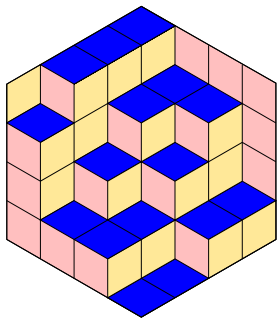


ALGEBRAIC COMBINATORICS

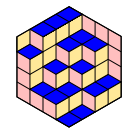
Graham Gordon

Cycle type factorizations in $\mathrm{GL}_n\mathbb{F}_q$

Volume 5, issue 6 (2022), p. 1427-1459.
https://doi.org/10.5802/alco.259

Algebraic Combinatorics is published by The Combinatorics Consortium and is a member of the Centre Mersenne for Open Scientific Publishing
www.tccpublishing.org www.centre-mersenne.org
e-ISSN: 2589-5486

Algebraic Combinatorics
Volume 5, issue 6 (2022), p. 1427–1459
https://doi.org/10.5802/alco.259



Cycle type factorizations in $\mathrm{GL}_n\mathbb{F}_q$

Graham Gordon

Abstract 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 cases, we provide explicit formulas. Our main tool is a standard character-theoretic technique due to Frobenius, which we make use of by finding simplified formulas for the necessary character values. For every case in which we are not able to compute an explicit formula, we at least determine the asymptotic behavior. We conclude with some results about the polynomiality of our enumerative formulas and some open problems.

1. Introduction

Factorization enumeration has a long, ongoing history filled with interesting combinatorics and topology [3, 5, 6, 8, 14, 17, 33]. For example, in [28], Stanley enumerated 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 introduce some notation in order to state Stanley's result. For each partition $\mu \vdash n$, let $\mathcal{C}_\mu \subset \mathfrak{S}_n$ denote the conjugacy class consisting of permutations with cycle type μ. Let $m_i(\mu)$ denote the multiplicity of i in μ. For $\lambda \vdash n$, let χ^λ_μ denote the irreducible character χ^λ of $\mathfrak{S}_n$ corresponding to λ evaluated on an element of $\mathcal{C}_\mu$. Let $\mathbb{N} = \{1, 2, 3, \ldots\}$ denote the positive integers. For any $\mu \vdash n$ and $k \in \mathbb{N}$, define

$$g_{k,\mu} = \#\{(t_1, \ldots, t_k) \in \mathcal{C}^k_{(n)} : t_1 \cdots t_k \in \mathcal{C}_\mu\}. \tag{1}$$

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

Manuscript received 9th February 2020, revised 14th February 2022 and 8th May 2022, accepted 7th August 2022.

Keywords. factorization enumeration, cycle type, q-analogues.

Acknowledgements. The author was partially supported by the National Science Foundation grant DMS-1764012.

Theorem 1.1 (Stanley [28, Theorem 3.1]). *For all $n, k \in \mathbb{N}$ and $\mu \vdash n$, the number of ordered k-tuples of n-cycles whose product has cycle type μ is*

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

and, more explicitly,

$$\frac{g_{k,\mu}}{\#\mathcal{C}_\mu} = \frac{(n-1)!^{k-1}}{n} \sum_{r=0}^{n-1} \frac{(-1)^{rk}}{\binom{n-1}{r}^{k-1}} \sum_{\nu \vdash r} (-1)^{\sum_{a \geqslant 1} m_{2a}(\nu)} \binom{m_1(\mu)-1}{m_1(\nu)} \prod_{j=2}^{r} \binom{m_j(\mu)}{m_j(\nu)}. \tag{3}$$

Theorem 1.1 was proved using a character-theoretic technique due to Frobenius which we describe in Section 2.1. The simplicity of (2) comes from the fact that $\chi_{(n)}^\lambda = 0$ unless λ is a **hook**, i.e., $\lambda = (n-r, 1^r)$ for some $r \in \{0, \ldots, n-1\}$ (see Corollary 2.3). The more explicit phrasing (3) is obtained by evaluating the hook characters explicitly [28, Lemma 2.2]. For some historical context, see the work of Bertram–Wei [1], Boccara [2], and Walkup [34]. In all three papers, the authors developed formulas enumerating factorizations of permutations into products of two cycles of various lengths. The use of character theory appears in [1, Section 3], and their results coincide with Stanley's in some cases. 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.

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. Given a matrix $g \in \mathrm{GL}_n \mathbb{F}_q$, we define the **cycle type** of g to be $\mu = (\mu_1, \ldots, \mu_\ell) \vdash n$ if the degrees of the irreducible factors of the characteristic polynomial of g are $\mu_1, \ldots, \mu_\ell$ in weakly decreasing order, and we write $\mathrm{type}(g) = \mu$. This definition is built on work by Kung [18] and Stong [32] which suggests 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 $\mathfrak{S}_n$. 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 μ. Note that $\{\mathcal{T}_\mu(q) : \mu \vdash n\}$ is a partition of $\mathrm{GL}_n \mathbb{F}_q$.

Recent work by Huang, Lewis, Morales, Reiner, and Stanton [16, 21, 22] investigated the **regular elliptic** elements of $\mathrm{GL}_n \mathbb{F}_q$, which are those matrices whose characteristic polynomial is irreducible over $\mathbb{F}_q$. Their work suggests that the regular elliptic elements are analogous to the n-cycles in $\mathfrak{S}_n$ from the perspective of enumerating factorizations. This agrees with our definition of cycle type, as both the n-cycles of $\mathfrak{S}_n$ and the regular elliptic elements of $\mathrm{GL}_n \mathbb{F}_q$ have cycle type (n).

We also consider the **regular semisimple** elements of $\mathrm{GL}_n \mathbb{F}_q$, which are those matrices whose characteristic polynomial has no repeated irreducible factors. Let $\mathcal{T}_\mu^\square(q)$ denote the set of regular semisimple elements with cycle type μ. 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 for $n \geqslant 2$. 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_μ denote the cardinality of the centralizer of an element of $\mathcal{C}_\mu$ in $\mathfrak{S}_n$.

Corollary 1.2 (to Corollary 2.16). *For all $n \in \mathbb{N}$ and $\mu \vdash n$,*

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

In analogy with (1), we define for any $\mu \vdash n, k \in \mathbb{N}$, and prime power q,

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

In this paper, we consider the quantities $g_{k,\mu}(q)$ and $g^{\square}_{k,\mu}(q)$ to be $\mathrm{GL}_n\,\mathbb{F}_q$-analogues of $g_{k,\mu}$, and we seek simple formulas for computing them. Note that $g_{k,\mu}(q) = g^{\square}_{k,\mu}(q)$ if all the parts of μ are distinct. Furthermore, as suggested by Corollary 1.2 and proved in Theorem 1.8 below, $g_{k,\mu}(q)$ and $g^{\square}_{k,\mu}(q)$ have the same asymptotic behavior as $q \to \infty$.

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

$$[m]_q = 1 + q + q^2 + \cdots + q^{m-1}, \tag{4}$$

$$[m]_q! = \prod_{\ell=1}^{m} [\ell]_q, \quad \text{and} \tag{5}$$

$$\begin{bmatrix} m \\ \ell \end{bmatrix}_q = \frac{[m]_q!}{[\ell]_q![m-\ell]_q!}, \tag{6}$$

each of which is an integer polynomial in q, for non-negative integers $\ell \leqslant m$.

Theorem 1.3. *For all $n, k \in \mathbb{N}$ with $n > 2$, all prime powers q, and all $\mu \vdash n$ with $m_1(\mu) = 1$, we have*

$$g^{\square}_{k,\mu}(q) = \frac{\#\mathcal{T}_{(n)}(q)^k \cdot \#\mathcal{T}^{\square}_\mu(q)}{\#\,\mathrm{GL}_n\,\mathbb{F}_q} \cdot \sum_{r=0}^{n-1} \frac{(-1)^{rk}\chi_\mu^{(n-r,1^r)}}{\left(q^{\binom{r+1}{2}} \cdot \begin{bmatrix} n-1 \\ r \end{bmatrix}_q\right)^{k-1}}. \tag{7}$$

Compare (7) with the analogous formula (2) from the symmetric group. As one particular consequence, it follows that, for the cases of μ discussed in Theorem 1.3, we have

$$\lim_{q\to 1} \frac{g^{\square}_{k,\mu}(q) \cdot \#\,\mathrm{GL}_n\,\mathbb{F}_q}{\#\mathcal{T}^{\square}_\mu(q) \cdot \#\mathcal{T}_{(n)}(q)^k} = \frac{g_{k,\mu} \cdot \#\mathfrak{S}_n}{\#\mathcal{C}_\mu \cdot \#\mathcal{C}^k_{(n)}}, \tag{8}$$

where the limit is taken after substituting for each term on the left side the rational function which agrees with it on prime powers. Equation (8) gives some justification that $g^{\square}_{k,\mu}(q)$ is a q-analogue of $g_{k,\mu}$ in the traditional $q \to 1$ sense.

The following special case of Theorem 1.3 is especially simple.

Corollary 1.4. *For all $n, k \in \mathbb{N}$ with $n > 2$ and all prime powers q, we have*

$$g_{k,(n-1,1)}(q) = g^{\square}_{k,(n-1,1)}(q) = \frac{\#\mathcal{T}_{(n)}(q)^k \cdot \#\mathcal{T}_{(n-1,1)}(q)}{\#\,\mathrm{GL}_n\,\mathbb{F}_q} \cdot \left(1 + \frac{(-1)^{nk-n-k}}{q^{\binom{n}{2}(k-1)}}\right). \tag{9}$$

Compare (9) with the analogous formula

$$g_{k,(n-1,1)} = \frac{\#\mathcal{C}^k_{(n)} \cdot \#\mathcal{C}_{(n-1,1)}}{\#\mathfrak{S}_n} \cdot \left(1 + (-1)^{nk-n-k}\right) \tag{10}$$

from the symmetric group. Observe that (10) is zero unless both n and k are even, which can be proved by comparing the sign of an $(n-1)$-cycle with the sign of a k-fold product of n-cycles. Interestingly, this behavior is not mimicked by (9), highlighting a fundamental difference between cycle type in $\mathrm{GL}_n\,\mathbb{F}_q$ and cycle type in $\mathfrak{S}_n$.

Our second main 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 μ. The rest of the necessary notation is contained in Table 1 below.

THEOREM 1.5. *For all $n, k \in \mathbb{N}$ and prime powers q, we have*

$$g_{k,(n)}(q) = P_{n,k+1}(q) \sum_{d|n} (-1)^{n(k+1)/d} d^k D_{n,k+1,d}(q) \sum_{c|d} \boldsymbol{\mu}(d/c) C_{n,k+1,c}(q), \tag{11}$$

using the notation in Table 1.

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

$$g_{k,(n)} = \frac{(n-1)!^k}{n} \sum_{r=0}^{n-1} \left(\frac{(-1)^r}{\binom{n-1}{r}} \right)^{k-1}. \tag{12}$$

Unfortunately, it is not immediately obvious how to compare (11) with (12).

TABLE 1. Functions and their values for $n \in \mathbb{N}$, $d \mid n$, $c \mid d$, and prime powers q. The lcm in the denominator of $C_{n,k,c}(q)$ is computed in $\mathbb{Z}$.

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

REMARK 1.6. There are many cases not addressed by Theorems 1.3 and 1.5. 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.

Our approach to proving Theorems 1.3 and 1.5 is to apply the same character-theoretic technique due to Frobenius that Stanley used in [28]. Fortunately, Green explicitly computed all characters of the finite general linear groups [15]. Using Green's results, we prove the following formula for evaluating **primary** characters of $\mathrm{GL}_n \mathbb{F}_q$ on regular semisimple elements. See Sections 2 and 3 for missing notation. In particular, primary characters are denoted $\chi^{f \mapsto \lambda}$, where $f \in \mathbb{F}_q[z] \smallsetminus \{z\}$ is monic, irreducible, and non-constant, and λ is a partition such that $|\lambda| \cdot \deg f = n$. Also note that $\ell_f \in \mathbb{Z}$ and the codomain of the function θ is $\mathbb{C}^\times$.

THEOREM 1.7. *Suppose $n \in \mathbb{N}$, $d \mid n$, $\lambda \vdash n/d$, q is a prime power, $f \in \mathcal{F}_d(q)$, $\mu \vdash n$, $g \in \mathcal{T}_\mu^\square(q)$, and $h_1, \ldots, h_{\ell(\mu)}$ are the distinct irreducible factors of the characteristic polynomial of g. If some part of μ 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*

$$\chi^{f \mapsto \lambda}(g) = (-1)^{\frac{n}{d}(d-1)} \chi_{\tilde{\mu}}^{\lambda} \prod_{i=1}^{\ell(\mu)} \frac{1}{\tilde{\mu}_i} \sum_{\substack{\beta_i \in \mathbb{F}_{q^{\mu_i}} \\ h_i(\beta_i)=0}} \theta(\beta_i)^{\ell_f \cdot [\tilde{\mu}_i]_{q^d}}. \tag{13}$$

Theorem 1.7 also enables us to determine the asymptotic behavior of $g_{k,\mu}(q)$. We define

$$p_{k,\mu}(q) = \frac{g_{k,\mu}(q)}{\#\mathcal{T}_{(n)}(q)^k}, \tag{14}$$

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 $k \geqslant 2$. Of course, Theorems 1.3 and 1.5 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

$$p^{\square}_{k,\mu}(q) = \frac{g^{\square}_{k,\mu}(q)}{\#\mathcal{T}_{(n)}(q)^k} \tag{15}$$

Again, Theorems 1.3 and 1.5 provide exact formulas for $p^{\square}_{k,\mu}(q)$ in some special cases. However, we are able to compute $\lim_{q\to\infty} p_{k,\mu}(q)$ and $\lim_{q\to\infty} p^{\square}_{k,\mu}(q)$ for all $\mu \vdash n$.

