Cycle Indices in Arithmetic Geometry

by

Gilyoung Cheong

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2021

Doctoral Committee:

Professor Michael E. Zieve, Co-Chair
Professor Mircea Immanuel Mustaţă, Co-Chair
Professor Alexander Barvinok
Professor Mel Hochster
Professor Seth Pettie
Professor John R. Stembridge

Gilyoung Cheong
gcheong@umich.edu
ORCID iD: 0000-0002-6593-4862

For my grandmothers

ACKNOWLEDGEMENTS

First, I would like to thank my advisors, Mike Zieve and Mircea Mustaţă, for their guidance, kindness, and patience throughout my PhD program, let alone the process of writing this thesis. I am grateful for a collaboration with Melanie Matchett Wood, which shaped my mathematical interests leading to this thesis. I would like to thank Yifeng Huang for sharing his brilliance in our collaborations. Thank you to my favorite teachers, Sasha Barvinok, Mel Hochster, John Stembridge, and Seth Pettie, for serving on my thesis defense committee. I would also like to extend my deepest gratitude to Teresa Stokes for guiding me through each step toward the defense.

I would like to thank Bhargav Bhatt, Kwun Chung, Bill Fulton, Ofir Gorodetsky, Haoyang Guo, Nathan Kaplan, Dohyeong Kim, Shizhang Li, Yuan Liu, Alison Miller, Shubhodip Mondal, Eric Rains, Emanuel Reinecke, Brad Rodgers, Yinan Nancy Wang, Jakub Witaszek, and Myungjun Yu for helpful mathematical conversations. Thank you to Jordan Ellenberg, Wei Ho, Luc Illusie, Tasho Kaletha, Chan-Ho Kim, Minhyong Kim, Karol Koziol, Jeff Lagarias, Karen Smith, and Andrew Snowden for advice on my career as a mathematician. I deeply thank my former teachers, Atanas Iliev, Dano Kim, and Yongmin Kim, for their guidance prior to my PhD program.

Finally, I would like to thank my parents, uncle Sungwook, aunt Youngsug, my brother, and Cassandra for their support and encouragement throughout this long journey toward my PhD degree as a family.

TABLE OF CONTENTS

CHAPTER

ABSTRACT

A cycle index is a polynomial that encodes information about the orbits of a finite group action on a finite set, which is used in combinatorics to count various objects up to group actions. In this thesis, we give a general framework for the cycle indices of a sequence of finite group actions on finite sets and study how certain cycle indices can be used in algebraic geometry and number theory.

As motivating examples, we will see how the zeta series of a projective variety over a finite field is related to the cycle indices of symmetric groups and how the distribution of the cokernel of a Haar random matrix over the p-adic integers is related to the cycle indices of conjugation actions of general linear groups on matrices over the finite field $\mathbb{F}_p$ of p elements.

CHAPTER I

Introduction

A **generating function** is a power series $f_{\boldsymbol{a}}(u) = a_0 + a_1u + a_2u^2 + \cdots$, whose coefficients consist of information $\boldsymbol{a} = (a_0, a_1, a_2, \dots)$ that we would like to understand. When $a_0, a_1, a_2, \dots$ come from objects that form a particular structure, we may try to reflect such a structure to the generating function $f_{\boldsymbol{a}}(u)$. Then such a reflection often helps us see a feature of $a_0, a_1, a_2, \dots$ that was not obvious in the first place.

For example, let a_n be the number of ways to color n points without ordering, with the colors chosen from a finite set X, allowing repetitions. That is, we have $a_n = |\mathrm{Sym}^n(X)|$, where $\mathrm{Sym}^n(X) := X^n/S_n$ with respect to the action of S_n on X^n by permuting coordinates. One can quickly realize that

$$f_{\boldsymbol{a}}(u) = \sum_{n=0}^{\infty} |\mathrm{Sym}^n(X)|u^n = (1 + u + u^2 + \cdots)^{|X|} = \left(\frac{1}{1-u}\right)^{|X|}$$

since a monomial of the form $u^{d_1} \cdots u^{d_l}$ corresponds to a coloring with l colors on $d_1, \dots, d_l$ points.

When X is a compact complex manifold, it turns out that we have

$$\sum_{n=0}^{\infty} \chi(\mathrm{Sym}^n(X))u^n = \left(\frac{1}{1-u}\right)^{\chi(X)},$$

a rational formula for the generating function of the Euler characteristics of the symmetric powers of X, which is due to Macdonald in [Mac1962A]. This generalizes the counting result in the previous paragraph when X is a finite set by giving it the discrete topology. In the same paper, Macdonald also showed that we can compute all the Betti numbers of the symmetric powers of X in a similar manner. That is, we have

$$\sum_{n=0}^{\infty} \chi_t(\mathrm{Sym}^n(X))u^n = \frac{(1-tu)^{b_1(X)} \cdots (1-t^{2d-1}u)^{b_{2d-1}(X)}}{(1-u)^{b_0(X)} \cdots (1-t^{2d}u)^{b_{2d}(X)}},$$

where d is the (complex) dimension of X and

$$\chi_t(Y) := \sum_{i=0}^{\infty}(-t)^i b_i(Y),$$

a power series[1] in t with integral coefficients, defined for any topological space Y with finite singular Betti numbers. This generalizes the result about the Euler characteristics of $(\mathrm{Sym}^n(X))_{n\in\mathbb{Z}_{\geqslant 0}}$ by taking $t = 1$.

There is an arithmetic analogue of the rational generating functions we have discussed so far. Let X be a quasi-projective variety over a finite field $\mathbb{F}_q$. Then the symmetric powers $\mathrm{Sym}^n(X)$ are also varieties over $\mathbb{F}_q$, so we can discuss their sets $\mathrm{Sym}^n(X)(\mathbb{F}_q)$ of $\mathbb{F}_q$-points. Consider the **zeta series** $\boldsymbol{Z}_X(u)$ of X, with the following three equivalent expressions[2]:

$$\boldsymbol{Z}_X(u) = \prod_{x\in|X|} \frac{1}{1-u^{\deg(x)}} = \exp\left(\sum_{r=1}^{\infty} \frac{|X(\mathbb{F}_{q^r})|u^r}{r}\right) = \sum_{n=0}^{\infty} |\mathrm{Sym}^n(X)(\mathbb{F}_q)|u^n,$$

[1] We shall call $\chi_t(Y)$ the **Poincaré series** of Y although it is more common to use the terminology for $\chi_{(-t)}(Y)$, the generating function for $b_i(Y)$. If $b_i(Y) = 0$ for all large enough i, we have $\chi_1(Y) = \chi(Y)$, the Euler characteristic of Y.

