm}|}{2}$ for all $\lambda^{\pm}$
2. For $0 < u < 1$, the push-forward under CL of the measure on symplectic signed partitions given by choosing n with probability $(1-u^2)u^{2n}$ and taking $\lambda_{z-1}^{\pm}(\alpha)$ where α is uniform in $Sp(2n,q)$ is equal to the measure on partitions given by choosing n with probability $(1-u^2q)(u^2q)^n$ and taking $\lambda_{z-1}(\alpha)$ where α is uniform in $GL(n,q^2)$.

5.5 Counting Jordan Blocks

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 24 gives a generating function for $X_{2n}(\alpha)$.

Lemma 24

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

PROOF: This follows immediately from the cycle index for the symplectic groups and the equation after Theorem 41. □

With Lemma 24, the mean of X_{2n} over $Sp(2n,q)$ is straightforward to compute.

Theorem 42 $EX_{2n} = \frac{3}{2}logn + O(1)$

PROOF: Differentiating both sides of the generating function of Lemma 24 with respect to x and then setting $x = 1$ gives:

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

The term coming from the first sum is $O(1)$. By Theorem 39, $\bar{I}_{m,q} = \frac{q^{\frac{m}{2}}}{m} + O(q^{\frac{m}{4}})$ 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,

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

□

5.6 Number of Parts of the Partition Corresponding to $z - 1$

Let $P_{Sp,2n}(k,q)$ be the probability that an element of $Sp(2n,q)$ has a k dimensional fixed space, and let $P_{Sp,\infty}(k,q)$ be the $n \to \infty$ limit of $P_{Sp,2n}(k,q)$. Rudvalis and Shinoda [51] proved that:

1. $P_{Sp,2n}(2k,q) = \frac{1}{|Sp(2k,q)|}\sum_{i=0}^{n-k}\frac{(-1)^i q^{2\binom{i}{2}}}{|Sp(2i,q)|q^{2ik}}$
2. $P_{Sp,2n}(2k+1,q) = \frac{1}{|Sp(2k,q)|q^{2k+1}}\sum_{i=0}^{n-k-1}\frac{(-1)^i q^{2\binom{i}{2}}}{|Sp(2i,q)|q^{2i(k+1)}}$
3. $P_{Sp,\infty}(k,q) = [\prod_{r=1}^{\infty}(\frac{1}{1+\frac{1}{q^r}})]\frac{(\frac{1}{q})^{\frac{k^2+k}{2}}}{(1-\frac{1}{q})\cdots(1-\frac{1}{q^k})}$

Some elementary linear algebra and the third Rudvalis/Shinoda formula give the following result.

Theorem 43 *For $n \geq 2l$, the lth moment of the distribution of fixed vectors in the natural action of $Sp(2n,q)$ is equal to:*

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

PROOF: To see that for $n \geq 2l$ the lth moment is independent of n, alter the second and third paragraphs of the proof of Theorem 37 by replacing the word "Hermitian" by "skew-symmetric" and by defining the matrix M' as:

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

It thus suffices to compute the lth moment for the $n \to \infty$ limit distribution. By the Rudvalis/Shinoda formula for $P_{Sp,\infty}(k,q)$, the lth moment is $M_l(x)$ where:

$$M_l(x) \prod_{i=1}^{\infty}(1+x^i) = \sum_{k=0}^{\infty} \frac{x^{\frac{k^2+k}{2}}}{x^{kl}(1-x)\cdots(1-x^k)}$$

and $x = \frac{1}{q}$. So the theorem follows from showing that $M_l(x)$ satisfies $M_0 = 1$ and $M_l = (1+\frac{1}{x^{l-1}})M_{l-1}$ for $l \geq 1$. $M_0 = 1$ because it is the sum of the probabilities of a distribution.

Note that the coefficient of x^r in the kth term on the right hand side is $|S_k|$, where S_k is the set of partitions of $r+lk$ into k distinct parts. This is because the denominator gives all partitions into at most k parts, and the numerator corresponds to adding i to the ith part for each i ranging from 1 to k.