Theorem 1.8. *For all $n, k \in \mathbb{N}$ with $k \geqslant 2$ and $\mu \vdash n$, we have*

$$\lim_{q\to\infty} p_{k,\mu}(q) = \lim_{q\to\infty} p^{\square}_{k,\mu}(q) = \frac{1}{z_\mu}. \tag{16}$$

In light of Corollary 1.2, one interpretation of Theorem 1.8 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 1.8 describes the asymptotics of $g_{k,\mu}(q)$ as $q \to \infty$, it does not address the specific behavior of $g_{k,\mu}(q)$ for small q. It turns out that Theorem 1.3 gives a family of examples where the function $g^{\square}_{k,\mu}(q)$ is a polynomial in q—see Corollary 6.1. However, $g_{k,(n)}(q)$ is not necessarily a polynomial, or even rational, function of q. This is because the lcm function in $C_{n,k,c}(q)$ is not rational. Instead, we have the following result.

Corollary 1.9 (to Theorem 1.5). *Suppose $n, k \in \mathbb{N}$ and n is prime. There exist polynomials $f_0, f_1, \ldots, f_{n-1} \in \mathbb{Q}[x]$ depending only on n and k with the property that, for each $i \in \{0, \ldots, n-1\}$, we have*

$$g_{k,(n)}(q) = f_i(q) \quad \text{for all prime powers } q \equiv i \pmod{n}. \tag{17}$$

In other words, $g_{k,(n)}(q)$ is a quasipolynomial function of q.

The rest of the paper is organized as follows. In Section 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 Section 3, we provide a concise retelling of Green's original formulation of the characters of the finite general linear groups [15]. In Section 4, we prove Theorems 1.3 and 1.5, our main enumerative results. In Section 5, we prove Theorem 1.8, our main asymptotic result. In Section 6, we discuss polynomiality, prove Corollary 1.9, and list some open problems.

2. Preliminaries

2.1. The character theory approach. We assume basic knowledge of the ordinary complex character theory of finite groups, as in Fulton–Harris [12] or Serre [27]. We will make use of a standard character-theoretic technique based on the following result due to Frobenius. For a straightforward proof, see Zagier's Appendix A

in Lando–Zvonkin [19]. Let G be a finite group, and let $\mathrm{Irr}(G)$ denote the set of all irreducible characters of G. For $\chi \in \mathrm{Irr}(G)$, let $\deg \chi$ denote the value of χ at the identity element of G.

THEOREM 2.1 (Frobenius [9]). *Let k be a positive integer, and, for each $i \in \{1, \ldots, k\}$, let A_i be a union of conjugacy classes in G. For any $g \in G$, the number of tuples $(t_1, \ldots, t_k) \in A_1 \times \cdots \times A_k$ such that $t_1 \cdots t_k = g$ is given by*

$$\frac{1}{\#G} \sum_{\chi \in \mathrm{Irr}(G)} (\deg \chi)^{1-k} \chi(g^{-1}) \prod_{i=1}^{k} \sum_{t \in A_i} \chi(t). \tag{18}$$

COROLLARY 2.2. *For all $n, k \in \mathbb{N}$, $\mu \vdash n$, and prime powers q,*

$$g_{k,\mu}(q) = \frac{1}{\#\,\mathrm{GL}_n \mathbb{F}_q} \sum_{\chi \in \mathrm{Irr}(\mathrm{GL}_n \mathbb{F}_q)} (\deg \chi)^{1-k} \left(\sum_{g \in \mathcal{T}_{(n)}(q)} \chi(g) \right)^k \left(\sum_{h \in \mathcal{T}_\mu(q)} \chi(h) \right). \tag{19}$$

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

Proof. Consider applying Theorem 2.1 to the case of $k+1$ factors, the first k of which are regular elliptic and the last of which has cycle type μ. Each $\mathcal{T}_\mu(q)$ is a union of conjugacy classes (see Section 2.4.2), and so the hypotheses of Theorem 2.1 are satisfied. Moreover, each $\mathcal{T}_\mu(q)$ is closed under taking inverses, implying factorizations of the form

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

are in bijection with factorizations of the form

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

Thus,

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

Applying Theorem 2.1 with

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

gives the result since $\chi(g) = \chi(\mathrm{id}) = \deg \chi$. The final claim regarding regular semisimple elements follows from the same argument. □

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 [29] and Sagan [26]. See also Fulton–Harris [12] or Fulton [11] for added discussion on the irreducible characters of the symmetric groups.

A **partition** of n is a weakly decreasing sequence of non-negative integers $\mu = (\mu_1, \mu_2, \ldots)$ such that $\sum_{i \geqslant 1} \mu_i = n$, denoted by $\mu \vdash n$. Denote by $\varnothing$ the unique partition of 0 and by $\square$ the unique partition of 1. Let Par denote the set of all partitions of all non-negative integers. Each μ_i is called a **part** of μ. The number of nonzero parts of μ is called the **length** of μ and is denoted by $\ell(\mu)$. The **conjugate** of μ is denoted by μ' and defined by $\mu'_i = \#\{j \geqslant 1 : \mu_j \geqslant i\}$ for all $i \geqslant 0$. The **multiplicity** of a positive integer i in a partition μ is defined as $\#\{j \geqslant 1 : \mu_j = i\}$ and denoted by $m_i(\mu)$. 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 $r \in \{0, \ldots, n-1\}$ is called a **hook**. An important statistic on partitions is $\mu \mapsto z_\mu$ defined by $z_\mu = \prod_{i \geqslant 1} i^{m_i(\mu)} \cdot m_i(\mu)!$. If d is a positive integer, then we use $d\mu$ to denote the partition $(d\mu_1, d\mu_2, \ldots)$ of dn.

The conjugacy classes of $\mathfrak{S}_n$ are in bijection with the partitions of n as follows. If $\pi = (\pi_{1,1}, \ldots, \pi_{1,\mu_1}) \cdots (\pi_{\ell,1}, \ldots, \pi_{\ell,\mu_\ell}) \in \mathfrak{S}_n$ is a cycle decomposition of π with $\mu_1 \geqslant \mu_2 \geqslant \cdots \geqslant \mu_\ell$, then the conjugacy class of π is indexed by the partition $\mu = (\mu_1, \mu_2, \ldots, \mu_\ell)$. The partition μ is called the **cycle type** of the permutation π. Let $\mathcal{C}_\mu$ denote the conjugacy class consisting of those permutations with cycle type μ. The statistic $\mu \mapsto z_\mu$ has the following algebraic interpretation. If $\sigma \in \mathfrak{S}_n$ has cycle type μ, then z_μ is the number of permutations in $\mathfrak{S}_n$ which commute with σ. By the orbit-stabilizer theorem [7, Proposition 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 χ^λ denote the character indexed by λ. Let χ^λ_μ denote χ^λ 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 [24, 25]. See [29, Theorem 7.17.3] for a full statement and proof. We will use the following two special cases.

Corollary 2.3 (to the MN rule). *For all $n \in \mathbb{N}$ and $\lambda \vdash n$, we have*

$$\chi^\lambda_{(n)} = \begin{cases} (-1)^r, & \lambda = (n-r, 1^r) \text{ for some } r \in \{0, \ldots, n-1\}, \\ 0, & \text{otherwise}, \end{cases} \tag{20}$$

and

$$\chi^\lambda_{(n-1,1)} = \begin{cases} 1, & \lambda = (n), \\ (-1)^n, & \lambda = (1^n), \\ (-1)^{r-1}, & \lambda = (n-r, 2, 1^{r-2}) \text{ for some } r \in \{2, \ldots, n-2\}, \\ 0, & \text{otherwise}. \end{cases} \tag{21}$$

2.3. Finite fields. We assume some basic knowledge about finite fields, all of which can be found in Dummit–Foote [7]. Let q be a prime power. 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 $m \mid m'$. 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 $m \mid m'$, we have that $\mathbb{F}^\times_{q^m}$ is a subgroup of $\mathbb{F}^\times_{q^{m'}}$.

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

$$\mathbb{F}^\times_{q^d} = \bigsqcup_{c \mid d} \bigsqcup_{f \in \mathcal{F}_c(q)} \{\alpha \in \mathbb{F}^\times_{q^c} : f(\alpha) = 0\}. \tag{22}$$

Proof. Every element of $\mathbb{F}^\times_{q^d}$ 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. □

For each $n \in \mathbb{N}$, fix a generator ϵ of the cyclic group $\mathbb{F}^\times_{q^{n!}}$, and fix an injective group homomorphism $\theta : \mathbb{F}^\times_{q^{n!}} \to \mathbb{C}^\times$ mapping $\epsilon \mapsto e^{2\pi i/(q^{n!}-1)}$. Note that we omit the dependence of ϵ on n and rely on context instead. For each $d \in \{1, \ldots, n\}$, let ϵ_d denote ϵ raised to the power $(q^{n!}-1)/(q^d-1)$. The multiplicative order of ϵ_d is $q^d - 1$, and ϵ_d is a cyclic generator of $\mathbb{F}^\times_{q^d}$. Also, θ maps $\mathbb{F}^\times_{q^d}$ isomorphically onto the group of $(q^d-1)^{\text{th}}$ roots of unity.

Corollary 2.5. *For all $n \in \mathbb{N}$, $d \in \{1, \ldots, n\}$, and prime powers q,*

$$\{\xi \in \mathbb{C}^\times : \xi^{q^d-1} = 1\} \;=\; \bigsqcup_{c|d} \bigsqcup_{f \in \mathcal{F}_c(q)} \{\theta(\alpha) : \alpha \in \mathbb{F}_{q^c}^\times,\, f(\alpha) = 0\}. \tag{23}$$

Proof. Apply θ to each element on the left and right sides of (22). □

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

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

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

$$f(z) = \prod_{i=0}^{d-1} \left(z - \left(\epsilon_d^{\ell_f}\right)^{q^i} \right). \tag{24}$$

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

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

$$\theta_n : \mathbb{F}_{q^n}^\times \to \mathbb{Z}/(q^n - 1) \quad \text{by} \quad \theta_n\left(\epsilon_n^\ell\right) = \ell \mod q^n - 1 \quad \forall \ell \in \mathbb{Z}. \tag{25}$$

It follows that θ_n maps ϵ_d^ℓ to $\ell \cdot [n/d]_{q^d}$.

Corollary 2.6 (to Lemma 2.4). *For all $n \in \mathbb{N}$, $d \mid n$, and prime powers q,*

$$\{m \cdot [n/d]_{q^d} : m \in \mathbb{Z}/(q^n - 1)\} = \bigsqcup_{c|d} \bigsqcup_{f \in \mathcal{F}_c(q)} \{\theta_n(\alpha) : \alpha \in \mathbb{F}_{q^c}^\times,\, f(\alpha) = 0\}. \tag{26}$$

Proof. Apply θ_n to each element on the left and right sides of (22), recalling that $d \mid n$ and $\mathbb{F}_{q^d}^\times$ is the unique subgroup of $\mathbb{F}_{q^n}^\times$ of order $q^d - 1$. □

Example 2.7. Consider the case $q = 3$, $n = 4$, and $\theta : \epsilon \mapsto \zeta$, 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 the polynomials $f \in \mathcal{F}(q)$ with degree dividing n, together with all possible choices for ℓ_f modulo $q^d - 1$ and all possible choices for $\ell_f \cdot [n/\deg f]_{q^{\deg f}}$ modulo $q^n - 1$. For the sake of brevity, we omit most of the degree four polynomials, of which there are 18 total as per (34) below. Note that these values depend on the choice of ϵ.