[2] The second expression is evidently well-defined, so we often use this as the definition of $\boldsymbol{Z}_X(u)$. The fact that the first and the second expressions are the same can be found in [Mus, Proposition 2.7]. The fact that the first and the third expressions are the same can be found in [Mus, Proposition 7.31]. We provide a separate proof that the second and the third expressions as the same.

where $|X|$ now means the set of closed points of X. That is, the zeta series of X is the generating function of the $\mathbb{F}_q$-point counts of the symmetric powers of X. A result of Dwork [Dwo1960] says that the zeta series is rational. A cohomological version of this theorem due to Grothendieck says

$$\sum_{n=0}^{\infty} |\mathrm{Sym}^n(X)(\mathbb{F}_q)|u^n = \frac{\det(\mathrm{id}_{H^1(X)} - \mathrm{Fr}^*_{q,X,1}u)\cdots\det(\mathrm{id}_{H^{2d-1}(X)} - \mathrm{Fr}^*_{q,X,2d-1}u)}{\det(\mathrm{id}_{H^0(X)} - \mathrm{Fr}^*_{q,X,0}u)\cdots\det(\mathrm{id}_{H^{2d}(X)} - \mathrm{Fr}^*_{q,X,2d}u)},$$

where $H^i(X)$ is the i-th compactly supported étale cohomology group of $X_{/\overline{\mathbb{F}}_q} = X \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(\overline{\mathbb{F}}_q)$ with $\mathbb{Q}_l$-coefficients for some prime l not dividing q and $F = \mathrm{Fr}_{q,X}$ is the **Frobenius** endomorphism on X, which is the map from X to itself given by the identity on the underlying topological space and the q-th power map on the structure sheaf $\mathscr{O}_X$.

The first theorem we state combines the above rationality results altogether[3]:

Theorem I.1. *Let X be either a compact complex manifold of dimension d or a quasi-projective variety of dimension d over a finite field $\mathbb{F}_q$. Then for any endomorphism F on X, we have*

$$\sum_{n=0}^{\infty} L_t(\mathrm{Sym}^n(F)^*)u^n = \frac{\det(\mathrm{id}_{H^1(X)} - F_1^* tu)\cdots\det(\mathrm{id}_{H^{2d-1}(X)} - F^*_{2d-1}t^{2d-1}u)}{\det(\mathrm{id}_{H^0(X)} - F_0^* u)\cdots\det(\mathrm{id}_{H^{2d}(X)} - F^*_{2d}t^{2d}u)},$$

where

- *$H^i(X)$ is the i-th singular cohomology group of X with $\mathbb{Q}$-coefficients when X is a compact complex manifold,*
- *$H^i(X)$ is the i-th compactly supported étale cohomology group of $X_{/\overline{\mathbb{F}}_q} = X \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(\overline{\mathbb{F}}_q)$ with $\mathbb{Q}_l$-coefficients when X is a quasi-projective variety over $\mathbb{F}_q$ for some prime l,*

[3] Vakil discussed this in Arizona Winter School 2015 [Vak2015] when $t = 1$. The method we choose, a generalization of Macdonald's method, seems different from Vakil's.

- $\mathrm{Sym}^n(F)$ *is the endomorphism on* $\mathrm{Sym}^n(X)$ *induced by* F*,*
- F_i^* *is the endomorphism on* $H^i(X)$ *induced by* F*, and*
- $L_t(\phi) := \sum_{i=0}^{\infty}(-t)^i \mathrm{Tr}(\phi_i^*)$*, the alternating generating function of traces of a given graded linear endomorphism* $\phi = \bigoplus_{i=0}^{\infty} \phi_i$ *on a graded vector space* $V = \bigoplus_{i=0}^{\infty} V_i$ *with finite-dimensional* V_i *for all* $i \in \mathbb{Z}_{\geqslant 0}$*.*

Remark I.2. When X is a compact complex manifold of dimension d, we may take $F = \mathrm{id}_X$, the identity of X, in the singular setting of Theorem I.1 to recover Macdonald's formula, which we repeat here:

$$\sum_{n=0}^{\infty} \chi_t(\mathrm{Sym}^n(X))u^n = \frac{(1-tu)^{b_1(X)} \cdots (1-t^{2d-1}u)^{b_{2d-1}(X)}}{(1-u)^{b_0(X)} \cdots (1-t^{2d}u)^{b_{2d}(X)}}.$$

When X is a quasi-projective variety over $\mathbb{F}_q$, we may take $F = \mathrm{Fr}_{q,X}$ and $t = 1$ in the l-adic setting of Theorem I.1 to recover Grothendieck's formula, which we repeat here:

$$\sum_{n=0}^{\infty} |\mathrm{Sym}^n(X)(\mathbb{F}_q)|u^n = \frac{\det(\mathrm{id}_{H^1(X)} - \mathrm{Fr}_{q,X,1}^* u) \cdots \det(\mathrm{id}_{H^{2d-1}(X)} - \mathrm{Fr}_{q,X,2d-1}^* u)}{\det(\mathrm{id}_{H^0(X)} - \mathrm{Fr}_{q,X,0}^* u) \cdots \det(\mathrm{id}_{H^{2d}(X)} - \mathrm{Fr}_{q,X,2d}^* u)},$$

where we used the Grothendieck-Lefschetz trace formula $L_1(\mathrm{Fr}_{q,Y}^*) = |Y(\mathbb{F}_q)|$ for $Y = \mathrm{Sym}^n(X)$ with $l \nmid q$, noticing that $\mathrm{Sym}^n(\mathrm{Fr}_{q,X}) = \mathrm{Fr}_{q,\mathrm{Sym}^n(X)}$.

We will see that Theorem I.1 is a combinatorial corollary of the following:

Theorem I.3. *Assume the same hypotheses as in Theorem I.1. Let* G *be a subgroup of* S_n *with* $n \in \mathbb{Z}_{\geqslant 0}$*,*[4] *acting on* X^n *by permuting coordinates. Then*

$$L_t((F^n/G)^*) = Z_G(L_t(F^*), L_{t^2}((F^*)^2), \ldots, L_{t^n}((F^*)^n)),$$

[4] Note that S_0 is the trivial group because there is a unique map from the empty set to any set.

where F^n/G is the endomorphism of X^n/G induced by F and

$$Z_G(\boldsymbol{x}) = Z_G(x_1, \ldots, x_n) := \frac{1}{|G|} \sum_{g \in G} x_1^{m_1(g)} \cdots x_n^{m_n(g)} \in \mathbb{Q}[x_1, \ldots, x_n],$$

denoting by $m_i(g)$ the number of i-cycles in the cycle decomposition of g in S_n.