Let A_k be the set of partitions of $r+lk$ into k distinct parts with no parts of size 1. Removing the first column in such partitions shows that A corresponds bijectively to partitions of $r+(l-1)k$ into k distinct parts. Summing over all k gives that $\sum_k |A_k| = [x^r]M_{l-1}\prod_{r=1}^{\infty}(1+\frac{1}{q^r})$.

Let $B_k = S_k - A_k$ be the set of partitions of $r+lk$ into k distinct parts with a part of size 1. Removing the first column in such partitions shows that B_k corresponds bijectively to partitions of $r+(l-1)k$ into $k-1$ distinct parts. Thus

$$\begin{aligned} \sum_k |B_k| &= [x^r]\sum_{k=1}^{\infty} \frac{1}{x^{k(l-1)}} \frac{x^{\frac{(k-1)^2+(k-1)}{2}}}{(1-x)\cdots(1-x^{k-1})} \\ &= \frac{1}{x^{l-1}} \sum_{k=0}^{\infty} \frac{1}{x^{k(l-1)}} \frac{x^{\frac{k^2+k}{2}}}{(1-x)\cdots(1-x^k)} \\ &= \frac{1}{x^{l-1}}[x^r]M_{l-1}\prod_{r=1}^{\infty}(1+\frac{1}{q^r}) \end{aligned}$$

The theorem follows since $\sum_k |S_k| = \sum_k(|A_k|+|B_k|)$. $\square$

It should be straightforward to give total variation bounds between the distribution of $P_{Sp,2n}(k,q)$ and $P_{U,\infty}(k,q)$ as in Theorem 20. It would also be nice to have a representation theoretic proof of Theorem 37. Theorem 19 indicates that this is plausible.

5.7 Average Order of an Element of $Sp(2n,q)$

Let $v_{Sp,2n}$ be the average over $Sp(2n,q)$ of the order of an element of $Sp(2n,q)$. This section shows 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.

Theorem 44 *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:*

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

PROOF: The proof uses the cycle index for the symplectic groups and Theorem 11, in a similar way as in Theorem 33. □

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 $x \to x^q$.

Lemma 25 *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 23, 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 $\phi = \bar{\phi}$. □

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

Theorem 45 *For fixed q and growing n, $log(v_{Sp,2n}) \geq nlog(q) - log(n) + o(log(n))$.*

PROOF: From Lemma 25, 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 44, 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 [57] that $log(\Phi(N)) = log(N) + O(log(log(N)))$ proves the theorem. □

Chapter 6

The Orthogonal Groups

6.1 Chapter Overview

Section 6.2 discusses Wall's work on the conjugacy classes of the finite orthogonal groups [61]. Section 6.3 obtains a cycle index for the orthogonal groups and uses the orthogonal groups to define measures on orthogonal signed partitions and partitions. For all polynomials other than $\phi = z \pm 1$, these measures are specializations of measures in Chapter 2. Sections 6.4 and 6.6 examine the more mysterious case $\phi = z \pm 1$ and study the size and number of parts of the corresponding orthogonal signed partitions. Sections 6.5 and 6.7 use the cycle index of Section 6.3 to study the number of Jordan blocks and average order of an element of an orthogonal group.

6.2 Conjugacy Classes in the Orthogonal Groups

In this chapter it is assumed 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 [7]). 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 [6]. 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 5 *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

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

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

Although Wall does not state the following theorem, it is implicit in the discussion on pages 38-40 of [61]. The reason his statements seem different is that 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. In any case, Theorem 46 is basically a restatement of Wall's work. The polynomial $\bar{\phi}$ is defined as Section 5.2.

Theorem 46 *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:

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

The conjugacy class has size:

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

where

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

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 $c_{O,\phi,q}(\lambda^\pm)$.

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 [3]). It is worth remarking that orthogonal transvections exist only in the characteristic 2 case, which is excluded in this chapter.