We can also visualize the data from Table 2 in the complex plane as follows. Observe that θ maps ϵ_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 ℓ_f for some f in Table 2 with degree $d \mid n$, we have

$$\alpha = \epsilon_d^{\ell_f} = \epsilon_n^{\ell_f \cdot [n/d]_{q^d}}$$

is a root of f,

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

TABLE 2. Choices for ℓ_f and $\ell_f \cdot [n/\deg f]_{q^{\deg f}}$ with $q = 3$ and $n = 4$.

f	ℓ_f	$\ell_f \cdot [n/\deg f]_{q^{\deg f}}$
$z+2$	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	$4,12,28,36$	$4,12,28,36$
$\vdots$	$\vdots$	$\vdots$

FIGURE 1. Images under θ of roots of polynomials from Table 2

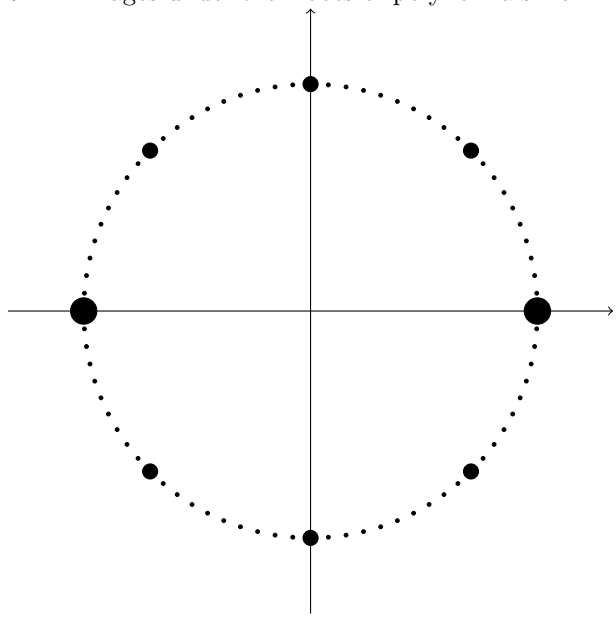


Figure 1 shows the complex plane and the images under θ of all the roots of all the polynomials $f \in \mathcal{F}_1(3) \sqcup \mathcal{F}_2(3) \sqcup \mathcal{F}_4(3)$. The images under θ of roots of polynomials in $\mathcal{F}_1(3)$ are labeled by the largest nodes, those for $\mathcal{F}_2(3)$ by the medium-sized nodes, and those for $\mathcal{F}_4(3)$ by the smallest nodes.

One can observe in Figure 1 the following instance of Corollary 2.5. The images under θ of the roots of polynomials in $\mathcal{F}_1(3) \sqcup \mathcal{F}_2(3)$ 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 Corollary 2.6 in either Table 2 or Figure 1. The images under θ_n of the roots of polynomials in $\mathcal{F}_1(3) \sqcup \mathcal{F}_2(3)$ are $0, 10, 20, \ldots, 70$. 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 $\mathrm{GL}_n\,\mathbb{F}_q$ 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 [30, Proposition 1.10.1].

2.4.1. *Indexing the* $\mathrm{GL}_n \mathbb{F}_q$ *conjugacy classes.* We first 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 $\mathbb{F}_q[z] \times V_g \to V_g$ 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 [7, Theorem 12.1.6], there exists a unique function $\underline{\lambda}^g : \mathcal{F}(q) \to \mathrm{Par}$ such that

$$V_g \cong \bigoplus_{f \in \mathcal{F}(q)} \bigoplus_{i \geqslant 1} \mathbb{F}_q[z] \Big/ \left(f(z)^{\underline{\lambda}^g(f)_i} \right) \tag{27}$$

as $\mathbb{F}_q[z]$-modules, where $\underline{\lambda}^g(f)_i$ denotes the i^{th} part of $\underline{\lambda}^g(f)$. We say that g **determines the isomorphism** (27). 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 $\underline{\lambda} : \mathcal{F}(q) \to \mathrm{Par}$ 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 $\underline{\lambda} : \mathcal{F}(q) \to \mathrm{Par}$ to be

$$\|\underline{\lambda}\| = \sum_{f \in \mathcal{F}(q)} |\underline{\lambda}(f)| \cdot \deg f. \tag{28}$$

Computing dimensions of each side in the isomorphism given in (27) 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 [15], 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 (27) to write down a specific matrix whose conjugacy class is indexed by $\underline{\lambda}$ as follows. If $h(z) = z^n - a_{n-1} z^{n-1} - \cdots - a_1 z - a_0 \in \mathbb{F}_q[z]$, 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 (27), g is in the same conjugacy class as any block-diagonal matrix whose diagonal blocks are those nonempty matrices $A(f^{\underline{\lambda}(f)_i})$ for $f \in \mathcal{F}(q)$ and $i \geqslant 1$. 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 2.8. 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

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

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 $\operatorname{supp}\underline{\lambda} = \{f \in \mathcal{F}(q) : \underline{\lambda}(f) \neq \varnothing\}$. Observe $\|\underline{\lambda}\| < \infty$ implies $\#\operatorname{supp}\underline{\lambda} < \infty$. Call an index $\underline{\lambda}$ **primary** if $\#\operatorname{supp}\underline{\lambda} = 1$. If $\underline{\lambda}$ is primary with $\operatorname{supp}\underline{\lambda} = \{f\}$ 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 $\mathrm{GL}_n\,\mathbb{F}_q$. 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 $\mathrm{GL}_n\,\mathbb{F}_q$. For $\mu \vdash n$ and $i \in \mathbb{N}$, define $s_i(\mu) = \sum_{j=1}^{i} \mu_j$.

THEOREM 2.9 ([30, Theorem 1.10.7]). *For all $n \in \mathbb{N}$, prime powers q, and $\underline{\lambda} : \mathcal{F}(q) \to$ Par with $\|\underline{\lambda}\| = n$, we have*

$$\#\mathcal{C}_{\underline{\lambda}} = \frac{\gamma_n(q)}{\prod_{f\in\mathcal{F}(q)} \prod_{i\geqslant 1} \prod_{j=1}^{m_i(\underline{\lambda}(f))} \left((q^{\deg f})^{s_i(\underline{\lambda}(f)')} - (q^{\deg f})^{s_i(\underline{\lambda}(f)')-j}\right)}. \tag{29}$$

EXAMPLE 2.10. Consider $\mathrm{GL}_3\,\mathbb{F}_2$. 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 $\underline{\lambda} : \mathcal{F}(2) \to \mathrm{Par}$ satisfying $\|\underline{\lambda}\| = 3$, which index the conjugacy classes and irreducible characters of $\mathrm{GL}_3\,\mathbb{F}_2$. The primary ones are

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

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

$$\underline{\lambda}_{\mathrm{o}}(f) = \begin{cases} (1) & \text{if } f = f_1, \\ (1) & \text{if } f = f_2, \\ \varnothing & \text{otherwise.} \end{cases}$$

We now name all of the conjugacy classes, indicate a member in rational canonical form, and indicate what function $\mathcal{F}(2) \to \mathrm{Par}$ indexes the class.

The conjugacy class U_1 of $\left[\begin{smallmatrix} 1&0&0\\0&1&0\\0&0&1 \end{smallmatrix}\right]$ is indexed by $f_1 \mapsto (1,1,1)$.

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

The conjugacy class U_3 of $\left[\begin{smallmatrix} 0&0&1\\1&0&1\\0&1&1 \end{smallmatrix}\right]$ is indexed by $f_1 \mapsto (3)$.

The conjugacy class E of $\left[\begin{smallmatrix} 0&0&1\\1&0&0\\0&1&1 \end{smallmatrix}\right]$ is indexed by $f_3 \mapsto (1)$.

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

The conjugacy class C_{o} of $\left[\begin{smallmatrix} 0&1&0\\1&1&0\\0&0&1 \end{smallmatrix}\right]$ is indexed by $\underline{\lambda}_{\mathrm{o}}$.

The conjugacy classes are named as follows. The **u**nipotent classes are U_1, U_2, and U_3. The regular **e**lliptic classes are E and $\tilde{E}$. The **o**dd **o**ne **o**ut is C_{o}. As an example of Theorem 2.9, 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 2.9,

$$\#U_2 = \frac{\gamma_3(2)}{\prod_{i=1}^{2}\left(2^{s_i((2,1))} - 2^{s_i((2,1))-1}\right)} = \frac{2^{\binom{3}{2}}[3]_2!}{(2^2-2^1)(2^3-2^2)} = 21. \tag{30}$$

2.4.2. *Cycle type, regular semisimple elements, and regular elliptic elements.* Recall the definition of **cycle type** for $\mathrm{GL}_n \mathbb{F}_q$ from the introduction. The definition given in the introduction is equivalent to the following. For any matrix $g \in \mathrm{GL}_n \mathbb{F}_q$, $\mathrm{type}(g) = \mu$ if and only if

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

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

$$\mathcal{T}_\mu(q) = \{g \in \mathrm{GL}_n \mathbb{F}_q : \mathrm{type}(g) = \mu\}. \tag{31}$$

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 $\mathrm{GL}_n \mathbb{F}_q$.

Example 2.11. Using the notation from Example 2.10 above, $\mathcal{T}_{(1,1,1)}(2) = U_1 \cup U_2 \cup U_3$, $\mathcal{T}_{(2,1)}(2) = C_{\mathrm{o}}$, and $\mathcal{T}_{(3)}(2) = E \cup \tilde{E}$.

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 [20] for a discussion on the regular semisimple variety in algebraic groups in both characteristic zero and positive characteristic. In particular, Lehrer gives a formula [20, Corollary 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 $\mathrm{GL}_n \mathbb{F}_q$.

Theorem 2.12 (Fulman [10]). *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 $\underline{\lambda}^g(f) \in \{\varnothing, (1)\}$ for all $f \in \mathcal{F}(q)$.*

Remark 2.13. Theorem 2.12 explains our choice of the notation $\mathcal{T}_\mu^{\square}(q)$ due to the fact that the partition (1) can alternatively be represented by its Young diagram, $\square$.

We will take Fulman's characterization as the definition of regular semisimple elements in this paper. In other words, we define an element of $\mathrm{GL}_n \mathbb{F}_q$ to be regular semisimple if its characteristic polynomial has no repeated factors.

Corollary 2.14. *Suppose $n \in \mathbb{N}$, q is a prime power, $g \in \mathrm{GL}_n \mathbb{F}_q$ is regular semisimple and $h_1, \ldots, h_\ell \in \mathcal{F}(q)$ are the distinct irreducible factors of the characteristic polynomial of g. Then g determines the isomorphism*

$$V_g \cong \mathbb{F}_q[z]/(h_1(z)) \oplus \cdots \oplus \mathbb{F}_q[z]/(h_\ell(z)). \tag{32}$$

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

$$\mathcal{T}_\mu^{\square}(q) = \{g \in \mathcal{T}_\mu(q) : g \text{ is regular semisimple}\}. \tag{33}$$

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 2.15. Using the notation from Example 2.10 above, $\mathcal{T}^{\square}_{(1,1,1)}(2)$ is empty, $\mathcal{T}^{\square}_{(2,1)}(2) = C_{\mathrm{o}}$, and $\mathcal{T}^{\square}_{(3)}(2) = E \cup \tilde{E}$.

We now derive an explicit formula for $\#\mathcal{T}^{\square}_{\mu}(q)$ by combining Theorems 2.9 and 2.12. As mentioned by Green in [15], we have

$$\#\mathcal{F}_m(q) = \frac{1}{m}\sum_{s|m} \boldsymbol{\mu}(m/s)(q^s - 1) \tag{34}$$

for all $m \geqslant 1$ and prime powers q, a result originally due to Gauss in the case that q is prime [13].

COROLLARY 2.16. *Suppose $n \in \mathbb{N}$, $\mu \vdash n$, and q is a prime power. Then $\mathcal{T}^{\square}_{\mu}(q)$ is a union of conjugacy classes, each with cardinality*

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

Therefore,

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

Recall that Corollary 1.2 states that, for large q, the set $\mathcal{T}^{\square}_{\mu}(q)$ comprises approximately $1/z_\mu$ of $\mathrm{GL}_n\,\mathbb{F}_q$. We now show how it follows from Corollary 2.16.

Proof of Corollary 1.2. First, we prove the regular semisimple portion of the claim. By Corollary 2.16 and the fact that $\gamma_n(q) = \#\,\mathrm{GL}_n\,\mathbb{F}_q$ for prime powers q,

$$\frac{\#\mathcal{T}^{\square}_{\mu}(q)}{\#\,\mathrm{GL}_n\,\mathbb{F}_q} = \frac{\prod_{i\geqslant 1}\binom{\#\mathcal{F}_i(q)}{m_i(\mu)}}{\prod_{i=1}^{\ell(\mu)} q^{\mu_i} - 1}. \tag{35}$$

For each $i \geqslant 1$,

$$\binom{\#\mathcal{F}_i(q)}{m_i(\mu)} \tag{36}$$

is a polynomial in q with degree $i \cdot m_i(\mu)$ with leading coefficient $1/i^{m_i(\mu)}m_i(\mu)!$. Therefore, the numerator of the right side of (35) is a degree-$|\mu|$ polynomial in q with leading coefficient $1/z_\mu$. The denominator of the right side of (35) is a degree-$|\mu|$ polynomial in q with leading coefficient 1. The result follows from taking the $q \to \infty$ limit of (35).

