

©Copyright 2020

Graham Gordon

# Cycle type factorizations in the finite general linear groups

Graham Gordon

A dissertation  
submitted in partial fulfillment of the  
requirements for the degree of

Doctor of Philosophy

University of Washington

2020

Reading Committee:

Sara Billey, Chair

Jarod Alper

Julia Pevtsova

Program Authorized to Offer Degree:  
Mathematics

University of Washington

**Abstract**

Cycle type factorizations in the finite general linear groups

Graham Gordon

Chair of the Supervisory Committee:  
Professor Sara Billey  
Mathematics

Recent work by Huang, Lewis, Morales, Reiner, and Stanton suggests that the regular elliptic elements of  $\mathrm{GL}_n \mathbb{F}_q$  are somehow analogous to the  $n$ -cycles of the symmetric group. In 1981, Stanley enumerated the factorizations of permutations into products of  $n$ -cycles. We study the analogous problem in  $\mathrm{GL}_n \mathbb{F}_q$  of enumerating factorizations into products of regular elliptic elements. More precisely, we define a notion of cycle type for  $\mathrm{GL}_n \mathbb{F}_q$  and seek to enumerate the tuples of a fixed number of regular elliptic elements whose product has a given cycle type. In some special cases, we provide explicit formulas, using a standard character-theoretic technique due to Frobenius by introducing simplified formulas for the necessary character values. We also address, for large  $q$ , the problem of computing the probability that the product of a random tuple of regular elliptic elements has a given cycle type. Next, we prove some results regarding the polynomiality of our enumerative formulas. We conclude by slightly extending our main enumerative results and listing some open problems.

## TABLE OF CONTENTS

	Page
Chapter 1: Introduction . . . . .	1
1.1 History and motivation . . . . .	1
1.2 Main results . . . . .	4
1.3 Related recent work . . . . .	8
1.4 Outline . . . . .	10
Chapter 2: Preliminaries . . . . .	11
2.1 The character theory approach . . . . .	11
2.2 The symmetric groups and partitions . . . . .	12
2.3 Finite fields . . . . .	14
2.4 The finite general linear groups . . . . .	17
Chapter 3: Characters of the finite general linear groups . . . . .	26
3.1 Computing the irreducible $\mathrm{GL}_n \mathbb{F}_q$ characters . . . . .	26
3.2 Degrees of the irreducible $\mathrm{GL}_n \mathbb{F}_q$ characters . . . . .	28
3.3 Certain character values . . . . .	30
Chapter 4: Enumerative results . . . . .	32
4.1 Main tool . . . . .	32
4.2 Proof of first enumerative result . . . . .	37
4.3 Proof of second enumerative result . . . . .	39
Chapter 5: Probabilistic result . . . . .	44
5.1 Prerequisite lemmas . . . . .	44
5.2 Proof of probabilistic result . . . . .	47
Chapter 6: Polynomiality results . . . . .	50

6.1	Proofs of polynomiality results . . . . .	50
Chapter 7:	Further work . . . . .	54
7.1	Slightly expanding the main result . . . . .	54
7.2	An analogue of factorizations into transpositions . . . . .	55
7.3	An analogue of a result of Boccara . . . . .	59
7.4	Open problems . . . . .	61
7.5	Conclusion . . . . .	63
Bibliography	. . . . .	64
Appendix A:	Quasipolynomial data . . . . .	67
A.1	Data for $n = 2$ . . . . .	67
A.2	Data for $n = 3$ . . . . .	70

## ACKNOWLEDGMENTS

There are many people and circumstances which have contributed to the writing of this thesis. I can only attempt to acknowledge some of them.

I want to thank Sara Billey for her first-class mentoring. When I ran off to the magical world of factorization enumeration, Sara still read every word of my writing and provided indispensable feedback.

I want to thank all my fellow graduate students at UW and elsewhere for their friendship over the years. I am grateful for the many useful interactions I have had with Becca Hoberg, Cathy Hsu, Tuomas Tajakka, and Lucas Van Meter, just to name a few. I also want to thank Jair Taylor for showing me Frobenius's formula for enumerating factorizations via character theory. I also want to thank the prelim exam system for preparing me for research.

I want to thank my parents, John and Kitty. Dad, thanks for helping me with inclined-plane problems in my high school physics homework. Mom, thanks for providing me with algebra-themed *Learning Wrap-Ups* when I was home sick from elementary school. Thank you, both, for all your support throughout my life.

I want to thank Jason Fulman, Jia Huang, Joseph Kung, Joel Lewis, Alejandro Morales, Vic Reiner, Richard Stanley, Dennis Stanton, and Richard Stong for their research which directly influenced my own.

I want to thank Carol Newborg and Tom Weimer for housing an unemployed grad student while parts of this thesis were being written in a dark corner of their luxurious basement.

I want to thank Mira Weimer for loving and believing in me, even when all I wanted to do was play *Stardew Valley* and eat lentil soup.

# DEDICATION

to Grickolas

## Chapter 1

## INTRODUCTION

**1.1 History and motivation**

Factorization enumeration has a long, ongoing history filled with interesting combinatorics, geometry, and topology [3, 6, 7, 9, 15, 19, 35]. For example, in [30], Stanley enumerates the ordered factorizations of an arbitrary permutation in  $\mathfrak{S}_n$  into a product of  $n$ -cycles. We are interested in finding an analogue of Stanley's result for the finite general linear group  $\mathrm{GL}_n \mathbb{F}_q$ .

We assume some basic knowledge of the representation theory of  $\mathfrak{S}_n$ . For each partition  $\mu \vdash n$ , let  $\mathcal{C}_\mu \subset \mathfrak{S}_n$  denote the conjugacy class consisting of permutations with cycle type  $\mu$ . Let  $m_i(\mu)$  denote the multiplicity of  $i$  in  $\mu$ . For  $\lambda \vdash n$ , let  $\chi_\mu^\lambda$  denote the irreducible character  $\chi^\lambda$  of  $\mathfrak{S}_n$  corresponding to  $\lambda$  evaluated on an element of  $\mathcal{C}_\mu$ . Let  $\mathbb{N} = \{1, 2, 3, \dots\}$  denote the positive integers. For any  $\mu \vdash n$  and  $k \in \mathbb{N}$ , define

$$g_{k,\mu} = \#\{(t_1, \dots, t_k) \in \mathcal{C}_{(n)}^k : t_1 \cdots t_k \in \mathcal{C}_\mu\}. \quad (1.1.1)$$

The quantity  $g_{k,\mu}$  is  $\#\mathcal{C}_\mu$  times as large as the aforementioned quantity Stanley computes.

**Theorem 1.1.1** (Stanley [30, Thm. 3.1]). *For all  $n, k \in \mathbb{N}$  and  $\mu \vdash n$ , the number of ordered  $k$ -tuples of  $n$ -cycles whose product equals an arbitrary fixed permutation of cycle type  $\mu$  is*

$$\frac{g_{k,\mu}}{\#\mathcal{C}_\mu} = \frac{(n-1)!^{k-1}}{n} \sum_{r=0}^{n-1} \frac{(-1)^{rk} \chi_\mu^{(n-r, 1^r)}}{\binom{n-1}{r}^{k-1}}, \quad (1.1.2)$$

and, more explicitly,

$$\frac{g_{k,\mu}}{\#\mathcal{C}_\mu} = \frac{(n-1)!^{k-1}}{n} \sum_{r=0}^{n-1} \frac{(-1)^{rk}}{\binom{n-1}{r}^{k-1}} \sum_{\nu \vdash r} (-1)^{\sum_{a \geq 1} m_{2a}(\nu)} \binom{m_1(\mu) - 1}{m_1(\nu)} \prod_{j=2}^r \binom{m_j(\mu)}{m_j(\nu)}. \quad (1.1.3)$$

Theorem 1.1.1 is proved using a character-theoretic technique due to Frobenius which we describe in Section 2.1. The more explicit phrasing (1.1.3) is obtained by expressing the character values  $\chi_\mu^{(n-r, 1^r)}$  explicitly [30, Lem. 2.2]. For the sake of brevity, we will express formulas using the symbols  $\chi_\mu^{(n-r, 1^r)}$  with the understanding that there exists an explicit formula for computing such character values.

For further history on the enumeration of factorizations of permutations into products of  $n$ -cycles, see the work of Bertram-Wei [1], Boccara [2], and Walkup [36]. Walkup developed a recursion for the number of ways to factor a given permutation in  $\mathfrak{S}_n$  into the product of two  $n$ -cycles. Boccara expressed the number of factorizations of a given permutation in  $\mathfrak{S}_n$  into the product of an  $n$ -cycle and an  $m$ -cycle in terms of the definite integral of a certain polynomial, for  $2 \leq m \leq n$ . Bertram-Wei developed some recursive and some explicit formulas for the number of ways to factor a given permutation in  $\mathfrak{S}_n$  into the product of an  $n$ -cycle and an  $m$ -cycle for various  $m \leq n$ . Stanley's result of course only applies to factoring permutations into products of  $n$ -cycles, but it applies to cases with more than two factors, unlike the other results mentioned.

Let  $\mathrm{GL}_n \mathbb{F}_q$  denote the group of  $n \times n$  invertible matrices with entries in the finite field  $\mathbb{F}_q$  with  $q$  elements. Consider the **regular elliptic** elements of  $\mathrm{GL}_n \mathbb{F}_q$ , which are those matrices whose characteristic polynomial is irreducible over  $\mathbb{F}_q$ . Recent work by Huang, Lewis, Morales, Reiner, and Stanton [17, 23, 24] suggests that the regular elliptic elements are analogous to the  $n$ -cycles in  $\mathfrak{S}_n$  from the perspective of enumerating factorizations.

Given a matrix  $g \in \mathrm{GL}_n \mathbb{F}_q$ , we define the **cycle type** of  $g$  to be  $\mu = (\mu_1, \dots, \mu_\ell) \vdash n$  if the degrees of the irreducible factors of the characteristic polynomial of  $g$  are  $\mu_1, \dots, \mu_\ell$  in weakly decreasing order, and we write  $\mathrm{type}(g) = \mu$ . For each  $\mu \vdash n$ , let  $\mathcal{T}_\mu(q) \subset \mathrm{GL}_n \mathbb{F}_q$  denote the subset of matrices of cycle type  $\mu$ . In particular,  $\mathcal{T}_{(n)}(q)$  is the set of regular elliptic elements. Note that  $\{\mathcal{T}_\mu(q) : \mu \vdash n\}$  is a partition of  $\mathrm{GL}_n \mathbb{F}_q$ . This definition is built on the statement made by Stong in the conclusion of [34] that a degree- $m$  divisor of the characteristic polynomial of a matrix in  $\mathrm{GL}_n \mathbb{F}_q$  is the analog of a cycle of length  $m$  in a permutation in  $\mathfrak{S}_n$ . One can obtain the normalized generating function for our definition of

cycle type from Stong's [34] generalization  $\tilde{Z}_n(q; x)$  of Kung's [20] cycle index  $Z(\mathrm{GL}_n \mathbb{F}_q; x)$  by making the variable substitution  $x_{p,b} \mapsto x_m^j$  if  $p$  has degree  $m$  and  $b \vdash j$ . The substitution  $x_{p,b} \mapsto x_m^j$  is mentioned explicitly by Fulman in Section 5 of [11].

Toward the end of enumerating factorizations into products of regular elliptic elements, for any  $\mu \vdash n, k \in \mathbb{N}$ , and prime power  $q$ , we define

$$g_{k,\mu}(q) = \#\{(t_1, \dots, t_k) \in \mathcal{T}_{(n)}(q)^k : t_1 \cdots t_k \in \mathcal{T}_\mu(q)\}. \quad (1.1.4)$$

In this thesis, we consider the quantity  $g_{k,\mu}(q)$  to be a  $\mathrm{GL}_n \mathbb{F}_q$ -analogue of  $g_{k,\mu}$ , and we seek efficient ways to compute  $g_{k,\mu}(q)$ . We also consider the **regular semisimple** elements of  $\mathrm{GL}_n \mathbb{F}_q$ , which are those matrices with squarefree characteristic polynomials. Let  $\mathcal{T}_\mu^\square(q)$  denote the set of regular semisimple elements with cycle type  $\mu$ . We explain this choice of notation in Section 2.4.2. Note that  $\{\mathcal{T}_\mu^\square(q) : \mu \vdash n\}$  is not a partition of  $\mathrm{GL}_n \mathbb{F}_q$  in general, as not all elements of  $\mathrm{GL}_n \mathbb{F}_q$  are regular semisimple. However, as the following result implies, for large  $q$ , an arbitrarily large proportion of  $\mathrm{GL}_n \mathbb{F}_q$  is regular semisimple. Let  $z_\mu$  denote the cardinality of the centralizer of an element of  $\mathcal{C}_\mu$  in  $\mathfrak{S}_n$ .

**Corollary 1.1.2** (to Cor. 2.4.8). *For all  $n \in \mathbb{N}$  and  $\mu \vdash n$ ,*

$$\lim_{q \rightarrow \infty} \frac{\#\mathcal{T}_\mu^\square(q)}{\#\mathrm{GL}_n \mathbb{F}_q} = \lim_{q \rightarrow \infty} \frac{\#\mathcal{T}_\mu(q)}{\#\mathrm{GL}_n \mathbb{F}_q} = \frac{1}{z_\mu}.$$

We are also interested in enumerating factorizations of regular semisimple elements. For any  $k \in \mathbb{N}, \mu \vdash n$ , and prime power  $q$ , we define

$$g_{k,\mu}^\square(q) = \#\{(t_1, \dots, t_k) \in \mathcal{T}_{(n)}(q)^k : t_1 \cdots t_k \in \mathcal{T}_\mu^\square(q)\}. \quad (1.1.5)$$

We consider the quantity  $g_{k,\mu}^\square(q)$  to also be a  $\mathrm{GL}_n \mathbb{F}_q$ -analogue of  $g_{k,\mu}$ , and we seek efficient ways to compute  $g_{k,\mu}^\square(q)$ .

## 1.2 Main results

The following theorem is our first enumerative result. To state the theorem, and throughout the thesis, we make use of the standard  $q$ -analogues

$$[m]_q = 1 + q + q^2 + \cdots + q^{m-1}, \quad (1.2.1)$$

$$[m]_q! = \prod_{\ell=1}^m [\ell]_q, \quad \text{and} \quad (1.2.2)$$

$$\begin{bmatrix} m \\ \ell \end{bmatrix}_q = \frac{[m]_q!}{[\ell]_q! [m-\ell]_q!}, \quad (1.2.3)$$

each of which is a polynomial in  $q$  with integer coefficients, for  $\ell, m \in \mathbb{N}$ . Recall the notation  $m_i(\mu)$  denoting the multiplicity of  $i \in \mathbb{N}$  in a partition  $\mu$ .

**Theorem 1.2.1.** *For all  $n, k, \ell \in \mathbb{N}$  with  $n > 2$  and  $\ell > 1$ , all prime powers  $q$ , and all  $\mu \vdash n$  with  $m_1(\mu) = 1$ , we have*

$$g_{k,\mu}^\square(q) = \frac{\#\mathcal{T}_{(n)}(q)^k \cdot \#\mathcal{T}_\mu^\square(q)}{\#\mathrm{GL}_n \mathbb{F}_q} \cdot \sum_{r=0}^{n-1} \frac{(-1)^{rk} \chi_\mu^{(n-r, 1^r)}}{\left( q^{\binom{r+1}{2}} \cdot \begin{bmatrix} n-1 \\ r \end{bmatrix}_q \right)^{k-1}}. \quad (1.2.4)$$

Compare (1.2.4) with the rephrasing

$$g_{k,\mu} = \frac{\#\mathcal{C}_{(n)}^k \cdot \#\mathcal{C}_\mu}{\#\mathfrak{S}_n} \cdot \sum_{r=0}^{n-1} \frac{(-1)^{rk} \chi_\mu^{(n-r, 1^r)}}{\binom{n-1}{r}^{k-1}} \quad (1.2.5)$$

of (1.1.2). Note, in particular, that, for the cases of  $\mu$  discussed in Theorem 1.2.1, we have

$$\lim_{q \rightarrow 1} \frac{g_{k,\mu}^\square(q) / \#\mathcal{T}_{(n)}(q)^k}{\#\mathcal{T}_\mu^\square(q) / \#\mathrm{GL}_n \mathbb{F}_q} = \frac{g_{k,\mu} / \#\mathcal{C}_{(n)}^k}{\#\mathcal{C}_\mu / \#\mathfrak{S}_n}. \quad (1.2.6)$$

Equation (1.2.6) gives some justification that, after normalizing appropriately,  $g_{k,\mu}^\square(q)$  is a  $q$ -analogue of  $g_{k,\mu}$  in the traditional  $q \rightarrow 1$  sense.

One special case of Theorem 1.2.1 is especially simple. Note that  $g_{k,\mu}(q) = g_{k,\mu}^\square(q)$  if all the parts of  $\mu$  are distinct.

**Corollary 1.2.2.** *For all  $n, k \in \mathbb{N}$  with  $n > 2$  and all prime powers  $q$ , we have*

$$g_{k,(n-1,1)}(q) = \frac{\#\mathcal{T}_{(n)}(q)^k \cdot \#\mathcal{T}_{(n-1,1)}(q)}{\#\mathrm{GL}_n \mathbb{F}_q} \cdot \left( 1 + \frac{(-1)^{nk-n-k}}{q^{\binom{n}{2}(k-1)}} \right). \quad (1.2.7)$$

Compare (1.2.7) to the analogous formula

$$g_{k,(n-1,1)} = \frac{\#\mathcal{C}_{(n)}^k \cdot \#\mathcal{C}_{(n-1,1)}}{\#\mathfrak{S}_n} \cdot (1 + (-1)^{nk-n-k}) \quad (1.2.8)$$

from the symmetric group. Observe that (1.2.8) is zero unless both  $n$  and  $k$  are even. However, this behavior is not mimicked by (1.2.7).

Our second enumerative result is an explicit, albeit complicated, formula for  $g_{k,(n)}(q)$ , which involves nested sums over divisors of  $n$ . We require some more notation before stating the result. We denote the usual Möbius function by  $\boldsymbol{\mu}$  to differentiate it from a partition named  $\mu$ . The rest of the necessary notation is contained in Table 1.1 below. Note that the lcm in the denominator of  $C_{n,k,c}(q)$  from Table 1.1 is computed in  $\mathbb{Z}$ .

**Theorem 1.2.3.** *For all  $n, k \in \mathbb{N}$  and prime powers  $q$ , we have*

$$g_{k,(n)}(q) = P_{n,k+1}(q) \sum_{d|n} (-1)^{n(k+1)/d} d^k D_{n,k+1,d}(q) \sum_{c|d} \boldsymbol{\mu}(d/c) C_{n,k+1,c}(q), \quad (1.2.9)$$

using the notation in Table 1.1.

The analogous formula from  $\mathfrak{S}_n$  is

$$g_{k,(n)} = \frac{(n-1)!^k}{n} \sum_{r=0}^{n-1} \left( \frac{(-1)^r}{\binom{n-1}{r}} \right)^{k-1}. \quad (1.2.10)$$

Unfortunately, it is not immediately obvious how to compare (1.2.9) with (1.2.10).

**Remark 1.2.4.** The polynomiality of (1.2.1)–(1.2.3) implies that each of  $\gamma_n(q)$ ,  $P_{n,k}(q)$ ,  $\deg_{n,d,r}(q)$ , and  $D_{n,k,d}(q)$  is rational in  $q$  with rational coefficients. In particular,  $\gamma_n$  and  $\deg_{n,d,r}$  are polynomials in  $q$  with integer coefficients. The only thing preventing  $g_{k,(n)}(q)$  from being a rational function as well is that  $C_{n,k,c}(q)$  is not rational in general due to the fact that the lcm function is not rational.

**Remark 1.2.5.** There are many cases not addressed by Theorems 1.2.1 and 1.2.3. One family of unaddressed cases is when  $m_1(\mu) > 1$ . Another is when  $\ell > 1$  and  $m_1(\mu) = 0$ . It is an open problem to find efficient formulas for  $g_{k,\mu}(q)$  in these cases.

Table 1.1: Functions and their values for  $n \in \mathbb{N}$ ,  $d|n$ ,  $c|d$ , and prime powers  $q$ 

$f$	$f(q)$
$\gamma_n$	$q^{\binom{n}{2}}(q-1)^n[n]_q!$
$P_{n,k}$	$\frac{1}{\gamma_n(q)} \left( \frac{(-1)^n \gamma_n(q)}{n(q^n-1)} \right)^k$
$\text{deg}_{n,d,r}$	$q^{d\binom{r+1}{2}} \cdot \frac{\prod_{i=1}^n (q^i-1)}{\prod_{j=1}^{n/d} (q^{jd}-1)} \cdot \left[ \begin{matrix} n/d-1 \\ r \end{matrix} \right]_{q^d}$
$D_{n,k,d}$	$\sum_{r=0}^{\frac{n}{d}-1} (-1)^{rk} \text{deg}_{n,d,r}(q)^{2-k}$
$C_{n,k,c}$	$\sum_{s_1, \dots, s_k   n} \frac{(q^n-1) \prod_{i=1}^k [(q^{s_i}-1)^{\mu(n/s_i)}]}{\text{lcm}\left(\frac{q^n-1}{q^c-1}, q^{s_1-1}, \dots, q^{s_k-1}\right)}$

Our approach to proving Theorems 1.2.1 and 1.2.3 is to apply the same character-theoretic technique due to Frobenius that Stanley used in [30]. The same approach is used in [17, 23, 24], and simplifying certain character evaluations in  $\text{GL}_n \mathbb{F}_q$  is the key that unlocks their results. In order to use this approach ourselves, we first prove the following result regarding the evaluation of **primary** characters of  $\text{GL}_n \mathbb{F}_q$  on regular semisimple elements. See Chapters 2 and 3 for missing notation. In particular, primary characters are denoted  $\chi^{f \mapsto \lambda}$ , where  $f \in \mathbb{F}_q[z] \setminus \{z\}$  is monic, irreducible, and non-constant, and  $\lambda$  is a partition such that  $|\lambda| \cdot \deg f = n$ . Also note that  $\ell_f \in \mathbb{Z}$  and the codomain of the function  $\theta$  is  $\mathbb{C}^\times$ .

**Theorem 1.2.6.** *Suppose  $n \in \mathbb{N}$ ,  $d|n$ ,  $\lambda \vdash n/d$ ,  $q$  is a prime power,  $f \in \mathcal{F}_d(q)$ ,  $\mu \vdash n$ ,  $g \in \mathcal{T}_\mu^\square(q)$ , and  $h_1, \dots, h_{\ell(\mu)}$  are the distinct irreducible factors of the characteristic polynomial of  $g$ . If some part of  $\mu$  is not divisible by  $d$ , then  $\chi^{f \mapsto \lambda}(g) = 0$ . Otherwise, there exists  $\tilde{\mu} \vdash n/d$*

such that  $\mu = d\tilde{\mu}$ , and

$$\chi^{f \mapsto \lambda}(g) = (-1)^{\frac{n}{d}(d-1)} \chi_{\tilde{\mu}}^\lambda \prod_{i=1}^{\ell(\mu)} \frac{1}{\tilde{\mu}_i} \sum_{\substack{\beta_i \in \mathbb{F}_q^{\mu_i} \\ h_i(\beta_i)=0}} \theta(\beta_i)^{\ell_f[\tilde{\mu}_i]_q d}. \quad (1.2.11)$$

Theorem 1.2.6 also enables us to answer probabilistic questions about multiplying regular elliptic elements randomly. We define

$$p_{k,\mu}(q) = \frac{g_{k,\mu}(q)}{\#\mathcal{T}_\mu(q)^k}, \quad (1.2.12)$$

which is the probability that the product of a randomly chosen  $k$ -tuple of regular elliptic elements is in  $\mathcal{T}_\mu(q)$ . We are only concerned with the nontrivial cases  $k \geq 2$ . Of course, Theorems 1.2.1 and 1.2.3 provide exact formulas for  $p_{k,\mu}(q)$  in certain special cases, but we are also interested in the behavior of  $p_{k,\mu}(q)$  as  $q$  becomes arbitrarily large. For the case of regular semisimple elements, we define

$$p_{k,\mu}^\square(q) = \frac{g_{k,\mu}^\square(q)}{\#\mathcal{T}_\mu^\square(q)^k} \quad (1.2.13)$$

Again, Theorems 1.2.1 and 1.2.3 provide exact formulas for  $p_{k,\mu}^\square(q)$  in some special cases. However, we are able to compute  $\lim_{q \rightarrow \infty} p_{k,\mu}(q)$  and  $\lim_{q \rightarrow \infty} p_{k,\mu}^\square(q)$  for all  $\mu \vdash n$ .

**Theorem 1.2.7.** *For all  $n, k \in \mathbb{N}$  with  $k \geq 2$  and  $\mu \vdash n$ , we have*

$$\lim_{q \rightarrow \infty} p_{k,\mu}(q) = \lim_{q \rightarrow \infty} p_{k,\mu}^\square(q) = \frac{1}{z_\mu}. \quad (1.2.14)$$

According to Corollary 1.1.2, one interpretation of Theorem 1.2.7 is that, for large  $q$ , random products of regular elliptic elements are approximately distributed uniformly throughout  $\mathrm{GL}_n \mathbb{F}_q$ . We do not currently have a heuristic explanation for this behavior, nor do we know how random products of regular elliptic elements are distributed among individual conjugacy classes.

Even though Theorem 1.2.7 describes the asymptotics of  $g_{k,\mu}(q)$  as  $q \rightarrow \infty$ , it does not address the specific behavior of  $g_{k,\mu}(q)$  for small  $q$ . It turns out that Theorem 1.2.1 gives a family of examples where the function  $g_{k,\mu}^\square(q)$  is a polynomial in  $q$ . See Corollary 6.1.1.

However, as discussed in Remark 1.2.4 above,  $g_{k,(n)}(q)$  is not necessarily a polynomial, or even a rational function, of  $q$ . Instead, we have the following result.