The orthogonal symmetries in $O^+(n,q)$ can be counted directly. It is shown on page 117 of Artin [3] that all such maps τ have the following description. Write $V = U \perp W$ where U is a non-singular line with respect to the inner product. Letting I be the identity map, define $\tau|_U = -I, \tau|_V = I$ and extend by linearity. Thus orthogonal symmetries correspond to non-singular lines in V. It is shown by induction on pages 145-6 of Artin [3] that there are q^{n-1} isotropic vectors in an n dimensional space endowed with the inner product used in the definition of $O^+(n,q)$. Thus the number of orthogonal symmetries in $O^+(n,q)$ is equal to:

$$\frac{q^n - q^{n-1}}{q-1} = q^{n-1}$$

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 46 and Lemma 11, which says that the dimension of the fixed space of α is the number of parts of $\lambda^{\pm}_{z-1}(\alpha)$. So the class size formulas of Wall imply that the total number of orthogonal symmetries in $O^+(n,q)$ for n odd is:

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

6.3 The Cycle Index for the Orthogonal Groups

Define:

$$\begin{aligned} Z_{O(n,q)} &= \frac{1}{|O^+(n,q)|} \sum_{\alpha \in O^+(n,q)} \prod_{\phi = z\pm 1} x_{\phi,\lambda^{\pm}_{\phi}(\alpha)} \prod_{\phi \neq z, z\pm 1} x_{\phi,\lambda_{\phi}(\alpha)} \\ &+ \frac{1}{|O^-(n,q)|} \sum_{\alpha \in O^-(n,q)} \prod_{\phi = z\pm 1} x_{\phi,\lambda^{\pm}_{\phi}(\alpha)} \prod_{\phi \neq z, z\pm 1} x_{\phi,\lambda_{\phi}(\alpha)} \end{aligned}$$

The cycle index for the orthogonal groups has the following factorization.

Theorem 47

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

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

PROOF: The first equation follows from Theorem 46 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.

Set all of the x variables in the cycle index for the orthogonal groups equal to 1, and let $A(u)$ be the term corresponding to the polynomial $z-1$ or $z+1$. This gives the equation:

$$\frac{1+u}{1-u} = A(u)^2 [\frac{\prod_{i=1}^{\infty}(1-\frac{u^2}{q^{2i-1}})^2}{1-u^2}]$$

where the term in braces corresponds to the polynomials other than $z \pm 1$ and is obtained by using Theorem 41 and the fact that these terms are identical in the cycle indices of the symplectic and orthogonal groups. Thus,

$$A(u) = \frac{1+u}{\prod_{i=1}^{\infty}(1-\frac{u^2}{q^{2i-1}})}$$

The second equality of the theorem now follows by multiplying the first equality of the theorem by the equation:

$$\frac{1-u}{1+u} = (\frac{\prod_{i=1}^{\infty}(1-\frac{u^2}{q^{2i-1}})}{1+u})^2 \prod_{\substack{\phi=\bar{\phi} \\ \phi \neq z \pm 1}} \prod_{i=1}^{\infty}(1-\frac{u}{q^{\frac{im_\phi}{2}}}) \prod_{\{\phi,\bar{\phi}\},\phi \neq \bar{\phi}} \prod_{i=1}^{\infty}(1-\frac{u^2}{q^{im_\phi}})$$

□

Remark The probabilistic interpretation for the tower $O(n,q)$ differs from that of the other groups. For $0 < u < 1$, pick an integer n with the probability of $n = 0$ equal to $\frac{1-u}{1+u}$ and probability of $n \geq 1$ equal to $\frac{1-u}{1+u}2u^n$. If $n \geq 1$, choose $O^+(n,q)$ or $O^-(n,q)$ with probability $\frac{1}{2}$ and then choose within that group uniformly. This defines random orthogonal signed partitions $\lambda^{\pm}_{z-1}, \lambda^{\pm}_{z+1}$ and random partitions λ_ϕ for $\phi \neq z \pm 1$. If $\phi \neq z \pm 1$, the random partitions λ_ϕ are the same as for the symplectic groups and are specializations of measures from Chapter 2 (see Section 5.3).

The orthogonal signed partitions $\lambda^{\pm}_{z-1}$ and $\lambda^{\pm}_{z+1}$ have the same distribution, so future work should focus on studying $\lambda^{\pm}_{z-1}$. Sections 6.4 and 6.6 begin this undertaking. It would be desirable to have a probabilistic algorithm for growing the random partition $\lambda^{\pm}_{z-1}$.