Second, we prove the remaining claim using what we have already proved. Observe that $\#\mathcal{T}^{\square}_{\mu}(q) \leqslant \#\mathcal{T}_{\mu}(q)$ implies

$$\frac{1}{z_\mu} = \lim_{q\to\infty}\frac{\#\mathcal{T}^{\square}_{\mu}(q)}{\#\,\mathrm{GL}_n\,\mathbb{F}_q} \leqslant \lim_{q\to\infty}\frac{\#\mathcal{T}_{\mu}(q)}{\#\,\mathrm{GL}_n\,\mathbb{F}_q} \tag{37}$$

for each $\mu \vdash n$. However,

$$\sum_{\mu\vdash n}\frac{1}{z_\mu} = 1 = \sum_{\mu\vdash n}\frac{\#\mathcal{T}_{\mu}(q)}{\#\,\mathrm{GL}_n\,\mathbb{F}_q}, \tag{38}$$

because cycle type partitions $\mathrm{GL}_n\,\mathbb{F}_q$. This implies that the limit

$$\lim_{q\to\infty}\frac{\#\mathcal{T}_{\mu}(q)}{\#\,\mathrm{GL}_n\,\mathbb{F}_q} \tag{39}$$

cannot exceed $1/z_\mu$, as desired. □

In addition to Theorem 2.12, we will make use of the following characterization of regular semisimple elements, which appears as the final corollary in [4, Section 3]. 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 2.17 (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 its characteristic polynomial is irreducible. Equivalently, the set of regular elliptic elements in $\mathrm{GL}_n \mathbb{F}_q$ is $\mathcal{T}_{(n)}(q) = \mathcal{T}^{\square}_{(n)}(q)$. This is just one of several characterizations of regular elliptic elements that we will find useful.

Proposition 2.18 ([22, Proposition 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* (42) *in Section* 3.1 *below.*
(iii) *The element g stabilizes no proper nontrivial subspaces of V.*
(iv) *The element g determines the isomorphism*

$$V_g \cong \mathbb{F}_q[z]/(h_1(z)), \tag{40}$$

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 1.7.

Corollary 2.19 (to Theorem 2.17 and Proposition 2.18). *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*

$$V_g \cong \mathbb{F}_q[z]/(h_1(z)) \oplus \cdots \oplus \mathbb{F}_q[z]/(h_\ell(z)) \tag{41}$$

as in (32)*, where $h_1, \ldots, h_\ell \in \mathcal{F}(q)$ are distinct and irreducible. Suppose g stabilizes a subspace $U \subset V$. Let $\widetilde{U} \subset \bigoplus_{i=1}^{\ell} \mathbb{F}_q[z]/(h_i(z))$ denote the submodule corresponding to U under the isomorphism* (41)*. Then there exists a subset $I \subset \{1, \ldots, \ell\}$ such that $\widetilde{U} = \bigoplus_{i \in I} \mathbb{F}_q[z]/(h_i(z))$.*

Proof. By Theorem 2.17, it suffices to show that, for each $i \in \{1, \ldots, \ell\}$, 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 2.18, we are done. □

3. $\mathrm{GL}_n \mathbb{F}_q$ character theory

In this section, 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 [15]. The notation and language we use vary from Green's original choices. For another exposition see Macdonald [23, Chapter IV].

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

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

$$\mathfrak{P}_\nu = \left\{ \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1\ell} \\ 0 & A_{22} & \cdots & A_{2\ell} \\ & & \ddots & \vdots \\ 0 & 0 & 0 & A_{\ell\ell} \end{bmatrix} \in \mathrm{GL}_n\,\mathbb{F}_q : A_{ii} \in \mathrm{GL}_{\nu_i}\,\mathbb{F}_q \text{ for all } 1 \leqslant i \leqslant \ell \right\}. \tag{42}$$

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

$$A = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1\ell} \\ 0 & A_{22} & \cdots & A_{2\ell} \\ & & \ddots & \vdots \\ 0 & 0 & 0 & A_{\ell\ell} \end{bmatrix} \in \mathfrak{P}_\nu \implies \pi_i^\nu(A) = A_{ii}. \tag{43}$$

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

$$\left(\bigodot_{i=1}^{\ell} \chi_i \right)(g) = \frac{1}{\#\mathfrak{P}_\nu} \sum_{\substack{x \in \mathrm{GL}_n\,\mathbb{F}_q \\ xgx^{-1} \in \mathfrak{P}_\nu}} \prod_{i=1}^{\ell} \chi_i\left(\pi_i^\nu(xgx^{-1})\right). \tag{44}$$

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 **Jrreducible** characters, J, in terms of the B's. Finally, we define the irreducible characters $\chi^{\underline{\lambda}}$ of $\mathrm{GL}_n\,\mathbb{F}_q$ in terms of the J's.[(1)] The names Primary-support, paraBolic, and Jrreducible were not used by Green.

For each $b \in \mathbb{Z}$ and $d \in \mathbb{N}$, we define the **P**rimary-support character, P_d^b, of $\mathrm{GL}_d\,\mathbb{F}_q$ as follows:

$$P_d^b(g) = \begin{cases} \left(\prod_{i=1}^{\ell(\mu)-1} (1 - t^i) \right) \cdot \sum_{i=1}^{\deg h} \theta(\epsilon_{\deg h}^{\ell_h})^{q^i b} & \text{if } \underline{\lambda}^g = h \mapsto \mu \text{ is primary,} \\ 0 & \text{otherwise.} \end{cases} \tag{45}$$

For each $d \in \mathbb{Z}$, each $\nu \in \mathrm{Par} \setminus \{\varnothing\}$ such that d divides every part of ν, and each function $\alpha : d\mathbb{Z} \to \mathbb{Z}$, we define the para**B**olic character, B_ν^α, of $\mathrm{GL}_{|\nu|}\,\mathbb{F}_q$ by

$$B_\nu^\alpha = \bigodot_{i=1}^{\ell(\nu)} P_{\nu_i}^{\alpha(\nu_i)}. \tag{46}$$

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

$$J_f^\lambda = (-1)^{|\lambda| \cdot (\deg f - 1)} \cdot \sum_{\nu \vdash |\lambda|} \frac{1}{z_\nu} \cdot \chi_\nu^\lambda \cdot B_{(\deg f)\nu}^{\ell_f \cdot \alpha_{\deg f}}. \tag{47}$$

[(1)] One might refer to this as the 'PBJ' method.

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

$$\chi^{\underline{\lambda}} = \bigodot_{f \in \operatorname{supp} \underline{\lambda}} J_f^{\underline{\lambda}(f)}. \tag{48}$$

Theorem 3.1 (Green [15, Theorem 14]). *For all $n \in \mathbb{N}$ and prime powers q, the set $\{\chi^{\underline{\lambda}} : \|\underline{\lambda}\| = n\}$ is the set of distinct, irreducible, complex characters of $\mathrm{GL}_n \mathbb{F}_q$.*

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 $J_f^{\varnothing}$ denote the empty function, which is the identity element with respect to $\odot$, we can define

$$\chi^{\underline{\lambda}} = \bigodot_{f \in \mathcal{F}(q)} J_f^{\underline{\lambda}(f)}. \tag{49}$$

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 $\lambda \in \mathrm{Par}$.

Example 3.2. Using the notation from Example 2.10, we record in Table 3 the character table for $\mathrm{GL}_3 \mathbb{F}_2$. Our choice of ϵ was made such that $f_3(\epsilon_3) = 0$. 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.

Table 3. The character table of $\mathrm{GL}_3 \mathbb{F}_2$, where $\zeta_7 = e^{2\pi i/7}$

	U_1	U_2	U_3	E	$\tilde{E}$	C_{o}
$f_1 \mapsto (1,1,1)$	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
$\underline{\lambda}_{\mathrm{o}}$	7	-1	-1	0	0	1

3.2. Degrees of the irreducible $\mathrm{GL}_n \mathbb{F}_q$ characters. Green also gave an explicit formula for the degrees of the irreducible characters $\chi^{\underline{\lambda}}$. For any partition λ, let $b(\lambda) = \sum_{i=1}^{\ell(\lambda)} (i-1)\lambda_i$ and define

$$[\lambda : q] = q^{b(\lambda)} \cdot \frac{\prod_{1 \leqslant i < j \leqslant \ell(\lambda)} \left(q^{(\lambda_i - \lambda_j) - (i-j)} - 1\right)}{\prod_{i=1}^{\ell(\lambda)} \prod_{j=1}^{\lambda_i + \ell(\lambda) - i} (q^j - 1)}. \tag{50}$$

Theorem 3.3 (Green [15, Theorem 14]). *For all $n \in \mathbb{N}$, prime powers q, and $\underline{\lambda} : \mathcal{F}(q) \to \mathrm{Par}$ with $\|\underline{\lambda}\| = n$, the degree of the irreducible character $\chi^{\underline{\lambda}}$ of $\mathrm{GL}_n \mathbb{F}_q$ is given by*

$$\deg \chi^{\underline{\lambda}} = (q-1)^n \cdot [n]_q! \cdot \prod_{f \in \mathcal{F}(q)} \left[\underline{\lambda}(f) : q^{\deg f}\right]. \tag{51}$$

Example 3.4. We use Theorem 3.3 to calculate $\deg \chi^{f_1 \mapsto (2,1)}$. By Theorem 3.3,

$$\deg \chi^{f_1 \mapsto (2,1)} = [3]_2! \cdot [(2,1) : 2] = [3]_2! \cdot \frac{6}{\prod_{j=1}^{3} (2^j - 1) \cdot \prod_{k=1}^{1} (2^k - 1)} = 6,$$

which agrees with $\chi^{f \mapsto (2,1)}$ evaluated at U_1 as recorded in Table 3.

The degrees of primary characters indexed by $z-1 \mapsto \lambda$ for $\lambda \vdash n$ have an alternate, combinatorial description, which we mention briefly. Recall that, for a **standard Young tableau** T of shape λ, the **major index** of 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. Furthermore, the major index of T is denoted $\operatorname{maj} T$. Recall also that, given a cell a in row i and columns j of the Ferrers diagram of λ, denoted $a \in \lambda$, the **hooklength** of a is defined by $h(a) = (\lambda_i - i) + (\lambda'_j - j) + 1$.

THEOREM 3.5 (Stanley [29], Steinberg [31]). *For all $n \in \mathbb{N}$, $\lambda \vdash n$, and prime powers q, we have*

$$\deg \chi^{z-1\mapsto\lambda} = q^{b(\lambda)} \cdot \frac{\prod_{i=1}^{n} q^i - 1}{\prod_{a\in\lambda} q^{h(a)} - 1} = \sum_T q^{\operatorname{maj} T}, \tag{52}$$

where the sum ranges over all standard Young tableaux T of shape λ.

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 3.6 (Steinberg [31]). *For all $n \in \mathbb{N}$, prime powers q, partitions $\lambda, \mu \vdash n$, and $g \in \mathcal{T}_\mu^{\square}(q)$, we have $\chi^{z-1\mapsto\lambda}(g) = \chi^\lambda_\mu$.*

Regular elliptic elements, in particular, have nice character-theoretic properties as well. The following result echoes Corollary 2.3.

COROLLARY 3.7 (to Corollary 2.3, Proposition 2.18, Theorem 3.1, and Theorem 3.3). *Suppose $n \in \mathbb{N}$, q is a prime power, $\underline{\lambda} : \mathcal{F}(q) \to$ Par with $\|\underline{\lambda}\| = n$, and $g \in \mathcal{T}_{(n)}(q)$. If $\chi^{\underline{\lambda}}(g) \neq 0$, then there exist $d \mid n$, $f \in \mathcal{F}_d(q)$, and $r \in \{0, \ldots, n/d-1\}$ such that $\underline{\lambda} = f \mapsto (n/d - r, 1^r)$ is primary. Moreover,*

$$\deg \chi^{f\mapsto(n/d-r,1^r)} = \deg_{n,d,r}(q), \tag{53}$$

as defined in Table 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 $d \mid n$, $f \in \mathcal{F}_d(q)$, and $r \in \{0, \ldots, n/d-1\}$, we define

$$\chi^{f,r} = \chi^{f\mapsto(n/d-r,1^r)}. \tag{54}$$

We can now write down a further simplified version of (19).

COROLLARY 3.8 (to Corollary 2.2 and Corollary 3.7). *For all $n, k \in \mathbb{N}$, $\mu \vdash n$, and prime powers q, we have*

$$g_{k,\mu}(q) = \frac{1}{\gamma_n(q)} \sum_{d,f,r} \deg_{n,d,r}(q)^{1-k} \left(\sum_{g\in\mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right)^k \left(\sum_{h\in\mathcal{T}_\mu(q)} \chi^{f,r}(h) \right), \tag{55}$$

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

4. Proofs of main results

4.1. Main tool. We begin with our main tool, Theorem 1.7, 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 1.7, 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 $h_1, \ldots, h_{\ell(\mu)}$ with $\deg h_i = \mu_i$ for each $i \in \{1, \ldots, \ell(\mu)\}$. Note that this implies each diagonal block $\pi_i^\mu(g) \in \mathrm{GL}_{\mu_i}(q)$ is in the primary conjugacy class indexed by $h_i \mapsto \square$.

Lemma 4.1. *For all $n \in \mathbb{N}$, $d \mid n$, $\nu \vdash n/d$, $\mu \vdash n$, prime powers q, $g \in \mathcal{T}_\mu^\square(q)$, and $\alpha : d\mathbb{Z} \to \mathbb{Z}$, we have $B_{d\nu}^\alpha(g) = 0$ unless $d\nu = \mu$.*

Proof. By definition,

$$B_{d\nu}^\alpha(g) = \frac{1}{\#\mathfrak{P}_{d\nu}} \sum_{\substack{x \in \mathrm{GL}_n \mathbb{F}_q \\ xgx^{-1} \in \mathfrak{P}_{d\nu}}} \prod_{i=1}^{\ell(\nu)} P_{d\nu_i}^{\alpha(d\nu_i)} \left(\pi_i^{d\nu}(xgx^{-1})\right). \tag{56}$$

Consider a single summand in (56), which is a product of Primary-support character values. By definition, 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 (56) does not vanish, and hence each block $\pi_i^{d\nu}(xgx^{-1})$ is primary.