**Corollary 1.2.8** (to Thm. 1.2.3). *Suppose  $n, k \in \mathbb{N}$  and  $n$  is prime. There exist polynomials  $f_0, f_1, \dots, f_{n-1} \in \mathbb{Q}[x]$  depending only on  $n$  and  $k$ , each with degree  $kn^2$  and leading coefficient  $n^{-(k+1)}$ , satisfying the following properties. For each  $i \in \{0, \dots, n-1\}$ , we have*

$$g_{k,(n)}(q) = f_i(q) \quad \text{for all prime powers } q \equiv i \pmod{n}. \quad (1.2.15)$$

*In other words,  $g_{k,(n)}(q)$  is a quasipolynomial in  $q$  of quasiperiod  $n$ . Furthermore,*

$$f_0 = f_2 = f_3 = \dots = f_{n-1}, \quad \text{but } f_1 \neq f_0. \quad (1.2.16)$$

### 1.3 Related recent work

Our main objective is to find an analogue for  $\mathrm{GL}_n \mathbb{F}_q$  of a result from the 1980s using a notion of a cycle for a matrix which was also suggested in the 1980s. However, our results fit into a body of research that has developed only in the last decade. In this section, we outline some of the central results in this area.

In [24], Lewis-Reiner-Stanton enumerated the factorizations of a **Singer cycle** into a product of **reflections**. A Singer cycle in  $\mathrm{GL}_n \mathbb{F}_q$  is characterized by having an eigenvalue of multiplicative order  $q^n - 1$ . A reflection simply has fixed-space of dimension  $n - 1$ . Their perspective is that the Singer cycles of  $\mathrm{GL}_n \mathbb{F}_q$  are analogous to the  $n$ -cycles of  $\mathfrak{S}_n$  and the reflections of  $\mathrm{GL}_n \mathbb{F}_q$  are analogous to the transpositions of  $\mathfrak{S}_n$ . Here is one of their main results.

**Theorem 1.3.1** (Lewis-Reiner-Stanton [24]). *For all  $n \in \mathbb{N}$  with  $n \geq 2$  and prime powers  $q$ , the number of  $\ell$ -tuples of reflections in  $\mathrm{GL}_n \mathbb{F}_q$  whose product is a fixed, arbitrary Singer cycle equals*

$$[n]_q^{\ell-1} \sum_{i=0}^{\ell-n} (-1)^i (q-1)^{\ell-i-1} \binom{\ell}{i} \left[ \begin{matrix} \ell - i - 1 \\ n - 1 \end{matrix} \right]_q$$

In [23], Lewis-Morales compute the generating function for the number of factorizations of a Singer cycle into a product of elements whose fixed-space dimensions are prescribed. Here is one of their main results, which makes use of the  $q$ -**Pochhammer symbol**

$$(a; q)_m = (1 - a)(1 - aq)(1 - aq^2) \cdots (1 - aq^{m-1}).$$

**Theorem 1.3.2** (Lewis-Morales [23]). *Fix a Singer cycle  $c \in \mathrm{GL}_n \mathbb{F}_q$ . Let  $a_{r_1, \dots, r_k}(q)$  be the number of tuples  $(u_1, \dots, u_k)$  of elements of  $\mathrm{GL}_n \mathbb{F}_q$  such that  $u_1 \cdots u_k = c$  and the fixed-space dimension of  $u_i$  is  $r_i$  for all  $i \in \{1, \dots, k\}$ . Then*

$$\sum_{r_1, \dots, r_k} \frac{a_{r_1, \dots, r_k}(q)}{(\#\mathrm{GL}_n \mathbb{F}_q)^{k-1}} \cdot x_1^{r_1} \cdots x_k^{r_k} = \sum_{\substack{\mathbf{p}=(p_1, \dots, p_k) \\ 0 \leq p_i \leq n}} \frac{M_{\tilde{\mathbf{p}}}^{n-1}(q)}{\prod_{p \in \tilde{\mathbf{p}}} \begin{bmatrix} n-1 \\ p \end{bmatrix}_q} \cdot \frac{(x_1; q^{-1})_{p_1}}{(q; q)_{p_1}} \cdots \frac{(x_k; q^{-1})_{p_k}}{(q; q)_{p_k}}, \quad (1.3.1)$$

where  $\tilde{\mathbf{p}}$  is the result of deleting all copies of  $n$  from  $\mathbf{p}$ ,

$$M_{r_1, \dots, r_k}^m(q) = \sum_{d=0}^{\min(r_i)} (-1)^d q^{\binom{d+1}{2} - kd} \begin{bmatrix} m \\ d \end{bmatrix}_q \prod_{i=1}^k \begin{bmatrix} m-d \\ r_i-d \end{bmatrix}_q$$

for  $k > 0$ , and  $M_{\emptyset}^m(q) = 0$ .

In [17], Huang-Lewis-Reiner enumerated the factorizations of a fixed, arbitrary Singer cycle into a product of elements whose fixed-space codimensions sum to  $n$ . More precisely, they proved the following.

**Theorem 1.3.3** (Huang-Lewis-Reiner [17]). *For all  $n \in \mathbb{N}$  and prime powers  $q$ , if  $c \in \mathrm{GL}_n \mathbb{F}_q$  is any Singer cycle and  $\alpha = (\alpha_1, \dots, \alpha_m)$  satisfies  $n = \sum_{i=1}^m \alpha_i$  and  $\alpha_i > 0$  for all  $i \in \{1, \dots, m\}$ , then the number of  $m$ -tuples  $(g_1, \dots, g_m) \in (\mathrm{GL}_n \mathbb{F}_q)^k$  such that  $g_1 \cdots g_m = c$  and  $g_i$  has fixed-space codimension  $\alpha_i$  for each  $i \in \{1, \dots, m\}$  equals*

$$q^{\sum_{i=1}^m (\alpha_i - 1)(n - \alpha_i)} \cdot (q^n - 1)^{m-1}$$

The results described in the previous three paragraphs can be united in the following way. The  $\ell = n$  case of Theorem 1.3.1 coincides with the  $m = n$  case of Theorem 1.3.3. Furthermore, both of these can be recovered from the  $k = n$  case of Theorem 1.3.2 as  $(\#\mathrm{GL}_n \mathbb{F}_q)^{-(n-1)}$  times the coefficient of  $x_1^{n-1} \cdots x_n^{n-1}$  in (1.3.1).

## **1.4 Outline**

The rest of the thesis is organized as follows. In Chapter 2, we discuss some preliminary information, including the character-theoretic technique and details regarding the symmetric groups, finite fields, and the finite general linear groups. In Chapter 3, we provide a concise retelling of Green's original formulation of the characters of the finite general linear groups [16]. In Chapter 4, we prove Theorems 1.2.1 and 1.2.3, our main enumerative results. In Chapter 5, we prove Theorem 1.2.7, our main probabilistic result. In Chapter 6, we discuss polynomiality and prove Corollary 1.2.8. In Chapter 7, we slightly extend our main results and list some open problems. In the appendix, we provide some data related to Corollary 1.2.8.

## Chapter 2

## PRELIMINARIES

**2.1 The character theory approach**

We assume basic knowledge of the ordinary complex character theory of finite groups. All characters we refer to in this thesis are complex. See Fulton-Harris [13] or Serre [29] for a review. We will make use of a standard character-theoretic technique based on the following remarkable result due to Frobenius. Let  $G$  be a finite group, and let  $\text{Irr}(G)$  denote the set of all irreducible characters of  $G$ . For  $\chi \in \text{Irr}(G)$ , let  $\deg \chi$  denote the value of  $\chi$  at the identity element of  $G$ . For a straightforward proof of the following theorem, see Zagier's Appendix A in Lando-Zvonkin's book [21].

**Theorem 2.1.1** (Frobenius [10]). *Let  $k$  be a positive integer, and, for each  $i \in \{1, \dots, k\}$ , let  $A_i$  be a union of conjugacy classes in  $G$ . For any  $g \in G$ , the number of tuples  $(t_1, \dots, t_k) \in A_1 \times \dots \times A_k$  such that  $t_1 \cdots t_k = g$  is given by*

$$\frac{1}{\#G} \sum_{\chi \in \text{Irr}(G)} (\deg \chi)^{1-k} \chi(g^{-1}) \prod_{i=1}^k \sum_{t \in A_i} \chi(t). \quad (2.1.1)$$

**Corollary 2.1.2.** *For all  $n, k \in \mathbb{N}$ ,  $\mu \vdash n$ , and prime powers  $q$ ,*

$$g_{k,\mu}(q) = \frac{1}{\#\text{GL}_n \mathbb{F}_q} \sum_{\chi \in \text{Irr}(\text{GL}_n \mathbb{F}_q)} (\deg \chi)^{1-k} \left( \sum_{g \in \mathcal{T}_{(n)}(q)} \chi(g) \right)^k \left( \sum_{h \in \mathcal{T}_\mu(q)} \chi(h) \right). \quad (2.1.2)$$

Moreover, the same is true when both  $g_{k,\mu}(q)$  is replaced with  $g_{k,\mu}^\square(q)$  and  $\mathcal{T}_\mu(q)$  is replaced with  $\mathcal{T}_\mu^\square(q)$ .

*Proof.* Consider applying Theorem 2.1.1 to the case of  $k+1$  factors, the first  $k$  of which are regular elliptic and the last of which has cycle type  $\mu$ . Each  $\mathcal{T}_\mu(q)$  is a union of conjugacy

classes, and so the hypotheses of Theorem 2.1.1 are satisfied. Moreover, each  $\mathcal{T}_\mu(q)$  is closed under taking inverses, implying factorizations of the form

$$(t_1, \dots, t_k) \in \mathcal{T}_{(n)}(q)^k \quad \text{such that} \quad t_1 \cdots t_k \in \mathcal{T}_\mu(q)$$

are in bijection with factorizations of the form

$$(t_1, \dots, t_k, t_{k+1}) \in \mathcal{T}_{(n)}(q)^k \times \mathcal{T}_\mu(q) \quad \text{such that} \quad t_1 \cdots t_{k+1} = \text{id}.$$

Thus,

$$g_{k,\mu}(q) = \#\{(t_1, \dots, t_k, t_{k+1}) \in \mathcal{T}_{(n)}(q)^k \times \mathcal{T}_\mu(q) : t_1 \cdots t_{k+1} = \text{id}\}.$$

Applying Theorem 2.1.1 with

$$A_1 = A_2 = \cdots = A_k = \mathcal{T}_{(n)}(q), \quad A_{k+1}(q) = \mathcal{T}_\mu(q), \quad \text{and} \quad g = \text{id}$$

gives the result. The final claim regarding regular semisimple elements follows from the same argument.  $\square$

## 2.2 The symmetric groups and partitions

We will require some specific information about the irreducible characters of the symmetric group  $\mathfrak{S}_n$ . This information can be found in Stanley [31] and Sagan [28]. See also Fulton-Harris [13] or Fulton [12] for added discussion on the irreducible characters of the symmetric groups.

A **partition** of  $n$  is a weakly decreasing sequence of non-negative integers  $\mu = (\mu_1, \mu_2, \dots)$  such that  $\sum_{i \geq 1} \mu_i = n$ , denoted by  $\mu \vdash n$ . Denote by  $\emptyset$  the unique partition of 0 and by  $\square$  the unique partition of 1. Let  $\text{Par}$  denote the set of all partitions of all non-negative integers. Each  $\mu_i$  is called a **part** of  $\mu$ . The number of nonzero parts of  $\mu$  is called the **length** of  $\mu$  and is denoted by  $\ell(\mu)$ . The **conjugate** of  $\mu$  is denoted by  $\mu'$  and defined by  $\mu'_i = \#\{j \geq 1 : \mu_j \geq i\}$  for all  $i \geq 0$ . The **multiplicity** of a positive integer  $i$  in a partition  $\mu$  is defined as  $\#\{j \geq 1 : \mu_j = i\}$  and denoted by  $m_i(\mu)$ . Also define  $s_i(\mu) = \sum_{j=1}^i \mu_j$ . In general, if some part of a partition is repeated, we denote this with a superscript. Moreover,

we omit zeros. For example,  $(3, 2^4)$  is the same as  $(3, 2, 2, 2, 2)$ . A partition of the form  $(n - r, 1^r) \vdash n$  for some  $r \in \{0, \dots, n - 1\}$  is called a **hook**. An important statistic on partitions is  $\mu \mapsto z_\mu$  defined by  $z_\mu = \prod_{i \geq 1} i^{m_i(\mu)} \cdot m_i(\mu)!$ . If  $d$  is a positive integer, then we use  $d\mu$  to denote the partition  $(d\mu_1, d\mu_2, \dots)$  of  $dn$ .

The conjugacy classes of  $\mathfrak{S}_n$  are in bijection with the partitions of  $n$  as follows. If  $\pi = (\pi_{1,1}, \dots, \pi_{1,\mu_1}) \cdots (\pi_{\ell,1}, \dots, \pi_{\ell,\mu_\ell}) \in \mathfrak{S}_n$  is a cycle decomposition of  $\pi$  with  $\mu_1 \geq \mu_2 \geq \dots \geq \mu_\ell$ , then the conjugacy class of  $\pi$  is indexed by the partition  $\mu = (\mu_1, \mu_2, \dots, \mu_\ell) \vdash n$ . The partition  $\mu$  is called the **cycle type** of the permutation  $\pi$ . Let  $\mathcal{C}_\mu$  denote the conjugacy class consisting of those permutations with cycle type  $\mu$ . The statistic  $\mu \mapsto z_\mu$  has the following algebraic interpretation. If  $\sigma \in \mathfrak{S}_n$  has cycle type  $\mu$ , then  $z_\mu$  is the number of permutations in  $\mathfrak{S}_n$  which commute with  $\sigma$ . By the orbit-stabilizer theorem [8, Prop. 4.3.6],  $\#\mathcal{C}_\mu = n!/z_\mu$ .

The irreducible characters of  $\mathfrak{S}_n$  are indexed by partitions of  $n$  in a standard way. If  $\lambda \vdash n$ , let  $\chi^\lambda$  denote the character indexed by  $\lambda$ . Let  $\chi_\mu^\lambda$  denote  $\chi^\lambda$  evaluated on any element of  $\mathcal{C}_\mu$ . There is a combinatorial formula, known as the Murnaghan-Nakayama (MN) rule, for computing the irreducible character values for the symmetric groups [26, 27]. See [31, Thm. 7.17.3] for a full statement and proof. We will use the following two special cases.

**Corollary 2.2.1** (to the MN rule). *For all  $n \in \mathbb{N}$  and  $\lambda \vdash n$ , we have*

$$\chi_{(n)}^\lambda = \begin{cases} (-1)^r, & \lambda = (n - r, 1^r) \text{ for some } r \in \{0, \dots, n - 1\}, \\ 0, & \text{otherwise,} \end{cases} \quad (2.2.1)$$

and

$$\chi_{(n-1,1)}^\lambda = \begin{cases} 1, & \lambda = (n), \\ (-1)^n, & \lambda = (1^n), \\ (-1)^{r-1}, & \lambda = (n - r, 2, 1^{r-2}) \text{ for some } r \in \{2, \dots, n - 2\}, \\ 0, & \text{otherwise.} \end{cases} \quad (2.2.2)$$

Recall Theorem 1.1.1. The simplicity of (1.1.2) is due to Corollary 2.2.1. In particular, the

character value  $\chi_{(n)}^\lambda$  is only nonzero on the  $n$  partitions  $\lambda = (n-r, 1^r)$  for  $r \in \{0, \dots, n-1\}$ .

### 2.3 Finite fields

We assume some basic knowledge about finite fields, all of which can be found in Dummit-Foote [8]. For all positive integers  $m$ , there is a degree  $m$  field extension  $\mathbb{F}_{q^m}$  of  $\mathbb{F}_q$ . For positive integers  $m$  and  $m'$ , we have the containment  $\mathbb{F}_{q^m} \subset \mathbb{F}_{q^{m'}}$  if and only if  $m|m'$ . For any field  $\mathbb{F}$ , let  $\mathbb{F}^\times$  denote the multiplicative group of its nonzero elements, called the **unit group**. The unit group of any finite field is cyclic. Moreover, in the case  $m|m'$ , we have that  $\mathbb{F}_{q^m}^\times$  is a subgroup of  $\mathbb{F}_{q^{m'}}^\times$ .

Let  $\mathcal{F}(q) \subset \mathbb{F}_q[z]$  denote the set of monic, nonconstant, irreducible polynomials over  $\mathbb{F}_q$ , excluding  $z$  itself. For each  $d \in \mathbb{N}$ , let  $\mathcal{F}_d(q) = \{f \in \mathcal{F}(q) : \deg f = d\}$ . Let  $\sqcup$  denote disjoint union.

**Lemma 2.3.1.** *For all  $d \in \mathbb{N}$  and prime powers  $q$ ,*

$$\mathbb{F}_{q^d}^\times = \bigsqcup_{c|d} \bigsqcup_{f \in \mathcal{F}_c(q)} \{\alpha \in \mathbb{F}_{q^c}^\times : f(\alpha) = 0\}. \quad (2.3.1)$$

*Proof.* Every element of  $\mathbb{F}_{q^d}^\times$  is the root of an element of  $\mathcal{F}(q)$  with degree dividing  $d$ . The union is disjoint because distinct monic, irreducible polynomials over  $\mathbb{F}_q$  do not have shared roots.  $\square$

For each  $n \in \mathbb{N}$ , fix a generator  $\varepsilon$  of the cyclic group  $\mathbb{F}_{q^{n!}}^\times$ , and fix an injective group homomorphism  $\theta : \mathbb{F}_{q^{n!}}^\times \rightarrow \mathbb{C}^\times$  defined by mapping  $\varepsilon \mapsto e^{2\pi i/(q^{n!}-1)}$ . Note that we omit the dependence of  $\varepsilon$  on  $n$ . Context will suffice. For each  $d \in \{1, \dots, n\}$ , let  $\varepsilon_d$  denote  $\varepsilon$  raised to the power  $(q^{n!} - 1)/(q^d - 1)$ . The multiplicative order of  $\varepsilon_d$  is  $q^d - 1$ , and  $\varepsilon_d$  is a cyclic generator of  $\mathbb{F}_{q^d}^\times$ . Also,  $\theta$  maps  $\mathbb{F}_{q^d}^\times$  isomorphically onto the group of  $(q^d - 1)^{\text{th}}$  roots of unity.

**Corollary 2.3.2.** *For all  $n \in \mathbb{N}$ ,  $d \in \{1, \dots, n\}$ , and prime powers  $q$ ,*

$$\{\xi \in \mathbb{C}^\times : \xi^{q^d-1} = 1\} = \bigsqcup_{c|d} \bigsqcup_{f \in \mathcal{F}_c(q)} \{\theta(\alpha) : \alpha \in \mathbb{F}_{q^c}^\times, f(\alpha) = 0\}. \quad (2.3.2)$$

*Proof.* Apply  $\theta$  to each element on the left and right sides of (2.3.1).  $\square$

For each  $d \in \mathbb{N}$ , the Galois group of  $\mathbb{F}_{q^d}$  over  $\mathbb{F}_q$  is cyclic of order  $d$ , generated by the field automorphism

$$\mathbb{F}_{q^d} \rightarrow \mathbb{F}_{q^d}, \quad \alpha \mapsto \alpha^q.$$

Therefore, for each  $f \in \mathcal{F}_d(q)$ , if  $\alpha$  is any root of  $f$ , then  $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{d-1}}$  are distinct and are all the roots of  $f$ . Since  $\mathbb{F}_{q^d}^\times$  is generated by  $\varepsilon_d$ , there exists some  $\ell \in \mathbb{Z}$  such that  $\varepsilon_d^\ell$  is a root of  $f$ . Assign to  $f$  an arbitrary integer  $\ell_f$  such that  $\varepsilon_d^{\ell_f}$  is a root of  $f$ . To combine the previous three sentences,

$$f(z) = \prod_{i=0}^{d-1} \left( z - \left( \varepsilon_d^{\ell_f} \right)^{q^i} \right). \quad (2.3.3)$$

Observe that the choice of  $\ell_f$  is unique up to multiplication by powers of  $q$  and addition by multiples of  $q^d - 1$ . Our results are independent of the choice of  $\ell_f$ .

In case we are considering a polynomial  $f$  with degree  $d$  dividing  $n$ , we will also make use of the quantity  $\ell_f [n/d]_{q^d}$ , viewing it as an element of  $\mathbb{Z}/(q^n - 1)$ . More precisely, define the group isomorphism

$$\theta_n : \mathbb{F}_{q^n}^\times \rightarrow \mathbb{Z}/(q^n - 1) \quad \text{by} \quad \theta_n(\varepsilon_n^\ell) = \ell \pmod{q^n - 1} \quad \forall \ell \in \mathbb{Z}. \quad (2.3.4)$$

It follows that  $\theta_n$  maps  $\varepsilon_d^\ell$  to  $\ell [n/d]_{q^d}$ .

**Corollary 2.3.3** (to Lem. 2.3.1). *For all  $n \in \mathbb{N}$ ,  $d|n$ , and prime powers  $q$ ,*

$$\{m \cdot [n/d]_{q^d} : m \in \mathbb{Z}/(q^n - 1)\} = \bigsqcup_{c|d} \bigsqcup_{f \in \mathcal{F}_c(q)} \{\theta_n(\alpha) : \alpha \in \mathbb{F}_{q^c}^\times, f(\alpha) = 0\}. \quad (2.3.5)$$

*Proof.* Apply  $\theta_n$  to each element on the left and right sides of (2.3.1), recalling that  $d|n$  and  $\mathbb{F}_{q^d}^\times$  is the unique subgroup of  $\mathbb{F}_{q^n}^\times$  of order  $q^d - 1$ .  $\square$

**Example 2.3.4.** Consider the case  $q = 3$ ,  $n = 4$ , and  $\theta : \varepsilon \mapsto \zeta$ , where

$$\zeta = e^{2\pi i / (q^n - 1)}.$$

We write  $\mathbb{F}_3$  as  $\{0, 1, 2\}$  under addition and multiplication modulo 3. We record in Table 2.1 the polynomials  $f \in \mathcal{F}(q)$  with degree dividing  $n$ , together with all possible choices for  $\ell_f$  modulo  $q^d - 1$  and all possible choices for  $\ell_f[n/\deg f]_{q^{\deg f}}$  modulo  $q^n - 1$ . For the sake of brevity, we omit most of the degree four polynomials. Note that these values depend on the choice of  $\varepsilon$ .

Table 2.1: Choices for  $\ell_f$  and  $\ell_f[n/\deg f]_{q^{\deg f}}$  with  $q = 3$  and  $n = 4$ .

$f$	$\ell_f$	$\ell_f[n/\deg f]_{q^{\deg f}}$
$z + 2$	0	0
$z + 1$	1	40
$z^2 + 2z + 2$	1, 3	10, 30
$z^2 + 1$	2, 6	20, 60
$z^2 + z + 2$	5, 7	50, 70
$z^4 + 2z^3 + 2$	1, 3, 9, 27	1, 3, 9, 27
$z^4 + 2z^3 + z^2 + 1$	2, 6, 18, 54	2, 6, 18, 54
$z^4 + z^3 + 2z + 1$	4, 12, 28, 36	4, 12, 28, 36
$\vdots$	$\vdots$	$\vdots$

We can also visualize the data from Table 2.1 in the complex plane as follows. Observe that  $\theta$  maps  $\varepsilon_n$  to

$$\xi = \zeta^{\frac{q^{n!}-1}{q^n-1}},$$

a  $(q^n - 1)^{\text{th}} = 80^{\text{th}}$  root of unity. Given a choice of  $\ell_f$  for some  $f$  in Table 2.1 with degree  $d|n$ , we have

$$\alpha = \varepsilon_d^{\ell_f} = \varepsilon_n^{\ell_f[n/d]_{q^d}}$$

is a root of  $f$ ,

$$\theta(\alpha) = \xi^{\ell_f[n/d]_{q^d}} \in \mathbb{C}^\times, \quad \text{and} \quad \theta_n(\alpha) = \ell_f[n/d]_{q^d} \in \mathbb{Z}/(q^n - 1).$$

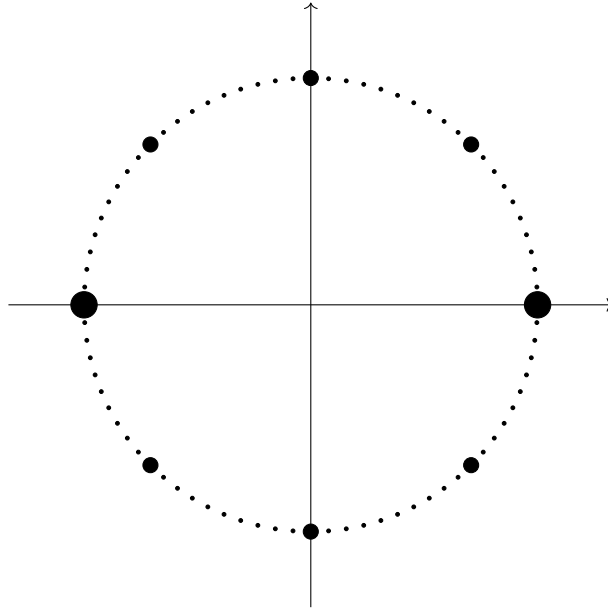
Figure 2.1: Images under  $\theta$  of roots of polynomials from Table 2.1

Figure 2.1 shows the complex plane and the images under  $\theta$  of all the roots of all the polynomials  $f \in \mathcal{F}_1(3) \sqcup \mathcal{F}_2(3) \sqcup \mathcal{F}_4(3)$ . The images under  $\theta$  of roots of polynomials in  $\mathcal{F}_1(3)$  are labeled by the largest nodes, those for  $\mathcal{F}_2(3)$  by the medium-sized nodes, and those for  $\mathcal{F}_4(3)$  by the smallest nodes.

One can observe in Figure 2.1 the following instance of Cor. 2.3.2. The images under  $\theta$  of the roots of polynomials in  $\mathcal{F}_1(3) \sqcup \mathcal{F}_2(3)$  precisely form the set of  $(q^2 - 1)^{\text{th}} = 8^{\text{th}}$  roots of unity, pictorially represented by the medium and large nodes.

One can also observe the following instance of Cor. 2.3.3 in either Table 2.1 or Fig. 2.1. The images under  $\theta_n$  of the roots of polynomials in  $\mathcal{F}_1(3) \sqcup \mathcal{F}_2(3)$  are  $0, 10, 20, \dots, 70$ . These are precisely the multiples of  $(q^n - 1)/(q^2 - 1) = 10$  in  $\mathbb{Z}/(q^n - 1)$ .