Remark I.4. The polynomial $Z_G(x_1, \ldots, x_n)$ in Theorem I.3 is called the **cycle index** of G in S_n. This polynomial was independently introduced by Redfield [Red1927] and Pólya [Pol1937] (or [PR1987]) to count the number of colorings on a graph modulo symmetries (e.g., Theorem III.1). Applying Theorem I.3 to the case where X is a compact complex manifold and $F = \mathrm{id}_X$, we get

$$\chi_t(X^n/G) = Z_G(\chi_t(X), \chi_{t^2}(X), \ldots, \chi_{t^n}(X)),$$

which is a result of Macdonald [Mac1962A]. When we take X to be a quasi-projective variety over $\mathbb{F}_q$ and $F = \mathrm{Fr}_{q,X}$, Theorem I.3 computes the number $|(X^n/G)(\mathbb{F}_q)|$ of $\mathbb{F}_q$-points on the quotient variety X^n/G as follows:

$$|(X^n/G)(\mathbb{F}_q)| = Z_G(|X(\mathbb{F}_q)|, |X(\mathbb{F}_{q^2})|, \ldots, |X(\mathbb{F}_{q^n})|)$$

by applying the Grothendieck-Lefschetz trace formula $L_1((\mathrm{Fr}_{q,Y}^*)^r) = |Y(\mathbb{F}_{q^r})|$, where Y is any variety over $\mathbb{F}_q$ and $r \in \mathbb{Z}_{\geqslant 1}$. Using Theorem I.3, we can obtain an analogue of Theorem I.1 for alternating groups, which is available in [Che2020]. We do not discuss this analogue in this thesis.

Remark I.5. Theorems I.1 and I.3 hold in much greater generality (e.g., Theorem III.13 and Corollary III.14). A sufficient set of axioms for theses statements to be true is given in Section 3.4.

The key formula (Lemma II.12) about the generating function of the cycle indices of $(S_n)_{n\geqslant 0}$, which is used in showing that Theorem I.3 implies Theorem I.1, is

$$\sum_{n=0}^{\infty} Z_{S_n}(x_1, \ldots, x_n)u^n = \prod_{r\in\mathbb{Z}_{\geqslant 1}} \sum_{m\in\mathbb{Z}_{\geqslant 0}} \frac{x_r^m u^{mr}}{m! r^m} = \exp\left(\sum_{r=1}^{\infty} \frac{x_r u^r}{r}\right).$$

A proof of this implication is provided more generally in the proof of Corollary III.10. To get an idea about how this formula can be used, apply

$$|\mathrm{Sym}^n(X)(\mathbb{F}_q)| = Z_{S_n}(|X(\mathbb{F}_q)|, |X(\mathbb{F}_{q^2})|, \ldots, |X(\mathbb{F}_{q^n})|),$$

a special case of Theorem I.3, to the above identity to get

$$\sum_{n=0}^{\infty} |\mathrm{Sym}^n(X)(\mathbb{F}_q)|u^n = \exp\left(\sum_{r=1}^{\infty} \frac{|X(\mathbb{F}_{q^r})|u^r}{r}\right),$$

which shows the equivalence of the two definitions of the zeta series $Z_X(u)$ of X.

The formula for the generating function of the cycle indices of symmetric groups is an example of what we call a **factorization formula** in Chapter II. More specifically, Lemma II.11 provides a general factorization formula for the cycle indices of a sequence $(G_n \circlearrowright E_n)_{n\geqslant 0}$ of finite group actions on finite sets with certain conditions (to be explained in Chapter II). We will see that the cycle index of S_n can be identified as the cycle index of its conjugation action to itself. Another use of the factorization formula for the generating function of $(Z_{S_n}(\boldsymbol{x}))_{n\geqslant 0}$ is a proof of the following theorem by Lloyd and Shepp [SL1966], as explained in [CNY20]:

Proposition I.6 (Lloyd and Shepp)**.** *Given distinct $d_1, \ldots, d_r \in \mathbb{Z}_{\geqslant 1}$ and not necessarily distinct $k_1, \ldots, k_r \in \mathbb{Z}_{\geqslant 0}$, where $r \in \mathbb{Z}_{\geqslant 0}$, we have*

$$\lim_{n\to\infty} \operatorname*{Prob}_{g\in S_n} \left(\begin{array}{c} m_{d_j}(g) = k_j \\ \text{for } 1 \leqslant j \leqslant r \end{array} \right) = \prod_{j=1}^{r} \frac{e^{-1/d_j}(1/d_j)^{k_j}}{k_j!},$$

which means that the number of cycles of length $d_1, \ldots, d_r$ of a random permutation of n letters are asymptotically given by independent Poisson random variables with means $1/d_1, \ldots, 1/d_r$ when n is large.

The analogous result for matrices over $\mathbb{F}_q$ is the following:

Theorem I.7. *Fix any distinct monic irreducible polynomials $P_1(t), \ldots, P_r(t) \in \mathbb{F}_q[t]$ and P_j^∞-torsion $\mathbb{F}_q[t]$-module H_j of finite length for $1 \leqslant j \leqslant r$, where $r \in \mathbb{Z}_{\geqslant 0}$. Then*

$$\lim_{n \to \infty} \underset{A \in \mathrm{Mat}_n(\mathbb{F}_q)}{\mathrm{Prob}} \left(\begin{array}{c} A[P_j^\infty] \simeq H_j \\ \\ \textit{for } 1 \leqslant j \leqslant r \end{array} \right) = \prod_{j=1}^{r} \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_j)|} \prod_{i=1}^{\infty} (1 - q^{-i \deg(P_j)}),$$

where $A[P_j^\infty]$ is the (P_j)-part of the $\mathbb{F}_q[t]$-module structure on $\mathbb{F}_q^n$, whose t-action is given by the multiplication by A. In particular, given any distinct $a_1, \ldots, a_r \in \mathbb{F}_q$, we have

$$\lim_{n \to \infty} \underset{A \in \mathrm{Mat}_n(\mathbb{F}_q)}{\mathrm{Prob}} \left(\begin{array}{c} a_1, \ldots, a_r \textit{ are not} \\ \\ \textit{eigenvalues of } A \end{array} \right) = \left(\prod_{i=1}^{\infty} (1 - q^{-i}) \right)^r .$$

Remark I.8. Theorem I.7 is proven by using the factorization formula for the cycle indices of conjugation actions of $\mathrm{GL}_n(\mathbb{F}_q)$ on $\mathrm{Mat}_n(\mathbb{F}_q)$, the set of $n \times n$ matrices over $\mathbb{F}_q$ for $n \in \mathbb{Z}_{\geqslant 0}$ just as Proposition I.6 can be proven by using the factorization formula for the cycle indices of $(S_n)_{n \in \mathbb{Z}_{\geqslant 0}}$.

Matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ can be seen as $\mathbb{F}_q[t]$-modules or sheaves over $\mathbb{A}^1_{\mathbb{F}_q} = \mathrm{Spec}(\mathbb{F}_q[t])$. We will see that the next theorem generalizes Theorem I.7 by taking $X = \mathbb{A}^1_{\mathbb{F}_q}$:

Theorem I.9. *Let X be a smooth, projective, and geometrically irreducible curve over $\mathbb{F}_q$ minus finitely many closed points. Given any distinct closed points $p_1, \dots, p_r$ of X, let H_j be a finite length module over $\mathscr{O}_{X,p_j}$ for $1 \leqslant j \leqslant r$, where $r \in \mathbb{Z}_{\geqslant 0}$. Then*

$$\lim_{n \to \infty} \operatorname*{Prob}_{[\mathcal{F}] \in \boldsymbol{Mod}_{\mathscr{O}_X}^{=q^n}} \left(\begin{array}{c} \mathcal{F}_{p_j} \simeq H_j \\ \\ \textit{for } 1 \leqslant j \leqslant r \end{array} \right) = \prod_{j=1}^{r} \frac{1}{|\mathrm{Aut}_{\mathscr{O}_{X,p_j}}(H_j)|} \prod_{i=1}^{\infty} (1 - q^{-i \deg(p_j)}),$$

where $\boldsymbol{Mod}_{\mathscr{O}_X}^{=q^n}$ is the set of isomorphism classes $[\mathcal{F}]$ of torsion coherent $\mathscr{O}_X$-modules $\mathcal{F}$ with $\sum_{p \in |X|} \dim_{\mathbb{F}_q}(\mathcal{F}_p) = n$, or equivalently $|\bigoplus_{p \in |X|} \mathcal{F}_p| = q^n$, denoting by $|X|$ to mean the set of closed points of X.

The last result in this section is about Haar random matrices in $\mathrm{Mat}_n(\mathbb{Z}_p)$, the group of matrices over $\mathbb{Z}_p$, the ring of p-adic integers. This will be seen as an application of Theorem I.7:

Theorem I.10. *Let $P_1(t), \dots, P_r(t) \in \mathbb{Z}_p[t]$ be monic polynomials such that the reduction modulo p gives distinct irreducible polynomials $\overline{P}_1(t), \dots, \overline{P}_r(t) \in \mathbb{F}_p[t]$, where $r \in \mathbb{Z}_{\geqslant 1}$. Suppose that $\deg(P_r) = 1$. Given any finite abelian p-group H, we have*

$$\lim_{n \to \infty} \operatorname*{Prob}_{A \in \mathrm{Mat}_n(\mathbb{Z}_p)} \left(\begin{array}{c} \mathrm{coker}(P_j(A)) = 0 \\ \\ \textit{for } 1 \leqslant j \leqslant r-1 \\ \\ \textit{and } \mathrm{coker}(P_r(A)) \simeq H \end{array} \right) = \frac{1}{|\mathrm{Aut}_{\mathbb{Z}}(H)|} \prod_{j=1}^{r} \prod_{i=1}^{\infty} (1 - q^{-i \deg(P_j)}).$$

1.1 Contributions

Theorems I.1 and I.3 are from [Che2020] due to the author. Theorem I.7 is originally due to Boreico [Bor2016], independently found later by the author and

Huang in [CH2018], where they proved Theorem I.10. Theorem I.9 is from joint work in process by the author, Haoyang Guo, and Yifeng Huang.

1.2 Outline

In Chapter II, we give a formal definition of the cycle index of an action of a finite group G on a finite set E. We will see that given a specific set of hypotheses, the generating function of a family $G_n \circlearrowright E_n$ of such actions index by $n \in \mathbb{Z}_{\geqslant 0}$ admits an interesting factorization, which is the content of Theorem II.11. Then we discuss examples of such factorizations, which we use in deducing Theorem I.1 from Theorem I.3 and proving Theorem I.7 in later chapters.

In Chapter III, we provide the combinatorial origin of Theorem I.3, called the Pólya enumeration theorem, which is about counting the number of colorings on the vertices of a graph modulo symmetries. We give a Hodge-theoretic analogue of this theorem due to Cheah [Che1994] and then prove Theorem III.13, a more general theorem that will imply Theorems I.3 as well as their analogues.

In Chapter IV, we prove Theorems I.7 and I.10, restated as Theorems IV.1 and C. Finally, in Chapter V, we prove Theorem I.9, restated as Theorem V.1.

CHAPTER II

Cycle Indices and Their Factorization Formulas

In this chapter, we establish a formalism for cycle indices of finite group actions and discuss two main examples (Examples II.3 and II.4) we will use later. The most important content of this chapter is Lemma II.11, a combinatorial factorization formula of the generating function of a sequence of cycle indices.

2.1 Cycle indices of finite group actions

Setting II.1. Suppose that we are given

- a set map $d : \mathscr{P} \to \mathbb{Z}_{\geqslant 1}$ with a nonempty set $\mathscr{P}$;
- a set map $s : \mathcal{I} \to \mathbb{Z}_{\geqslant 0}$ with a nonempty set $\mathcal{I}$;
- a unique element $* \in \mathcal{I}$ such that $s(*) = 0$;
- a finite group G acting on a finite set E (on the left);
- a set injection $i : E/G \hookrightarrow \mathrm{Hom}_{\mathbf{Set}}(\mathscr{P}, \mathcal{I})$ from the set E/G of G-orbits into the set $\mathrm{Hom}_{\mathbf{Set}}(\mathscr{P}, \mathcal{I})$ of set maps from $\mathscr{P}$ to $\mathcal{I}$ so that each orbit $Ge = [e] \in E/G$ corresponds to $i([e]) \in \mathrm{Hom}_{\mathbf{Set}}(\mathscr{P}, \mathcal{I})$. We may write $i(e)_p := i([e])(p)$ for our

convenience, which makes sense if we consider the composition $E \to E/G \xrightarrow{i} \mathrm{Hom}_{\mathbf{Set}}(\mathscr{P}, \mathcal{I})$. We define $\boldsymbol{d} : \mathrm{Hom}_{\mathbf{Set}}(\mathscr{P}, \mathcal{I}) \to \mathbb{Z}_{\geqslant 0} \sqcup \{\infty\}$ by

$$\boldsymbol{d}((i_p)_{p \in \mathscr{P}}) := \sum_{p \in \mathscr{P}} s(i_p) d(p)$$

and require

- $\boldsymbol{d}(i(E/G)) \subset \mathbb{Z}_{\geqslant 0}$ (i.e., the image $i(E/G)$ only takes finite $\boldsymbol{d}$-values);
- a set map $N : \mathscr{P} \times \mathcal{I} \to \mathbb{Z}_{\geqslant 1}$ such that $|G_e| = \prod_{p \in \mathscr{P}} N(p, i_p(e))$ for any $e \in E$, where G_e is the stabilizer subgroup of the given G-action at $e \in E$.