For each $i \in \{1, \ldots, \ell(\nu)\}$, 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 $i \in \{1, \ldots, \ell(\mu)\}$. Computing degrees show that $d\nu_i = \deg \tilde{h}_i = \deg h_{\sigma(i)} = \mu_{\sigma(i)}$ for all $i \in \{1, \ldots, \ell(\mu)\}$. This implies $d\nu = \mu$. □

We require some more terminology before moving forward. Given $\mu \vdash n$, refer to a flag $S_\bullet$ of nested subspaces

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

of V as a **μ-flag** if

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

for all $j \in \{1, \ldots, \ell(\mu)\}$. Refer to an ordered basis $(e_1, \ldots, e_n)$ of V as a **basis for $S_\bullet$** if

$$\left(e_1, \ldots, e_{\sum_{i=1}^{j} \mu_i}\right)$$

is a basis for S_j for each $j \in \{1, \ldots, \ell(\mu)\}$. Conversely, each ordered basis $(e_1, \ldots, e_n)$ for V determines a μ-flag by taking the j^{th} subspace in the flag to be the span of $\left(e_1, \ldots, e_{\sum_{i=1}^{j} \mu_i}\right)$ for each $j \in \{1, \ldots, \ell(\mu)\}$. Given a μ-flag $S_\bullet$, say that a matrix in $\mathrm{GL}_n \mathbb{F}_q$ **stabilizes** $S_\bullet$ if it stabilizes S_j for each $j \in \{1, \ldots, \ell(\mu)\}$.

Lemma 4.2. *For all $n \in \mathbb{N}$, $\mu \vdash n$, prime powers q, and $g \in \mathcal{T}_\mu^\square(q)$, we have*

$$\#\left\{x \in \mathrm{GL}_n \mathbb{F}_q : xgx^{-1} \in \mathfrak{P}_\mu\right\} = \#\mathfrak{P}_\mu \cdot \prod_{i \geqslant 1} m_i(\mu)!. \tag{57}$$

Proof. Viewing g abstractly as a linear transformation on V, the left side of (57) 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 $\mathcal{B} = (v_1, \ldots, v_n)$ for V, being an element of $\mathfrak{P}_\mu$ is equivalent to stabilizing the μ-flag determined by $\mathcal{B}$. Therefore, the left side of (57) is the product of

(1) the number of μ-flags that g stabilizes and
(2) the number of ordered bases for a given μ-flag.

The second part is $\#\mathfrak{P}_\mu$.

For the first part, consider a μ-flag

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

that g stabilizes. For each $i \in \{1, \ldots, \ell(\mu)\}$, 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 (32), let $E_i \subset V$ denote the subspace corresponding to $\mathbb{F}_q[z]/(h_i(z))$ for each $i \in \{1, \ldots, \ell(\mu)\}$. By Corollary 2.19, 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 $Q_{\ell(\mu)-m_1(\mu)+1}, \ldots, Q_{\ell(\mu)}$ are all 1-dimensional and thus form a permutation of the $m_1(\mu)$ subspaces $E_{\ell(\mu)-m_1(\mu)+1}, \ldots, E_{\ell(\mu)}$. Likewise,

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

are all 2-dimensional and thus form a permutation of the $m_2(\mu)$ subspaces

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

as there are no 1-dimensional E_i's remaining. Continuing in this fashion, we see that the sequence $(Q_1, \ldots, Q_{\ell(\mu)})$ of quotients is one of $\prod_{i \geqslant 1} m_i(\mu)!$ total possibilities. Since the quotients determine $S_\bullet$ uniquely, the result follows. □

We are now ready to prove Theorem 1.7. For $d \mid n$, $f \in \mathcal{F}_d(q)$, and $\lambda \vdash n/d$, it states that, if some part of μ 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

$$\chi^{f \mapsto \lambda}(g) = (-1)^{\frac{n}{d}(d-1)} \chi^\lambda_{\tilde{\mu}} \prod_{i=1}^{\ell(\mu)} \frac{1}{\tilde{\mu}_i} \sum_{\substack{\beta_i \in \mathbb{F}_{q^{\mu_i}} \\ h_i(\beta_i) = 0}} \theta(\beta_i)^{\ell_f \cdot [\tilde{\mu}_i]_{q^d}}. \tag{58}$$

Proof of Theorem 1.7. By definitions (47) and (48), we have

$$\chi^{f \mapsto \lambda}(g) = J^\lambda_f(g) = (-1)^{\frac{n}{d}(d-1)} \cdot \sum_{\nu \vdash \frac{n}{d}} \frac{\chi^\lambda_\nu}{z_\nu} B^{\ell_f \cdot \alpha_d}_{d\nu}(g). \tag{59}$$

By Lemma 4.1, $B^{\ell_f \cdot \alpha_d}_{d\nu}(g) = 0$ unless $d\nu = \mu$. If some part of μ 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 (59) does not vanish. In this case, (59) reduces to

$$\chi^{f \mapsto \lambda}(g) = (-1)^{\frac{n}{d}(d-1)} \frac{\chi^\lambda_{\tilde{\mu}}}{z_{\tilde{\mu}}} B^{\ell_f \cdot \alpha_d}_\mu(g). \tag{60}$$

By definitions (44) and (46), we can rewrite (60) as

$$\chi^{f \mapsto \lambda}(g) = (-1)^{\frac{n}{d}(d-1)} \cdot \frac{\chi^\lambda_{\tilde{\mu}}}{z_{\tilde{\mu}}} \cdot \frac{1}{\#\mathfrak{P}_\mu} \sum_{\substack{x \in \mathrm{GL}_n \mathbb{F}_q \\ xgx^{-1} \in \mathfrak{P}_\mu}} \prod_{i=1}^{\ell(\mu)} P^{\ell_f \cdot \alpha_d(\mu_i)}_{\mu_i}(\pi^\mu_i(xgx^{-1})). \tag{61}$$

Consider the summation in (61). It can be rewritten as

$$\sum_{\substack{x\in \mathrm{GL}_n\,\mathbb{F}_q \\ xgx^{-1}\in\mathfrak{P}_\mu}} \prod_{s\geqslant 1} \prod_{\{j\in\mathbb{N}\,:\,\mu_j=s\}} P_s^{\ell_f\cdot\alpha_d(s)}(\pi_j^\mu(xgx^{-1})). \tag{62}$$

For each x such that $xgx^{-1}\in\mathfrak{P}_\mu$, consider the corresponding summand in (62). We repeat a similar argument to the one presented toward the end of the proof of Lemma 4.2. Note 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 $P_s^{\ell_f\cdot\alpha_d(s)}$ in (62) depends only on the characteristic polynomial of the argument. This implies that the product of the Primary-support characters in (62) is constant over the sum. Therefore,

$$\chi^{f\mapsto\lambda}(g)=(-1)^{\frac{n}{d}(d-1)}\cdot\frac{\chi^\lambda_{\tilde\mu}}{z_{\tilde\mu}}\cdot\frac{\#\{x\in\mathrm{GL}_n\,\mathbb{F}_q : xyx^{-1}\in\mathfrak{P}_\mu\}}{\#\mathfrak{P}_\mu}\cdot\prod_{i=1}^{\ell(\mu)}P_{\mu_i}^{\ell_f\cdot\alpha_d(\mu_i)}(\pi_i^\mu(g)). \tag{63}$$

By Lemma 4.2, (63) reduces to

$$\chi^{f\mapsto\lambda}(g)=(-1)^{\frac{n}{d}(d-1)}\cdot\chi^\lambda_{\tilde\mu}\cdot\prod_{i=1}^{\ell(\mu)}\frac{1}{\tilde\mu_i}P_{\mu_i}^{\ell_f\cdot\alpha_d(\mu_i)}(\pi_i^\mu(g)). \tag{64}$$

Consider the Primary-support character evaluations in (64). By (24) and definition (45),

$$P_{\mu_i}^{\ell_f\cdot\alpha_d(\mu_i)}(\pi_i^\mu(g))=\sum_{j=1}^{\mu_i}\theta(\epsilon_{\mu_i}^{\ell_{h_i}})^{q^j\ell_f\cdot[\tilde\mu_i]_{q^d}}=\sum_{\substack{\beta_i\in\mathbb{F}_{q^{\mu_i}}\\ h_i(\beta_i)=0}}\theta(\beta_i)^{\ell_f\cdot[\tilde\mu_i]_{q^d}}. \tag{65}$$

Substituting (65) into (64) gives the result. □

Example 4.3. Returning to Example 3.2, we compute $\chi^{f_3\mapsto(1)}(c)$ for $c\in E$. In the notation of Theorem 1.7, 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 ϵ_3,ϵ_3^2, and ϵ_3^4. By Theorem 1.7,

$$\begin{aligned}\chi^{f_3\mapsto(1)}(c)&=(-1)^{\frac{3}{3}(3-1)}\cdot\chi^{(1)}_{(1)}\cdot\sum_{h_1(\beta)=0}\theta(\beta)\\&=\theta(\epsilon_3)+\theta(\epsilon_3^2)+\theta(\epsilon_3^4)=\zeta_7+\zeta_7^2+\zeta_7^4.\end{aligned}$$

We see this exact value in Table 3 above.

4.2. Proof of first main result. We can now apply Theorem 1.7 to prove our main results. We begin with Theorem 1.3, which addresses the family of cases where $\mu\vdash n>2$ and $m_1(\mu)=1$. Recall that Theorem 1.3 states, under these assumptions on μ and n,

$$g^\square_{k,\mu}(q)=\frac{\#\mathcal{T}_{(n)}(q)^k\cdot\#\mathcal{T}^\square_\mu(q)}{\#\,\mathrm{GL}_n\,\mathbb{F}_q}\cdot\sum_{r=0}^{n-1}\frac{(-1)^{rk}\chi_\mu^{(n-r,1^r)}}{\left(q^{\binom{r+1}{2}}\cdot\begin{bmatrix}n-1\\ r\end{bmatrix}_q\right)^{k-1}} \tag{66}$$

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

In the rest of this section and later, we will require some additional notation. We will consider the logical propositions "$q-1\mid\ell_f$" for various $f\in\mathcal{F}_1(q)$. Even though

ℓ_f denotes an arbitrary choice, these propositions are well-defined for the following reason. For any two possible choices ℓ_f and ℓ'_f, there exist $i, j \in \mathbb{Z}$ such that

$$\ell'_f = q^i \ell_f + j(q-1), \tag{67}$$

so $q-1 \mid \ell_f$ if and only if $q-1 \mid \ell'_f$.

Proof of Theorem 1.3. By Corollary 3.8, we have

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

Applying Theorem 1.7, we see that $\chi^{f,r}$ vanishes on $\mathcal{T}^{\square}_{\mu}(q)$ unless $d = 1$. Therefore,

$$g^{\square}_{k,\mu}(q) = \frac{1}{\gamma_n(q)} \sum_{r=0}^{n-1} \deg_{n,1,r}(q)^{1-k} \sum_{f \in \mathcal{F}_1(q)} \left(\sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right)^k \left(\sum_{h \in \mathcal{T}^{\square}_{\mu}(q)} \chi^{f,r}(h) \right). \tag{68}$$

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 $\mathcal{T}^{\square}_{\mu}(q)$ have equal sizes and each conjugacy class is uniquely determined by a set $\{h_1, \ldots, h_\ell\}$ of distinct polynomials such that $h_i \in \mathcal{F}_{\mu_i}(q)$ for each $i \in \{1, \ldots, \ell\}$. Thus, by Theorem 1.7, $\sum_{h \in \mathcal{T}^{\square}_{\mu}(q)} \chi^{f,r}(h)$ is a multiple of

$$\sum_{\substack{\{h_1,\ldots,h_\ell\} \\ h_i \in \mathcal{F}_{\mu_i}(q)}} \prod_{i=1}^{\ell} \sum_{\substack{\beta_i \in \mathbb{F}_{q^{\mu_i}} \\ h_i(\beta_i)=0}} \theta(\beta_i)^{\ell_f \cdot [\mu_i]_q}. \tag{69}$$

Since $m_1(\mu) = 1$, we have that (69) factors as

$$\left(\sum_{\substack{\{h_1,\ldots,h_{\ell-1}\} \\ h_i \in \mathcal{F}_{\mu_i}(q)}} \prod_{i=1}^{\ell-1} \sum_{\substack{\beta_i \in \mathbb{F}_{q^{\mu_i}} \\ h_i(\beta_i)=0}} \theta(\beta_i)^{\ell_f \cdot [\mu_i]_q} \right) \cdot \left(\sum_{h_\ell \in \mathcal{F}_1(q)} \sum_{\substack{\beta_\ell \in \mathbb{F}_q \\ h_\ell(\beta_\ell)=0}} \theta(\beta_\ell)^{\ell_f} \right). \tag{70}$$