## 2.4 The finite general linear groups

The finite general linear group  $\text{GL}_n \mathbb{F}_q$  is the group of  $n \times n$  invertible matrices with entries in the finite field  $\mathbb{F}_q$  with  $q$  elements. We will occasionally have need to view the elements

of  $\mathrm{GL}_n \mathbb{F}_q$  abstractly as linear transformations on an  $n$ -dimensional  $\mathbb{F}_q$ -vector space. The cardinality of  $\mathrm{GL}_n \mathbb{F}_q$  is  $\gamma_n(q)$  as defined in Table 1.1 [32, Prop. 1.10.1].

#### 2.4.1 Indexing the $\mathrm{GL}_n \mathbb{F}_q$ conjugacy classes

We discuss how to index the conjugacy classes and irreducible characters of  $\mathrm{GL}_n \mathbb{F}_q$ . Let  $V = \mathbb{F}_q^n$ . Then  $\mathrm{GL}_n \mathbb{F}_q$  acts on  $V$  via matrix multiplication.

Consider a fixed  $g \in \mathrm{GL}_n \mathbb{F}_q$ . Let  $V_g$  denote the vector space  $V$  endowed with an  $\mathbb{F}_q[z]$ -module structure by defining the action  $\mathbb{F}_q[z] \times V_g \rightarrow V_g$  to be  $(f(z), v) \mapsto f(g)(v)$ . The polynomial ring  $\mathbb{F}_q[z]$  is a principal ideal domain, and  $V$  is finite-dimensional as an  $\mathbb{F}_q$ -vector space, hence  $V_g$  is finitely generated as an  $\mathbb{F}_q[z]$ -module. By the structure theorem for finitely generated modules over principal ideal domains [8, Thm. 12.1.6], there exists a unique function  $\underline{\lambda}^g : \mathcal{F}(q) \rightarrow \mathrm{Par}$  such that

$$V_g \cong \bigoplus_{f \in \mathcal{F}(q)} \bigoplus_{i \geq 1} \mathbb{F}_q[z] / (f(z)^{\underline{\lambda}^g(f)_i}) \quad (2.4.1)$$

as  $\mathbb{F}_q[z]$ -modules, where  $\underline{\lambda}^g(f)_i$  denotes the  $i^{\mathrm{th}}$  part of  $\underline{\lambda}^g(f)$ . We say that  $g$  **determines the isomorphism** (2.4.1). Moreover,  $g_1$  and  $g_2$  are conjugate in  $\mathrm{GL}_n \mathbb{F}_q$  if and only if  $\underline{\lambda}^{g_1} = \underline{\lambda}^{g_2}$ . If  $g$  is clear from context, we omit the superscript from  $\underline{\lambda}^g$ . The function  $\underline{\lambda} : \mathcal{F}(q) \rightarrow \mathrm{Par}$  is said to **index** the conjugacy class of  $g \in \mathrm{GL}_n \mathbb{F}_q$ , and we denote this conjugacy class by  $\mathcal{C}_{\underline{\lambda}}$ .

Define the **norm** of an index  $\underline{\lambda} : \mathcal{F}(q) \rightarrow \mathrm{Par}$  to be

$$\|\underline{\lambda}\| = \sum_{f \in \mathcal{F}(q)} |\underline{\lambda}(f)| \cdot \deg f. \quad (2.4.2)$$

Computing dimensions of each side in the isomorphism given in (2.4.1) implies the equation  $n = \|\underline{\lambda}\|$ . Therefore, to each conjugacy class  $C \subset \mathrm{GL}_n \mathbb{F}_q$ , we can associate a unique index  $\underline{\lambda}$  with  $n = \|\underline{\lambda}\|$  such that  $C = \mathcal{C}_{\underline{\lambda}}$ . In [16], Green shows that the condition  $n = \|\underline{\lambda}\|$  is necessary and sufficient for  $\underline{\lambda}$  to be the index of some conjugacy class in  $\mathrm{GL}_n \mathbb{F}_q$ . Thus, conversely, to every index  $\underline{\lambda}$  with  $\|\underline{\lambda}\| = n$ , there exists a unique conjugacy class of  $\mathrm{GL}_n \mathbb{F}_q$  with index  $\underline{\lambda}$ .

Given  $\underline{\lambda}$ , one can read off the characteristic and minimal polynomials of  $g$  as follows. The minimal polynomial is  $\prod_{f \in \mathcal{F}(q)} f^{\underline{\lambda}(f)_1}$ , and the characteristic polynomial is  $\prod_{f \in \mathcal{F}(q)} f^{|\underline{\lambda}(f)|}$ .

Moreover, we can use the isomorphism (2.4.1) to write down a specific matrix whose conjugacy class is indexed by  $\underline{\lambda}$  as follows. If  $h(z) = z^n - a_{n-1}z^{n-1} - \cdots - a_1z - a_0 \in \mathbb{F}_q[z]$ , then the **companion matrix** of  $h$  is defined by

$$A(h) = \begin{bmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & a_{n-1} \end{bmatrix},$$

where  $A(1)$  is the empty matrix. Given  $g \in \mathrm{GL}_n \mathbb{F}_q$  which determines the isomorphism (2.4.1),  $g$  is in the same conjugacy class as any block-diagonal matrix whose diagonal blocks are those nonempty matrices  $A(f^{\lambda(f)i})$  for  $f \in \mathcal{F}(q)$  and  $i \geq 1$ . Any block-diagonal matrix with these diagonal blocks arranged in any order of non-increasing size from the upper-left corner to the lower-right corner is said to be a **rational canonical form** of  $g$ . Furthermore, if  $g$  itself is in this form, say that  $g$  is in **rational canonical form**.

**Example 2.4.1.** Consider the matrix

$$g = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \mathrm{GL}_3 \mathbb{F}_2.$$

This matrix is block-diagonal, with diagonal blocks of size 2 and 1. The blocks are the companion matrices of the polynomials  $z^2 - z - 1$  and  $z - 1 \in \mathbb{F}_2[z]$ , respectively. Thus,  $g$  is in rational canonical form. The conjugacy class of  $g$  has index  $\underline{\lambda}$  defined by

$$\underline{\lambda}(f) = \begin{cases} (1) & \text{if } f = z^2 - z - 1, \\ (1) & \text{if } f = z - 1, \\ \emptyset & \text{otherwise.} \end{cases}$$

The characteristic polynomial of  $g$  is  $(z - 1)(z^2 - z - 1) = z^3 - 1 \in \mathbb{F}_2[z]$ , which is also its minimal polynomial.

Define the **support** of an index  $\underline{\lambda}$  by  $\text{supp } \underline{\lambda} = \{f \in \mathcal{F}(q) : \underline{\lambda}(f) \neq \emptyset\}$ . Observe  $\|\underline{\lambda}\| < \infty$  implies  $\#\text{supp } \underline{\lambda} < \infty$ . Call an index  $\underline{\lambda}$  **primary** if  $\#\text{supp } \underline{\lambda} = 1$ . If  $\underline{\lambda}$  is primary with  $\text{supp } \underline{\lambda} = \{f\}$  and  $\underline{\lambda}(f) = \lambda$ , then we denote  $\underline{\lambda}$  simply by  $f \mapsto \lambda$ . For example,  $z - 1 \mapsto (1^n)$  is the index for the identity matrix of  $\text{GL}_n \mathbb{F}_q$ . We refer to a conjugacy class itself as primary if its index is primary, and we refer to an element as primary if it is a member of a primary conjugacy class.

The following result allows us to compute the sizes of conjugacy classes in  $\text{GL}_n \mathbb{F}_q$ . Recall that, for  $\mu \vdash n$  and  $i \in \mathbb{N}$ , we have defined  $\mu'$  to be the conjugate partition to  $\mu$ , and we have defined  $s_i(\mu) = \sum_{j=1}^i \mu_j$ .

**Theorem 2.4.2** ([32, Thm. 1.10.7]). *For all  $n \in \mathbb{N}$ , prime powers  $q$ , and  $\underline{\lambda} : \mathcal{F}(q) \rightarrow \text{Par}$  with  $\|\underline{\lambda}\| = n$ , we have*

$$\#\mathcal{C}_{\underline{\lambda}} = \frac{\gamma_n(q)}{\prod_{f \in \mathcal{F}(q)} \prod_{i \geq 1} \prod_{j=1}^{m_i(\underline{\lambda}(f))} ((q^{\deg f})^{s_i(\underline{\lambda}(f)')} - (q^{\deg f})^{s_i(\underline{\lambda}(f)')-j})}. \quad (2.4.3)$$

**Example 2.4.3.** Consider  $\text{GL}_3 \mathbb{F}_2$ . The degree 1, 2, and 3 polynomials in  $\mathcal{F}(2)$  are  $f_1 = z - 1$ ,  $f_2 = z^2 - z - 1$ ,  $f_3 = z^3 - z^2 - 1$ , and  $\tilde{f}_3 = z^3 - z - 1$ . There are six functions  $\underline{\lambda} : \mathcal{F}(2) \rightarrow \text{Par}$  satisfying  $\|\underline{\lambda}\| = 3$ , which index the conjugacy classes and irreducible characters of  $\text{GL}_3 \mathbb{F}_2$ . The primary ones are

$$f_1 \mapsto (1, 1, 1), f_2 \mapsto (2, 1), f_3 \mapsto (3), f_3 \mapsto (1), \text{ and } \tilde{f}_3 \mapsto (1).$$

There is only one more left to define. We call it  $\underline{\lambda}_0$ . It is defined by

$$\underline{\lambda}_0(f) = \begin{cases} (1) & \text{if } f = f_1, \\ (1) & \text{if } f = f_2, \\ \emptyset & \text{otherwise.} \end{cases}$$

We now name all of the conjugacy classes, indicate a member in rational canonical form,

and indicate what function  $\mathcal{F}(2) \rightarrow \text{Par}$  indexes the class.

The conjugacy class  $U_1$  of  $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$  is indexed by  $f_1 \mapsto (1, 1, 1)$ .

The conjugacy class  $U_2$  of  $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$  is indexed by  $f_1 \mapsto (2, 1)$ .

The conjugacy class  $U_3$  of  $\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$  is indexed by  $f_1 \mapsto (3)$ .

The conjugacy class  $E$  of  $\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$  is indexed by  $f_3 \mapsto (1)$ .

The conjugacy class  $\tilde{E}$  of  $\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$  is indexed by  $\tilde{f}_3 \mapsto (1)$ .

The conjugacy class  $C_0$  of  $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$  is indexed by  $\underline{\lambda}_0$ .

We chose these names for the following reasons. The **unipotent** classes are  $U_1, U_2$ , and  $U_3$ . The regular elliptic classes are  $E$  and  $\tilde{E}$ . The **odd one out** is  $C_0$ . As an example of Theorem 2.4.2, we compute the cardinality of  $U_2$ . Recall that the index for  $U_2$  is primary with support  $\{f_1\}$ . Furthermore, the image of  $f_1$  is  $(2, 1) = (2, 1)' \vdash 3$ , and  $m_1((2, 1)) = m_2((2, 1)) = 1$ . By Theorem 2.4.2,

$$\#U_2 = \frac{\gamma_3(2)}{\prod_{i=1}^2 (2^{s_i((2,1))} - 2^{s_i((2,1))-1})} = \frac{2^{\binom{3}{2}} [3]_2!}{(2^2 - 2)(2^3 - 2^2)} = 21. \quad (2.4.4)$$

#### 2.4.2 Cycle type, regular semisimple elements, and regular elliptic elements

Recall the definition of **cycle type** for  $\text{GL}_n \mathbb{F}_q$  from the introduction, which states that  $g \in \text{GL}_n \mathbb{F}_q$  has cycle type  $\mu \vdash n$  if the parts of  $\mu$  are the degrees of the irreducible factors of the characteristic polynomial of  $g$ . Equivalently,  $\text{type}(g) = \mu$  if and only if

$$m_i(\mu) = \sum_{f \in \mathcal{F}_i(q)} |\underline{\lambda}^g(f)| \quad (2.4.5)$$

for each  $i \in \{1, \dots, n\}$ . Recall that we define, for  $\mu \vdash n$  and  $q$  a prime power,

$$\mathcal{T}_\mu(q) = \{g \in \text{GL}_n \mathbb{F}_q : \text{type}(g) = \mu\}. \quad (2.4.6)$$

Since conjugate matrices have the same characteristic polynomial, each  $\mathcal{T}_\mu(q)$  is a union of conjugacy classes, and  $\{\mathcal{T}_\mu(q) : \mu \vdash n\}$  forms a partition of  $\text{GL}_n \mathbb{F}_q$ .

**Example 2.4.4.** Using the notation from Ex. 2.4.3 above,  $\mathcal{T}_{(1,1,1)}(2) = U_1 \cup U_2 \cup U_3$ ,  $\mathcal{T}_{(2,1)}(2) = C_0$ , and  $\mathcal{T}_{(3)}(2) = E \cup \tilde{E}$ .

Recall from the introduction that we mentioned Stong's [34] generalization  $\tilde{Z}_n(q; x)$  of Kung's [20] cycle index  $Z(\mathrm{GL}_n \mathbb{F}_q; x)$  for  $\mathrm{GL}_n \mathbb{F}_q$ . Our notation is more similar to Fulman's phrasing of Stong's cycle index, which we repeat here. Let  $x_q$  denote the alphabet of indeterminates  $\{x_{f,\lambda} : f \in \mathcal{F}(q), \lambda \in \mathrm{Par}\}$ . Define

$$Z_{\mathrm{GL}_n \mathbb{F}_q}(x_q) = \frac{1}{\gamma_n(q)} \sum_{g \in \mathrm{GL}_n \mathbb{F}_q} \prod_{f \in \mathcal{F}(q)} x_{f, \Delta^g(f)}.$$

In Stong's notation, variables of the form  $x_{p,b}$  were used, where  $p$  is a polynomial and  $b$  is a partition. Next, let  $x$  denote the alphabet of indeterminates  $\{x_i : i \in \mathbb{N}\}$ , and consider the variable substitution

$$x_{f,\lambda} \mapsto x_{\deg f}^{|\lambda|}.$$

Essentially, this substitution records the number of factors of  $f$  appearing in the characteristic polynomial of a given matrix. Using (2.4.5), we see that the effect this has on the cycle index is

$$Z_{\mathrm{GL}_n \mathbb{F}_q}(x_{f,\lambda} \mapsto x_{\deg f}^{|\lambda|}) = \frac{1}{\gamma_n(q)} \sum_{\mu \vdash n} \#\mathcal{T}_\mu(q) \cdot x_1^{m_1(\mu)} x_2^{m_2(\mu)} \cdots x_n^{m_n(\mu)}. \quad (2.4.7)$$

In words, we recover the normalized generating function for the cardinalities of the sets  $\mathcal{T}_\mu(q)$  for  $\mu \vdash n$ .

We now discuss a special class of matrices in  $\mathrm{GL}_n \mathbb{F}_q$ , the **regular semisimple** elements. An element of an algebraic group is called **regular** if the dimension of its centralizer is equal to the dimension of a maximal torus of the group. A matrix in  $\mathrm{GL}_n \mathbb{F}_q$  is called **semisimple** if it is diagonalizable over an algebraic closure of  $\mathbb{F}_q$ . A matrix in  $\mathrm{GL}_n \mathbb{F}_q$  is called **regular semisimple** if it is both regular and semisimple. See Lehrer's work [22] for a discussion on the regular semisimple variety in algebraic groups in both characteristic zero and positive characteristic. In particular, Lehrer gives a formula [22, Cor. 8.5] enumerating the regular semisimple elements in  $\mathrm{GL}_n \mathbb{F}_q$ . Fulman gave the following combinatorial characterization

of the regular semisimple elements of  $\mathrm{GL}_n \mathbb{F}_q$ , which also explains our choice of the notation  $\mathcal{T}_\mu^\square(q)$ . We will take Fulman's characterization as the definition of regular semisimple elements in this thesis.

**Theorem 2.4.5** (Fulman [11]). *For all  $n \in \mathbb{N}$  and prime powers  $q$ , a matrix  $g \in \mathrm{GL}_n \mathbb{F}_q$  is regular semisimple if and only if  $\underline{\lambda}^g(f) \in \{\emptyset, \square\}$  for all  $f \in \mathcal{F}(q)$ .*

**Corollary 2.4.6.** *Suppose  $n \in \mathbb{N}$ ,  $q$  is a prime power,  $g \in \mathrm{GL}_n \mathbb{F}_q$  is regular semisimple and  $h_1, \dots, h_\ell \in \mathcal{F}(q)$  are the distinct irreducible factors of the characteristic polynomial of  $g$ . Then  $g$  determines the isomorphism*

$$V_g \cong \mathbb{F}_q[z]/(h_1(z)) \oplus \dots \oplus \mathbb{F}_q[z]/(h_\ell(z)). \quad (2.4.8)$$

Recall that we define, for  $\mu \vdash n$  and  $q$  a prime power,

$$\mathcal{T}_\mu^\square(q) = \{g \in \mathcal{T}_\mu(q) : g \text{ is regular semisimple}\}. \quad (2.4.9)$$

The set  $\{\mathcal{T}_\mu^\square(q) : \mu \vdash n\}$  is not a partition of  $\mathrm{GL}_n \mathbb{F}_q$  in general because not all matrices in  $\mathrm{GL}_n \mathbb{F}_q$  are regular semisimple. However each  $\mathcal{T}_\mu^\square(q)$  is still a union of conjugacy classes, and the set  $\{\mathcal{T}_\mu^\square(q) : \mu \vdash n\}$  at least partitions the set of regular semisimple elements in  $\mathrm{GL}_n \mathbb{F}_q$ .

**Example 2.4.7.** Using the notation from Ex. 2.4.3 above,  $\mathcal{T}_{(1,1,1)}^\square(2)$  is empty,  $\mathcal{T}_{(2,1)}^\square(2) = C_0$ , and  $\mathcal{T}_{(3)}^\square(2) = E \cup \tilde{E}$ .

Recall that Corollary 1.1.2 states that, for large  $q$ , the set  $\mathcal{T}_\mu^\square(q)$  comprises approximately  $1/z_\mu$  of  $\mathrm{GL}_n \mathbb{F}_q$ . We can also derive an explicit formula for  $\#\mathcal{T}_\mu^\square(q)$  by combining Theorems 2.4.2 and 2.4.5. As mentioned by Green in [16] and by Stanley in [32, Eq. (1.103)], we have

$$\#\mathcal{F}_m(q) = \frac{1}{m} \sum_{s|m} \mu(m/s)(q^s - 1) \quad (2.4.10)$$

for all  $m \geq 1$  and prime powers  $q$ , a result originally due to Gauss in the case that  $q$  is prime [14]. Note that our phrasing replaces  $q^s$  with  $q^s - 1$  to exclude the polynomial  $f(z) = z$  from the degree-1 polynomials.

**Corollary 2.4.8.** *Suppose  $n \in \mathbb{N}$ ,  $\mu \vdash n$ , and  $q$  is a prime power. Then  $\mathcal{T}_\mu^\square(q)$  is a union of conjugacy classes, each with cardinality*

$$\frac{\gamma_n(q)}{\prod_{i=1}^{\ell(\mu)} (q^{\mu_i} - 1)}.$$

Therefore,

$$\#\mathcal{T}_\mu^\square(q) = \frac{\gamma_n(q)}{\prod_{i=1}^{\ell(\mu)} (q^{\mu_i} - 1)} \cdot \prod_{i \geq 1} \binom{\#\mathcal{F}_i(q)}{m_i(\mu)}.$$

Unfortunately, we do not have an explicit formula for  $\#\mathcal{T}_\mu(q)$  in general. In fact, in Theorem 1.2.3 and Corollary 1.2.2, we have technically only dealt with regular semisimple elements since  $\mathcal{T}_{(n)}(q) = \mathcal{T}_{(n)}^\square(q)$  and  $\mathcal{T}_{(n-1,1)}(q) = \mathcal{T}_{(n-1,1)}^\square(q)$ . Following Stong's [34, Prop. 19] and Fulman's [11, Sec. 5] calculations, we have, for an indeterminate  $u$ ,

$$1 + \sum_{n \geq 1} Z_{\mathrm{GL}_n \mathbb{F}_q}(x_{f,\lambda} \mapsto x_{\deg f}^{|\lambda|}) u^n = \prod_{m \geq 1} \prod_{r \geq 1} \left( \frac{1}{1 - (u/q^r)^m x_m} \right)^{\#\mathcal{F}_m(q)}. \quad (2.4.11)$$

Recalling (2.4.7), we see that (2.4.11) at least gives a generating-function approach toward computing  $\#\mathcal{T}_\mu(q)$ .

In addition to Fulman's theorem, we will make use of the following characterization of regular semisimple elements, which appears as the final Corollary in Section 3 of Brickman-Fillmore [4]. Recall that a matrix  $g \in \mathrm{GL}_n \mathbb{F}_q$  is said to **stabilize** a subspace  $U \subset V$  if  $g(u) \in U$  for all  $u \in U$ . Recall also that the **lattice of stable subspaces** of a matrix  $g \in \mathrm{GL}_n \mathbb{F}_q$  is the set of subspaces  $U \subset V$  that  $g$  stabilizes, ordered by inclusion.

**Theorem 2.4.9** (Brickman-Fillmore [4]). *For all  $n \in \mathbb{N}$  and prime powers  $q$ , a matrix  $g \in \mathrm{GL}_n \mathbb{F}_q$  is regular semisimple if and only if the lattice of stable subspaces of  $g$  is a Boolean lattice.*

Next, we discuss another special class of matrices in  $\mathrm{GL}_n \mathbb{F}_q$ , the **regular elliptic** elements. Recall from the introduction that we have defined a matrix  $g \in \mathrm{GL}_n \mathbb{F}_q$  to be regular elliptic if and only if its characteristic polynomial is irreducible. Equivalently, the set of regular elliptic elements in  $\mathrm{GL}_n \mathbb{F}_q$  is  $\mathcal{T}_{(n)}(q) = \mathcal{T}_{(n)}^\square(q)$ . This is just one of several characterizations of regular elliptic elements that we will find useful.

**Proposition 2.4.10** ([24, Prop. 4.4]). *For all  $n \in \mathbb{N}$  and prime powers  $q$ , the following are equivalent for an element  $g \in \mathrm{GL}_n \mathbb{F}_q$ .*

(i) *The element  $g$  is regular elliptic.*

(ii) *For all  $x \in \mathrm{GL}_n \mathbb{F}_q$ ,  $xgx^{-1} \in \mathfrak{P}_\nu \implies \nu = (n)$ , where  $\mathfrak{P}_\nu$  is defined by (3.1.1) in Section 3.1 below.*

(iii) *The element  $g$  stabilizes no proper nontrivial subspaces of  $V$ .*

(iv) *The element  $g$  determines the isomorphism*

$$V_g \cong \mathbb{F}_q[z]/(h_1(z)), \quad (2.4.12)$$

where  $h_1 \in \mathcal{F}_n(q)$  is the characteristic polynomial of  $g$ .

Finally, we combine the results about regular semisimple and regular elliptic elements. The next result, which classifies the possible stable subspaces of a regular semisimple element, will be central in proving our main tool, Theorem 1.2.6.

**Corollary 2.4.11** (to Thm. 2.4.9 and Prop. 2.4.10). *Suppose  $n \in \mathbb{N}$ ,  $q$  is a prime power, and  $g \in \mathrm{GL}_n \mathbb{F}_q$  is a regular semisimple element which determines the isomorphism*

$$V_g \cong \mathbb{F}_q[z]/(h_1(z)) \oplus \cdots \oplus \mathbb{F}_q[z]/(h_\ell(z)) \quad (2.4.13)$$

as in (2.4.8), where  $h_1, \dots, h_\ell \in \mathcal{F}(q)$  are distinct and irreducible. Suppose  $g$  stabilizes a subspace  $U \subset V$ . Let  $\tilde{U} \subset \bigoplus_{i=1}^{\ell} \mathbb{F}_q[z]/(h_i(z))$  denote the submodule corresponding to  $U$  under the isomorphism (2.4.13). Then there exists a subset  $I \subset \{1, \dots, \ell\}$  such that  $\tilde{U} = \bigoplus_{i \in I} \mathbb{F}_q[z]/(h_i(z))$ .

*Proof.* By Theorem 2.4.9, it suffices to show that, for each  $i \in \{1, \dots, \ell\}$ ,  $g$  stabilizes no proper nontrivial subspace of  $\mathbb{F}_q[z]/(h_i(z))$ . Consider the restriction of  $g$  to  $\mathbb{F}_q[z]/(h_i(z))$ . Since each  $h_i$  is irreducible, the restriction of  $g$  to  $\mathbb{F}_q[z]/(h_i(z))$  is regular elliptic. By Proposition 2.4.10, we are done.  $\square$

## Chapter 3

# CHARACTERS OF THE FINITE GENERAL LINEAR GROUPS

In this chapter, we describe how to compute the values of all the irreducible characters of  $\mathrm{GL}_n \mathbb{F}_q$ . Just as with the symmetric groups, we will index the irreducible characters of  $\mathrm{GL}_n \mathbb{F}_q$  in the same way that we have indexed its conjugacy classes. The following is a condensed review of the topic, based on Green's work [16]. The notation and language we use vary from Green's original choices. For another exposition see Macdonald [25].

### 3.1 Computing the irreducible $\mathrm{GL}_n \mathbb{F}_q$ characters

We first introduce more notation. For each positive integer  $d$ , define the function  $\alpha_d : d\mathbb{Z} \rightarrow \mathbb{Z}$  by  $\alpha_d(m) = [m/d]_{q^d}$ . Given a polynomial  $f \in \mathcal{F}(q)$ , we will consider the function  $\ell_f \alpha_{\deg f}$ , which is obtained by scaling  $\alpha_{\deg f}$  by the integer  $\ell_f$ .