Remark II.2. We recall that by the orbit-stabilizer theorem, the size of the stabilizer subgroup is constant on any orbit. Hence, the notation $|G_{[e]}|$ is well-defined even though $G_{[e]}$ is not.

Example II.3 (Symmetric groups)**.** We take $G = S_n = E$, and consider the conjugation action. Take $\mathscr{P} = \mathbb{Z}_{\geqslant 1}$ and $\mathcal{I} = \mathbb{Z}_{\geqslant 0}$. Define $i : S_n/S_n \hookrightarrow \mathrm{Hom}_{\mathbf{Set}}(\mathbb{Z}_{\geqslant 1}, \mathbb{Z}_{\geqslant 0})$ by $[e] \mapsto (m_p(e))_{p \in \mathbb{Z}_{\geqslant 1}}$. We know i is injective because the n-tuple $(m_1(e), \ldots, m_n(e))$ determines the orbit of $e \in E = S_n$ and all the other $m_p(e)$ with $p > n$ are zeros. We define both $d : \mathscr{P} = \mathbb{Z}_{\geqslant 1} \to \mathbb{Z}_{\geqslant 1}$ and $s : \mathcal{I} = \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0}$ to be the identity maps, and thus we get $* = 0$. Then $\boldsymbol{d} : \mathrm{Hom}_{\mathbf{Set}}(\mathbb{Z}_{\geqslant 1}, \mathbb{Z}_{\geqslant 0}) \to \mathbb{Z}_{\geqslant 0} \sqcup \{\infty\}$ is given by $\boldsymbol{d}(f) = \sum_{p \in \mathbb{Z}_{\geqslant 1}} f(p)p$. Note that any element of the image $i(S_n/S_n)$ takes only finite $\boldsymbol{d}$-values. In fact, we have $\boldsymbol{d}(m_p(e))_{p \in \mathbb{Z}_{\geqslant 1}} = n$ for any $e \in E = S_n$. Moreover, we have $\boldsymbol{d}^{-1}(n) = i(S_n/S_n)$. Indeed, for any $(i_p)_{p \in \mathscr{P}}$ with $\boldsymbol{d}((i_p)_{p \in \mathscr{P}}) = \sum_{p \in \mathbb{Z}_{\geqslant 1}} i_p p = n$, we have $i_p = 0$ for any $p > n$, and thus we can choose any $e \in S_n$ with i_p p-cycles for $1 \leqslant p \leqslant n$ that are disjoint to each other to have $i([e]) = (i_p)_{p \in \mathbb{Z}_{\geqslant 1}}$. This shows that $\boldsymbol{d}^{-1}(n) \subset i(S_n/S_n)$, and the other inclusion holds as well since for any $e \in S_n$, we have $m_1(e) + 2m_2(e) + \cdots + nm_n(e) = n$.

To check the last condition, fix $e \in E = S_n$. For any $g \in G = S_n$, we have $g \in (S_n)_e$ if and only if $geg^{-1} = e$. Say $e = e_1 \cdots e_r$ is the cycle decomposition of e in S_n. Then we have $geg^{-1} = ge_1g^{-1}ge_2g^{-1} \cdots ge_rg^{-1}$, so $g \in (S_n)_e$ if and only if g permutes $e_1, \dots, e_r$ by conjugation because $g(\alpha_1 \ \cdots \ \alpha_p)g^{-1} = (g(\alpha_1) \ \cdots \ g(\alpha_p))$. We claim that there are $m_p(e)!p^{m_p(e)}$ ways to construct the p-cycles of $g \in S_n$ that permutes $e_1, \dots, e_r$, the cycles of e, by conjugation. To see this, consider the p-cycles $e_{j_1}, \dots, e_{j_{m_p(e)}}$ among $e_1, \dots, e_r$. There are $m_p(e)!$ ways to assign $ge_{j_1}g^{-1}, \dots, ge_{j_{m_p(e)}}g^{-1}$ to $e_{j_1}, \dots, e_{j_{m_p(e)}}$ and then for each p-cycle $(\alpha_1 \ \cdots \ \alpha_p)$ among $e_{j_1}, \dots, e_{j_{m_p(e)}}$, since

$$g(\alpha_1 \ \cdots \ \alpha_p)g^{-1} = (g(\alpha_1) \ \cdots \ g(\alpha_p)),$$

there are p ways to determine $g(\alpha_1), \dots, g(\alpha_p)$. This shows the claim that the number of such $g \in S_n$ is

$$|(S_n)_e| = \prod_{p \geqslant 1} m_p(e)!p^{m_p(e)},$$

so we may take $N(p, m) = m!p^m$ as required.

Example II.4 (Matrices over finite fields)**.** We take $G = \mathrm{GL}_n(\mathbb{F}_q)$ and $E = \mathrm{Mat}_n(\mathbb{F}_q)$, and consider the conjugation action. Take $\mathscr{P} = |\mathbb{A}^1_{\mathbb{F}_q}|$, the set of closed points of $\mathbb{A}^1_{\mathbb{F}_q} = \mathrm{Spec}(\mathbb{F}_q[t])$, which we identify with the set of monic irreducible polynomials of $\mathbb{F}_q[t]$, and $\mathcal{I} = \mathcal{P}$, the set of partitions. Define $i : \mathrm{Mat}_n(\mathbb{F}_q)/\mathrm{GL}_n(\mathbb{F}_q) \to$