The latter factor in (70) 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 2.6, $\theta(\beta_\ell)$ ranges over all $(q-1)^{\text{th}}$ roots of unity. Since $\deg f = d = 1$, we can take $\ell_f \in \{1, \ldots, q-1\}$. Thus, the only non-zero contribution to the sum over $f \in \mathcal{F}_1(q)$ in (68) 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 (68) gives

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

By Corollary 2.3 and Theorem 3.6,

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

Since both character values only depend on r, we have

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

which simplifies to the result, using the notation from Table 1. □

Next is the case of $\mu = (n-1,1)$, which is addressed by Corollary 1.4. 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 1.4 states that

$$g_{k,(n-1,1)}(q) = \frac{\#\mathcal{T}_{(n)}(q)^k \cdot \#\mathcal{T}_{(n-1,1)}(q)}{\#\operatorname{GL}_n \mathbb{F}_q} \cdot \left(1 + \frac{(-1)^{nk-n-k}}{q^{\binom{n}{2}(k-1)}}\right) \tag{71}$$

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

Proof of Corollary 1.4. Apply Corollary 2.3 to Theorem 1.3, observing that $\chi^{(n-r,1^r)}_{(n-1,1)}$ is only nonzero when $r \in \{0, n-1\}$. □

4.3. Proof of second main result. Our second main result, Theorem 1.5, 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, and recall that Theorem 1.5 states that

$$g_{k,(n)}(q) = P_{n,k+1}(q) \sum_{d|n} (-1)^{n(k+1)/d} d^k D_{n,k+1,d}(q) \sum_{c|d} \boldsymbol{\mu}(d/c) C_{n,k+1,c}(q) \tag{72}$$

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

Proof of Theorem 1.5. By Corollary 3.8 and the fact that $\mu = (n)$, we have

$$g_{k,\mu}(q) = \frac{1}{\gamma_n(q)} \sum_{d|n} \sum_{r=0}^{\frac{n}{d}-1} \deg_{n,d,r}(q)^{1-k} \sum_{f \in \mathcal{F}_d(q)} \left(\sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right)^{k+1}. \tag{73}$$

By Theorem 2.9, 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

$$\sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) = \frac{\gamma_n(q)}{q^n - 1} \sum_{p \in \mathcal{F}_n(q)} \chi^{f,r}(g_p), \tag{74}$$

where g_p denotes an arbitrary regular elliptic element with characteristic polynomial p. Substituting (74) into (73), we have

$$g_{k,\mu}(q) = \frac{1}{\gamma_n(q)} \left(\frac{\gamma_n(q)}{q^n-1}\right)^{k+1} \sum_{d|n} \sum_{r=0}^{\frac{n}{d}-1} \deg_{n,d,r}(q)^{1-k} \sum_{f \in \mathcal{F}_d(q)} \left(\sum_{p \in \mathcal{F}_n(q)} \chi^{f,r}(g_p) \right)^{k+1}. \tag{75}$$

Observe that $\mathcal{T}_{(n)}(q) = \mathcal{T}^{\square}_{(n)}(q)$, so we can evaluate primary characters on $\mathcal{T}_{(n)}(q)$ using Theorem 1.7. Applying Theorem 1.7 and Corollary 2.3 to (75) gives

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

Using the notation established in Table 1, this is equivalent to

(76)
$$\frac{g_{k,\mu}(q)}{P_{n,k+1}(q)} = \sum_{d|n} ((-1)^{n/d} d)^{k+1} D_{n,k+1,d}(q) \sum_{f \in \mathcal{F}_d(q)} \left(\sum_{p \in \mathcal{F}_n(q)} \sum_{\substack{\alpha \in \mathbb{F}_{q^n}^{\times} \\ p(\alpha)=0}} \theta(\alpha)^{\ell_f \cdot [n/d]_{q^d}} \right)^{k+1}.$$

Theorem 1.5 now follows from Corollary 4.4 below, which we phrase in terms of k rather than $k+1$ for the sake of simplifying the expressions. □

Corollary 4.4 (to Lemma 4.5 and Lemma 4.6). *For all $n, k \in \mathbb{N}$, $d \mid n$, and prime powers q,*

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

Before proving Corollary 4.4, 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 "$b \mid \ell_f \cdot [n/d]_{q^d}$" or equivalently "$b$ divides $\ell_f \cdot [n/d]_{q^d}$", where $d \mid n$, $f \in \mathcal{F}_d(q)$, and b is a number that divides $q^n - 1$. These are not of the same form as "$q - 1 \mid \ell_f$," which we considered earlier. However, they are still 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, for any two possible choices ℓ_f and ℓ'_f with $\deg f = d$, there exist $i, j \in \mathbb{Z}$ such that

$$\ell'_f = q^i \ell_f + j(q^d - 1) \tag{77}$$

and thus

$$\ell'_f \cdot [n/d]_{q^d} = q^i \ell_f \cdot [n/d]_{q^d} + j(q^n - 1) \tag{78}$$

from multiplying both sides by $[n/d]_{q^d}$. It follows that, for any $b \mid q^n - 1$, we have $b \mid \ell_f \cdot [n/d]_{q^d}$ if and only if $b \mid \ell'_f \cdot [n/d]_{q^d}$.

Lemma 4.5. *For all $n \in \mathbb{N}$, $d \mid n$, prime powers q, and $f \in \mathcal{F}_d(q)$,*

$$\sum_{p \in \mathcal{F}_n(q)} \sum_{\substack{\alpha \in \mathbb{F}_{q^n}^{\times} \\ p(\alpha)=0}} \theta(\alpha)^{\ell_f \cdot [n/d]_{q^d}} = \sum_{s|n} \boldsymbol{\mu}(n/s)(q^s - 1) \delta_{q^s - 1 \mid \ell_f \cdot [n/d]_{q^d}}. \tag{79}$$

Proof. By Möbius inversion, it suffices to prove

$$\sum_{s|n} \sum_{p \in \mathcal{F}_s(q)} \sum_{\substack{\alpha \in \mathbb{F}_{q^s}^\times \\ p(\alpha)=0}} \theta(\alpha)^{\ell_f \cdot [n/d]_{q^d}} = (q^n-1)\delta_{q^n-1 \mid \ell_f \cdot [n/d]_{q^d}}. \tag{80}$$

Corollary 2.5 implies that, on the left side of (80), $\theta(\alpha)$ ranges precisely over all $(q^n-1)^{\text{th}}$ roots of unity. The sum of the $(\ell_f \cdot [n/d]_{q^d})^{\text{th}}$ powers of all $(q^n-1)^{\text{th}}$ roots of unity is zero unless q^n-1 divides $\ell_f \cdot [n/d]_{q^d}$, in which case the sum is q^n-1. □

Lemma 4.6. *For all $n \in \mathbb{N}$, $d \mid n$, prime powers q, and $b \mid q^n-1$,*

$$\#\{f \in \mathcal{F}_d(q) : \ b \mid \ell_f \cdot [n/d]_{q^d}\} = \frac{1}{d} \sum_{c|d} \boldsymbol{\mu}(d/c) \frac{q^n-1}{\operatorname{lcm}\left([n/c]_{q^c}, b\right)} \tag{81}$$

Proof. By Möbius inversion, it suffices to prove

$$\sum_{c|d} c \cdot \#\{f \in \mathcal{F}_c(q) : \ b \mid \ell_f \cdot [n/c]_{q^c}\} = \frac{q^n-1}{\operatorname{lcm}\left([n/d]_{q^d}, b\right)}. \tag{82}$$

View each value $\ell_f \cdot [n/c]_{q^c}$ as an element of $\mathbb{Z}/(q^n-1)$, as in the context of Corollary 2.6. Modulo q^n-1, there are exactly c distinct choices for each $\ell_f \cdot [n/c]_{q^c}$. Namely, given a choice for ℓ_f,

$$\ell_f, q\ell_f, q^2\ell_f, \ldots, q^{c-1}\ell_f \qquad \bmod q^n-1$$

are also valid choices for ℓ_f, and so

$$\ell_f \cdot [n/c]_{q^c}, q\ell_f \cdot [n/c]_{q^c}, q^2\ell_f \cdot [n/c]_{q^c}, \ldots, q^{c-1}\ell_f \cdot [n/c]_{q^c} \qquad \bmod q^n-1$$

are all the possible choices for $\ell_f \cdot [n/c]_{q^c}$ in $\mathbb{Z}/(q^n-1)$. Recalling definition (25), we see that those values are precisely the images under θ_n of the roots of f. Thus, another way to interpret the sum on the left side of (82) is

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

Therefore, by Corollary 2.6, the left side of (82) 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 (82). □

Proof of Corollary 4.4. Using Lemma 4.5 and expanding the k^{th} power in the statement, it remains to show

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

equals

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

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

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

equals

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

This follows from Lemma 4.6. □

5. Asymptotic result

5.1. Prerequisite lemmas. We require some lemmas before proving Theorem 1.8, and we introduce more notation to do so. For a complex number α, let $\bar{\alpha}$ denote the complex conjugate of α, and let $\|\alpha\| = \sqrt{\alpha\bar{\alpha}} \in [0,\infty)$ denote the usual norm of α. Define the function $D : \mathbb{N} \to \mathbb{N} \cup \{0\}$ by

$$D(n) = \begin{cases} 0 & \text{if } n = 1, \\ \max\{s \in \mathbb{N} : s \mid n \text{ and } s < n\} & \text{if } n > 1. \end{cases} \tag{83}$$

In other words, $D(n)$ is the largest proper divisor of n, unless $n = 1$, and $D(1) = 0$. Note that $D(n) \leqslant n/2$ 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 $f, g : S \to [0,\infty)$, then we write $f = O(g)$ to denote that there exist $m \in [0,\infty)$ and $s_0 \in S$ such that $f(s) \leqslant m \cdot g(s)$ 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 $s \in S$.

Remark 5.1. Our aim is to use big O statements to evaluate limits as $q \to \infty$. Therefore, in all expressions involving big O notation in this section, we will take S to be the set of prime powers and use q to denote the argument of each relevant function.

Lemma 5.2. *For all* $n \in \mathbb{N}$, $d \mid n$, *and* $r \in \{0, \ldots, \frac{n}{d} - 1\}$, *we have*

$$\frac{1}{\deg_{n,d,r}(q)} = O\left(q^{-e(n,d,r)}\right), \tag{84}$$

where we define

$$e(n,d,r) = d\binom{r+1}{2} + \binom{n+1}{2} - d\binom{\frac{n}{d}+1}{2} + dr\left(\tfrac{n}{d} - 1 - r\right). \tag{85}$$

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 fact that $\deg_{n,d,r}$ is a rational function of q 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 $r \in \{0, \ldots, \frac{n}{d} - 1\}$. The minimum value of $e(n,d,r)$ on $\{0, \ldots, \frac{n}{d} - 1\}$ is therefore achieved at $r = 0$. Observe that $e(n,d,0) = \frac{n}{2}\left(n - \frac{n}{d}\right)$, 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. □

Lemma 5.3. *For all* $n \in \mathbb{N}, d \mid n, r \in \{0, \ldots, n/d - 1\}$, *we have*

$$\max_{\substack{f \in \mathcal{F}_d(q) \\ f(z) \neq z-1}} \frac{\left\| \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right\|}{\#\mathcal{T}_{(n)}(q)} = O\left(q^{D(n)-n}\right). \tag{86}$$

Proof. Applying Theorem 1.7, Corollary 2.3, (34), Corollary 2.16, and Lemma 4.5, we have

$$\frac{1}{\#\mathcal{T}_{(n)}(q)} \left\| \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right\| = \frac{d \cdot \left| \sum_{s \mid n} \boldsymbol{\mu}(n/s)(q^s - 1)\delta_{q^s - 1 \mid \ell_f[n/d]_{q^d}} \right|}{\sum_{s \mid n} \boldsymbol{\mu}(n/s)(q^s - 1)} \tag{87}$$

for all prime powers q and $f \in \mathcal{F}_d(q)$. The denominator on the right side of (87) is a degree-n polynomial in q, independent of f. However, the numerator on the right side of (87) is not necessarily a polynomial in q at all, as it also depends on ℓ_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

$$\begin{aligned}\left|\sum_{s|n} \boldsymbol{\mu}(n/s)(q^s-1)\delta_{q^s-1|\ell_f\cdot[n/d]_{q^d}}\right| &\leqslant \sum_{\substack{s|n\\ s<n}} |\boldsymbol{\mu}(n/s)(q^s-1)| \\ &\leqslant \sum_{\substack{s|n\\ s<n}} q^s < 1 + \sum_{\substack{s|n\\ s<n}} q^s.\end{aligned} \tag{88}$$

Therefore, in this case

$$\frac{1}{\#\mathcal{T}_{(n)}(q)}\left\|\sum_{g\in\mathcal{T}_{(n)}(q)} \chi^{f,r}(g)\right\| \leqslant d\cdot\frac{1+\sum_{s|n,\, s<n} q^s}{\sum_{s|n}\boldsymbol{\mu}(n/s)(q^s-1)}. \tag{89}$$