We require a process called **parabolic induction**, which we describe now. If  $\nu = (\nu_1, \dots, \nu_\ell) \vdash n$ , let  $\mathfrak{P}_\nu$  denote the **parabolic subgroup** of  $\mathrm{GL}_n \mathbb{F}_q$  consisting of block upper triangular matrices with block sizes  $\nu_1, \dots, \nu_\ell$ . Explicitly,

$$\mathfrak{P}_\nu = \left\{ \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1\ell} \\ 0 & A_{22} & \cdots & A_{2\ell} \\ 0 & 0 & \ddots & \vdots \\ 0 & 0 & 0 & A_{\ell\ell} \end{bmatrix} \in \mathrm{GL}_n \mathbb{F}_q : A_{ii} \in \mathrm{GL}_{\nu_i} \mathbb{F}_q \text{ for all } 1 \leq i \leq \ell \right\}. \quad (3.1.1)$$

For each  $i \in \{1, \dots, \ell\}$ , let  $\pi_i^\nu : \mathfrak{P}_\nu \rightarrow \mathrm{GL}_{\nu_i} \mathbb{F}_q$  denote projection onto the  $i^{\mathrm{th}}$  diagonal block:

$$A = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1\ell} \\ 0 & A_{22} & \cdots & A_{2\ell} \\ 0 & 0 & \ddots & \vdots \\ 0 & 0 & 0 & A_{\ell\ell} \end{bmatrix} \in \mathfrak{P}_\nu \implies \pi_i^\nu(A) = A_{ii}. \quad (3.1.2)$$

Given arbitrary characters  $\chi_i$  of  $\mathrm{GL}_{\nu_i} \mathbb{F}_q$  for each  $i \in \{1, \dots, \ell\}$ , we define their parabolic induction product  $\bigodot_{i=1}^\ell \chi_i$ , which is a character of  $\mathrm{GL}_{|\nu|} \mathbb{F}_q$ , by

$$\left( \bigodot_{i=1}^\ell \chi_i \right) (g) = \frac{1}{\#\mathfrak{P}_\nu} \sum_{\substack{x \in \mathrm{GL}_{|\nu|} \mathbb{F}_q \\ xgx^{-1} \in \mathfrak{P}_\nu}} \prod_{i=1}^{\ell(\nu)} \chi_i(\pi_i^\nu(xgx^{-1})). \quad (3.1.3)$$

We now define the irreducible characters of  $\mathrm{GL}_n \mathbb{F}_q$  in four steps. First, we define the Primary-support characters,  $P$ . Second, we define the paraBolic characters,  $B$ , in terms of the  $P$ 's. Third, we define the Irreducible characters,  $J$ , in terms of the  $B$ 's. Finally, we define the irreducible characters  $\chi^\lambda$  of  $\mathrm{GL}_n \mathbb{F}_q$  in terms of the  $J$ 's. We refer to this as the ‘PBJ’ method. The names **Primary-support**, **paraBolic**, and **Irreducible** were not used by Green.

For each  $b \in \mathbb{Z}$  and  $d \in \mathbb{N}$ , we define the Primary-support character,  $P_d^b$ , of  $\mathrm{GL}_d \mathbb{F}_q$  as follows. For any  $\mu \in \mathrm{Par} \setminus \{\emptyset\}$ , let  $\kappa(\mu, t) = \prod_{i=1}^{\ell(\mu)-1} (1 - t^i)$ , where  $\kappa(\mu, t) = 1$  if  $\ell(\mu) = 1$ . Then define

$$P_d^b(g) = \begin{cases} \kappa(\mu, q^{\deg h}) \sum_{i=1}^{\deg h} \theta(\varepsilon_{\deg h}^{\ell_h})^{q^{ib}} & \text{if } \lambda^g = h \mapsto \mu \text{ is primary,} \\ 0 & \text{otherwise.} \end{cases} \quad (3.1.4)$$

The fact that  $P_d^k$  vanishes away from primary conjugacy classes explains the name **Primary-support**. For each  $d \in \mathbb{Z}$ , each  $\nu \in \mathrm{Par} \setminus \{\emptyset\}$  such that  $d$  divides every part of  $\nu$ , and each function  $\alpha : d\mathbb{Z} \rightarrow \mathbb{Z}$ , we define the paraBolic character,  $B_\nu^\alpha$ , of  $\mathrm{GL}_{|\nu|} \mathbb{F}_q$  by

$$B_\nu^\alpha = \bigodot_{i=1}^{\ell(\nu)} P_{\nu_i}^{\alpha(\nu_i)}. \quad (3.1.5)$$

For each  $f \in \mathcal{F}(q)$  and  $\lambda \in \text{Par}$ , we define the Irreducible character,  $J_f^\lambda$ , of  $\text{GL}_{|\lambda| \cdot \deg f} \mathbb{F}_q$  by

$$J_f^\lambda = (-1)^{|\lambda| \cdot (\deg f - 1)} \cdot \sum_{\nu \vdash |\lambda|} \frac{1}{z_\nu} \cdot \chi_\nu^\lambda \cdot B_{(\deg f)\nu}^{\ell_f \alpha_{\deg f}}. \quad (3.1.6)$$

Finally, for each index  $\underline{\lambda} : \mathcal{F}(q) \rightarrow \text{Par}$  satisfying  $\|\underline{\lambda}\| = n$ , we define the irreducible character  $\chi^\lambda$  of  $\text{GL}_n \mathbb{F}_q$  by

$$\chi^\lambda = \bigodot_{f \in \text{supp } \underline{\lambda}} J_f^{\lambda(f)}. \quad (3.1.7)$$

**Theorem 3.1.1** (Green [16, Theorem 14]). *For all  $n \in \mathbb{N}$  and prime powers  $q$ , the set  $\{\chi^\lambda : \|\underline{\lambda}\| = n\}$  is the set of distinct, irreducible, complex characters of  $\text{GL}_n \mathbb{F}_q$ .*

Green also showed that  $\odot$  is commutative and associative, so it makes sense to use an arbitrary finite indexing set for the parabolic induction product. In fact, letting  $J_f^\emptyset$  denote the empty function, which is the identity element with respect to  $\odot$ , we can define

$$\chi^\lambda = \bigodot_{f \in \mathcal{F}(q)} J_f^{\lambda(f)}. \quad (3.1.8)$$

Note that we have indexed the irreducible characters in the same way that we indexed the conjugacy classes. Moreover, we also refer to an irreducible character as **primary** if its index is primary, and we use the usual  $f \mapsto \lambda$  notation for its index. Thus, **primary characters** are those of the form  $\chi^{f \mapsto \lambda}$  for some  $f \in \mathcal{F}(q)$  and  $\lambda \in \text{Par}$ .

**Example 3.1.2.** Using the notation from Example 2.4.3, we record in Table 3.1 the character table for  $\text{GL}_3 \mathbb{F}_2$ . Our choice of  $\varepsilon$  was made such that  $f_3(\varepsilon_3) = 0$ . The rows correspond to the characters, and the columns correspond to the conjugacy classes. In the row labels, we write, for instance,  $f_1 \mapsto (2, 1)$  instead of  $\chi^{f_1 \mapsto (2, 1)}$  for simplicity. Let  $\zeta_7 = e^{2\pi i/7}$ .

### 3.2 Degrees of the irreducible $\text{GL}_n \mathbb{F}_q$ characters

Green also gives an explicit formula for the degrees of the irreducible characters  $\chi^\lambda$ . For any  $m \in \mathbb{N}$  and prime power  $q$ , let  $\psi_m(q) = (q^m - 1) \cdots (q^2 - 1)(q - 1)$ . For any partition  $\lambda$ , let  $b(\lambda) = \sum_{i=1}^{\ell(\lambda)} (i - 1)\lambda_i$  and define

$$[\lambda : q] = q^{b(\lambda)} \frac{\prod_{1 \leq i < j \leq \ell(\lambda)} (q^{(\lambda_i - \lambda_j) - (i - j)} - 1)}{\prod_{i=1}^{\ell(\lambda)} \psi_{\lambda_i + \ell(\lambda) - i}(q)}. \quad (3.2.1)$$

Table 3.1: The character table of  $\mathrm{GL}_3 \mathbb{F}_2$ 

	$U_1$	$U_2$	$U_3$	$E$	$\tilde{E}$	$C_0$
$f_1 \mapsto (1, 1, 1)$	8	0	0	1	1	-1
$f_1 \mapsto (2, 1)$	6	2	0	-1	-1	0
$f_1 \mapsto (3)$	1	1	1	1	1	1
$f_3 \mapsto (1)$	3	-1	1	$\zeta_7 + \zeta_7^2 + \zeta_7^4$	$\zeta_7^3 + \zeta_7^5 + \zeta_7^6$	0
$\tilde{f}_3 \mapsto (1)$	3	-1	1	$\zeta_7^3 + \zeta_7^5 + \zeta_7^6$	$\zeta_7 + \zeta_7^2 + \zeta_7^4$	0
$\lambda_0$	7	-1	-1	0	0	1

**Theorem 3.2.1** (Green [16, Theorem 14]). *For all  $n \in \mathbb{N}$ , prime powers  $q$ , and  $\underline{\lambda} : \mathcal{F}(q) \rightarrow \text{Par}$  with  $\|\underline{\lambda}\| = n$ , the degree of the irreducible character  $\chi^\lambda$  of  $\mathrm{GL}_n \mathbb{F}_q$  is given by*

$$\deg \chi^\lambda = \psi_n(q) \prod_{f \in \mathcal{F}(q)} [\underline{\lambda}(f) : q^{\deg f}]. \quad (3.2.2)$$

**Example 3.2.2.** We use Theorem 3.2.1 to calculate  $\deg \chi^{f_1 \mapsto (2,1)}$ . By Theorem 3.2.1,

$$\deg \chi^{f_1 \mapsto (2,1)} = \psi_3(2) \cdot [(2, 1) : 2] = \psi_3(2) \cdot \frac{6}{\psi_3(2) \cdot \psi_1(2)} = 6,$$

which agrees with  $\chi^{f_1 \mapsto (2,1)}$  evaluated at  $U_1$  as recorded in Table 3.1.

The primary characters indexed by  $z - 1 \mapsto \lambda$  for  $\lambda \vdash n$  are called **unipotent**, and their degrees have an alternate, combinatorial description, which we mention briefly. Steinberg described the unipotent characters geometrically and computed their degrees explicitly [33, Eq. (2.9)]. Stanley then gave the following combinatorial formula for  $\deg \chi^{z-1 \mapsto \lambda}$ . We recall some usual notions to state the result. Given  $i \in \{1, \dots, \ell(\lambda)\}$  and  $j \in \{1, \dots, \lambda_i\}$ , define the **hook length** of  $(i, j) \in \lambda$  by

$$h_\lambda(i, j) = \lambda_i + \lambda'_j - (i + j) - 1. \quad (3.2.3)$$

Define the  **$q$ -hook formula** by

$$f^\lambda(q) = q^{b(\lambda)} \frac{[n]_q!}{\prod_{(i,j) \in \lambda} [h_\lambda(i, j)]_q}, \quad (3.2.4)$$

Furthermore, recall that, for a **standard Young tableau**  $T$  of shape  $\lambda$ , the **major index** of  $T$ , denoted  $\text{maj} T$ , is defined as the sum of all entries  $i$  in  $T$  for which  $i + 1$  appears in a lower row of  $T$  than  $i$ .

**Theorem 3.2.3** (Stanley [31, Cor. 7.21.5]). *For all  $n \in \mathbb{N}$ ,  $\lambda \vdash n$ , and prime powers  $q$ , we have*

$$\deg \chi^{z^{-1} \mapsto \lambda} = f^\lambda(q) = \sum_T q^{\text{maj} T},$$

where the sum is over all standard Young tableaux of shape  $\lambda$ .

### 3.3 Certain character values

Regular semisimple elements have many nice properties. The following theorem, which follows from Steinberg's work, describes one such property.

**Theorem 3.3.1** (Steinberg [33]). *For all  $n \in \mathbb{N}$ , prime powers  $q$ , partitions  $\lambda, \mu \vdash n$ , and  $g \in \mathcal{T}_\mu^\square(q)$ , we have  $\chi^{z^{-1} \mapsto \lambda}(g) = \chi_\mu^\lambda$ .*

Regular elliptic elements, in particular, have nice character-theoretic properties as well. The following result echoes Corollary 2.2.1.

**Corollary 3.3.2** (to Cor. 2.2.1, Prop. 2.4.10, Thm. 3.1.1, and Thm. 3.2.1). *Suppose  $n \in \mathbb{N}$ ,  $q$  is a prime power,  $\underline{\lambda} : \mathcal{F}(q) \rightarrow \text{Par}$  with  $\|\underline{\lambda}\| = n$ , and  $g \in \mathcal{T}_{(n)}(q)$ . If  $\chi^{\underline{\lambda}}(g) \neq 0$ , then there exist  $d|n$ ,  $f \in \mathcal{F}_d(q)$ , and  $r \in \{0, \dots, n/d - 1\}$  such that  $\underline{\lambda} = f \mapsto (n/d - r, 1^r)$  is primary. Moreover,*

$$\deg \chi^{f \mapsto (n/d - r, 1^r)} = \deg_{n,d,r}(q), \tag{3.3.1}$$

as defined in Table 1.1.

It follows that, when using the Frobenius formula to enumerate factorizations involving regular elliptic elements, one only needs to consider characters of the form  $\chi^{f \mapsto (n/d - r, 1^r)}$ . Therefore, when  $n$  is understood from context, and for any  $d|n$ ,  $f \in \mathcal{F}_d(q)$ , and  $r \in \{0, \dots, n/d - 1\}$ , we define

$$\chi^{f,r} = \chi^{f \mapsto (n/d - r, 1^r)}. \tag{3.3.2}$$

We can now write down a further simplified version of (2.1.2).

**Corollary 3.3.3** (to Cor. 2.1.2 and Cor. 3.3.2). *For all  $n, k \in \mathbb{N}$ ,  $\mu \vdash n$ , and prime powers  $q$ , we have*

$$g_{k,\mu}(q) = \frac{1}{\gamma_n(q)} \sum_{d,f,r} \deg_{n,d,r}(q)^{1-k} \left( \sum_{g \in \mathcal{T}_n(q)} \chi^{f,r}(g) \right)^k \left( \sum_{h \in \mathcal{T}_\mu(q)} \chi^{f,r}(h) \right), \quad (3.3.3)$$

where the sum is over all  $d$  dividing  $n$ ,  $f \in \mathcal{F}_d(q)$ , and  $r \in \{0, \dots, n/d - 1\}$ . Moreover, the same is true when both  $g_{k,\mu}(q)$  is replaced with  $g_{k,\mu}^\square(q)$  and  $\mathcal{T}_\mu(q)$  is replaced with  $\mathcal{T}_\mu^\square(q)$ .

## Chapter 4

## ENUMERATIVE RESULTS

## 4.1 Main tool

We begin with our main tool, Theorem 1.2.6, a result that allows us to evaluate primary characters on regular semisimple elements more easily. We present some lemmas before giving the proof. In the preliminary lemmas and in Theorem 1.2.6, the hypotheses include “ $\mu \vdash n$  and  $g \in \mathcal{T}_\mu^\square(q)$ .” In all the proofs, we will assume  $g$  is in rational canonical form and denote the distinct irreducible factors of the characteristic polynomial of  $g$  by  $h_1, \dots, h_{\ell(\mu)}$  with  $\deg h_i = \mu_i$  for each  $i \in \{1, \dots, \ell(\mu)\}$ . Note that this implies each  $\pi_i^\mu(g) \in \mathrm{GL}_{\mu_i}(q)$  is in the primary conjugacy class indexed by  $h_i \mapsto \square$ .

**Lemma 4.1.1.** *For all  $n \in \mathbb{N}$ ,  $d|n$ ,  $\nu \vdash n/d$ ,  $\mu \vdash n$ , prime powers  $q$ ,  $g \in \mathcal{T}_\mu^\square(q)$ , and  $\alpha : d\mathbb{Z} \rightarrow \mathbb{Z}$ , we have  $B_{d\nu}^\alpha(g) = 0$  unless  $d\nu = \mu$ .*

*Proof.* By definitions (3.1.3) and (3.1.5),

$$B_{d\nu}^\alpha(g) = \frac{1}{\#\mathfrak{P}_{d\nu}} \sum_{\substack{x \in \mathrm{GL}_n \mathbb{F}_q \\ xgx^{-1} \in \mathfrak{P}_{d\nu}}} \prod_{i=1}^{\ell(\nu)} P_{d\nu_i}^{\alpha(d\nu_i)}(\pi_i^{d\nu}(xgx^{-1})). \quad (4.1.1)$$

Consider a single summand in (4.1.1), which is a product of Primary-support character values. By definition (3.1.4), the Primary-support characters vanish away from primary conjugacy classes. Thus, the product of them vanishes if any diagonal block of  $xgx^{-1}$  is not primary. So assume the product of the  $P$  characters in (4.1.1) does not vanish, and hence each block  $\pi_i^{d\nu}(xgx^{-1})$  is primary.

For each  $i \in \{1, \dots, \ell(\nu)\}$ , let  $\tilde{h}_i$  be the characteristic polynomial of  $\pi_i^{d\nu}(xgx^{-1})$ . Since  $xgx^{-1} \in \mathfrak{P}_{d\nu}$  has a block-upper-triangular structure, its characteristic polynomial equals

$\prod_{i=1}^{\ell(\nu)} \tilde{h}_i$ . The fact that each  $\pi_i^{d\nu}(xgx^{-1})$  is primary implies that each  $\tilde{h}_i$  is a power  $\rho_i^{a_i}$  of an irreducible polynomial  $\rho_i \in \mathcal{F}(q)$ . On the other hand,  $g$  is regular semisimple, meaning its characteristic polynomial has no repeated factors. Thus, each  $a_i = 1$  and there exists a permutation  $\sigma \in \mathfrak{S}_{\ell(\mu)}$  such that  $\rho_i = \tilde{h}_i = h_{\sigma(i)}$  for all  $i \in \{1, \dots, \ell(\mu)\}$ . Computing degrees show that  $d\nu_i = \deg \tilde{h}_i = \deg h_{\sigma(i)} = \mu_{\sigma(i)}$  for all  $i \in \{1, \dots, \ell(\mu)\}$ . This implies  $d\nu = \mu$ .  $\square$

We require some more terminology before moving forward. Recall from Section 2.4.1 that we have defined  $V = \mathbb{F}_q^n$ . Given  $\mu \vdash n$ , refer to a flag  $S_\bullet$  of nested subspaces

$$S_1 \subset S_2 \subset \dots \subset S_{\ell(\mu)}$$

of  $V$  as a  $\mu$ -**flag** if

$$\dim S_j = \sum_{i=1}^j \mu_i$$

for all  $j \in \{1, \dots, \ell(\mu)\}$ . Refer to an ordered basis  $(v_1, \dots, v_n)$  of  $V$  as a **basis for  $S_\bullet$**  if

$$\left( v_1, \dots, v_{\sum_{i=1}^j \mu_i} \right)$$

is a basis for  $S_j$  for each  $j \in \{1, \dots, \ell(\mu)\}$ . Conversely, each ordered basis  $(v_1, \dots, v_n)$  for  $V$  **determines a  $\mu$ -flag** by taking the  $j^{\text{th}}$  subspace in the flag to be the span of  $\left( v_1, \dots, v_{\sum_{i=1}^j \mu_i} \right)$  for each  $j \in \{1, \dots, \ell(\mu)\}$ . Given a  $\mu$ -flag  $S_\bullet$ , say that a matrix in  $\text{GL}_n \mathbb{F}_q$  **stabilizes  $S_\bullet$**  if it stabilizes  $S_j$  for each  $j \in \{1, \dots, \ell(\mu)\}$ .

**Lemma 4.1.2.** *For all  $n \in \mathbb{N}$ ,  $\mu \vdash n$ , prime powers  $q$ , and  $g \in \mathcal{T}_\mu^\square(q)$ , we have*

$$\#\{x \in \text{GL}_n \mathbb{F}_q : xgx^{-1} \in \mathfrak{P}_\mu\} = \#\mathfrak{P}_\mu \cdot \prod_{i \geq 1} m_i(\mu)!. \quad (4.1.2)$$

*Proof.* Viewing  $g$  abstractly as a linear transformation on  $V$ , the left side of (4.1.2) is the number of ordered bases of  $V$  with respect to which the matrix representing  $g$  is an element of  $\mathfrak{P}_\mu$ . For any fixed basis  $\mathcal{B} = (v_1, \dots, v_n)$  for  $V$ , being an element of  $\mathfrak{P}_\mu$  is equivalent to stabilizing the  $\mu$ -flag determined by  $\mathcal{B}$ . Therefore, the left side of (4.1.2) is the product of

- (1) the number of  $\mu$ -flags that  $g$  stabilizes and

(2) the number of ordered bases for a given  $\mu$ -flag.

The proof will be complete once we compute these two quantities.

The number of ordered bases for a given  $\mu$ -flag is simply  $\#\mathfrak{B}_\mu$ . To see this, fix a basis for  $V$  which is also a basis for a fixed  $\mu$ -flag,  $S_\bullet$ . Observe that the columns of a matrix form a basis for  $S_\bullet$  if and only if the matrix is in  $\mathfrak{B}_\mu$ .

The number of  $\mu$ -flags that  $g$  stabilizes is slightly harder to compute. Consider a  $\mu$ -flag

$$S_\bullet = S_1 \subset S_2 \subset \cdots \subset S_{\ell(\mu)}$$

that  $g$  stabilizes. We must count how many choices there are for  $S_\bullet$ . For each  $i \in \{1, \dots, \ell(\mu)\}$ , let  $Q_i$  denote the quotient  $S_i/S_{i-1}$ , with the convention that  $S_0$  is zero-dimensional. Note that  $\dim Q_i = \mu_i$ . Under the isomorphism (2.4.8), let  $E_i \subset V$  denote the subspace corresponding to  $\mathbb{F}_q[z]/(h_i(z))$  for each  $i \in \{1, \dots, \ell(\mu)\}$ . By Corollary 2.4.11, the only subspaces of  $V$  that  $g$  stabilizes are direct sums of the  $E_i$ 's. Therefore, each  $S_j$  is a direct sum of the  $E_i$ 's. This implies each  $Q_i$  is also a direct sum of the  $E_i$ 's. Working backwards from  $Q_{\ell(\mu)}$  to  $Q_1$ , we see that  $Q_{\ell(\mu)-m_1(\mu)+1}, \dots, Q_{\ell(\mu)}$  are all 1-dimensional and thus form a permutation of  $E_{\ell(\mu)-m_1(\mu)+1}, \dots, E_{\ell(\mu)}$ . There are therefore  $m_1(\mu)!$  ways to choose the final  $m_1(\mu)$  quotients. Likewise,

$$Q_{\ell(\mu)-m_1(\mu)-m_2(\mu)+1}, \dots, Q_{\ell(\mu)-m_1(\mu)}$$

are all 2-dimensional and thus form a permutation of

$$E_{\ell(\mu)-m_1(\mu)-m_2(\mu)+1}, \dots, E_{\ell(\mu)-m_1(\mu)},$$

as there are no 1-dimensional  $E_i$ 's remaining, giving  $m_2(\mu)!$  choices for those quotients. Continuing, we see that there are  $\prod_{i \geq 1} m_i(\mu)!$  choices for  $Q_1, \dots, Q_{\ell(\mu)}$ . Observing that the quotients determine  $S_\bullet$  uniquely, the result follows.  $\square$

We are now ready to prove Theorem 1.2.6. Recall that given  $d|n$ ,  $f \in \mathcal{F}_d(q)$ , and  $\lambda \vdash n/d$ , it provides a simple formula for  $\chi^{f \mapsto \lambda}(g)$ . Specifically, Theorem 1.2.6 states that, if some

part of  $\mu$  is not divisible by  $d$ , then  $\chi^{f \mapsto \lambda}(g) = 0$ , and otherwise, there exists  $\tilde{\mu} \vdash n/d$  such that  $\mu = d\tilde{\mu}$ , and we have

$$\chi^{f \mapsto \lambda}(g) = (-1)^{\frac{n}{d}(d-1)} \chi_{\tilde{\mu}}^{\lambda} \prod_{i=1}^{\ell(\mu)} \frac{1}{\tilde{\mu}_i} \sum_{\substack{\beta_i \in \mathbb{F}_q^{\mu_i} \\ h_i(\beta_i)=0}} \theta(\beta_i)^{\ell_f[\tilde{\mu}_i]_q^d}. \quad (4.1.3)$$

*Proof of Theorem 1.2.6.* By definitions (3.1.6) and (3.1.7), we have

$$\chi^{f \mapsto \lambda}(g) = J_f^{\lambda}(g) = (-1)^{\frac{n}{d}(d-1)} \cdot \sum_{\nu \vdash \frac{n}{d}} \frac{\chi_{\nu}^{\lambda}}{z_{\nu}} B_{d\nu}^{\ell_f \alpha_d}(g) \quad (4.1.4)$$

By Lemma 4.1.1,  $B_{d\nu}^{\ell_f \alpha_d}(g) = 0$  unless  $d\nu = \mu$ . If some part of  $\mu$  is not divisible by  $d$ , then  $\chi^{f \mapsto \lambda}(g) = 0$ , proving the first statement in the lemma. Otherwise, there exists a unique partition  $\tilde{\mu} \vdash n/d$  such that  $\mu = d\tilde{\mu}$ , and only the summand corresponding to  $\tilde{\mu}$  in (4.1.4) does not vanish. Therefore, (4.1.4) reduces to

$$\chi^{f \mapsto \lambda}(g) = (-1)^{\frac{n}{d}(d-1)} \frac{\chi_{\tilde{\mu}}^{\lambda}}{z_{\tilde{\mu}}} B_{\tilde{\mu}}^{\ell_f \alpha_d}(g). \quad (4.1.5)$$

By definitions (3.1.3) and (3.1.5), we can rewrite (4.1.5) as

$$\chi^{f \mapsto \lambda}(g) = (-1)^{\frac{n}{d}(d-1)} \cdot \frac{\chi_{\tilde{\mu}}^{\lambda}}{z_{\tilde{\mu}}} \cdot \frac{1}{\#\mathfrak{P}_{\tilde{\mu}}} \sum_{\substack{x \in \mathrm{GL}_n \mathbb{F}_q \\ xgx^{-1} \in \mathfrak{P}_{\tilde{\mu}}}} \prod_{i=1}^{\ell(\mu)} P_{\mu_i}^{\ell_f \alpha_d(\mu_i)}(\pi_i^{\mu}(xgx^{-1})). \quad (4.1.6)$$

Consider the summation in (4.1.6). It can be rewritten as

$$\sum_{\substack{x \in \mathrm{GL}_n \mathbb{F}_q \\ xgx^{-1} \in \mathfrak{P}_{\tilde{\mu}}}} \prod_{s \geq 1} \prod_{\{j \in \mathbb{N} : \mu_j = s\}} P_s^{\ell_f \alpha_d(s)}(\pi_j^{\mu}(xgx^{-1})). \quad (4.1.7)$$