Corollary 10 gives the $q \to \infty$ limit of the cycle index of the orthogonal groups.

Corollary 10 *Regard all polynomials of the same degree m as equivalent (i.e. set $x_{\phi,\lambda^\pm} = x_1^{|\lambda^\pm|}$ and $x_{\phi,\lambda} = x_{m_\phi}^{|\lambda|}$ in the cycle index of the orthogonal groups). Then letting $q \to \infty$ gives:*

$$(1+ux_1)^2 \prod_{m \ even} e^{\frac{x_m u^m}{m}} \prod_{m=1}^{\infty} e^{\frac{(x_m)^2 u^{2m}}{2m}}$$

Proof: Setting $x_{\phi,\lambda^\pm} = x_1^{|\lambda^\pm|}$ and $x_{\phi,\lambda} = x_{m_\phi}^{|\lambda|}$ in the first equation of Theorem 47 gives:

$$[(1+ux_1)\prod_{r=1}^{\infty}(\frac{1}{1-\frac{(ux_1)^2}{q^{2r-1}}})]^2 \prod_{\substack{m=1 \\ m\ even}}^{\infty} \prod_{r=1}^{\infty}(\frac{1}{1-\frac{(ux_m)^m}{q^{\frac{rm}{2}}}})^{\bar{I}_{m,q}} \prod_{m=1}^{\infty}\prod_{r=1}^{\infty}(\frac{1}{1-\frac{(ux_m)^{2m}}{q^{rm}}})^{\frac{I_{m,q}-\bar{I}_{m,q}}{2}}$$

Now let $q \to \infty$. □

6.4 Size of the Partition Corresponding to $z-1$

This section gives a generating function for the size of the random orthogonal signed partition $\lambda^{\pm}_{z-1}$.

Theorem 48 *The generating function in the variable x for $|\lambda^{\pm}_{z-1}|$ is:*

$$\frac{1+ux}{1+u}\frac{\prod_{i=1}^{\infty}(1-\frac{u^2}{q^{2i-1}})}{\prod_{i=1}^{\infty}(1-\frac{(xu)^2}{q^{2i-1}})}$$

PROOF: One approach to this theorem is to use Theorem 11 (Steinberg's count of unipotent elements), as was done for the unitary and symplectic groups. A simpler method is to specialize the second equation in Theorem 47 by setting $x_{z-1,\lambda^{\pm}_{z-1}} = x^{|\lambda^{\pm}_{z-1}|}$ and all other variables equal to zero. □

6.5 Counting Jordan Blocks

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 26 gives a generating function for $X_n(\alpha)$.

Lemma 26

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

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 49 $EX_n = \frac{3}{2}log(n) + O(1)$

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 42. □

6.6 Number of Parts in the Partition Corresponding to $z - 1$

Let $P^+_{O,n}(k,q)$ and $P^-_{O,n}(k,q)$ be the respective probabilities that an element of $O^+(n,q)$ and an element of $O^-(n,q)$ have a k dimensional fix space. Let $P_{O,\infty}(k,q)$ be the $n \to \infty$ limit of either of these probabilities. Rudvalis and Shinoda [51] prove that:

$$P_{O,\infty}(k,q) = [\prod_{r=0}^{\infty}(\frac{1}{1+\frac{1}{q^r}})]\frac{(\frac{1}{q})^{\frac{k^2-k}{2}}}{(1-\frac{1}{q})\cdots(1-\frac{1}{q^k})}$$

Combining this formula with some elementary linear algebra gives the following result, which is the orthogonal analog of Theorems 17, 37, and 43.

Theorem 50 *For $n \geq 2(l+1)$, the lth moment of the distribution of fixed vectors in the natural action of $O^+(n,q)$ or $O^-(n,q)$ is:*

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

PROOF: Arguing as in the unitary and symplectic cases, it will be shown that for $n \geq 2(l+1)$, the lth moment is independent of n. By the logic of the first paragraph of Theorem 37, and the fact that n even and n odd have the same $n \to \infty$ limit by the work Rudvalis/Shinoda explained above, the next two paragraphs prove what we want.