$\mathrm{Hom}_{\mathbf{Set}}(|\mathbb{A}^1_{\mathbb{F}_q}|, \mathcal{P})$ as follows. Given an orbit $[A] \in \mathrm{Mat}_n(\mathbb{F}_q)/\mathrm{GL}_n(\mathbb{F}_q)$ of a matrix A, consider the $\mathbb{F}_q[t]$-module structure $A \circlearrowright \mathbb{F}_q^n$ on $\mathbb{F}_q^n$ by defining the t-action to be the multiplication by A. Since $\mathbb{F}_q[t]$ is a PID, we have a unique decomposition

$$(A \circlearrowright \mathbb{F}_q^n) \simeq \bigoplus_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} \left(\frac{\mathbb{F}_q[t]}{(P(t))^{\lambda_{P,1}(A)}} \oplus \cdots \oplus \frac{\mathbb{F}_q[t]}{(P(t))^{\lambda_{P,l_{A,P}}(A)}} \right)$$

as $\mathbb{F}_q[t]$-modules. Define the partition $\lambda_P(A) := [\lambda_{P,1}(A), \ldots, \lambda_{P,l_{A,P}}(A)]$. Then we define $i([A]) := (\lambda_P(A))_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|}$, or more precisely as $i([A]) : P \mapsto \lambda_P(A)$. We note that i is injective because the above $\mathbb{F}_q[t]$-module structure precisely determines the orbit of A. We define $d : |\mathbb{A}^1_{\mathbb{F}_q}| \to \mathbb{Z}_{\geqslant 1}$ by $d(P) := \deg(P)$ and $s : \mathcal{P} \to \mathbb{Z}_{\geqslant 0}$ by $s(\nu) = |\nu| = \nu_1 + \cdots + \nu_l$ given $\nu = [\nu_1, \ldots, \nu_l]$. It follows that $* = \varnothing$, the empty partition, and $\boldsymbol{d} : \mathrm{Hom}_{\mathbf{Set}}(|\mathbb{A}^1_{\mathbb{F}_q}|, \mathcal{P}) \to \mathbb{Z}_{\geqslant 0} \sqcup \{\infty\}$ is given by

$$\boldsymbol{d}((\nu_P)_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|}) = \sum_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} |\nu_P| \deg(P).$$

We claim that $\boldsymbol{d}^{-1}(n) = i(\mathrm{Mat}_n(\mathbb{F}_q)/\mathrm{GL}_n(\mathbb{F}_q))$. To see this, choose any $(\nu_P)_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} \in \mathrm{Hom}_{\mathbf{Set}}(|\mathbb{A}^1_{\mathbb{F}_q}|, \mathcal{P})$ with $\boldsymbol{d}((\nu_P)_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|}) = \sum_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} |\nu_P| \deg(P) = n$. Then consider the $\mathbb{F}_q[t]$-module

$$H_{P,\nu_P} := \bigoplus_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} \left(\frac{\mathbb{F}_q[t]}{(P(t))^{\nu_{P,1}}} \oplus \cdots \oplus \frac{\mathbb{F}_q[t]}{(P(t))^{\nu_{P,l_P}}} \right),$$

where $\nu_P = [\nu_{P,1}, \ldots, \nu_{P,l_P}]$. The $\mathbb{F}_q$-dimension of this module is $\sum_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} |\nu_P| \deg(P) = n$, so as an $\mathbb{F}_q$-vector space, we may consider it as $\mathbb{F}_q^n$, and let A be the endomorphism on this vector space by the action of t, which can be seen as an element of $\mathrm{Mat}_n(\mathbb{F}_q)$. This gives us $i([A]) = (\lambda_P(A))_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} = (\nu_P)_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|}$, which shows the claim.

To check the last condition, fix $A \in \mathrm{Mat}_n(\mathbb{F}_q)$. Observe that we have

$$\mathrm{GL}_n(\mathbb{F}_q)_A = \mathrm{Aut}_{\mathbb{F}_q[t]}(A).$$

That is, the stabilizer subgroup of the conjugation action $\mathrm{GL}_n(\mathbb{F}_q) \circlearrowleft \mathrm{Mat}_n(\mathbb{F}_q)$ at A is precisely the automorphism group of the $\mathbb{F}_q[t]$-module $A \circlearrowleft \mathbb{F}_q^n$. Note that

$$(A \circlearrowleft \mathbb{F}_q^n) \simeq \bigoplus_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} H_{P,\lambda_P(A)}.$$

The right-hand side of the above is a finite product, and the only $\mathbb{F}_q[t]$-linear map from $H_{P_1,\nu}$ to $H_{P_2,\nu'}$ is the trivial map for distinct $P_1, P_2 \in |\mathbb{A}^1_{\mathbb{F}_q}|$ and any partitions ν, ν'. This implies that

$$\mathrm{Aut}_{\mathbb{F}_q[t]}(A) \simeq \prod_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} \mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\lambda_P(A)})$$

so that

$$|\mathrm{GL}_n(\mathbb{F}_q)_A| = |\mathrm{Aut}_{\mathbb{F}_q[t]}(A)| = \prod_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} |\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\lambda_P(A)})|.$$

Hence, we may take $N(P, \nu) = |\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|$, where $H_{P,\nu}$ is defined similarly as above for any partition $\nu = [\nu_1, \ldots, \nu_l]$.

Definition II.5. Given Setting II.1, we define the **cycle index** of the action $G \circlearrowleft E$ as the polynomial

$$\mathcal{Z}_{[E/G]}(\boldsymbol{x}) := \frac{1}{|G|} \sum_{e \in E} x_{[e]},$$

where the sequence $\boldsymbol{x} = (x_{[e]})_{[e] \in E/G}$ is given by

$$x_{[e]} := \begin{cases} \text{a formal variable} & \text{if } \boldsymbol{d}(i([e])) = \boldsymbol{d}((i_p(e))_{p \in \mathscr{P}}) = \sum_{p \in \mathscr{P}} s(i_p(e)) d(p) \neq 0, \\ 1 & \text{if } \boldsymbol{d}(i([e])) = \boldsymbol{d}((i_p(e))_{p \in \mathscr{P}}) = \sum_{p \in \mathscr{P}} s(i_p(e)) d(p) = 0. \end{cases}$$

Using $i : E/G \hookrightarrow \mathrm{Hom}_{\mathbf{Set}}(\mathscr{P}, \mathcal{I})$ with $\boldsymbol{d}(i(E/G)) \subset \mathbb{Z}_{\geqslant 0}$, we may instead write

$$\mathcal{Z}_{[E/G]}(\boldsymbol{x}) = \frac{1}{|G|} \sum_{e \in E} \prod_{p \in \mathscr{P}} x_{p, i_p(e)},$$

where the sequence $\boldsymbol{x} = (x_{p,i})_{p\in\mathscr{P},i\in\mathcal{I}}$ is given by

$$x_{p,i} := \begin{cases} \text{a formal variable} & \text{if } s(i) \neq 0, \\ 1 & \text{if } s(i) = 0. \end{cases}$$

We note that $\prod_{p\in\mathscr{P}} x_{p,i_p(e)}$ is a finite product. This is because $\boldsymbol{d}(i(E/G)) \subset \mathbb{Z}_{\geqslant 0}$ so that $\sum_{p\in\mathscr{P}} s(i_p(e))d(p)$ is finite, which implies that only finitely many $p \in \mathscr{P}$ gives nonzero $s(i_p(e))$ since all $d(p) \geqslant 1$.