Observe that $1+\sum_{s|n,\,s<n} q^s$ is a degree-$D(n)$ polynomial in q, and the right side of (89) is independent of f. Moreover, the condition $q^n - 1 \nmid \ell_f \cdot [n/d]_{q^d}$ is equivalent to $f(z) \neq z-1$ because

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

The result now follows from computing the maximum of (89) over $f \in \mathcal{F}_d(q) \smallsetminus \{z-1\}$. □

Lemma 5.4. *For all $n\in\mathbb{N}$, $\mu\vdash n$, $d\mid n$, $r\in\{0,\dots,\frac{n}{d}-1\}$, we have*

$$\max_{f\in\mathcal{F}_d(q)} \frac{\left\|\sum_{g\in\mathcal{T}_\mu^{\square}(q)}\chi^{f,r}(g)\right\|}{\gamma_n(q)} = O(1). \tag{90}$$

Proof. Consider a fixed prime power q and polynomial $f\in\mathcal{F}_d(q)$ to begin. By Theorem 1.7, if some part of μ 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 2.12, 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 1.7, Corollary 2.16, 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

$$\frac{\gamma_n(q)(-1)^{\frac{n}{d}(d-1)}\chi_{\tilde{\mu}}^{(n/d-r,1^r)}}{\prod_{i=1}^{\ell(\mu)}(q^{\mu_i}-1)} \sum_{\substack{\{h_1,\dots,h_{\ell(\mu)}\}\subset\mathcal{F}(q)\\ \deg h_i=\mu_i\,\forall i}} \prod_{i=1}^{\ell(\mu)}\frac{1}{\tilde{\mu}_i}\sum_{\substack{\alpha_i\in\mathbb{F}_{q^{\mu_i}}\\ h_i(\alpha_i)=0}}\theta(\alpha_i)^{\ell_f\cdot[\tilde{\mu}_i]_{q^d}}. \tag{91}$$

We can now separate the outer sum in (91) according to the degrees of the distinct polynomials $h_i\in\mathcal{F}_{\mu_i}(q)$. Doing so transforms (91) into

$$\frac{\gamma_n(q)(-1)^{\frac{n}{d}(d-1)}\chi_{\tilde{\mu}}^{(n/d-r,1^r)}}{\prod_{i=1}^{\ell(\mu)}(q^{\mu_i}-1)} \prod_{s\geqslant 1}\left(\frac{d}{s}\right)^{m_s(\mu)} \sum_{\{p_1,\dots,p_{m_s(\mu)}\}\subset\mathcal{F}_s(q)} \prod_{i=1}^{m_s(\mu)}\sum_{\substack{\beta_i\in\mathbb{F}_{q^s}\\ p_i(\beta_i)=0}}\theta(\beta_i)^{\ell_f\cdot[s/d]_{q^d}}. \tag{92}$$

Computing the norm, applying the triangle inequality, recalling that θ maps into the unit circle in $\mathbb{C}$, and applying Corollary 2.16 gives

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

Thus,

$$\frac{1}{\gamma_n(q)} \left\| \sum_{g \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(g) \right\| \leqslant \frac{\#\mathcal{T}_\mu^\square(q)}{\gamma_n(q)} \cdot \left| \chi_{\tilde{\mu}}^{(n/d-r,1^r)} \right| \cdot d^{\,\ell(\mu)}. \tag{93}$$

The right side of (93) does not depend on f, which implies

$$\max_{f \in \mathcal{F}_d(q)} \frac{1}{\gamma_n(q)} \left\| \sum_{g \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(g) \right\| \leqslant \frac{\#\mathcal{T}_\mu^\square(q)}{\gamma_n(q)} \cdot \left| \chi_{\tilde{\mu}}^{(n/d-r,1^r)} \right| \cdot d^{\,\ell(\mu)}. \tag{94}$$

Moreover, by Corollary 1.2, for sufficiently large q, the right side of (94) is arbitrarily close to the constant value $|\chi_{\tilde{\mu}}^{(n/d-r,1^r)}| \cdot d^{\ell(\mu)}/z_\mu$. The result follows. □

5.2. Proof of asymptotic result. Recall that we have defined

$$p_{k,\mu}(q) = \frac{g_{k,\mu}(q)}{\#\mathcal{T}_{(n)}(q)^k} \quad \text{and} \quad p_{k,\mu}^\square(q) = \frac{g_{k,\mu}^\square(q)}{\#\mathcal{T}_{(n)}(q)^k} \tag{95}$$

for all $n, k \in \mathbb{N}$, $k \geqslant 2$, and $\mu \vdash n$. We can now prove our asymptotic result, Theorem 1.8, which states

$$\lim_{q \to \infty} p_{k,\mu}(q) = \lim_{q \to \infty} p_{k,\mu}^\square(q) = \frac{1}{z_\mu}. \tag{96}$$

Proof of Theorem 1.8. We will first prove that $\lim_{q\to\infty} p_{k,\mu}^\square(q) = 1/z_\mu$. From this, it follows that $\lim_{q\to\infty} p_{k,\mu}(q) = 1/z_\mu$ because, for all prime powers q, we have $p_{k,\nu}(q) \geqslant p_{k,\nu}^\square(q)$ 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 (15) and by Corollary 3.8, we have

$$p_{k,\mu}^\square(q) = \sum_{d \mid n} \sum_{r=0}^{\frac{n}{d}-1} \sum_{f \in \mathcal{F}_d(q)} \left(\frac{\sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g)}{\#\mathcal{T}_{(n)}(q)} \right)^k \left(\frac{\sum_{h \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(h)}{\gamma_n(q) \cdot \deg_{n,d,r}(q)^{k-1}} \right). \tag{97}$$

We want to compute $\lim_{q\to\infty} p_{k,\mu}^\square(q)$, but the index set for the summation over $f \in \mathcal{F}_d(q)$ in (97) itself depends on q. Therefore, for each $d \mid n$, $r \in \{0, \ldots, n/d - 1\}$, and

$f \in \mathcal{F}_d(q)$ we define

$$\Phi_{k,\mu,d,r}(q) = \sum_{f \in \mathcal{F}_d(q)} \left(\frac{\sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g)}{\#\mathcal{T}_{(n)}(q)} \right)^k \left(\frac{\sum_{h \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(h)}{\gamma_n(q) \cdot \deg_{n,d,r}(q)^{k-1}} \right) \tag{98}$$

so that

$$p_{k,\mu}^\square(q) = \sum_{d \mid n} \sum_{r=0}^{\frac{n}{d}-1} \Phi_{k,\mu,d,r}(q), \tag{99}$$

where the number of terms in the summation is fixed, even as q varies. Theorem 1.8 now follows from Lemma 5.5 below, which computes the limiting behavior of $\Phi_{k,\mu,d,r}(q)$ for each $d \mid n$ and $r \in \{0, \ldots, n/d-1\}$. □

Lemma 5.5. *For all $n, k \in \mathbb{N}, \mu \vdash n, d \mid n$, and $r \in \{0, \ldots, n/d-1\}$, we have*

$$\lim_{q \to \infty} \Phi_{k,\mu,d,r}(q) = \begin{cases} 0 & \text{if } d > 1 \text{ or } r > 0, \\ 1/z_\mu & \text{if } d = 1 \text{ and } r = 0. \end{cases} \tag{100}$$

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

$$\frac{\#\mathcal{F}_d(q)}{\deg_{n,d,r}(q)^{k-1}} \cdot \max_{f \in \mathcal{F}_d(q)} \left(\frac{\left\| \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right\|}{\#\mathcal{T}_{(n)}(q)} \right)^k \cdot \max_{f \in \mathcal{F}_d(q)} \frac{\left\| \sum_{h \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(h) \right\|}{\gamma_n(q)} \tag{101}$$

for all prime powers q. We proceed to investigate the asymptotic dependence on q of (101). Recall from (34) that $\#\mathcal{F}_d(q) = O(q^d)$. Combining this with Lemmas 5.2, 5.3, and 5.4, we have

$$\|\Phi_{k,\mu,d,r}(q)\| = O\left(q^{d+k(D(n)-n)-(k-1)\cdot e(n,d,r)}\right). \tag{102}$$

By hypothesis, $k \geqslant 2$, implying $d + k \cdot (D(n) - n) \leqslant d - k \cdot n/2 \leqslant 0$. Moreover, by Lemma 5.2, $(k-1) \cdot e(n,d,r) > 0$. It follows that $\lim_{q \to \infty} \Phi_{k,\mu,d,r}(q) = 0$ if $d > 1$.

Next, consider the case $d = 1$. Observing that $z - 1 \in \mathcal{F}_1(q)$ for all prime powers q and applying Theorem 3.6, we can rewrite $\Phi_{k,\mu,1,r}(q)$ as

$$\Phi_{k,\mu,1,r}(q) = \frac{\#\mathcal{T}_\mu^\square}{\gamma_n(q)} \cdot \frac{(-1)^{rk} \chi_\mu^{(n-r,1^r)}}{\left(q^{\binom{r+1}{2}} \begin{bmatrix} n-1 \\ r \end{bmatrix}_q\right)^{k-1}} \tag{103}$$

$$+ \sum_{\substack{f \in \mathcal{F}_1(q) \\ f(z) \neq z-1}} \left(\frac{\sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g)}{\#\mathcal{T}_{(n)}(q)} \right)^k \left(\frac{\sum_{h \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(h)}{\gamma_n(q) \cdot \deg_{n,1,r}(q)^{k-1}} \right). \tag{104}$$

We repeat the same analysis as before, but apply it only to (104). Observe that (104) is bounded above by

$$\frac{(\#\mathcal{F}_1(q)) - 1}{\deg_{n,1,r}(q)^{k-1}} \cdot \max_{\substack{f \in \mathcal{F}_1(q) \\ f(z) \neq z-1}} \left(\frac{\left\| \sum_{g \in \mathcal{T}_{(n)}(q)} \chi^{f,r}(g) \right\|}{\#\mathcal{T}_{(n)}(q)} \right)^k \cdot \max_{\substack{f \in \mathcal{F}_1(q) \\ f(z) \neq z-1}} \frac{\left\| \sum_{h \in \mathcal{T}_\mu^\square(q)} \chi^{f,r}(h) \right\|}{\gamma_n(q)} \tag{105}$$

Applying Lemmas 5.2, 5.3, and 5.4 again, we see that (105) is

$$O\left(q^{1+k(D(n)-n)-(k-1)\cdot e(n,1,r)}\right). \tag{106}$$

Observe that $1+k(D(n)-n) < 0$ even if $n = 1$ due to the fact that $k \geqslant 2$ and $D(1) = 0$, and $(k-1)\cdot e(n,1,r) \geqslant 0$ by Lemma 5.2. Therefore, $1+k\cdot(D(n)-n)-(k-1)\cdot e(n,1,r)$ is negative. It follows that the limit as $q \to \infty$ of (104) is zero. By Corollary 1.2, the limit as $q \to \infty$ of (103) equals

$$\begin{cases} 0 & \text{if } r > 0, \\ 1/z_\mu & \text{if } r = 0. \end{cases} \tag{107}$$

The result now follows, as (103) makes the only potentially nontrivial contribution in the limit $q \to \infty$. □

6. Further work

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

Corollary 6.1 (to Theorem 1.3). *Suppose $n, k \in \mathbb{N}$ with $n > 2$. If $\mu \vdash n$ with $m_1(\mu) = 1$, then $g^{\square}_{k,\mu}(q)$ is a polynomial function of q with rational coefficients.*

Proof. By Theorem 1.3, $g^{\square}_{k,\mu}(q)$ agrees with a rational function P/Q with rational coefficients at all prime powers. In particular, since $g^{\square}_{k,\mu}(q)$ is an enumeration of certain factorizations, $P(q)/Q(q) \in \mathbb{Z}$ for all prime powers q. Using polynomial division over $\mathbb{Q}$, we see that there exist polynomials R and S with rational coefficients such that

$$\frac{P}{Q} = R + \frac{S}{Q} \tag{108}$$

and $\deg S < \deg Q$. Choose a positive integer d such that $d \cdot R$ has integer coefficients. This guarantees $d \cdot R(q) \in \mathbb{Z}$ for all prime powers q. It follows that

$$d \cdot \left(\frac{P(q)}{Q(q)} - R(q) \right) = d \cdot \frac{S(q)}{Q(q)} \in \mathbb{Z} \tag{109}$$

for all prime powers q. Taking q to be sufficiently large and recalling $\deg S < \deg Q$ shows that S is identically zero. Thus, $P/Q = R$, a polynomial with rational coefficients. □

One might wonder if $g_{k,\mu}(q)$ or $g^{\square}_{k,\mu}(q)$ is a polynomial function of q for other values of μ, such as $\mu = (n)$. Note that, for all n, $g_{1,(n)}(q) = \#\mathcal{T}_{(n)}(q)$ is, in fact, a polynomial function of q. Unfortunately, $g_{k,(n)}(q)$ fails to be a polynomial function of q when $k \geqslant 2$. However, we can at least prove Corollary 1.9, which states that $g_{k,(n)}(q)$ is a quasipolynomial function of q in the case that n is prime and $k \geqslant 2$.