First suppose that n is odd. Let V be the vector space on which one of $O^+(n,q)$ or $O^-(n,q)$ acts. It must be shown that given an $l * l$ non-singular, symmetric inner product matrix M, there exist linearly independent vectors $\{v_1, \cdots, v_l\} \in V$ with inner product matrix M. Consider the hardest case $n = 2l+1$ (if $n > 2l+1$ is odd add an identity block to the matrix M' to be constructed). On a vector space W with the same dimension as V, define a symmetric, non-singular inner product matrix M' which looks like:

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

where ϵ is chosen either as a square or a non-square in F_q so as to make the Witt type of the bilinear form giving M' correspond to the orthogonal group acting (see Proposition 5).

Next suppose that n is even. As above, given an $l * l$ non-singular symmetric inner product matrix M, it must be shown that there exist linearly independent vectors $\{v_1, \cdots, v_l\} \in V$ with inner product matrix M. Consider the hardest case $n = 2(l+1)$ (for larger even n add an identity block to the matrix M' to be constructed). On a vector space W with the same dimension as V, define a symmetric, non-singular inner product matrix M' which looks like:

$$\begin{pmatrix} 0 & I_l & 0 & 0 \\ I_l & M & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \epsilon \end{pmatrix}$$

where ϵ is chosen either as a square or a non-square in F_q so as to make the Witt type of the bilinear form giving M' correspond to the orthogonal group acting (see Proposition 5).

We compute the lth moments for the $n \to \infty$ limit, this time by direct algebra rather than by a visual argument. It must be shown that the lth moment $M_l(q)$ satisfies $M_0 = 1$, $M_l = (q^l + 1)M_{l-1}$

for $l \geq 1$. Note that $M_0 = 1$ because it is the sum of the probabilities of a distribution. By the Rudvalis/Shinoda formula, $M_l(q)$ is defined by:

$$M_l \prod_{r=0}^{\infty}(1+\frac{1}{q^r}) = \sum_{k=0}^{\infty} q^{kl} \frac{(\frac{1}{q})^{\frac{k^2-k}{2}}}{(1-\frac{1}{q})\cdots(1-\frac{1}{q^k})}$$

The right-hand side may be rewritten as:

$$\begin{aligned}
& [(\sum_{k=0}^{\infty} q^{kl} \frac{(\frac{1}{q})^{\frac{k^2-k}{2}}}{(1-\frac{1}{q})\cdots(1-\frac{1}{q^k})}) - (\sum_{k=1}^{\infty} q^{kl} \frac{(\frac{1}{q})^{\frac{k^2-k}{2}}}{(1-\frac{1}{q})\cdots(1-\frac{1}{q^{k-1}})})] + [\sum_{k=1}^{\infty} q^{kl} \frac{(\frac{1}{q})^{\frac{k^2-k}{2}}}{(1-\frac{1}{q})\cdots(1-\frac{1}{q^{k-1}})}] \\
= \; & [1 + \sum_{k=1}^{\infty} q^{k(l-1)} \frac{(\frac{1}{q})^{\frac{k^2-k}{2}}}{(1-\frac{1}{q})\cdots(1-\frac{1}{q^k})}] + [\sum_{k=1}^{\infty} q^{kl} \frac{(\frac{1}{q})^{\frac{k^2-k}{2}}}{(1-\frac{1}{q})\cdots(1-\frac{1}{q^{k-1}})}] \\
= \; & [M_{l-1}(q) \prod_{r=0}^{\infty}(1+\frac{1}{q^r})] + [\sum_{k=0}^{\infty} \frac{q^{(k+1)l}}{q^k} \frac{(\frac{1}{q})^{\frac{k^2-k}{2}}}{(1-\frac{1}{q})\cdots(1-\frac{1}{q^k})}] \\
= \; & [M_{l-1}(q) \prod_{r=0}^{\infty}(1+\frac{1}{q^r})] + [q^l \sum_{k=0}^{\infty} q^{k(l-1)} \frac{(\frac{1}{q})^{\frac{k^2-k}{2}}}{(1-\frac{1}{q})\cdots(1-\frac{1}{q^k})}] \\
= \; & (q^l+1) M_{l-1}(q) \prod_{r=0}^{\infty}(1+\frac{1}{q^r})
\end{aligned}$$

which completes the proof. □

6.7 Average Order of an Element of $O(n,q)$

Let $v_{O,n}$ be one half of the sum of the average orders of elements of $O^+(n,q)$ and $O^-(n,q)$. It will be shown that for fixed q and growing n, $log(v_{O,n}) \geq nlog(q) - log(n) + o(log(n))$.