For each  $x$  such that  $xgx^{-1} \in \mathfrak{P}_{\tilde{\mu}}$ , consider the corresponding summand in (4.1.7). We repeat a similar argument to the one presented toward the end of the proof of Lemma 4.1.2. Observe that the characteristic polynomials of  $\{\pi_j^{\mu}(xgx^{-1}) : j \in \mathbb{N}, \mu_j = 1\}$  have degree 1 and hence are a permutation of  $\{h_j : j \in \mathbb{N}, \mu_j = 1\}$ . Likewise, the characteristic polynomials of  $\{\pi_j^{\mu}(xgx^{-1}) : j \in \mathbb{N}, \mu_j = 2\}$  have degree 2 and hence are a permutation of  $\{h_j : j \in \mathbb{N}, \mu_j = 2\}$ , as there are no degree-1 factors remaining. Continuing, we see that, for each  $s \in \mathbb{N}$ ,

the degree- $s$  characteristic polynomials of the diagonal blocks of  $xgx^{-1}$  are a permutation of the degree- $s$  irreducible factors of the characteristic polynomial of  $g$ . Moreover, the value of each  $P_s^{\ell_f \alpha_d(s)}$  in (4.1.7) depends only on the characteristic polynomial of the argument. This implies that the product of the Primary-support characters in (4.1.7) is constant over the sum. Therefore,

$$\chi^{f \mapsto \lambda}(g) = (-1)^{\frac{n}{d}(d-1)} \cdot \frac{\chi_{\tilde{\mu}}^\lambda}{z_{\tilde{\mu}}} \cdot \frac{\#\{x \in \mathrm{GL}_n \mathbb{F}_q : xyx^{-1} \in \mathfrak{P}_\mu\}}{\#\mathfrak{P}_\mu} \cdot \prod_{i=1}^{\ell(\mu)} P_{\mu_i}^{\ell_f \alpha_d(\mu_i)}(\pi_i^\mu(g)). \quad (4.1.8)$$

By Lemma 4.1.2, (4.1.8) reduces to

$$\chi^{f \mapsto \lambda}(g) = (-1)^{\frac{n}{d}(d-1)} \cdot \chi_{\tilde{\mu}}^\lambda \cdot \prod_{i=1}^{\ell(\mu)} \frac{1}{\tilde{\mu}_i} P_{\mu_i}^{\ell_f \alpha_d(\mu_i)}(\pi_i^\mu(g)). \quad (4.1.9)$$

Consider the Primary-support character evaluations in (4.1.9). By (2.3.3) and definition (3.1.4),

$$P_{\mu_i}^{\ell_f \alpha_d(\mu_i)}(\pi_i^\mu(g)) = \kappa(\square, q^{\deg h_i}) \sum_{j=1}^{\deg h_i} \theta(\varepsilon_{\deg h_i}^{\ell_{h_i}})^{q^j \ell_f \alpha_d(\mu_i)} \quad (4.1.10)$$

$$= \sum_{j=1}^{\mu_i} \theta(\varepsilon_{\mu_i}^{\ell_{h_i}})^{q^j \ell_f [\tilde{\mu}_i]_{q^d}} = \sum_{\substack{\beta_i \in \mathbb{F}_{q^{\mu_i}} \\ h_i(\beta_i)=0}} \theta(\beta_i)^{\ell_f [\tilde{\mu}_i]_{q^d}}. \quad (4.1.11)$$

Substituting (4.1.11) into (4.1.9) gives the result.  $\square$

**Example 4.1.3.** Returning to Example 3.1.2, we compute  $\chi^{f_3 \mapsto (1)}(c)$  for  $c \in E$ . In the notation of Theorem 1.2.6, we have  $d = 3, f = f_3, \lambda = (1), \mu = (3), \tilde{\mu} = (1), h_1 = f_3$ , and  $\ell_f = 1$ . The roots of  $h_1$  are  $\varepsilon_3, \varepsilon_3^2$ , and  $\varepsilon_3^4$ . By Theorem 1.2.6,

$$\begin{aligned} \chi^{f_3 \mapsto (1)}(c) &= (-1)^{\frac{3}{3}(3-1)} \cdot \chi_{(1)}^{(1)} \cdot \sum_{h_1(\beta)=0} \theta(\beta) \\ &= \theta(\varepsilon_3) + \theta(\varepsilon_3^2) + \theta(\varepsilon_3^4) = \zeta_7 + \zeta_7^2 + \zeta_7^4. \end{aligned}$$

We see this exact value in Table 3.1 above.

## 4.2 Proof of first enumerative result

We can now apply Theorem 1.2.6 to prove our enumerative results. We begin with Theorem 1.2.1, which addresses the family of cases  $\mu = (\mu_1, \dots, \mu_\ell) \vdash n > 2$ , where  $\ell > 1$  and  $\mu_{\ell-1} > \mu_\ell = 1$ . Recall that Theorem 1.2.1 states that, under these assumptions on  $\mu$  and  $n$ ,

$$g_{k,\mu}^\square(q) = \frac{\#\mathcal{T}_{(n)}(q)^k \cdot \#\mathcal{T}_\mu^\square(q)}{\#\mathrm{GL}_n \mathbb{F}_q} \cdot \sum_{r=0}^{n-1} \frac{(-1)^{rk} \chi_\mu^{(n-r, 1^r)}}{\left( q^{\binom{r+1}{2}} \cdot \left[ \begin{smallmatrix} n-1 \\ r \end{smallmatrix} \right]_q \right)^{k-1}} \quad (4.2.1)$$

for all  $k \in \mathbb{N}$  and prime powers  $q$ .

Note that if all the parts of  $\mu$  are distinct, i.e.  $\mu_1 > \dots > \mu_\ell$ , then  $\mathcal{T}_\mu^\square(q) = \mathcal{T}_\mu(q)$ , and consequently  $g_{k,\mu}(q) = g_{k,\mu}^\square(q)$ . However, even in the event that some of the parts of  $\mu$  agree, we are still able to find an explicit formula for  $g_{k,\mu}^\square(q)$ , although  $\mathcal{T}_\mu^\square(q)$  might be empty if  $q$  is small.

In the rest of this section and later, we will require some additional notation. We will consider the logical propositions “ $q-1|\ell_f$ ” for various  $f \in \mathcal{F}_1(q)$ . Even though  $\ell_f$  denotes an arbitrary choice, these propositions are well-defined for the following reason. Suppose for the chosen  $\ell_f$ , we have  $q-1|\ell_f$ . Now, suppose  $\ell'_f$  is another choice of  $\ell_f$ . Then there exist  $i, j \in \mathbb{Z}$  such that

$$\ell'_f = q^i \ell_f + j(q-1), \quad (4.2.2)$$

which is divisible by  $q-1$  by the assumption that  $q-1|\ell_f$ .

*Proof of Theorem 1.2.1.* By Corollary 3.3.3, we have

$$g_{k,\mu}^\square(q) = \frac{1}{\gamma_n(q)} \sum_{d|n} \sum_{r=0}^{\frac{n}{d}-1} \deg_{n,d,r}(q)^{1-k} \sum_{f \in \mathcal{F}_d(q)} \left( \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right)^k \left( \sum_{h \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(h) \right).$$

Applying Theorem 1.2.6, we see that  $\chi^{f,r}$  vanishes on  $\mathcal{T}_\mu^\square(q)$  unless  $d=1$ . Therefore,

$$g_{k,\mu}^\square(q) = \frac{1}{\gamma_n(q)} \sum_{r=0}^{n-1} \deg_{n,1,r}(q)^{1-k} \sum_{f \in \mathcal{F}_1(q)} \left( \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right)^k \left( \sum_{h \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(h) \right). \quad (4.2.3)$$

We proceed to show that only the  $f(z) = z - 1$  term does not vanish in the sum over  $f \in \mathcal{F}_1(q)$ . Consider an individual polynomial  $f \in \mathcal{F}_1(q)$ . Recall from Section 2.4.1 that the conjugacy classes in  $\mathcal{T}_\mu^\square(q)$  have equal sizes and each conjugacy class is uniquely determined by a set  $\{h_1, \dots, h_\ell\}$  of distinct polynomials such that  $h_i \in \mathcal{F}_{\mu_i}(q)$  for each  $i \in \{1, \dots, \ell\}$ . Thus, by Theorem 1.2.6,  $\sum_{h \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(h)$  is a multiple of

$$\sum_{\substack{\{h_1, \dots, h_\ell\} \\ h_i \in \mathcal{F}_{\mu_i}(q)}} \prod_{i=1}^{\ell} \sum_{\substack{\beta_i \in \mathbb{F}_q^{\mu_i} \\ h_i(\beta_i)=0}} \theta(\beta_i)^{\ell_f [\mu_i]_q}. \quad (4.2.4)$$

Since  $\mu_\ell$  is the only part of  $\mu$  equal to 1, we have that (4.2.4) factors as

$$\left( \sum_{\substack{\{h_1, \dots, h_{\ell-1}\} \\ h_i \in \mathcal{F}_{\mu_i}(q)}} \prod_{i=1}^{\ell-1} \sum_{\substack{\beta_i \in \mathbb{F}_q^{\mu_i} \\ h_i(\beta_i)=0}} \theta(\beta_i)^{\ell_f [\mu_i]_q} \right) \cdot \left( \sum_{h_\ell \in \mathcal{F}_1(q)} \sum_{\substack{\beta_\ell \in \mathbb{F}_q \\ h_\ell(\beta_\ell)=0}} \theta(\beta_\ell)^{\ell_f} \right). \quad (4.2.5)$$

The latter factor in (4.2.5) is

$$\sum_{h_\ell \in \mathcal{F}_1(q)} \sum_{\substack{\beta_\ell \in \mathbb{F}_q \\ h_\ell(\beta_\ell)=0}} \theta(\beta_\ell)^{\ell_f} = \begin{cases} 0, & q-1 \nmid \ell_f, \\ q-1, & q-1 \mid \ell_f, \end{cases}$$

because, by Corollary 2.3.3,  $\theta(\beta_\ell)$  ranges over all  $(q-1)^{\text{th}}$  roots of unity. Since  $\deg f = d = 1$ , we can take  $\ell_f \in \{1, \dots, q-1\}$ . Thus, the only non-zero contribution to the sum over  $f \in \mathcal{F}_1(q)$  in (4.2.3) comes from the term corresponding to  $\ell_f = q-1$  and hence  $f(z) = z - 1$ .

Eliminating the vanishing terms not corresponding to  $f(z) = z - 1$  in (4.2.3) gives

$$g_{k,\mu}^\square(q) = \frac{1}{\gamma_n(q)} \sum_{r=0}^{n-1} \deg_{n,1,r}(q)^{1-k} \left( \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{z-1,r}(g) \right)^k \left( \sum_{h \in \mathcal{T}_\mu^\square(q)} \chi^{z-1,r}(h) \right).$$

By Corollary 2.2.1 and Theorem 3.3.1,

$$\begin{aligned} g \in \mathcal{T}_{(n)}(q) &\implies \chi^{z-1,r}(g) = (-1)^r, & \text{and} \\ h \in \mathcal{T}_\mu^\square(q) &\implies \chi^{z-1,r}(h) = \chi_\mu^{(n-r,1^r)}. \end{aligned}$$

Since both character values only depend on  $r$ , we have

$$g_{k,\mu}^{\square}(q) = \frac{1}{\gamma_n(q)} \sum_{r=0}^{n-1} \deg_{n,1,r}(q)^{1-k} (\#\mathcal{T}_{(n)}(q)(-1)^r)^k (\#\mathcal{T}_{\mu}^{\square}(q)\chi_{\mu}^{(n-r,1^r)}),$$

which simplifies to the result, using the notation from Table 1.1.  $\square$

Next is the case of  $\mu = (n-1, 1)$ , which is addressed by Corollary 1.2.2. In this case,  $g_{k,(n-1,1)}(q)$  equals the number of  $k$ -tuples of regular elliptic elements whose product has exactly one eigenvalue in  $\mathbb{F}_q$  and acts as a regular elliptic element on an  $(n-1)$ -dimensional subspace of  $V$ . Recall that Corollary 1.2.2 states that

$$g_{k,(n-1,1)}(q) = \frac{\#\mathcal{T}_{(n)}(q)^k \cdot \#\mathcal{T}_{(n-1,1)}(q)}{\#\mathrm{GL}_n \mathbb{F}_q} \cdot \left( 1 + \frac{(-1)^{nk-n-k}}{q^{\binom{n}{2}(k-1)}} \right) \quad (4.2.6)$$

for all  $n > 2$ ,  $k \in \mathbb{N}$ , and prime powers  $q$ .

*Proof of Corollary 1.2.2.* Apply Corollary 2.2.1 to Theorem 1.2.1, observing that  $\chi_{(n-1,1)}^{(n-r,1^r)}$  is only nonzero when  $r \in \{0, n-1\}$ .  $\square$

### 4.3 Proof of second enumerative result

Our second enumerative result, Theorem 1.2.3, addresses the case  $\mu = (n)$ . In this case, the quantity  $g_{k,(n)}(q)$  equals the number of  $k$ -tuples of regular elliptic elements whose product is also regular elliptic. Recall the notation and definitions from Table 1.1, and recall that Theorem 1.2.3 states that

$$g_{k,(n)}(q) = P_{n,k+1}(q) \sum_{d|n} (-1)^{n(k+1)/d} d^k D_{n,k+1,d}(q) \sum_{c|d} \mu(d/c) C_{n,k+1,c}(q) \quad (4.3.1)$$

for all  $n, k \in \mathbb{N}$  and prime powers  $q$ .

*Proof of Theorem 1.2.3.* By Corollary 3.3.3 and the fact that  $\mu = (n)$ , we have

$$g_{k,\mu}(q) = \frac{1}{\gamma_n(q)} \sum_{d|n} \sum_{r=0}^{\frac{n}{d}-1} \deg_{n,d,r}(q)^{1-k} \sum_{f \in \mathcal{F}_d(q)} \left( \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right)^{k+1}. \quad (4.3.2)$$

By Theorem 2.4.2, the size of each conjugacy class comprising  $\mathcal{T}_{(n)}(q)$  is  $\gamma_n(q)/(q^n - 1)$ . Since characters are constant on conjugacy classes, we have

$$\sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) = \frac{\gamma_n(q)}{q^n - 1} \sum_{p \in \mathcal{F}_n(q)} \chi^{f,r}(g_p), \quad (4.3.3)$$

where  $g_p$  denotes an arbitrary regular elliptic element with characteristic polynomial  $p$ . Substituting (4.3.3) into (4.3.2), we have

$$g_{k,\mu}(q) = \frac{1}{\gamma_n(q)} \left( \frac{\gamma_n(q)}{q^n - 1} \right)^{k+1} \sum_{d|n} \sum_{r=0}^{\frac{n}{d}-1} \deg_{n,d,r}(q)^{1-k} \sum_{f \in \mathcal{F}_d(q)} \left( \sum_{p \in \mathcal{F}_n(q)} \chi^{f,r}(g_p) \right)^{k+1}. \quad (4.3.4)$$

Observe that  $\mathcal{T}_{(n)}(q) = \mathcal{T}_{(n)}^\square(q)$ , so we can evaluate primary characters on  $\mathcal{T}_{(n)}(q)$  using Theorem 1.2.6. Applying Theorem 1.2.6 and Corollary 2.2.1 to (4.3.4) gives

$$g_{k,\mu}(q) = \frac{1}{\gamma_n(q)} \left( \frac{(-1)^n \gamma_n(q)}{n(q^n - 1)} \right)^{k+1} \sum_{d|n} ((-1)^{n/d} d)^{k+1} \sum_{r=0}^{\frac{n}{d}-1} (-1)^{r(k+1)} \deg_{n,d,r}(q)^{1-k} \\ \times \sum_{f \in \mathcal{F}_d(q)} \left( \sum_{p \in \mathcal{F}_n(q)} \sum_{\substack{\alpha \in \mathbb{F}_{q^n}^\times \\ p(\alpha)=0}} \theta(\alpha)^{\ell_f[n/d]_{q^d}} \right)^{k+1}.$$

Using the notation established in Table 1.1, this is equivalent to

$$\frac{g_{k,\mu}(q)}{P_{n,k+1}(q)} = \sum_{d|n} ((-1)^{n/d} d)^{k+1} D_{n,k+1,d}(q) \sum_{f \in \mathcal{F}_d(q)} \left( \sum_{p \in \mathcal{F}_n(q)} \sum_{\substack{\alpha \in \mathbb{F}_{q^n}^\times \\ p(\alpha)=0}} \theta(\alpha)^{\ell_f[n/d]_{q^d}} \right)^{k+1}. \quad (4.3.5)$$

Theorem 1.2.3 now follows from Corollary 4.3.1 below, which we phrase in terms of  $k$  rather than  $k + 1$  for the sake of simplifying the expressions.  $\square$

**Corollary 4.3.1** (to Lem. 4.3.2 and Lem. 4.3.3). *For all  $n, k \in \mathbb{N}$ ,  $d|n$ , and prime powers  $q$ ,*

$$\sum_{f \in \mathcal{F}_d(q)} \left( \sum_{p \in \mathcal{F}_n(q)} \sum_{\substack{\alpha \in \mathbb{F}_{q^n}^\times \\ p(\alpha)=0}} \theta(\alpha)^{\ell_f[n/d]_{q^d}} \right)^k = \frac{1}{d} \sum_{c|d} \boldsymbol{\mu}(d/c) C_{n,k,c}(q).$$

Before proving Corollary 4.3.1, we prove two lemmas. Given a logical proposition  $\mathcal{P}$ , let  $\delta_{\mathcal{P}}$  equal 1 if  $\mathcal{P}$  is true and 0 if  $\mathcal{P}$  is false. We will make logical propositions of the form “ $b|\ell_f[n/d]_{q^d}$ ” or equivalently “ $b$  divides  $\ell_f[n/d]_{q^d}$ ”, where  $d|n$ ,  $f \in \mathcal{F}_d(q)$ , and  $b$  is a number that divides  $q^n - 1$ . Such statements are well-defined for the following reason. First,  $b$  dividing an element of  $\mathbb{Z}/(q^n - 1)$  is well-defined simply because  $b$  itself divides  $q^n - 1$ . Second, suppose for the chosen  $\ell_f$ , we have  $b|\ell_f[n/d]_{q^d}$ , where  $d|n$  and  $b|q^n - 1$ . Now, suppose  $\ell'_f$  is another choice of  $\ell_f$ . Then there exist  $i, j \in \mathbb{Z}$  such that

$$\ell'_f = q^i \ell_f + j(q^d - 1). \quad (4.3.6)$$

Observe that  $(q^d - 1)[n/d]_{q^d} = q^n - 1$ . Multiplying both sides of (4.3.6) by  $[n/d]_{q^d}$ , we have

$$\ell'_f[n/d]_{q^d} = q^i \ell_f[n/d]_{q^d} + j(q^n - 1), \quad (4.3.7)$$

which is divisible by  $b$  by the assumption that  $b$  divides both  $\ell_f[n/d]_{q^d}$  and  $q^n - 1$ .

**Lemma 4.3.2.** *For all  $n \in \mathbb{N}$ ,  $d|n$ , prime powers  $q$ , and  $f \in \mathcal{F}_d(q)$ ,*

$$\sum_{p \in \mathcal{F}_n(q)} \sum_{\substack{\alpha \in \mathbb{F}_{q^n}^\times \\ p(\alpha)=0}} \theta(\alpha)^{\ell_f[n/d]_{q^d}} = \sum_{s|n} \boldsymbol{\mu}(n/s)(q^s - 1)\delta_{q^s-1|\ell_f[n/d]_{q^d}}. \quad (4.3.8)$$

*Proof.* By Möbius inversion, it suffices to prove

$$\sum_{s|n} \sum_{p \in \mathcal{F}_s(q)} \sum_{\substack{\alpha \in \mathbb{F}_{q^s}^\times \\ p(\alpha)=0}} \theta(\alpha)^{\ell_f[n/d]_{q^d}} = (q^n - 1)\delta_{q^n-1|\ell_f[n/d]_{q^d}}. \quad (4.3.9)$$

Corollary 2.3.2 implies that, on the left side of (4.3.9),  $\theta(\alpha)$  ranges precisely over all  $(q^n - 1)^{\text{th}}$  roots of unity. The sum of the  $(\ell_f[n/d]_{q^d})^{\text{th}}$  powers of all  $(q^n - 1)^{\text{th}}$  roots of unity is zero unless  $q^n - 1$  divides  $\ell_f[n/d]_{q^d}$ , in which case the sum is  $q^n - 1$ .  $\square$

**Lemma 4.3.3.** *For all  $n \in \mathbb{N}$ ,  $d|n$ , prime powers  $q$ , and  $b|q^n - 1$ ,*

$$\#\{f \in \mathcal{F}_d(q) : b|\ell_f[n/d]_{q^d}\} = \frac{1}{d} \sum_{c|d} \boldsymbol{\mu}(d/c) \frac{q^n - 1}{\text{lcm}([n/c]_{q^c}, b)} \quad (4.3.10)$$

*Proof.* By Möbius inversion, it suffices to prove

$$\sum_{c|d} c \cdot \#\{f \in \mathcal{F}_c(q) : b|\ell_f[n/c]_{q^c}\} = \frac{q^n - 1}{\text{lcm}([n/d]_{q^d}, b)}. \quad (4.3.11)$$

View each value  $\ell_f[n/c]_{q^c}$  as an element of  $\mathbb{Z}/(q^n - 1)$ , as in the context of Corollary 2.3.3. Modulo  $q^n - 1$ , there are exactly  $c$  distinct choices for each  $\ell_f[n/c]_{q^c}$ . Namely, given a choice for  $\ell_f$ ,

$$\ell_f, q\ell_f, q^2\ell_f, \dots, q^{c-1}\ell_f \quad \text{mod } q^n - 1$$

are also valid choices for  $\ell_f$ , and so

$$\ell_f[n/c]_{q^c}, q\ell_f[n/c]_{q^c}, q^2\ell_f[n/c]_{q^c}, \dots, q^{c-1}\ell_f[n/c]_{q^c} \quad \text{mod } q^n - 1$$

are all the possible choices for  $\ell_f[n/c]_{q^c}$  in  $\mathbb{Z}/(q^n - 1)$ . Recalling definition (2.3.4), we see that those values are precisely the images under  $\theta_n$  of the roots of  $f$ . Thus, another way to interpret the sum on the left side of (4.3.11) is

$$\sum_{c|d} \sum_{f \in \mathcal{F}_c(q)} \sum_{\substack{\alpha \in \mathbb{F}_{q^c} \\ f(\alpha)=0}} \delta_{b|\theta_n(\alpha)}.$$

Therefore, by Corollary 2.3.3, the left side of (4.3.11) counts the elements of  $\mathbb{Z}/(q^n - 1)$  that are divisible by both  $[n/d]_{q^d}$  and  $b$ , which is exactly the right side of (4.3.11).  $\square$

*Proof of Cor. 4.3.1.* Using Lemma 4.3.2 and expanding the  $k^{\text{th}}$  power in the statement, it remains to show

$$\sum_{s_1, \dots, s_k | n} \#\{f \in \mathcal{F}_d(q) : \text{lcm}(q^{s_1} - 1, \dots, q^{s_k} - 1) | \ell_f[n/d]_{q^d}\} \cdot \prod_{i=1}^k \mu(n/s_i)(q^{s_i} - 1)$$

equals

$$\frac{1}{d} \sum_{c|d} \mu(d/c) C_{n,k,c}(q).$$

By the definition of  $C_{n,k,c}(q)$ , this is equivalent to showing that

$$\#\{f \in \mathcal{F}_d(q) : \text{lcm}(q^{s_1} - 1, \dots, q^{s_k} - 1) | \ell_f[n/d]_{q^d}\}$$

equals

$$\frac{1}{d} \sum_{c|d} \boldsymbol{\mu}(d/c) \frac{q^n - 1}{\text{lcm}([n/c]_{q^c}, q^{s_1} - 1, \dots, q^{s_k} - 1)}.$$

This follows from Lemma 4.3.3.

□

## Chapter 5

## PROBABILISTIC RESULT

## 5.1 Prerequisite lemmas

We require some lemmas before proving Theorem 1.2.7, and we introduce more notation to do so. For a complex number  $\alpha = x + iy$ , let  $\bar{\alpha} = x - iy$  denote the complex conjugate of  $\alpha$ , and let  $\|\alpha\| = \sqrt{\alpha\bar{\alpha}} = \sqrt{x^2 + y^2} \in [0, \infty)$  denote the usual **modulus** of  $\alpha$ . Define the function  $D : \mathbb{N} \rightarrow \mathbb{N} \cup \{0\}$  by

$$D(n) = \begin{cases} 0 & \text{if } n = 1, \\ \max\{s \in \mathbb{N} : s|n \text{ and } s < n\} & \text{if } n > 1. \end{cases} \quad (5.1.1)$$

In other words,  $D(n)$  is the largest proper divisor of  $n$ , unless  $n = 1$ , and  $D(1) = 0$ . Note that  $D(n) \leq n/2$  for all  $n \in \mathbb{N}$ . In this section, we also make use of **big  $O$  notation**. Recall that if  $S$  is an infinite subset of  $\mathbb{N}$  and  $f, g : S \rightarrow [0, \infty)$ , then we write  $f = O(g)$  to denote that there exist  $m \in [0, \infty)$  and  $s_0 \in S$  such that  $f(s) \leq m \cdot g(s)$  for all  $s > s_0$ . In other words,  $f$  is big  $O$  of  $g$  if some constant multiple of  $g(s)$  is an upper bound on  $f(s)$  for all sufficiently large  $s \in S$ .

**Lemma 5.1.1.** *For all  $n \in \mathbb{N}$ ,  $d|n$ , and  $r \in \{0, \dots, \frac{n}{d} - 1\}$ , we have*

$$\frac{1}{\deg_{n,d,r}(q)} = O\left(q^{-e(n,d,r)}\right), \quad (5.1.2)$$

where we define

$$e(n,d,r) = d \binom{r+1}{2} + \binom{n+1}{2} - d \binom{\frac{n}{d}+1}{2} + dr \left(\frac{n}{d} - 1 - r\right). \quad (5.1.3)$$

Moreover,  $e(n,d,r)$  is positive unless  $d = 1$  and  $r = 0$ , and  $e(n,1,0) = 0$ .