Proof of Corollary 1.9. We will apply a similar reasoning to that stated in the proof of Corollary 6.1. Recall that $C_{n,k,c}(q)$ is not a rational function of q in general, which prevents $g_{k,(n)}(q)$ from being rational. Define for $i \in \{0, 1, \ldots, n-1\}$ the set

$$M_i = \{q \text{ prime power} : q \equiv i \pmod{n}\}. \tag{110}$$

The result will follow once we can show that, for each $c \mid n$ and $i \in \{0, \ldots, n-1\}$, 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 $i \in \{0, \ldots, n-1\}$ and choice of $c, s_1, \ldots, s_k \mid n$,

$$\operatorname{lcm}\left(\frac{q^n - 1}{q^c - 1}, q^{s_1} - 1, \ldots, q^{s_k} - 1 \right) \tag{111}$$

agrees with some polynomial on M_i. Since n is prime, we have $c, s_1, \ldots, s_k \in \{1, n\}$. Furthermore, if any $s_i = n$, we have that (111) 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 $s_1 = \cdots = s_k = 1$ and hence must show that

$$\operatorname{lcm}\left(\frac{q^n-1}{q^c-1}, q-1\right) \tag{112}$$

is a polynomial on each M_i.

Observe that, if $c = n$, then (112) equals $q-1$, a fixed polynomial in q, independent of the congruence class of q. Therefore, we now need only consider the case $c = s_1 = \cdots = s_k = 1$ and hence must show that

$$\operatorname{lcm}\left(\frac{q^n-1}{q-1}, q-1\right) \tag{113}$$

is a polynomial on each M_i.

Let $i \in \{0, \ldots, n-1\}$ and assume $q = na + i$ for some $a \in \mathbb{N}$. We can compute (113) as

$$\begin{aligned}\operatorname{lcm}\left(\frac{q^n-1}{q-1}, q-1\right) &= \frac{q^n-1}{\gcd\left([n]_q, q-1\right)} = \frac{q^n-1}{\gcd\left(n, q-1\right)} \\ &= \frac{q^n-1}{\gcd(n, na+i-1)} = \frac{q^n-1}{\gcd(n, i-1)} = \begin{cases} \frac{q^n-1}{n} & i = 1 \\ q^n - 1 & i \neq 1. \end{cases}\end{aligned} \tag{114}$$

The result now follows from the fact that (114) is a fixed polynomial in q for each fixed $i \in \{0, \ldots, n-1\}$. □

Example 6.2. We now use our main results to write down alternate formulas for $g_{2,(2)}(q)$ and $g_{2,(3)}(q)$. Note that Theorem 1.5 provides an explicit formula while Theorem 1.8 determines the degree of the polynomials $f_0, \ldots, f_{n-1}$ mentioned in Corollary 1.9. First, for $n = 2$, we have

$$g_{2,(2)}(q) = \frac{q(q-1)^3(q^4 - 3q^3 + 4q^2 - \frac{1}{2}q - \frac{1}{2})}{8} + (-1)^q \cdot \frac{q(q+1)(q-1)^3}{16} \tag{115}$$

for all prime powers q. Second, for $n = 3$, define polynomials

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

Letting $\zeta = e^{2\pi i/3}$, define

$$P_1 = \frac{f_0 + \zeta^2 f_1 + \zeta f_2}{3}, \quad P_2 = \frac{f_0 + \zeta f_1 + \zeta^2 f_2}{3}, \quad P_3 = \frac{f_0 + f_1 + f_2}{3}.$$

Finally, we have

$$g_{2,(3)}(q) = \zeta^q P_1(q) + \zeta^{2q} P_2(q) + P_3(q) \tag{116}$$

for all prime powers q.

Remark 6.3. Data suggest that $g_{k,(n)}(q)$ might be a quasipolynomial function of q for composite n as well. For instance, $g_{2,(6)}(q)$ agrees with a quasipolynomial on all prime powers. Of course, there are no prime powers congruent to 0 (mod 6). However, when $g_{2,(6)}(q)$ is replaced by the formula given in (11), it agrees with a fixed polynomial on multiples of 6.

6.2. 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 $g^{\square}_{k,\mu}(q)$ for cases not yet settled by this paper. However, we also present the following problems associated with strengthening the existing results.

We start with the observation that Theorems 1.3 and 1.5 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. Recall that $g_{k,(n)}(q)$ counts the k-tuples of regular elliptic elements whose product is *any* regular elliptic element in $\mathrm{GL}_n\,\mathbb{F}_q$. In particular, given a *fixed* regular elliptic element $c \in \mathrm{GL}_n\,\mathbb{F}_q$, computing $g_{k,(n)}(q)$ does not necessarily help one count the factorizations $c = t_1 \cdots t_k$ with $t_1, \ldots, t_k \in \mathcal{T}_{(n)}(q)$. For example, consider the case of $k = 2$ for $\mathrm{GL}_2\,\mathbb{F}_5$. There are ten different conjugacy classes consisting of regular elliptic elements, and the various orders of such elements are 3, 6, 8, 12, and 24. Given an arbitrary regular elliptic element $x \in \mathrm{GL}_2\,\mathbb{F}_5$ with order $3, 6$, or 12, there are 76 ordered pairs of regular elliptic elements whose product equals x. On the other hand, given an arbitrary regular elliptic element $y \in \mathrm{GL}_2\,\mathbb{F}_5$ with order 8 or 24, there are 64 ordered pairs of regular elliptic elements whose product equals y. Refining the enumeration provided by computing $g_{2,(2)}(5)$ to the level of individual conjugacy classes is thus more complicated than simply dividing $g_{2,(2)}(5)$ by the number of conjugacy classes that comprise $\mathcal{T}_{(2)}(5)$. Therefore, we propose the following problem.

Problem 6.4. *Refine Theorems* 1.3 *and* 1.5 *to the level of conjugacy classes.*

Next, we recall Corollary 1.9, which says if n is prime, then $g_{k,(n)}(q)$ is a quasipolynomial. Recall from Remark 6.3 that $g_{2,(6)}(q)$ is also a quasipolynomial. One might hope that $g_{k,(n)}(q)$ is, in fact, *always* a quasipolynomial.

Problem 6.5. *Prove that* $g_{k,(n)}(q)$ *is a quasipolynomial for composite* n *as well.*

We conclude with a problem about q-analogues. As can be seen in (8), for some choices of $\mu \vdash n$ and after appropriately normalizing, $g^{\square}_{k,\mu}(q)$ appears to be a q-analogue of $g_{k,\mu}$ in the traditional $q \to 1$ sense. Unfortunately, it is not clear whether $g_{k,(n)}(q)$ exhibits the same behavior.

Problem 6.6. *Establish a precise way in which* $g_{k,(n)}(q)$ *is a* q*-analogue of* $g_{k,(n)}$.

As a final remark, we point out a certain incompatibility of our definition of cycle type, inspired by [18, 32], with a related notion from more recent work. In [16, 21, 22], the dimension of the fixed space of an element in $\mathrm{GL}_n\,\mathbb{F}_q$ plays the analogous role to the number of cycles in a permutation in $\mathfrak{S}_n$. Whereas the cycle type in $\mathfrak{S}_n$ *is* a refinement of the number of cycles, our notion of cycle type in $\mathrm{GL}_n\,\mathbb{F}_q$ is *not* a refinement of the dimension of the fixed space. Still, it might be worth investigating ways to reconcile these two notions.

Acknowledgments

The author thanks Sara Billey, Jia Huang, Joseph Kung, Joel Lewis, Alejandro Morales, and Vic Reiner for their helpful advice and guidance during the preparation of the original manuscript. Furthermore, the author thanks the two anonymous referees whose feedback contributed greatly to a more polished paper.

References

[1] E. A. Bertram and V. K. Wei, *Decomposing a permutation into two large cycles: an enumeration*, SIAM J. Algebraic Discrete Methods **1** (1980), no. 4, 450–461.

[2] G. Boccara, *Nombre de représentations d'une permutation comme produit de deux cycles de longueurs données*, Discrete Math. **29** (1980), no. 2, 105–134.

[3] M. Bóna and B. Pittel, *On the cycle structure of the product of random maximal cycles*, Sém. Lothar. Combin. **80** ([2019–2021]), article no. Art. B30b (37 pages).

[4] L. Brickman and P. A. Fillmore, *The invariant subspace lattice of a linear transformation*, Canad. J. Math. **19** (1967), 810–822.

[5] G. Chapuy and C. Stump, *Counting factorizations of Coxeter elements into products of reflections*, J. Lond. Math. Soc. (2) **90** (2014), no. 3, 919–939.

[6] J. Dénes, *The representation of a permutation as the product of a minimal number of transpositions, and its connection with the theory of graphs*, Magyar Tud. Akad. Mat. Kutató Int. Közl. **4** (1959), 63–71.

[7] D. S. Dummit and R. M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[8] R. Ekedahl, S. Lando, M. Shapiro, and A. Vainshtein, *Hurwitz numbers and intersections on moduli spaces of curves*, Invent. Math. **146** (2001), no. 2, 297–327.

[9] F. G. Frobenius, *Gesammelte Abhandlungen. Bände I, II, III*, Herausgegeben von J.-P. Serre, Springer-Verlag, Berlin-New York, 1968.

[10] J. Fulman, *Cycle indices for the finite classical groups*, J. Group Theory **2** (1999), no. 3, 251–289.

[11] W. Fulton, *Young tableaux*, London Mathematical Society Student Texts, vol. 35, Cambridge University Press, Cambridge, 1997.

[12] W. Fulton and J. Harris, *Representation theory*, Graduate Texts in Mathematics, vol. 129, Springer-Verlag, New York, 1991.

[13] C. F. Gauss, *Disquisitiones arithmeticae*, Yale University Press, New Haven, Conn.-London, 1966, Translated into English by Arthur A. Clarke, S. J.

[14] 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** (1992), no. 5, 357–365.

[15] J. A. Green, *The characters of the finite general linear groups*, Trans. Amer. Math. Soc. **80** (1955), 402–447.

[16] J. Huang, J. B. Lewis, and V. Reiner, *Absolute order in general linear groups*, J. Lond. Math. Soc. (2) **95** (2017), no. 1, 223–247.

[17] D. M. Jackson, *Counting cycles in permutations by group characters, with an application to a topological problem*, Trans. Amer. Math. Soc. **299** (1987), no. 2, 785–801.

[18] J. P. S. Kung, *The cycle structure of a linear transformation over a finite field*, Linear Algebra Appl. **36** (1981), 141–155.

[19] S. K. Lando and A. K. Zvonkin, *Graphs on surfaces and their applications*, Encyclopaedia of Mathematical Sciences, vol. 141, Springer-Verlag, Berlin, 2004, With an appendix by Don B. Zagier.

[20] G. I. Lehrer, *The cohomology of the regular semisimple variety*, J. Algebra **199** (1998), no. 2, 666–689.

[21] J. B. Lewis and A. H. Morales, $\mathrm{GL}_n(\mathbb{F}_q)$*-analogues of factorization problems in the symmetric group*, European J. Combin. **58** (2016), 75–95.

[22] J. B. Lewis, V. Reiner, and D. Stanton, *Reflection factorizations of Singer cycles*, J. Algebraic Combin. **40** (2014), no. 3, 663–691.

[23] I. G. Macdonald, *Symmetric functions and Hall polynomials*, second ed., Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1995.

[24] F. D. Murnaghan, *On the Representations of the Symmetric Group*, Amer. J. Math. **59** (1937), no. 3, 437–488.

[25] T. Nakayama, *On some modular properties of irreducible representations of a symmetric group. I*, Jpn. J. Math. **18** (1941), 89–108.

[26] B. E. Sagan, *The symmetric group*, second ed., Graduate Texts in Mathematics, vol. 203, Springer-Verlag, New York, 2001.

[27] J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York-Heidelberg, 1977, Graduate Texts in Mathematics, Vol. 42.

[28] R. P. Stanley, *Factorization of permutations into n-cycles*, Discrete Math. **37** (1981), no. 2-3, 255–262.

[29] ———, *Enumerative combinatorics. Vol. 2*, Cambridge Studies in Advanced Mathematics, vol. 62, Cambridge University Press, Cambridge, 1999, With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin.

[30] ———, *Enumerative combinatorics. Volume 1*, second ed., Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 2012.

[31] R. Steinberg, *A geometric approach to the representations of the full linear group over a Galois field*, Trans. Amer. Math. Soc. **71** (1951), 274–282.

[32] R. Stong, *Some asymptotic results on finite vector spaces*, Adv. in Appl. Math. **9** (1988), no. 2, 167–199.
[33] R. Vakil, *Genus 0 and 1 Hurwitz numbers: recursions, formulas, and graph-theoretic interpretations*, Trans. Amer. Math. Soc. **353** (2001), no. 10, 4025–4038.
[34] D. W. Walkup, *How many ways can a permutation be factored into two n-cycles?*, Discrete Math. **28** (1979), no. 3, 315–319.

Graham Gordon, University of Washington, Seattle, WA 98195
Proof School, 973 Mission St, San Francisco, CA 94103
E-mail : ggordon@proofschool.org