Theorem 51 is proven using the cycle index of the orthogonal groups. As the proof technique is the same as that used for Theorem 33, the details are omitted.

Theorem 51 *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:

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

This gives the following bound.

Theorem 52 *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 25 and Theorem 51 and argue as in Theorem 45. $\square$

Suggestions for Future Research

This thesis has introduced some connections between probability and algebra. There is more work to be done in developing these ideas. Here are some possibilities.

1. Study the shapes of partitions under the measures $P_{x,y,q,t}(\lambda)$ for various specializations of the variables x, y, q, t. For instance find generating functions for various functionals of the partitions such as the number of parts, largest part, number of 1's, etc. (A generating function for the size was found as Corollary 1 of Section 2.5). It should also be possible to extend work of Vershik [59], [60] which shows that random partitions under measures such as the Plancharel measure have an asymptotic limit shape.

2. Read more group theoretic information off of the probabilistic algorithms. For instance, suppose one wants to estimate or bound the average order of a unipotent matrix (which is useful for bounding the average order an arbitrary element of $GL(n,q)$). One must study the joint distribution of the size and largest part of the partitions λ_ϕ, and analyzing how the partitions evolve stochastically may be the right way to approach this.

3. Find a probabilistic proof of the Rogers-Ramanujan identities (Section 3.7).

4. Develop probabilistic algorithms for picking from the measures $\lambda^{\pm}_{z\pm1}$ for the symplectic and orthogonal groups. These will be more complicated than the algorithms for the general linear and unitary groups, since there are size restrictions on the partitions (for instance in the symplectic groups $|\lambda^{\pm}_{z\pm1}|$ is always even). Presumably one adds $1 * 2$ or $2 * 1$ tiles according to some rules.

5. Study the cycle indices for the characteristic 2 cases for the symplectic and orthogonal groups. One can deduce from Wall [61] that these also factor and that results analogous to Theorem 39 go through. There must be interesting combinatorics here.

6. Read information off of the cycle indices for the classical groups. For instance extend Goh and Schmutz's [24] 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 some of the asymptotic work on semisimple and regular elements in the general linear groups (Sections 3.7 and 3.8).

7. Find "Lie Algebra" cycle indices. For instance Stong's cycle index for $Mat(n,q)$ (see Section 3.2) 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. Relate the work of this thesis to representation theory. For instance, what is the representation theoretic interpretation of the fact that the moments of the limit distribution of fixed vectors

in the unitary, symplectic, and orthogonal groups have nice product forms. Is the conjecture in Section 3.6 correct?

Bibliography

[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] Arratia, R. and Tavare, S., The cycle structure of random permutations. Ann. Probab. 20 (1992), no. 3, 1567-1591.

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

[4] Aschbacher, M., Finite group theory. Cambridge studies in advanced mathematics 10. Cambridge University Press, 1986.

[5] Bennett, C., Dempsey, K., and Sagan, B., Partition lattice q-analogs related to q-Stirling numbers. Journal of Algebraic Combinatorics 3 (1994), no. 3, 261-283.

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

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

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

[9] Celler, F., Leedham-Green, C., Murray, S., Niemeyer, A., and O'Brien, E.A., Generating random elements of a finite group. Communications in algebra, 23 (13), (1995), 4931-4948.

[10] Diaconis, P., Unpublished notes and lectures.

[11] Diaconis, P., Group representations in probability and statistics. Institute of Mathematical Statistics Lecture Notes Vol. 11, 1988.

[12] Diaconis, P. and Kemperman, J., Some new tools for Dirichlet priors, Bayesian statistics 5, 1996, pg. 97-106.

[13] Diaconis, P. and Shahshahani, M., On the eigenvalues of random matrices, J. Appl. Prob. 31 (1994), 49-61.