*Proof.* The first claim follows from the discussion in Remark 1.2.4 and then checking the degrees in  $q$  of the various polynomials which comprise  $\deg_{n,d,r}(q)$ . To prove the second claim, first observe that  $e(n, d, r)$  is a quadratic polynomial in  $r$  with critical point  $r = \frac{n}{d} - \frac{1}{2}$  and leading coefficient  $-d/2$ . This implies  $e(n, d, r)$  is increasing for  $r \in \{0, \dots, \frac{n}{d} - 1\}$ . The minimum value of  $e(n, d, r)$  on  $\{0, \dots, \frac{n}{d} - 1\}$  is therefore achieved at  $r = 0$ . Observe that  $e(n, d, 0) = \frac{n}{2} (n - \frac{n}{d})$ , which is positive unless  $d = 1$ . Therefore,  $e(n, d, r) > 0$  if  $d > 1$ . In the case  $d = 1$ , we have  $e(n, 1, r) = -\frac{1}{2}r^2 + (n - \frac{1}{2})r$ , which is positive unless  $r = 0$ . The result follows.  $\square$

**Lemma 5.1.2.** *For all  $n \in \mathbb{N}$ ,  $d|n$ ,  $r \in \{0, \dots, n/d - 1\}$ , we have*

$$\max_{\substack{f \in \mathcal{F}_d(q) \\ f(z) \neq z-1}} \frac{\left\| \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right\|}{\#\mathcal{T}_{(n)}(q)} = O(q^{D(n)-n}). \quad (5.1.4)$$

*Proof.* Applying Theorem 1.2.6, Corollary 2.2.1, (2.4.10), Corollary 2.4.8, and Lemma 4.3.2, we have

$$\frac{1}{\#\mathcal{T}_{(n)}(q)} \left\| \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right\| = \frac{d \cdot \left| \sum_{s|n} \boldsymbol{\mu}(n/s)(q^s - 1) \delta_{q^s-1|\ell_f[n/d]_{q^d}} \right|}{\sum_{s|n} \boldsymbol{\mu}(n/s)(q^s - 1)} \quad (5.1.5)$$

for all prime powers  $q$  and  $f \in \mathcal{F}_d(q)$ . The denominator on the right side of (5.1.5) is a degree- $n$  polynomial in  $q$ , independent of  $f$ . However, the numerator on the right side of (5.1.5) is not necessarily a polynomial in  $q$  at all, as it also depends on  $\ell_f$  which can vary with  $q$ , and the sum is inside of an absolute value. Fortunately, if  $q^n - 1$  does not divide  $\ell_f[n/d]_{q^d}$ , then

$$\begin{aligned} \left| \sum_{s|n} \boldsymbol{\mu}(n/s)(q^s - 1) \delta_{q^s-1|\ell_f[n/d]_{q^d}} \right| &\leq \sum_{\substack{s|n \\ s < n}} |\boldsymbol{\mu}(n/s)(q^s - 1)| \\ &\leq \sum_{\substack{s|n \\ s < n}} q^s < 1 + \sum_{\substack{s|n \\ s < n}} q^s. \end{aligned} \quad (5.1.6)$$

Therefore,

$$\frac{1}{\#\mathcal{T}_{(n)}(q)} \left\| \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right\| \leq d \cdot \frac{1 + \sum_{s|n, s < n} q^s}{\sum_{s|n} \boldsymbol{\mu}(n/s)(q^s - 1)}. \quad (5.1.7)$$

Observe that  $1 + \sum_{s|n, s < n} q^s$  is a degree- $D(n)$  polynomial in  $q$ , and the right side of (5.1.7) is independent of  $f$ . Moreover, the condition  $q^n - 1 \nmid \ell_f[n/d]_{q^d}$  is equivalent to  $f(z) \neq z - 1$  because we can assume  $\ell_f \leq q^d - 1$ , which shows

$$q^n - 1 \mid \ell_f[n/d]_{q^d} \implies \ell_f = q^d - 1 \implies f(1) = 0 \implies f(z) = z - 1.$$

The result now follows from computing the maximum of (5.1.7) over  $f \in \mathcal{F}_d(q) \setminus \{z - 1\}$ .  $\square$

**Lemma 5.1.3.** *For all  $n \in \mathbb{N}$ ,  $\mu \vdash n$ ,  $d|n$ ,  $r \in \{0, \dots, \frac{n}{d} - 1\}$ , we have*

$$\max_{f \in \mathcal{F}_d(q)} \frac{\left\| \sum_{g \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(g) \right\|}{\gamma_n(q)} = O(1). \quad (5.1.8)$$

*Proof.* Consider a fixed prime power  $q$  and polynomial  $f \in \mathcal{F}_d(q)$  to begin. Apply Theorem 1.2.6 to compute the character values. Observe that, if some part of  $\mu$  is not divisible by  $d$ , then  $\sum_{g \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(g) = 0$ , which satisfies the claim. So assume there exists  $\tilde{\mu} \vdash n/d$  such that  $\mu = d\tilde{\mu}$ . Recall that, by Theorem 2.4.5, the conjugacy classes in  $\mathcal{T}_\mu^\square(q)$  are in bijection with subsets  $\{h_1, \dots, h_{\ell(\mu)}\} \subset \mathcal{F}(q)$  of distinct polynomials with  $\deg h_i = \mu_i$  for each  $i \in \{1, \dots, \ell(\mu)\}$ . By Theorem 1.2.6, Corollary 2.4.8 and the fact that characters are constant on conjugacy classes, we have that  $\sum_{g \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(g)$  equals

$$\frac{\gamma_n(q)(-1)^{\frac{n}{d}(d-1)} \chi_{\tilde{\mu}}^{(n/d-r, 1^r)}}{\prod_{i=1}^{\ell(\mu)} (q^{\mu_i} - 1)} \sum_{\substack{\{h_1, \dots, h_{\ell(\mu)}\} \subset \mathcal{F}(q) \\ \deg h_i = \mu_i \forall i}} \prod_{i=1}^{\ell(\mu)} \frac{1}{\tilde{\mu}_i} \sum_{\substack{\alpha_i \in \mathbb{F}_{q^{\mu_i}} \\ h_i(\alpha_i) = 0}} \theta(\alpha_i)^{\ell_f[\tilde{\mu}_i]_{q^d}}. \quad (5.1.9)$$

We can now separate the sum in (5.1.9) according to the degrees of the distinct polynomials  $h_i \in \mathcal{F}_{\mu_i}(q)$ . Doing so transforms (5.1.9) into

$$\frac{\gamma_n(q)(-1)^{\frac{n}{d}(d-1)} \chi_{\tilde{\mu}}^{(n/d-r, 1^r)}}{\prod_{i=1}^{\ell(\mu)} (q^{\mu_i} - 1)} \prod_{s \geq 1} \binom{d}{s}^{m_s(\mu)} \sum_{\{p_1, \dots, p_{m_s(\mu)}\} \subset \mathcal{F}_s(q)} \prod_{i=1}^{m_s(\mu)} \sum_{\substack{\beta_i \in \mathbb{F}_{q^s} \\ p_i(\beta_i) = 0}} \theta(\beta_i)^{\ell_f[s/d]_{q^d}}. \quad (5.1.10)$$

Computing the norm, applying the triangle inequality, recalling that  $\theta$  maps into the unit

circle in  $\mathbb{C}$ , and applying Corollary 2.4.8 gives

$$\begin{aligned}
& \left\| \sum_{g \in \mathcal{T}_{\tilde{\mu}}^{\square}(q)} \chi^{f,r}(g) \right\| \\
& \leq \frac{\gamma_n(q) \left| \chi_{\tilde{\mu}}^{(n/d-r, 1^r)} \right|}{\prod_{i=1}^{\ell(\mu)} (q^{\mu_i} - 1)} \prod_{s \geq 1} \binom{d}{s}^{m_s(\mu)} \sum_{\{p_1, \dots, p_{m_s(\mu)}\} \subset \mathcal{F}_s(q)} \prod_{i=1}^{m_s(\mu)} \sum_{\substack{\beta_i \in \mathbb{F}_{q^s} \\ p_i(\beta_i) = 0}} \left\| \theta(\beta_i)^{\ell_f[s/d]_{q^d}} \right\| \\
& = \frac{\gamma_n(q) \left| \chi_{\tilde{\mu}}^{(n/d-r, 1^r)} \right|}{\prod_{i=1}^{\ell(\mu)} (q^{\mu_i} - 1)} \prod_{s \geq 1} \binom{d}{s}^{m_s(\mu)} \sum_{\{p_1, \dots, p_{m_s(\mu)}\} \subset \mathcal{F}_s(q)} s^{m_s(\mu)} \\
& = \frac{\gamma_n(q) \left| \chi_{\tilde{\mu}}^{(n/d-r, 1^r)} \right|}{\prod_{i=1}^{\ell(\mu)} (q^{\mu_i} - 1)} d^{\sum_{s \geq 1} m_s(\mu)} \prod_{s \geq 1} \binom{\#\mathcal{F}_s(q)}{m_s(\mu)} = \#\mathcal{T}_{\mu}^{\square}(q) \cdot \left| \chi_{\tilde{\mu}}^{(n/d-r, 1^r)} \right| \cdot d^{\ell(\mu)}.
\end{aligned}$$

Thus,

$$\frac{1}{\gamma_n(q)} \left\| \sum_{g \in \mathcal{T}_{\mu}^{\square}(q)} \chi^{f,r}(g) \right\| \leq \frac{\#\mathcal{T}_{\mu}^{\square}(q)}{\gamma_n(q)} \cdot \left| \chi_{\tilde{\mu}}^{(n/d-r, 1^r)} \right| \cdot d^{\ell(\mu)}. \quad (5.1.11)$$

The right side of (5.1.11) does not depend on  $f$ , which implies

$$\max_{f \in \mathcal{F}_d(q)} \frac{1}{\gamma_n(q)} \left\| \sum_{g \in \mathcal{T}_{\mu}^{\square}(q)} \chi^{f,r}(g) \right\| \leq \frac{\#\mathcal{T}_{\mu}^{\square}(q)}{\gamma_n(q)} \cdot \left| \chi_{\tilde{\mu}}^{(n/d-r, 1^r)} \right| \cdot d^{\ell(\mu)}. \quad (5.1.12)$$

Moreover, by Corollary 1.1.2, for sufficiently large  $q$ , the right side of (5.1.12) is arbitrarily close to the constant value  $\left| \chi_{\tilde{\mu}}^{(n/d-r, 1^r)} \right| \cdot d^{\ell(\mu)} / z_{\mu}$ . The result follows.  $\square$

## 5.2 Proof of probabilistic result

We can now prove our probabilistic result, Theorem 1.2.7. Recall that it states

$$\lim_{q \rightarrow \infty} p_{k,\mu}(q) = \lim_{q \rightarrow \infty} p_{k,\mu}^{\square}(q) = \frac{1}{z_{\mu}} \quad (5.2.1)$$

for all  $n \in \mathbb{N}$  and  $\mu \vdash n$ .

*Proof of Theorem 1.2.7.* We will first prove that  $\lim_{q \rightarrow \infty} p_{k,\mu}^{\square}(q) = 1/z_{\mu}$ . From this, it follows that  $\lim_{q \rightarrow \infty} p_{k,\mu}(q) = 1/z_{\mu}$  because, for all prime powers  $q$ , we have  $p_{k,\nu}(q) \geq p_{k,\nu}^{\square}(q)$  for all  $\nu \vdash n$  and  $\sum_{\nu \vdash n} p_{k,\nu}(q) = 1 = \sum_{\nu \vdash n} 1/z_{\nu}$ .

Consider the following formulation of  $p_{k,\mu}^\square(q)$ . By its definition (1.2.13) and by Corollary 3.3.3, we have

$$p_{k,\mu}^\square(q) = \sum_{d|n} \sum_{r=0}^{\frac{n}{d}-1} \sum_{f \in \mathcal{F}_d(q)} \left( \frac{\sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g)}{\#\mathcal{T}_{(n)}(q)} \right)^k \left( \frac{\sum_{h \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(h)}{\gamma_n(q) \cdot \deg_{n,d,r}(q)^{k-1}} \right). \quad (5.2.2)$$

We want to compute  $\lim_{q \rightarrow \infty} p_{k,\mu}^\square(q)$ , but the index set for the summation over  $f \in \mathcal{F}_d(q)$  in (5.2.2) itself depends on  $q$ . Therefore, for each  $d|n$ ,  $r \in \{0, \dots, n/d - 1\}$ , and  $f \in \mathcal{F}_d(q)$  we define

$$\Phi_{k,\mu,d,r}(q) = \sum_{f \in \mathcal{F}_d(q)} \left( \frac{\sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g)}{\#\mathcal{T}_{(n)}(q)} \right)^k \left( \frac{\sum_{h \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(h)}{\gamma_n(q) \cdot \deg_{n,d,r}(q)^{k-1}} \right) \quad (5.2.3)$$

so that

$$p_{k,\mu}^\square(q) = \sum_{d|n} \sum_{r=0}^{\frac{n}{d}-1} \Phi_{k,\mu,d,r}(q), \quad (5.2.4)$$

where the number of terms in the summation is fixed, even as  $q$  varies. Theorem 1.2.7 now follows from Lemma 5.2.1 below, which computes the limiting behavior of  $\Phi_{k,\mu,d,r}(q)$  for each  $d|n$  and  $r \in \{0, \dots, n/d - 1\}$ .  $\square$

**Lemma 5.2.1.** *For all  $n, k \in \mathbb{N}$ ,  $\mu \vdash n$ ,  $d|n$ , and  $r \in \{0, \dots, n/d - 1\}$ , we have*

$$\lim_{q \rightarrow \infty} \Phi_{k,\mu,d,r}(q) = \begin{cases} 0 & \text{if } d > 1 \text{ or } r > 0, \\ 1/z_\mu & \text{if } d = 1 \text{ and } r = 0. \end{cases} \quad (5.2.5)$$

*Proof.* Consider first the case that  $d > 1$  and  $r$  is arbitrary. Observe that  $\|\Phi_{k,\mu,d,r}(q)\|$  is bounded above by

$$\frac{\#\mathcal{F}_d(q)}{\deg_{n,d,r}(q)^{k-1}} \cdot \max_{f \in \mathcal{F}_d(q)} \left( \frac{\left\| \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right\|}{\#\mathcal{T}_{(n)}(q)} \right)^k \cdot \max_{f \in \mathcal{F}_d(q)} \frac{\left\| \sum_{h \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(h) \right\|}{\gamma_n(q)} \quad (5.2.6)$$

for all prime powers  $q$ . We proceed to investigate the asymptotic dependence on  $q$  of (5.2.6). Recall from (2.4.10) that  $\#\mathcal{F}_d(q) = O(q^d)$ . Combining this with Lemmas 5.1.1, 5.1.2, and 5.1.3, we have

$$\|\Phi_{k,\mu,d,r}(q)\| = O\left(q^{d+k(D(n)-n)-(k-1) \cdot e(n,d,r)}\right). \quad (5.2.7)$$

By hypothesis,  $k \geq 2$ , implying  $d+k \cdot (D(n)-n) \leq d-k \cdot n/2 \leq 0$ . Moreover, by Lemma 5.1.1,  $(k-1) \cdot e(n, d, r) > 0$ . It follows that  $\lim_{q \rightarrow \infty} \Phi_{k,\mu,d,r}(q) = 0$  if  $d > 1$ .

Next, consider the case  $d = 1$  and  $r > 0$ . Observing that  $z-1 \in \mathcal{F}_1(q)$  for all prime powers  $q$  and applying Theorem 3.3.1, we can rewrite  $\Phi_{k,\mu,1,r}(q)$  as

$$\Phi_{k,\mu,1,r}(q) = \frac{\#\mathcal{T}_\mu^\square}{\gamma_n(q)} \cdot \frac{(-1)^{rk} \chi_\mu^{(n-r, 1^r)}}{\left(q^{\binom{r+1}{2}} \begin{bmatrix} n-1 \\ r \end{bmatrix}_q\right)^{k-1}} \quad (5.2.8)$$

$$+ \sum_{\substack{f \in \mathcal{F}_1(q) \\ f(z) \neq z-1}} \left( \frac{\sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g)}{\#\mathcal{T}_{(n)}(q)} \right)^k \left( \frac{\sum_{h \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(h)}{\gamma_n(q) \cdot \deg_{n,d,r}(q)^{k-1}} \right). \quad (5.2.9)$$

We repeat the same analysis as before, but apply it only to (5.2.9). Observe that (5.2.9) is bounded above by

$$\frac{(\#\mathcal{F}_1(q)) - 1}{\deg_{n,d,r}(q)^{k-1}} \cdot \max_{\substack{f \in \mathcal{F}_1(q) \\ f(z) \neq z-1}} \left( \frac{\left\| \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right\|}{\#\mathcal{T}_{(n)}(q)} \right)^k \cdot \max_{\substack{f \in \mathcal{F}_1(q) \\ f(z) \neq z-1}} \frac{\left\| \sum_{h \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(h) \right\|}{\gamma_n(q)} \quad (5.2.10)$$

Applying Lemmas 5.1.1, 5.1.2, and 5.1.3 again, we see that (5.2.10) is

$$O\left(q^{1+k(D(n)-n)-(k-1) \cdot e(n,1,r)}\right). \quad (5.2.11)$$

As before,  $1 + k \cdot (D(n) - n) - (k-1) \cdot e(n, 1, r)$  is negative. It follows that the limit as  $q \rightarrow \infty$  of (5.2.9) is zero if  $d = 1$  and  $r > 0$ . Applying Corollary 1.1.2 to (5.2.8), we can conclude that  $\lim_{q \rightarrow \infty} \Phi_{k,\mu,1,r}(q) = 0$  if  $d = 1$  and  $r > 0$ .

Finally, we consider the case  $d = 1$  and  $r = 0$ . Carrying out the same analysis as in the previous paragraph, we see that

$$\|\Phi_{k,\mu,1,0}(q)\| = \frac{\#\mathcal{T}_\mu^\square(q)}{\gamma_n(q)} + O\left(q^{1+k(D(n)-n)}\right).$$

Observe that  $1 + k(D(n) - n) < 0$  even if  $n = 1$  due to the fact that  $k \geq 2$  and  $D(1) = 0$ . The result now follows from Corollary 1.1.2.  $\square$

## Chapter 6

## POLYNOMIALITY RESULTS

**6.1 Proofs of polynomiality results**

We discuss some results regarding how similar  $g_{k,\mu}(q)$  is to a polynomial for various choices of  $\mu$ . Recall that  $\gamma_n(q)$ ,  $P_{n,k}(q)$ ,  $\deg_{n,d,r}(q)$ , and  $D_{n,k,d}(q)$  are all rational in  $q$  with rational coefficients.

**Corollary 6.1.1** (to Thm. 1.2.1). *Suppose  $n, k, \ell \in \mathbb{N}$  with  $n > 2$  and  $\ell > 1$ . If  $\mu = (\mu_1, \dots, \mu_\ell)$  with  $\mu_{\ell-1} > \mu_\ell = 1$ , then  $g_{k,\mu}^\square(q)$  is a polynomial in  $q$  with rational coefficients.*

*Proof.* Theorem 1.2.1 implies that  $n^k z_\mu \cdot g_{k,\mu}^\square(q)$  is a rational function of  $q$  with integer coefficients which takes on integral values infinitely many times. Thus  $n^k z_\mu \cdot g_{k,\mu}^\square(q)$  is an integer polynomial in  $q$ . Dividing by  $n^k z_\mu \in \mathbb{N}$  gives the result.  $\square$

Next, we prove Corollary 1.2.8, which states that  $g_{k,(n)}(q)$  is a quasipolynomial in  $q$  of quasiperiod  $n$  in the case that  $n$  is prime. Note that  $g_{1,(n)}(q) = \#\mathcal{T}_{(n)}(q)$ , which is a polynomial in  $q$ , independent of  $n$  or the congruence class of  $q$ . However, when  $k \geq 2$ , Corollary 1.2.8 has more to say.

*Proof of Corollary 1.2.8.* We will apply a similar reasoning to that stated in the proof of Corollary 6.1.1. Recall that the function  $C_{n,k,c}(q)$  is not rational in  $q$  in general, which prevents  $g_{k,(n)}(q)$  from being rational. Define

$$M_i = \{q \text{ prime power} : q \equiv i \pmod{n}\}, \quad \text{for } i \in \{0, 1, \dots, n-1\}. \quad (6.1.1)$$

The quasipolynomiality result will follow once we can show that, for each  $c|n$  and  $i \in \{0, \dots, n-1\}$ , we have that  $C_{n,k,c}(q)$  becomes a polynomial in  $q$  when restricted to  $M_i$ .

In order to do this, it suffices to show that, for each  $i \in \{0, \dots, n-1\}$  and choice of  $c, s_1, \dots, s_k | n$ ,

$$\text{lcm} \left( \frac{q^n - 1}{q^c - 1}, q^{s_1} - 1, \dots, q^{s_k} - 1 \right) \quad (6.1.2)$$

agrees with some polynomial on  $M_i$ . Since  $n$  is prime, we have  $c, s_1, \dots, s_k \in \{1, n\}$ . Furthermore, if any  $s_i = n$ , we have that (6.1.2) equals  $q^n - 1$ , a fixed polynomial in  $q$ , independent of  $c$  or the congruence class of  $q$ . Therefore, for each choice of  $c \in \{1, n\}$ , we need only consider the case in which  $s_1 = \dots = s_k = 1$  and hence must show that

$$\text{lcm} \left( \frac{q^n - 1}{q^c - 1}, q - 1 \right) \quad (6.1.3)$$

is a polynomial on each  $M_i$ .

Observe that, if  $c = n$ , then (6.1.3) equals  $q - 1$ , a fixed polynomial in  $q$ , independent of the congruence class of  $q$ . Therefore, we now need only consider the case  $c = s_1 = \dots = s_k = 1$  and hence must show that

$$\text{lcm} \left( \frac{q^n - 1}{q - 1}, q - 1 \right) \quad (6.1.4)$$

is a polynomial on each  $M_i$ .

To finish the proof of quasipolynomiality, we now simplify (6.1.4). First, using the property that  $\text{lcm}(a, b) \text{gcd}(a, b) = ab$  for  $a, b \in \mathbb{N}$ , we have

$$\text{lcm} \left( \frac{q^n - 1}{q - 1}, q - 1 \right) = \frac{\frac{q^n - 1}{q - 1} \cdot (q - 1)}{\text{gcd} \left( \frac{q^n - 1}{q - 1}, q - 1 \right)} = \frac{q^n - 1}{\text{gcd}([n]_q, q - 1)}. \quad (6.1.5)$$

Next, the fact that  $[n]_q \equiv n \pmod{q - 1}$ , we can rewrite (6.1.5) as

$$\frac{q^n - 1}{\text{gcd}(n, q - 1)} \quad (6.1.6)$$

by reducing one argument of the gcd modulo the other. Let  $i \in \{0, \dots, n-1\}$  and assume  $q = na + i$  for some  $a \in \mathbb{N}$ . We can compute (6.1.6) as

$$\frac{q^n - 1}{\text{gcd}(n, q - 1)} = \frac{q^n - 1}{\text{gcd}(n, na + i - 1)} = \frac{q^n - 1}{\text{gcd}(n, i - 1)} = \begin{cases} \frac{q^n - 1}{n} & i = 1 \\ q^n - 1 & i \neq 1. \end{cases} \quad (6.1.7)$$

Quasipolynomiality now follows from the fact that (6.1.7) is a fixed polynomial in  $q$  for each fixed  $i \in \{0, \dots, n-1\}$ . The final claim follows from the fact that (6.1.7) is the same for all  $i \neq 1$ .

To determine the degrees and leading coefficients of  $f_0, \dots, f_{n-1}$ , we apply the quasipolynomiality of  $g_{k,(n)}(q)$  to the probabilistic result Theorem 1.2.7 to get

$$\lim_{q \rightarrow \infty} \frac{f_i(q)}{\frac{1}{n} \cdot \#\mathcal{T}_{(n)}(q)^k} = 1$$

for each  $i \in \{0, \dots, n-1\}$ . This implies each  $f_i(q)$  must have the same degree and leading coefficient as  $\frac{1}{n} \cdot \#\mathcal{T}_{(n)}(q)^k$ . By Corollary 2.4.8,  $\#\mathcal{T}_{(n)}(q) = \#\mathcal{F}_n(q) \cdot \gamma_n(q)/(q^n - 1)$ , which has degree  $n^2$  and leading coefficient  $n^{-1}$  by (2.4.10) and the definition of  $\gamma_n$ . Therefore,  $\frac{1}{n} \cdot \#\mathcal{T}_{(n)}(q)^k$ , and hence each  $f_i$ , has degree  $kn^2$  and leading coefficient  $n^{-(k+1)}$ .  $\square$

**Example 6.1.2.** We now use the main results of the thesis to write down alternate formulas for  $g_{2,(2)}(q)$  and  $g_{2,(3)}(q)$ . Note that Theorem 1.2.3 provides an explicit formula while Corollary 1.2.8 determines the degree of the polynomials  $f_0, \dots, f_{n-1}$ . Generating enough data points uniquely determines  $f_0, \dots, f_{n-1}$ . We also rely on [32, Prop. 4.4.1] to rephrase the quasipolynomials as sums of polynomials.

First, for  $n = 2$ , we have

$$g_{2,(2)}(q) = \frac{q(q-1)^3(q^4 - 3q^3 + 4q^2 - \frac{1}{2}q - \frac{1}{2})}{8} + (-1)^q \cdot \frac{q(q+1)(q-1)^3}{16} \quad (6.1.8)$$

for all prime powers  $q$ .

Second, for  $n = 3$ , define polynomials

$$\begin{aligned} f_0(q) &= \frac{q^6(q+1)^2(q-1)^4(q^6 - 4q^4 + 3q^3 + 5q^2 - 9q + 1)}{27}, \\ f_1(q) &= \frac{q^3(q+1)(q-1)^5(q^9 + 2q^8 - 2q^7 - 3q^6 + 5q^5 + q^4 - 9q^3 - 4q^2 - 2q + 2)}{27}, \\ f_2(q) &= \frac{q^6(q+1)^2(q-1)^4(q^6 - 4q^4 + 3q^3 + 5q^2 - 9q + 1)}{27}. \end{aligned}$$

Observe that  $f_0 = f_2$  and  $f_1 \neq f_0$ , in accordance with Corollary 1.2.8. Letting  $\zeta = e^{2\pi i/3}$ , define

$$P_0 = \frac{f_0 + f_1 + f_2}{3}, \quad P_1 = \frac{f_0 + \zeta^2 f_1 + \zeta f_2}{3}, \quad P_2 = \frac{f_0 + \zeta f_1 + \zeta^2 f_2}{3}.$$

Finally, we have

$$g_{2,(3)}(q) = P_0(q) + \zeta^q P_1(q) + \zeta^{2q} P_2(q) \quad (6.1.9)$$

for all prime powers  $q$ .