Lemma II.6. *Given Setting II.1, we have*

$$\mathcal{Z}_{[E/G]}(\boldsymbol{x}) = \sum_{[e]\in E/G} \frac{x_{[e]}}{|G_e|} = \sum_{[e]\in E/G} \frac{\prod_{p\in\mathscr{P}} x_{p,i_p(e)}}{|G_e|},$$

where G_e is the stabilizer of the given G-action at e.

Proof. By the orbit-stabilizer theorem, we have $|G| = |Ge||G_e|$, so

$$\begin{aligned} \mathcal{Z}_{[E/G]}(\boldsymbol{x}) &= \frac{1}{|G|}\sum_{e\in E} x_{[e]} \\ &= \frac{1}{|G|}\sum_{[e]\in E/G} |Ge| x_{[e]} \\ &= \sum_{[e]\in E/G} \frac{x_{[e]}}{|G_e|}, \end{aligned}$$

as desired. □

Example II.7. Assume the hypotheses in Example II.3. Then

$$\mathcal{Z}_{[S_n/S_n]}(\boldsymbol{x}) = \frac{1}{|S_n|}\sum_{e\in S_n} x_{[e]} = \frac{1}{|S_n|}\sum_{e\in S_n}\prod_{p\in\mathbb{Z}_{\geqslant 1}} x_{p,m_p(e)}.$$

Instead of $\prod_{p \in \mathbb{Z}_{\geqslant 1}} x_{p,m_p(e)} = x_{1,m_1(e)} \cdots x_{n,m_n(e)}$, we may write $x_1^{m_1(e)} \cdots x_n^{m_n(e)}$ because either expression precisely encodes information about the orbit $[e] = S_n e$, so we may identify

$$\mathcal{Z}_{[S_n/S_n]}(\boldsymbol{x}) = \frac{1}{|S_n|} \sum_{e \in S_n} x_{1,m_1(e)} \cdots x_{n,m_n(e)}$$

with

$$Z_{S_n}(x_1, \ldots, x_n) = \frac{1}{|S_n|} \sum_{e \in S_n} x_1^{m_1(e)} \cdots x_n^{m_n(e)},$$

which is the cycle index of S_n we defined in Remark I.4. However, we will not consider the cycle index of a general permutation group $G \leqslant S_n$ as a cycle index of a group action.

Example II.8. Assume the hypotheses in Example II.4. Then

$$\begin{aligned}\mathcal{Z}_{[\mathrm{Mat}_n(\mathbb{F}_q)/\mathrm{GL}_n(\mathbb{F}_q)]}(\boldsymbol{x}) &= \frac{1}{|\mathrm{GL}_n(\mathbb{F}_q)|} \sum_{A \in \mathrm{Mat}_n(\mathbb{F}_q)} x_{[A]} \\ &= \frac{1}{|\mathrm{GL}_n(\mathbb{F}_q)|} \sum_{A \in \mathrm{Mat}_n(\mathbb{F}_q)} \prod_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} x_{P,\lambda_P(A)}.\end{aligned}$$

Note that both of Examples II.3 and II.4 come with family of finite group actions parametrized by $n \in \mathbb{Z}_{\geqslant 0}$. This motivates the following modification of Setting II.1:

Setting II.9. Suppose that we are given

- a set map $d : \mathscr{P} \to \mathbb{Z}_{\geqslant 1}$ with a nonempty set $\mathscr{P}$;
- a set map $s : \mathcal{I} \to \mathbb{Z}_{\geqslant 0}$ with a nonempty set $\mathcal{I}$;
- a unique element $* \in \mathcal{I}$ such that $s(*) = 0$;
- a family of finite group actions on finite sets $G_n \circlearrowright E_n$ indexed by $n \in \mathbb{Z}_{\geqslant 0}$;

- a set injection $i^{(n)} : E_n/G_n \hookrightarrow \mathrm{Hom}_{\mathbf{Set}}(\mathscr{P}, \mathcal{I})$ for each $n \in \mathbb{Z}_{\geqslant 0}$. We write $i^{(n)}([e]) = (i_p^{(n)}(e))_{p\in\mathscr{P}}$. We define $\boldsymbol{d} : \mathrm{Hom}_{\mathbf{Set}}(\mathscr{P}, \mathcal{I}) \to \mathbb{Z}_{\geqslant 0} \sqcup \{\infty\}$ by

$$\boldsymbol{d}((i_p)_{p\in\mathscr{P}}) := \sum_{p\in\mathscr{P}} s(i_p)d(p)$$

and require

- $\boldsymbol{d}^{-1}(n) = i^{(n)}(E_n/G_n)$ for each $n \in \mathbb{Z}_{\geqslant 0}$. In particular, we have $\boldsymbol{d}(i^{(n)}([e])) = \sum_{p\in\mathscr{P}} s(i_p(e))d(p) = n$ for any $e \in E_n$;

- a set map $N : \mathscr{P} \times \mathcal{I} \to \mathbb{Z}_{\geqslant 1}$ such that $|(G_n)_e| = \prod_{p\in\mathscr{P}} N(p, i_p(e))$ for any $n \in \mathbb{Z}_{\geqslant 0}$ and $e \in E_n$.

Remark II.10. The assumption $\boldsymbol{d}^{-1}(n) = i^{(n)}(E_n/G_n)$ says that any $(i_p)_{p\in\mathscr{P}} \in \mathrm{Hom}_{\mathbf{Set}}(\mathscr{P}, \mathcal{I})$ satisfies $\sum_{p\in\mathscr{P}} s(i_p)d(p) = n$ if and only if it belongs to $i^{(n)}(E_n/G_n)$. This will be a crucial condition in Lemma II.11 for the factorization of the generating function of cycle indices.