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

[15] Erdos, P. and Szalay, M., On the statistical theory of partitions. Topics in Classical Number Theory, Vol. I, 1984, pg. 397-450.

[16] Erdos, P. and Turan, P., On some problems of statistical group theory, IV, Acta Math. Acad. Sci. Hungar. 19, Nos. 3-4, (1968), 413-435.

[17] Ewens, W.J., The sampling theory of selectively neutral alleles. Theoretical Population Biology 3 (1972), 87-112.

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

[19] 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.

[20] Fristedt, B., The structure of random partitions of large integers. Trans. Amer. Math. Soc. 337 (1993), no. 2, 703-735.

[21] Fulton, W., Young Tableaux. London Mathematical Society Student Texts 35, 1997.

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

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

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

[25] Goldman, J. and Rota,G-C., The number of subspaces of a vector space, (1969) Recent Progress in Combinatorics (Proc. Third Waterloo Conf. on Combinatorics, 1968) 75-83.

[26] 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.

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

[28] Greene, C., Nijenhuis, A. and Wilf, H., A probabilistic proof of a formula for the number of Young tableaux of a given shape. Adv. in Math 31 (1979), no. 1, 104-109.

[29] Greene, C., Nijenhuis, A. and Wilf, H., Another probabilistic method in the theory of Young tableaux. J. Combin. Theory Series A, 37 (1984), 127-135.

[30] 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.

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

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

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

[34] James, G. and Kerber, A., The representation theory of the symmetric group. Encyclopedia of Mathematics and its Applications, 16. Addison-Wesley Publishing Co., Reading, Mass., 1981.

[35] Kerov, S.V., The boundary of Young lattice and random Young tableaux. Formal power series and algebraic combinatorics. DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 24, pg. 133-158.

[36] Kerov, S.V., A q-analog of the hook walk algorithm for random Young tableaux. Journal of Algebraic Combinatorics 2 (1993), 383-396.

[37] Kerov, S.V. and Vershik, A.M., Asymptotic behavior of the Plancharel measure of the symmetric group and the limit form of Young tableaux. Dokl. Akad. Nauk SSSR 233 (1977), no. 6, 1024-1027.

[38] Knuth, D. and Trabb Pardo, L., Analysis of a simple factorization algorithm. Theoret. Comput. Sci. 3 (1976/77), no. 3, 321-348.

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

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

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

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

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

[44] Marsaglia, G. and Tsay, L.H., Matrices and the structure of random number sequences. Linear Algebra and its Applications, 67, 1985, 147-156.

[45] Mehta, M.L., Random matrices. Academic Press, San Diego. (1991).

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

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

[48] Nijenhuis, A., Solow, A., and Wilf, H., Bijective methods in the theory of finite vector spaces. Journal of Combinatorial Theory, Series A. 37 (1984), no. 2, 127-135.

[49] Pak, I.M. and Stoyanovskii, A.V., A bijective proof of the hook-length formula and its analogs. Journal of Functional Analysis and its Applications (1992).

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

[51] Rudvalis, A. and Shinoda, K., An enumeration in finite classical groups. Preprint; Department of Mathematics, U-Mass Amherst.

[52] Sagan, B., The symmetric group: representations, combinatorial algorithms, and symmetric functions. Wadsworth and Brooks/Cole 1991.

[53] Shinoda, K., Identities of Euler and finite classical groups. Proceedings of Asian Mathematical Conference, 1990 (Hong Kong, 1990), 423-427, World Sci. Publishing, River Edge, NJ, 1992.

[54] Stanley, R., Enumerative combinatorics, Vol. 1, The Wadsworth and Brooks/Cole Mathematical Series. Monterey, Calif. 1986.

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

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

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

[58] Suzuki, M. Group theory I. Springer-Verlag, 1982.

[59] Vershik, A.M., Asymptotic combinatorics and algebraic analysis. Proceedings of the International Congress of Mathematicians, Zurich 1994, 1384-1394.

[60] Vershik, A.M., Statistical mechanics of combinatorial partitions, and their limit shapes. Functional Analysis and its Applications, Vol. 30, No. 2, 1996, pg. 90-105.

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