**Remark 6.1.3.** Data suggest that, in general,  $g_{k,(n)}(q)$  is not a quasipolynomial when  $n$  is not prime. In fact, because Corollary 1.2.8 gives the degree of any polynomial that might agree with an infinite family of values of  $g_{k,(n)}(q)$  for fixed  $n, k$ , one can prove in specific instances that such a polynomial does not exist. For instance,  $g_{2,(4)}(q)$  is not a polynomial on the prime powers congruent to 2 (mod 4).

**Example 6.1.4.** The ordinary generating function of a quasipolynomial is rational [32, Prop. 4.4.1]. For example, using  $x$  as an indeterminate, we have

$$\sum_{q \geq 0} g_{2,(2)}(q)x^q = \frac{P(x)}{Q(x)},$$

where

$$\begin{aligned} P(x) &= 8x^{14} + 354x^{13} + 3642x^{12} + 16602x^{11} + 45042x^{10} + 74172x^9 + 83660x^8 \\ &\quad + 59820x^7 + 29412x^6 + 8322x^5 + 1434x^4 + 90x^3 + 2x^2, \quad \text{and} \\ Q(x) &= (1+x)^6(1-x)^9. \end{aligned}$$

See the appendix for more data on the generating functions for  $g_{k,(n)}(q)$  when  $n$  is prime.

## Chapter 7

## FURTHER WORK

In the interest of looking ahead toward new ideas, we include here several results and open problems that push outward on the horizon of this thesis. Ideally, an interested reader will become inspired and prove cool new results.

### 7.1 Slightly expanding the main result

We can make slight headway toward addressing more cases of calculating  $g_{k,\mu}(q)$  or  $g_{k,\mu}^\square(q)$  by solving the case of  $\mu = (n-2, 2)$  for  $n \geq 5$ . Since the parts of  $(n-2, 2)$  are distinct when  $n \geq 5$ , we have  $g_{k,(n-2,2)}(q) = g_{k,(n-2,2)}^\square(q)$ . We believe this case begins to display the limitations of the approach used in this thesis.

**Theorem 7.1.1.** *For all prime powers  $q$  and  $n, k \in \mathbb{N}$  with  $n \geq 5$ , if  $n$  is odd and  $q$  is even, we have*

$$g_{k,(n-2,2)}(q) = \frac{\#\mathcal{T}_{(n)}(q)^k \cdot \#\mathcal{T}_{(n-2,2)}(q)}{\#\mathrm{GL}_n \mathbb{F}_q} \cdot \sum_{r=0}^{n-1} \frac{(-1)^{rk} \chi_{(n-2,2)}^{(n-r,1^r)}}{\left(q^{\binom{r+1}{2}} \begin{bmatrix} n-1 \\ r \end{bmatrix}_q\right)^{k-1}}. \quad (7.1.1)$$

Compare Theorem 7.1.1 to the analogous formula

$$g_{k,(n-2,2)} = \frac{\#\mathcal{C}_{(n)}^k \cdot \#\mathcal{C}_{(n-2,2)}}{\#\mathfrak{S}_n} \cdot \sum_{r=0}^{n-1} \frac{(-1)^{rk} \chi_{(n-2,2)}^{(n-r,1^r)}}{\binom{n-1}{r}^{k-1}} \quad (7.1.2)$$

for the symmetric group, which is valid for all  $n \geq 5$ , regardless of parity. Unfortunately, if  $n$  is even or if  $q$  is odd, there is not yet as obvious a connection between  $g_{k,(n-2,2)}$  and  $g_{k,(n-2,2)}^\square(q)$ .

*Proof of Thm. 7.1.1.* Applying Theorem 1.2.6 to Corollary 3.3.3, we see that only the summands corresponding to  $d = 1$  or  $2$  in (3.3.3) are relevant. The rest vanish due to the fact

that 2 is a part of the partition  $(n - 2, 2)$ . Furthermore, under the assumption that  $n$  is odd, we have that  $n - 2$  is also odd, hence the  $d = 2$  summand itself vanishes. Therefore, we need only consider  $d = 1$ .

Next, consider an arbitrary summand of (3.3.3) corresponding to  $f \in \mathcal{F}_1(q)$  and  $r \in \{0, \dots, n - 1\}$ . Similar to the proof of Theorem 1.2.1, we have that  $\sum_{h \in \mathcal{T}_{(n-2,2)}(q)} \chi^{f,r}(h)$  is a multiple of

$$\sum_{h_2 \in \mathcal{F}_2(q)} \sum_{\substack{\beta_2 \in \mathbb{F}_{q^2}^\times \\ h_2(\beta_2) = 0}} \theta(\beta_2)^{\ell_f[2]_q} = (q^2 - 1)\delta_{q^2-1|\ell_f(q+1)} - (q - 1)\delta_{q-1|\ell_f(q+1)}. \quad (7.1.3)$$

The first condition  $q^2 - 1|\ell_f(q + 1)$  is only satisfied when  $q - 1|\ell_f$ , hence  $f(z) = z - 1$ . For the latter condition, observe that  $\gcd(q - 1, q + 1) = 1$  under the assumption that  $q$  is even. Thus, the condition  $q - 1|\ell_f(q + 1)$  is only satisfied when  $q - 1|\ell_f$  as well. Therefore, only the  $d = 1$  and  $f(z) = z - 1$  summands do not vanish in (3.3.3). The character evaluations are then governed by Theorem 3.3.1, and the result follows.  $\square$

## 7.2 An analogue of factorizations into transpositions

For  $n, k \in \mathbb{N}$ , let  $\tau = (2, 1^{n-2}) \vdash n$ , and define

$$T_{k,n} = \#\{(t_1, \dots, t_k) \in \mathcal{C}_\tau^k : t_1 \cdots t_k \in \mathcal{C}_{(n)}\}. \quad (7.2.1)$$

In words,  $T_{k,n}$  is the number of  $k$ -tuples of transpositions in  $\mathfrak{S}_n$  whose product is an  $n$ -cycle. Dividing by  $(n - 1)!$  enumerates the factorizations of a fixed but arbitrary  $n$ -cycle into a product of  $k$  transpositions.

**Theorem 7.2.1** (Hurwitz [18], Dénes [7]). *For all  $n \in \mathbb{N}$ , if  $c \in \mathfrak{S}_n$  is an arbitrary fixed  $n$ -cycle, then the number of minimal-length factorizations of  $c$  into a product of transpositions is*

$$\frac{T_{n-1,n}}{(n - 1)!} = n^{n-2}. \quad (7.2.2)$$

Hurwitz's proof, dating back to 1891, comes from the enumerative study of covering maps of Riemann surfaces, now known as Hurwitz theory. The number  $n^{n-2}$  is also the

number of trees on  $n$  labeled vertices, due to Cayley [5]. Dénes bijectively proved that  $T_{n-1,1} = (n-1)! \cdot n^{n-2}$ , the number of trees on  $n$  labeled vertices and  $n-1$  labeled edges.

One can also write down a general formula for  $T_{k,n}$  using Theorem 2.1.1 and the character theory of  $\mathfrak{S}_n$ . Following Stanley's technique in [30], we have

$$T_{k,n} = \frac{\#\mathcal{C}_{(n)} \cdot \#\mathcal{C}_\tau^k}{\#\mathfrak{S}_n} \cdot \sum_{r=0}^{n-1} \frac{(-1)^r \left( \chi_\tau^{(n-r,1^r)} \right)^k}{\binom{n-1}{r}^{k-1}}. \quad (7.2.3)$$

In the case  $k = n-1$ , (7.2.3) result simplifies to Theorem 7.2.1. Furthermore, in the cases  $k < n-1$ , the (7.2.3) returns zero.

Consider the following analogue of  $T_{k,n}$  for  $\mathrm{GL}_n \mathbb{F}_q$ . Recall that we have defined  $\tau = (2, 1^{n-1}) \vdash n$ . For  $n, k \in \mathbb{N}$  and a prime power  $q$ , define

$$T_{k,n}(q) = \#\{(t_1, \dots, t_k) \in \mathcal{T}_\tau^\square(q)^k : t_1 \cdots t_k \in \mathcal{T}_{(n)}(q)\}. \quad (7.2.4)$$

Compare the following result to (7.2.3).

**Theorem 7.2.2.** *Suppose  $n, k \in \mathbb{N}$  with  $n \geq 3$  and  $q$  is a prime power. Let  $a \in \mathbb{N} \cup \{0\}$  be maximal such that  $2^a | n$ , and let  $c_\tau^\square$  denote the centralizer of an arbitrary element of  $\mathcal{T}_\tau^\square(q)$  so that  $\#c_\tau^\square = (q^2 - 1)(q - 1)^{n-2}$ . Then*

$$T_{k,n}(q) = \left( \frac{\#\mathcal{T}_{(n)}(q) \cdot \#\mathcal{T}_\tau^\square(q)^k}{\gamma_n(q)} + \varepsilon_{k,n}(q) \right) \cdot \sum_{r=0}^{n-1} \frac{(-1)^r \left( \chi_\tau^{(n-r,1^r)} \right)^k}{\left( q^{\binom{r+1}{2}} \begin{bmatrix} n-1 \\ r \end{bmatrix}_q \right)^{k-1}}, \quad (7.2.5)$$

where

$$\varepsilon_{k,n}(q) = \frac{-\#\mathcal{F}_{n/2^a}(q^{2^{a-1}})}{n(q^n - 1)} \cdot \left( \frac{(-1)^{n/2}}{2} \cdot \frac{\gamma_n(q)}{\#c_\tau^\square} \cdot (q - 1) \cdot \binom{(q-1)/2}{n/2-1} \right)^k \quad (7.2.6)$$

if both  $q$  is odd and  $n$  is even, and  $\varepsilon_{k,n}(q)$  is zero otherwise.

*Proof.* We begin with a modified version of (3.3.3) which states

$$T_{k,n}(q) = \frac{1}{\gamma_n(q)} \sum_{d,f,r} \mathrm{deg}_{n,d,r}(q)^{1-k} \left( \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right) \left( \sum_{h \in \mathcal{T}_\tau^\square(q)} \chi^{f,r}(h) \right)^k, \quad (7.2.7)$$

where the sum is again over all  $d|n$ ,  $f \in \mathcal{F}_d(q)$ , and  $r \in \{0, 1, \dots, n/d - 1\}$ . Consider a fixed summand corresponding to a choice of  $d$ ,  $f$ , and  $r$ . Similar to the proofs of Theorem 1.2.1 and Lemma 5.1.3, using Theorem 1.2.6, we have that  $\sum_{h \in \mathcal{T}_\tau^\square(q)} \chi^{f,r}(h)$  is a multiple of

$$\left( \sum_{h_1 \in \mathcal{F}_2(q)} \sum_{\substack{\beta_1 \in \mathbb{F}_{q^2}^\times \\ h_1(\beta_1)=0}} \theta(\beta_1)^{\ell_f [2]_q} \right) \left( \sum_{\{h_2, \dots, h_{n-1}\} \subset \mathcal{F}_1(q)} \prod_{i=2}^{n-1} \sum_{\substack{\beta_i \in \mathbb{F}_q^\times \\ h_i(\beta_i)=0}} \theta(\beta_i)^{\ell_f} \right). \quad (7.2.8)$$

The factor on the left side of (7.2.8) equals

$$(q^2 - 1)\delta_{q^2-1|\ell_f(q+1)} - (q-1)\delta_{q-1|\ell_f(q+1)} = \begin{cases} q(q-1), & q \text{ even or } f = z-1, \\ -(q-1), & q \text{ odd and } f = z+1, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore, we need only consider  $d = 1$  in the summation (7.2.7). Moreover, if  $q$  is even, we need only consider  $f = z - 1$  in (7.2.7). In that case, Theorem 3.3.1 governs the character values, and the result with  $\varepsilon_{n,k}(q) = 0$  follows.

Suppose now that  $q$  is odd. The summand indexed by  $f = z - 1$  in (7.2.7) is still governed by Theorem 3.3.1. Therefore, it remains to show that the term indexed by  $f = z + 1$  in (7.2.7) equals

$$\varepsilon_{k,n}(q) \cdot \sum_{r=0}^{n-1} \frac{(-1)^r \left( \chi_\tau^{(n-r, 1^r)} \right)^k}{\left( q \binom{r+1}{2} \left[ \begin{smallmatrix} n-1 \\ r \end{smallmatrix} \right]_q \right)^{k-1}}.$$

We will do so by addressing the factor on the right side of (7.2.8). Since each of  $h_2, \dots, h_{n-1}$  has degree one and  $\ell_{z+1} = (q-1)/2$ , we have that the factor on the right side of (7.2.8) equals  $(-1)^{n/2-1} \binom{(q-1)/2}{n/2-1}$  if  $n$  is even and zero if  $n$  is odd by Lemma 7.2.3 below. This takes care of the case when  $n$  is odd and  $\varepsilon_{n,k}(q)$  is still zero.

Finally, suppose that both  $q$  is odd and  $n$  is even. Based on our reasoning so far and by applying Theorem 1.2.6, we have that  $\sum_{h \in \mathcal{T}_\tau^\square(q)} \chi^{z+1,r}(h)$  equals

$$\frac{\gamma_n(q)}{\#c_\tau^\square} \cdot \chi_\tau^{(n-r, 1^r)} \cdot \frac{1}{2} \cdot (-(q-1)) \cdot (-1)^{n/2-1} \binom{(q-1)/2}{n/2-1}.$$

Based on the definition of  $\varepsilon_{n,k}(q)$ , it remains to show that

$$\frac{1}{\gamma_n(q)} \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{z+1,r}(g) = \frac{-\#\mathcal{F}_{n/2^a}(q^{2^{a-1}}) \cdot (-1)^r}{n(q^n - 1)}.$$

By Theorem 1.2.6 and Lemma 4.3.2, we have

$$\frac{1}{\gamma_n(q)} \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{z+1,r}(g) = \frac{1}{q^n - 1} \cdot (-1)^r \cdot \frac{1}{n} \cdot \sum_{s|n} \boldsymbol{\mu}(n/s)(q^s - 1) \delta_{q^s - 1 | \frac{q^n - 1}{2}}.$$

Now, Lemma 7.2.4 below completes the proof.  $\square$

**Lemma 7.2.3.** *For all  $n \in \mathbb{N}$  and odd prime powers  $q$ , we have*

$$\sum_A \left( \prod_{\alpha \in A} \alpha \right)^{(q-1)/2} = \begin{cases} (-1)^{n/2-1} \binom{(q-1)/2}{n/2-1}, & n \text{ even,} \\ 0, & n \text{ odd,} \end{cases}$$

where the sum is over all subsets  $A$  of the set of  $(q-1)^{\text{th}}$  complex roots of unity such that  $\#A = n - 2$ .

*Proof.* Let  $\zeta = e^{2\pi i/(q-1)}$  be a primitive  $(q-1)^{\text{th}}$  root of unity. For each  $k \in \{0, \dots, q-1\}$ , let  $e_k(\zeta)$  denote the  $k^{\text{th}}$  elementary symmetric polynomial in  $\{\zeta, \zeta^2, \dots, \zeta^{q-1}\}$ . We need to compute  $e_{n-2}(\zeta^{(q-1)/2})$ .

Observe

$$x^{q-1} - 1 = \prod_{m=1}^{q-1} (x - \zeta^m) = \sum_{k=0}^{q-1} x^{q-1-k} (-1)^k e_k(\zeta).$$

Since  $q-1$  is even, exactly half of the  $((q-1)/2)^{\text{th}}$  powers of the  $(q-1)^{\text{th}}$  roots of unity equal 1, and the other half equal  $-1$ . Thus,

$$(x^2 - 1)^{(q-1)/2} = \prod_{m=1}^{q-1} (x - (\zeta^m)^{(q-1)/2}) = \sum_{k=0}^{q-1} x^{q-1-k} (-1)^k e_k(\zeta^{(q-1)/2}). \quad (7.2.9)$$

Therefore,  $e_{n-2}(\zeta^{(q-1)/2})$  equals the coefficient of  $x^{q-1-(n-2)}$  in

$$(x^2 - 1)^{(q-1)/2} = \sum_{k=0}^{\frac{q-1}{2}} \binom{(q-1)/2}{k} x^{2k} (-1)^{\frac{q-1}{2}-k}.$$

The result now follows by examining the term corresponding to  $2k = q-1 - (n-2)$ .  $\square$

**Lemma 7.2.4.** *For all  $n \in \mathbb{N}$  and prime powers  $q$  with  $n$  even and  $q$  odd, we have*

$$\sum_{s|n} \boldsymbol{\mu}(n/s)(q^s - 1)\delta_{q^s-1|\frac{q^n-1}{2}} = -\#\mathcal{F}_{n/2^a}(q^{2^{a-1}}),$$

where  $a \in \mathbb{N}$  is maximal such that  $2^a|n$ .

*Proof.* The condition  $q^s - 1|(q^n - 1)/2$  is equivalent to

$$(q - 1)[s]_q \left| \frac{(q - 1)[s]_q [n/s]_{q^s}}{2} \right.,$$

which is in turn equivalent to  $2|[n/s]_{q^s}$ . Since  $q$  is odd, we see that

$$[n/s]_{q^s} = 1 + q^s + (q^s)^2 + \cdots + (q^s)^{n/s-1}$$

is even precisely when  $n/s$  is even. Therefore,

$$\sum_{s|n} \boldsymbol{\mu}(n/s)(q^s - 1)\delta_{q^s-1|\frac{q^n-1}{2}} = \sum_{\substack{s|n \\ 2^a \nmid s}} \boldsymbol{\mu}(n/s)(q^s - 1).$$

Letting  $b = n/2^a$ , we have

$$\begin{aligned} \sum_{\substack{s|n \\ 2^a \nmid s}} \boldsymbol{\mu}(n/s)(q^s - 1) &= \sum_{\bar{s}|b} \boldsymbol{\mu}\left(\frac{n}{2^{a-1}\bar{s}}\right) \left(q^{2^{a-1}\bar{s}} - 1\right) = \sum_{\bar{s}|b} \boldsymbol{\mu}\left(2 \cdot \frac{b}{\bar{s}}\right) \left((q^{2^{a-1}})^{\bar{s}} - 1\right) \\ &= \boldsymbol{\mu}(2) \cdot \sum_{\bar{s}|b} \boldsymbol{\mu}\left(\frac{b}{\bar{s}}\right) \left((q^{2^{a-1}})^{\bar{s}} - 1\right) = -\#\mathcal{F}_b\left(q^{2^{a-1}}\right). \end{aligned}$$

□

### 7.3 An analogue of a result of Boccara

For  $n \in \mathbb{N}$  and  $\mu \vdash n$ , let  $\pi$  be an arbitrary permutation in  $\mathcal{C}_\mu$  and define

$$F_\mu = \#\{(s, t) \in \mathcal{C}_{(n)} \times \mathcal{C}_{(n-1,1)} : st = \pi\}. \quad (7.3.1)$$

In words,  $F_\mu$  equals the number of ways to express a fixed arbitrary permutation with cycle type  $\mu$  as the product of an  $n$ -cycle and an  $(n - 1)$ -cycle. Since  $\mathfrak{S}_n$  acts transitively on each of  $\mathcal{C}_{(n)}$ ,  $\mathcal{C}_{(n-1,1)}$ , and  $\mathcal{C}_\mu$  by conjugation, we have that  $F_\mu$  is well-defined. Unexpectedly, it follows from the work of Boccara that  $F_\mu$  only depends on  $n$  and the parity of  $n - \ell(\mu)$ .

**Corollary 7.3.1** (Boccara [2]). *For all  $n \in \mathbb{N}$  and  $\mu \vdash n$ ,*

$$F_\mu = \begin{cases} 0, & n - \ell(\mu) \text{ is even,} \\ 2(n-2)!, & n - \ell(\mu) \text{ is odd.} \end{cases} \quad (7.3.2)$$

Consider the following analogue of  $F_\mu$  for  $\mathrm{GL}_n \mathbb{F}_q$ . For  $\mu \vdash n$  and  $x$  an arbitrary element of  $\mathcal{T}_\mu^\square(q)$ , define

$$F_\mu(q) = \#\{(s, t) \in \mathcal{T}_{(n)}(q) \times \mathcal{T}_{(n-1,1)}(q) : st = x\}. \quad (7.3.3)$$

Even though the conjugation action of  $\mathrm{GL}_n \mathbb{F}_q$  on itself is not necessarily transitive on  $\mathcal{T}_{(n)}(q)$ ,  $\mathcal{T}_{(n-1,1)}(q)$ , or  $\mathcal{T}_\mu^\square(q)$ , we still have that  $F_\mu(q)$  is well-defined, as we will prove below. Perhaps more unexpectedly, we will also show that  $F_\mu(q)$  only depends on  $n$ ,  $q$ , and the parity of  $n - \ell(\mu)$ .

**Theorem 7.3.2.** *For all  $n \in \mathbb{N}$ ,  $\mu \vdash n$ , and prime powers  $q$ , we have*

$$F_\mu(q) = \frac{\#\mathcal{T}_{(n)}(q) \cdot \#\mathcal{T}_{(n-1,1)}(q)}{\#\mathrm{GL}_n \mathbb{F}_q} \left( 1 - \frac{(-1)^{n-\ell(\mu)}}{q^{\binom{n}{2}}} \right). \quad (7.3.4)$$

Compare 7.3.4 to the rephrasing

$$F_\mu = \frac{\#\mathcal{C}_{(n)} \cdot \#\mathcal{C}_{(n-1,1)}}{\#\mathfrak{S}_n} (1 - (-1)^{n-\ell(\mu)}) \quad (7.3.5)$$

of Boccara's result. In particular, the rightmost factors agree in the limit  $q \rightarrow 1$ . However, in the case when  $n - \ell(\mu)$  is even, there are zero such factorizations in the symmetric group, whereas there can be a nonzero number of such factorizations in  $\mathrm{GL}_n \mathbb{F}_q$ .

*Proof of Thm. 7.3.2.* Fix an arbitrary element  $x \in \mathcal{T}_\mu^\square(q)$ . Applying Theorem 2.1.1, we have

$$F_\mu(q) = \frac{1}{\#\mathrm{GL}_n \mathbb{F}_q} \sum_{\chi \in \mathrm{Irr} \mathrm{GL}_n \mathbb{F}_q} \frac{\chi(x^{-1})}{\deg \chi} \left( \sum_{g \in \mathcal{T}_{(n)}(q)} \chi(g) \right) \left( \sum_{h \in \mathcal{T}_{(n-1,1)}(q)} \chi(h) \right). \quad (7.3.6)$$

The simplifications that occur in the proof of Theorem 1.2.1 also occur in (7.3.6). Specifically, only the characters  $\chi^{z^{-1} \mapsto (n)}$  and  $\chi^{z^{-1} \mapsto (1^n)}$  correspond to non-vanishing summands in (7.3.6).

Note also that  $x^{-1} \in \mathcal{T}_\mu^\square(q)$ , as inversion does not affect cycle type. Applying Corollary 2.2.1, Theorem 3.3.1, and Theorem 3.2.1 gives

$$F_\mu(q) = \frac{\#\mathcal{T}_{(n)}(q) \cdot \#\mathcal{T}_{(n-1,1)}(q)}{\#\mathrm{GL}_n \mathbb{F}_q} \left( 1 - \frac{\chi_\mu^{(1^n)}}{q^{\binom{n}{2}}} \right). \quad (7.3.7)$$

Finally,  $\chi^{(1^n)}$  is the sign character, and the sign of a permutation with cycle type  $\mu$  is  $(-1)^{n-\ell(\mu)}$ .  $\square$

We can relax the condition that  $x$  is regular semisimple to obtain a more general result which is still quite concise. For  $x \in \mathrm{GL}_n \mathbb{F}_q$ , define

$$F_x(q) = \#\{(s, t) \in \mathcal{T}_{(n)}(q) \times \mathcal{T}_{(n-1,1)}(q) : st = x\}. \quad (7.3.8)$$

Let  $\mathrm{St} = \chi^{z^{-1} \rightarrow (1^n)}$  denote the **Steinberg character** of  $\mathrm{GL}_n \mathbb{F}_q$ , described geometrically by Steinberg in Section 3 of [33]. As the following result shows,  $F_x(q)$  depends only on  $n$ ,  $q$ , and the Steinberg character of  $x$ .

**Theorem 7.3.3.** *For all  $n \in \mathbb{N}$ , prime powers  $q$ , and  $x \in \mathrm{GL}_n \mathbb{F}_q$ , we have*

$$F_x(q) = \frac{\#\mathcal{T}_{(n)}(q) \cdot \#\mathcal{T}_{(n-1,1)}(q)}{\#\mathrm{GL}_n \mathbb{F}_q} \left( 1 - \frac{\mathrm{St}(x)}{q^{\binom{n}{2}}} \right). \quad (7.3.9)$$

*Proof.* The proof is almost identical to that of Theorem 7.3.2, except for the fact that the Steinberg character of an arbitrary element of  $\mathrm{GL}_n \mathbb{F}_q$  does not necessarily simplify to a sign depending on the cycle type of the element. Note that, when using (2.1.1), we technically need to plug in  $\mathrm{St}(x^{-1})$ . However, Steinberg's description [33, Thm. 3.1] of  $\mathrm{St}$  shows that  $\mathrm{St}(x^{-1}) = \mathrm{St}(x)$ .  $\square$

## 7.4 Open problems

In this section, we list some open problems. Of course, one can continue our present line of research by looking for explicit formulas for  $g_{k,\mu}(q)$  and  $g_{k,\mu}^\square(q)$  for cases not yet settled by this thesis. However, we also present the following problems associated with strengthening the existing results.

We start with the observation that Theorems 1.2.1 and 1.2.3 do not answer the question of how products of regular elliptic elements are distributed among the individual conjugacy classes that comprise the various cycle types. In particular, given a fixed regular elliptic element  $c \in \mathcal{T}_{(n)}$ , computing  $g_{k,(n)}(q)$  does not necessarily help one count the factorizations  $c = t_1 \cdots t_k$  with  $t_1, \dots, t_k \in \mathcal{T}_{(n)}$ . Therefore, we propose the following problem.

**Problem 7.4.1.** Refine Theorems 1.2.1 and 1.2.3 to the level of conjugacy classes.

Next, we recall Corollary 1.2.8, which says if  $n$  is prime, then  $g_{k,(n)}(q)$  is a quasipolynomial. Data suggest that, if  $n$  is not prime,  $g_{k,(n)}(q)$  still agrees with a polynomial at least on the set of prime powers congruent to 1 modulo  $n$ . This is a considerably weaker result, but it suggests  $g_{k,(n)}(q)$  might have some nice structure, even though Remark 6.1.3 points out that we cannot expect quasipolynomiality in general.

**Problem 7.4.2.** Prove that, even when  $n$  is not prime, there exists a polynomial  $f_1 \in \mathbb{Q}[x]$ , such that  $g_{k,(n)}(q) = f_1(q)$  for all prime powers  $q \equiv 1 \pmod{n}$ .

Still on the topic of quasipolynomials, we recall Example 6.1.4. The coefficients of the polynomial  $P(x)$  in Example 6.1.4 form a unimodal sequence of positive integers with no internal zeros. Based on the data presented in the appendix, we believe that the coefficients approximately form a bell curve in general.

**Problem 7.4.3.** Suppose  $n, k \in \mathbb{N}$  with  $n$  prime and

$$\sum_{q \geq 0} g_{k,(n)}(q)x^q = \frac{P(x)}{Q(x)},$$

where  $P$  and  $Q$  are relatively prime and the leading coefficient of  $P$  is positive. Find a mean  $\mu$ , a standard deviation  $\sigma$ , and a scaling factor  $\alpha$  such that

$$[x^m]P(x) \approx \frac{\alpha}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{m-\mu}{\sigma}\right)^2}$$

for each  $m \in \{0, \dots, \deg P\}$ , where  $[x^m]P(x)$  denotes the coefficient of  $x^m$  in  $P(x)$ .

We conclude with a problem about  $q$ -analogues. As noted by (1.2.6), for some choices of  $\mu \vdash n$  and after appropriately normalizing,  $g_{k,\mu}^\square(q)$  appears to be a  $q$ -analogue of  $g_{k,\mu}$  in the traditional  $q \rightarrow 1$  sense. Unfortunately, it is not clear whether  $g_{k,(n)}(q)$  exhibits the same behavior.

**Problem 7.4.4.** Establish a precise way in which  $g_{k,(n)}(q)$  is a  $q$ -analogue of  $g_{k,(n)}$ .

## 7.5 Conclusion

We have now reached a temporary end. In this thesis, we have shown how the linear algebra of regular semisimple elements leads us to simplified formulas for some  $\mathrm{GL}_n \mathbb{F}_q$  character values. Furthermore, our definition of cycle type for matrices allows us to see a connection between the character theory of  $\mathrm{GL}_n \mathbb{F}_q$  and that of  $\mathfrak{S}_n$ . Our character formula then allows us to count the number of tuples of regular elliptic elements whose product has a given cycle type. Even though we are coarsening the usual notion of factorization enumeration, we see an analogy between the results for  $\mathrm{GL}_n \mathbb{F}_q$  and those for  $\mathfrak{S}_n$ . We sincerely hope that the interested reader will continue investigating this analogy.

## BIBLIOGRAPHY

- [1] E. A. Bertram and V. K. Wei. Decomposing a permutation into two large cycles: an enumeration. *SIAM J. Algebraic Discrete Methods*, 1(4):450–461, 1980.
- [2] G. Boccara. Nombre de représentations d’une permutation comme produit de deux cycles de longueurs données. *Discrete Math.*, 29(2):105–134, 1980.
- [3] M. Bóna and B. Pittel. On the cycle structure of the product of random maximal cycles. *Séminaire Lotharingien de Combinatoire*, B80b, 2019.
- [4] L. Brickman and P. A. Fillmore. The invariant subspace lattice of a linear transformation. *Canad. J. Math.*, 19:810–822, 1967.
- [5] A. Cayley. A theorem on trees. *Quart. J. Math.*, 23:376–378, 1889.
- [6] G. Chapuy and C. Stump. Counting factorizations of coxeter elements into products of reflections. *Journal of the London Mathematical Society*, 90(3), 2014.
- [7] J. Dénes. The representation of a permutation as the product of a minimal number of transpositions and its connection with the theory of graphs. *Publ. Math. Inst. Hungar. Acad. Sci.*, 4:63–70, 1959.
- [8] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.
- [9] R. Ekedahl, S. Lando, M. Shapiro, and A. Vainshtein. Hurwitz numbers and intersections on moduli spaces of curves. *Invent. Math.*, 146(2):297–327, 2001.
- [10] F. G. Frobenius. *Gesammelte Abhandlungen. Bände I, II, III*. Herausgegeben von J.-P. Serre. Springer-Verlag, Berlin-New York, 1968.
- [11] J. Fulman. Cycle indices for the finite classical groups. *J. Group Theory*, 2(3):251–289, 1999.
- [12] W. Fulton. *Young tableaux*, volume 35 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1997.

- [13] W. Fulton and J. Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991.
- [14] C. F. Gauss. *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik*. Deutsch hrsg. von H. Mas. 1889.
- [15] I. P. Goulden and D. M. Jackson. The combinatorial relationship between trees, cacti and certain connection coefficients for the symmetric group. *European J. Combin.*, 13(5):357–365, 1992.
- [16] J. A. Green. The characters of the finite general linear groups. *Trans. Amer. Math. Soc.*, 80:402–447, 1955.
- [17] J. Huang, J. B. Lewis, and V. Reiner. Absolute order in general linear groups. *J. Lond. Math. Soc. (2)*, 95(1):223–247, 2017.
- [18] A. Hurwitz. Ueber riemann'sche flächen mit gegebenen verzweigungspunkten. *Mathematische Annalen*, 39:1–61, 1891.
- [19] D. M. Jackson. Counting cycles in permutations by group characters, with an application to a topological problem. *Trans. Amer. Math. Soc.*, 299(2):785–801, 1987.
- [20] J. P. S. Kung. The cycle structure of a linear transformation over a finite field. *Linear Algebra Appl.*, 36:141–155, 1981.
- [21] S. K. Lando and A. K. Zvonkin. *Graphs on surfaces and their applications*, volume 141 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2004. With an appendix by Don B. Zagier.
- [22] G. I. Lehrer. The cohomology of the regular semisimple variety. *J. Algebra*, 199(2):666–689, 1998.
- [23] J. B. Lewis and A. H. Morales.  $GL_n(\mathbb{F}_q)$ -analogues of factorization problems in the symmetric group. *European J. Combin.*, 58:75–95, 2016.
- [24] J. B. Lewis, V. Reiner, and D. Stanton. Reflection factorizations of Singer cycles. *J. Algebraic Combin.*, 40(3):663–691, 2014.
- [25] I. G. Macdonald. *Symmetric functions and Hall polynomials*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, second edition, 1995.

- [26] F. D. Murnaghan. On the representations of the symmetric group. *American Journal of Mathematics*, 59(3):437–488, 1937.
- [27] T. Nakayama. On some modular properties of irreducible representations of a symmetric group. i. *Jap. J. Math.*, 18, 04 2011.
- [28] B. E. Sagan. *The symmetric group*, volume 203 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2001.
- [29] J.-P. Serre. *Linear representations of finite groups*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, Vol. 42.
- [30] R. P. Stanley. Factorization of permutations into  $n$ -cycles. *Discrete Math.*, 37(2-3):255–262, 1981.
- [31] R. P. Stanley. *Enumerative combinatorics. Vol. 2*, volume 62 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1999. With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin.
- [32] R. P. Stanley. *Enumerative combinatorics. Volume 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2012.
- [33] R. Steinberg. A geometric approach to the representations of the full linear group over a Galois field. *Trans. Amer. Math. Soc.*, 71:274–282, 1951.
- [34] R. Stong. Some asymptotic results on finite vector spaces. *Adv. in Appl. Math.*, 9(2):167–199, 1988.
- [35] R. Vakil. Genus 0 and 1 Hurwitz numbers: recursions, formulas, and graph-theoretic interpretations. *Trans. Amer. Math. Soc.*, 353(10):4025–4038, 2001.
- [36] D. W. Walkup. How many ways can a permutation be factored into two  $n$ -cycles? *Discrete Math.*, 28(3):315–319, 1979.

## Appendix A

### QUASIPOLYNOMIAL DATA

In this appendix, we record examples of generating functions  $\sum_{q \geq 0} g_{k,(n)}(q)x^q = \frac{P(x)}{Q(x)}$  for various values of  $n$  and  $k$ . The polynomial  $Q$  is given in a factored form. The coefficients of  $P$  are listed, starting with the coefficient of the constant term, and proceeding from there in the order of increasing degree, including any zero coefficients along the way. A plot of coefficient of  $x^i$  in  $P$  vs.  $i$  is shown as well.

#### **A.1 Data for $n = 2$**

For  $k = 2$ ,  $Q(x) = (1 - x^2)^6(1 - x)^3$ , and the coefficients of  $P$  are 0, 0, 2, 90, 1434, 8322, 29412, 59820, 83660, 74172, 45042, 16602, 3642, 354, 8. See Figure A.1.

For  $k = 3$ ,  $Q(x) = (1 - x^2)^9(1 - x)^4$ , and the coefficients of  $P$  are 0, 0, 6, 2544, 150414, 2832552, 25864692, 140466432, 502153236, 1262969136, 2308097520, 3146061600, 3215949120, 2480195520, 1423451052, 600444672, 178803084, 35932752, 4388970, 281328, 6546, 24. See Figure A.2.

For  $k = 4$ ,  $Q(x) = (1 - x^2)^{12}(1 - x)^5$ , and the coefficients of  $P$  are 0, 0, 10, 38350, 10414444, 608226420, 14168512632, 175712777880, 1359028234964, 7189130779340, 27593939185010, 79866092451990, 179001772796760, 316162090064040, 445266739098912, 503209113122880, 457500147989256, 333960316977720, 194620759471662, 89553926081850, 32008285385660, 8665260706340, 1714167755240, 234448638120, 20388456804, 978049980, 20333782, 113890, 64. See Figure A.3.

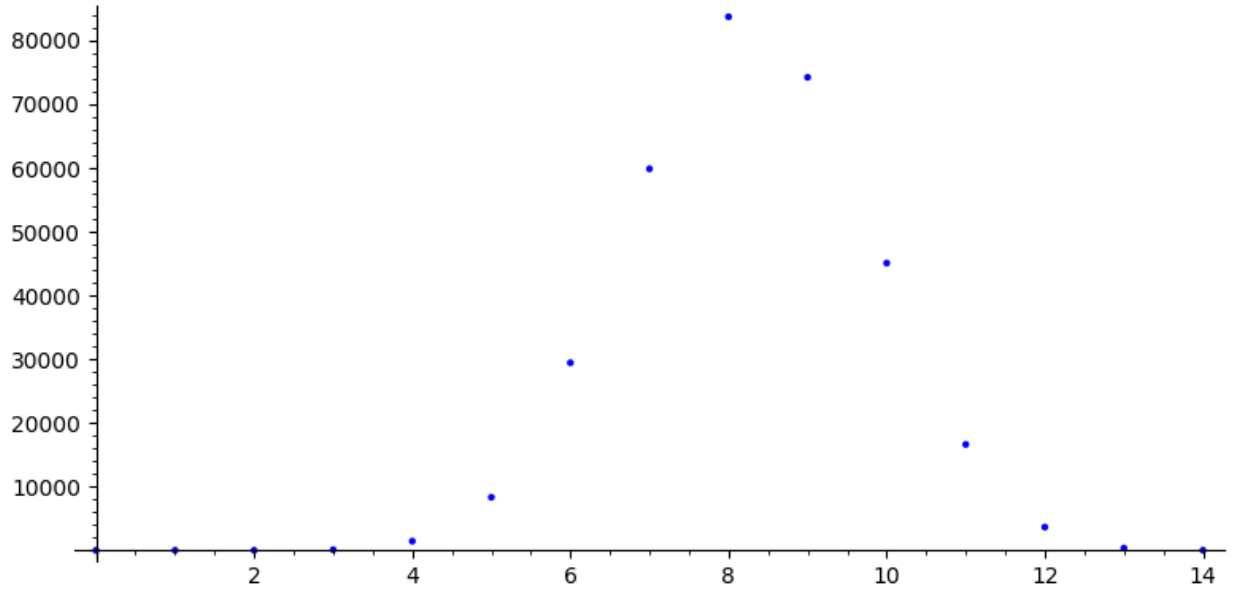
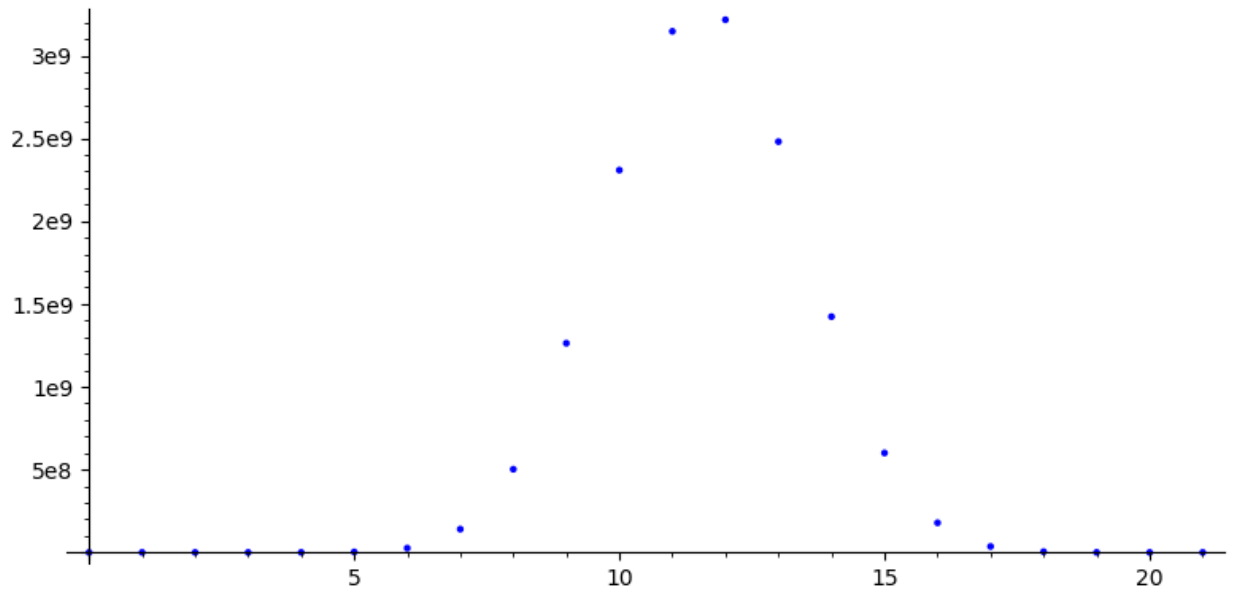
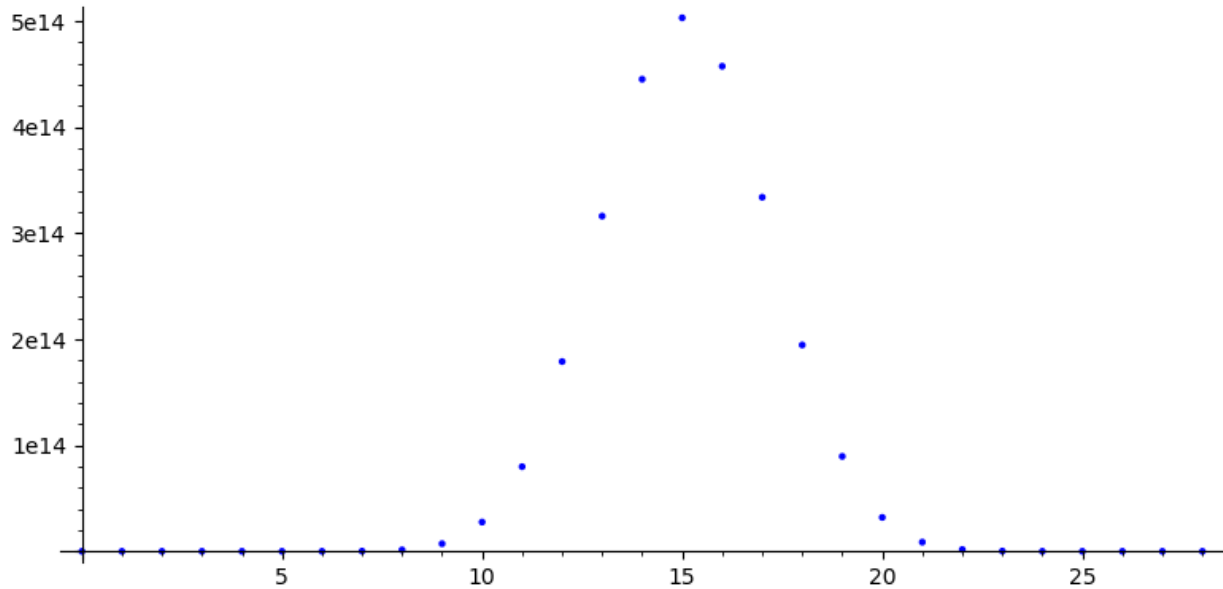
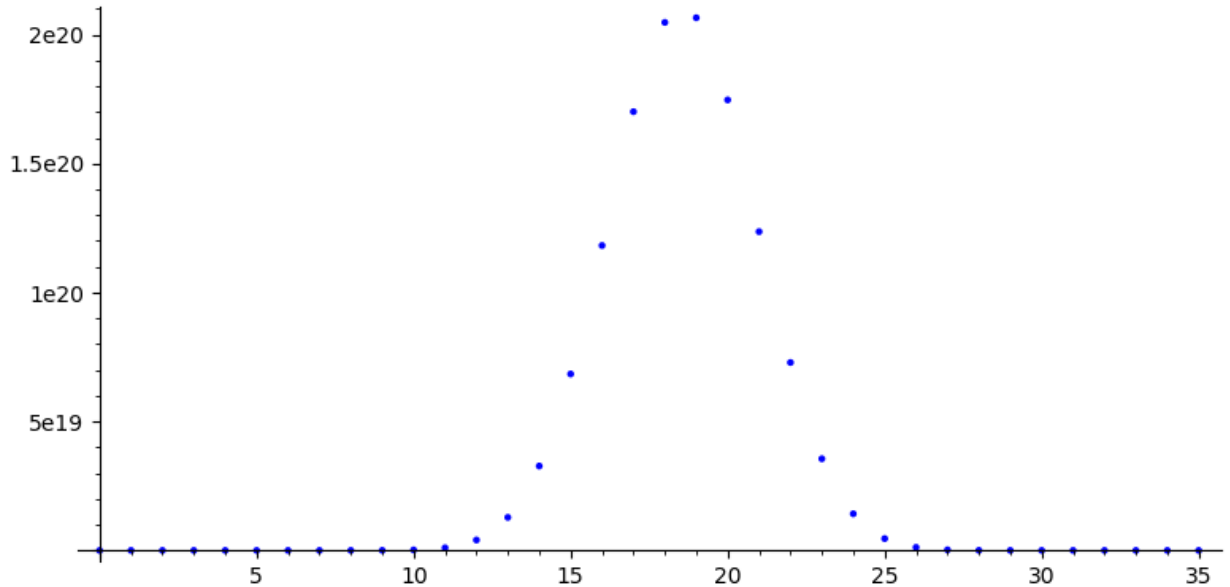
Figure A.1: Coefficients of numerator of rational generating function of  $g_{2,(2)}(q)$ Figure A.2: Coefficients of numerator of rational generating function of  $g_{3,(2)}(q)$ 

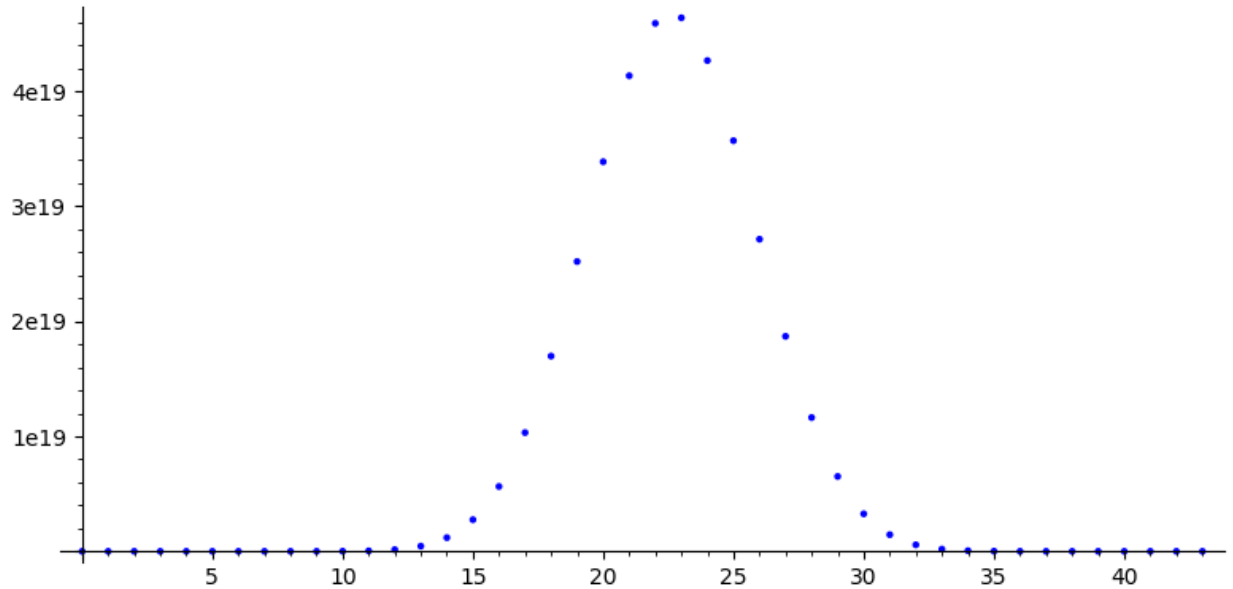
Figure A.3: Coefficients of numerator of rational generating function of  $g_{4,(2)}(q)$ 

For  $k = 5$ ,  $Q(x) = (1 - x^2)^{15}(1 - x)^6$ , and the coefficients of  $P$  are 0, 0, 22, 722076, 772955712, 128895748100, 7113196076580, 186185192181540, 2821166484082240, 27914903731981020, 194868608963338380, 1011146575197785180, 4044973921849149504, 12807657628009994532, 32720060506126369684, 68402486801160416100, 118214578961592475200, 170100697429290881180, 204711463903343925240, 206518973263930864980, 174663992843955550400, 123594025389379779180, 72858013207345228716, 35537158452596834188, 14201405061882768576, 4586821462617793140, 1175293807895064020, 232926581602773780, 34469329482006720, 3623187421921900, 251290432088220, 10267293455340, 205335267008, 1458218004, 1983378, 160. See Figure A.4.

Figure A.4: Coefficients of numerator of rational generating function of  $g_{5,(2)}(q)$ 

## A.2 Data for $n = 3$

For  $k = 2$ ,  $Q(x) = (1 - x^3)^{13}(1 - x)^6$ , and the coefficients of  $P$  are 0, 0, 576, 3487104, 995388480, 66386400192, 1816248953088, 27125979668928, 261737561606400, 1813767573036672, 9669691551539376, 41532287665475808, 148403559193309008, 451499431480807248, 1189785214909606320, 2751138536902718544, 5638002591179705040, 10319295977723754864, 16970050077793777152, 25189719513355720368, 33865829454550516128, 41340728524729171680, 45896375743258265280, 46378534302546967008, 42661341904789192608, 35697645276759381312, 27132996255738454368, 18690609179461576032, 11630774662212698496, 6509791332415545120, 3258739979140088736, 1448333293777130880, 566132036975667360, 192252030581100384, 55804817320881552, 13547625823376640, 2669199317633232, 408776928143472, 45647662380912, 3366706340880, 139830633072, 2491601904, 10968480, 1296. See Figure A.5

Figure A.5: Coefficients of numerator of rational generating function of  $g_{2,(3)}(q)$ 

For  $k = 3$ ,  $Q(x) = (1-x^3)^{20}(1-x)^8$ , and the coefficients of  $P$  are 0, 0, 33408, 12807129600, 60732485073792, 35230443538066944, 5751069208789094016, 396372370803872934912, 14565485088749017611264, 331287773817974177312256, 5164664253028761792192528, 59345878165100567955434880, 530042105333112870200804928, 3827963695106401693248529728, 23033398007261025364752423648, 118163520472739717810252366208, 526222228958639808980307218208, 2063627723728819667700182377728, 7209025603683282286447669928208, 22645765031715215742334094474688, 64465342513613023381229811820608, 167375032238213009955711751290048, 398493592331704537780131670450944, 873955472356301312462703639735168, 1772393208775467039719454937702752, 3334599077236439236946990279493696, 5836241603643442941022124088314880, 9524366699946308990588582638301376, 14521019544708878989865182674561696,

20716575767814624166242927618662016, 27693129752796547895455052008194816,  
 34722894346023510012510878586278976, 40869409192992000274867169460116928,  
 45182143896761338642148769085436736, 46932328521380851237700375602871904,  
 45811122337635337116552824501803392, 42017201261409359994480100783115040,  
 36200190282430276493183532844013376, 29281703709722867677118663595473472,  
 22220697584423997158314538128868928, 15803845675889183531178023573646624,  
 10521191385484220351017015115875200, 6546239185430941815755901050957664,  
 3799546189022040230738915884252224, 2052650255472844456300094387519424,  
 1029417617943875232198829193166144, 477751807608845255235343038887424,  
 204428604680792646585817350400128, 80299085708826231920541790483104,  
 28804184411367570076630992807360, 9377531907325293321832064927616,  
 2750307894432086389186949474112, 720151612193973660772094988768,  
 166506906822251270060407476096, 33533774462837070154550024064,  
 5782815647921459297887561152, 835467146045804943735359040,  
 98307024171677836854052032, 9077151349798831320542352, 625730591516637659718912,  
 30087576136521408476832, 917750599874336683392, 15473907288023747808,  
 116605988831180352, 273407270840256, 97104493440, 944784. See Figure A.6.

Beyond this point, the values are too large to present conveniently in this appendix. However, we hope that the data presented is sufficient for the reader to make comparisons with their own calculations.

Figure A.6: Coefficients of numerator of rational generating function of  $g_{3,(3)}(q)$ 