Note that we have already checked that Examples II.3 and II.4 both satisfy Setting II.9 by taking $i = i^{(n)}$ as well as $G = G_n$ and $E = E_n$ in the examples. The following lemma is the main result of this chapter, which we will apply for Examples II.3 and II.4:

Lemma II.11 (Factorization)**.** *Given Setting II.9, we have*

$$\begin{aligned}\sum_{n=0}^{\infty} \mathcal{Z}_{[E_n/G_n]}(\boldsymbol{x})u^n &= \sum_{n=0}^{\infty} \sum_{[e]\in E_n} \frac{\prod_{p\in\mathscr{P}} x_{p,i_p(e)}}{|G_n|} u^n \\ &= \prod_{p\in\mathscr{P}} \sum_{i\in\mathcal{I}} \frac{x_{p,i} u^{s(i)d(p)}}{N(p,i)}.\end{aligned}$$

Proof. Applying Lemma II.6, we have

$$\begin{aligned}
\sum_{n=0}^{\infty} \mathcal{Z}_{[E_n/G_n]}(\boldsymbol{x})u^n &= \sum_{n=0}^{\infty} \sum_{[e]\in E_n/G_n} \frac{x_{[e]}}{|(G_n)_e|} u^n \\
&= \sum_{n=0}^{\infty} \sum_{[e]\in E_n/G_n} \frac{\prod_{p\in\mathscr{P}} x_{p,i_p(e)}}{|(G_n)_e|} u^n \\
&= \sum_{n=0}^{\infty} \sum_{[e]\in E_n/G_n} \frac{\prod_{p\in\mathscr{P}} x_{p,i_p(e)}}{\prod_{p\in\mathscr{P}} N(p,i_p(e))} u^{\sum_{p\in\mathscr{P}} s(i_p(e))d(p)} \\
&= \sum_{n=0}^{\infty} \sum_{[e]\in E_n/G_n} \prod_{p\in\mathscr{P}} \frac{x_{p,i_p(e)}}{N(p,i_p(e))} u^{s(i_p(e))d(p)} \\
&= \prod_{p\in\mathscr{P}} \sum_{i\in\mathcal{I}} \frac{x_{p,i}u^{s(i)d(p)}}{N(p,i)},
\end{aligned}$$

where the last step uses the condition we discussed in Remark II.10. This finishes the proof. □

Corollary II.12. *We have*

$$\sum_{n=0}^{\infty} Z_{S_n}(\boldsymbol{x})u^n = \exp\left(\sum_{r=1}^{\infty} \frac{x_r u^r}{r}\right).$$

Proof. Recall from Example II.7 that taking $x_{p,m} = x_p^m$ gives us $\mathcal{Z}_{[S_n/S_n]}(\boldsymbol{x}) = Z_{S_n}(\boldsymbol{x})$. Applying Lemma II.11 and our observations from Example II.3, we have

$$\begin{aligned}
\sum_{n=0}^{\infty} Z_{S_n}(\boldsymbol{x})u^n &= \prod_{p\in\mathbb{Z}_{\geqslant 1}} \sum_{m\in\mathbb{Z}_{\geqslant 0}} \frac{x_p^m u^{mp}}{m!p^m} \\
&= \prod_{p=1}^{\infty} \sum_{m=0}^{\infty} \frac{(x_p u^p/p)^m}{m!} \\
&= \exp\left(\sum_{p=1}^{\infty} \frac{x_p u^p}{p}\right),
\end{aligned}$$

as desired. □

The following factorization result for the cycle indices of conjugation actions $\mathrm{GL}_n(\mathbb{F}_q) \circlearrowleft \mathrm{Mat}_n(\mathbb{F}_q)$ is due to Stong (Lemma 1 in [Sto1988]), whose argument is originally from Kung [Kun1981] (Corollary II.14 below), which was used for the cycle indices of restricted conjugation actions $\mathrm{GL}_n(\mathbb{F}_q) \circlearrowleft \mathrm{GL}_n(\mathbb{F}_q)$. Now, this is immediate by applying Lemma II.11 to our observations from Example II.4. We write $[\mathrm{Mat}_n/\mathrm{GL}_n](\mathbb{F}_q) := [\mathrm{Mat}_n(\mathbb{F}_q)/\mathrm{GL}_n(\mathbb{F}_q)]$ for convenience.

Corollary II.13. *We have*

$$\begin{aligned}\sum_{n=0}^{\infty} \mathcal{Z}_{[\mathrm{Mat}_n/\mathrm{GL}_n](\mathbb{F}_q)}(\boldsymbol{x})u^n &= \sum_{n=0}^{\infty} \sum_{A \in \mathrm{Mat}_n(\mathbb{F}_q)} \left(\frac{\prod_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} x_{P,\mu_P(A)}}{|\mathrm{GL}_n(\mathbb{F}_q)|} \right) u^n \\ &= \prod_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} \sum_{\nu \in \mathcal{P}} \frac{x_{P,\nu} u^{|\nu| \deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|}\end{aligned}$$

in $\mathbb{Q}[\boldsymbol{x}][\![u]\!]$.

For the following lemma, and throughout the rest of the thesis, we write $\mathcal{Z}_{\mathrm{GL}_n(\mathbb{F}_q)}(\boldsymbol{x}) := \mathcal{Z}_{[\mathrm{GL}_n(\mathbb{F}_q)/\mathrm{GL}_n(\mathbb{F}_q)]}(\boldsymbol{x})$ for convenience.

Corollary II.14 (Lemma 1 in [Kun1981])**.** *We have*

$$\begin{aligned}\sum_{n=0}^{\infty} \mathcal{Z}_{\mathrm{GL}_n(\mathbb{F}_q)}(\boldsymbol{x})u^n &= \sum_{n=0}^{\infty} \sum_{A \in \mathrm{GL}_n(\mathbb{F}_q)} \left(\frac{\prod_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} x_{P,\mu_P(A)}}{|\mathrm{GL}_n(\mathbb{F}_q)|} \right) u^n \\ &= \prod_{\substack{P \in |\mathbb{A}^1_{\mathbb{F}_q}|, \\ P(t) \neq t}} \sum_{\nu \in \mathcal{P}} \frac{x_{P,\nu} u^{|\nu| \deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|}\end{aligned}$$

in $\mathbb{Q}[\boldsymbol{x}][\![u]\!]$.

Remark II.15. Our proof of Corollary II.13 is one step shorter than Stong's proof. It will be interesting to check whether all the factorization formulas about cycle indices in the literature (e.g., the ones from Fulman's thesis [Ful1997]) can be obtained by applying Lemma II.11. Moreover, all the cycle indices in the literature that we are aware of have to do with some conjugation actions, but we speculate that there are many examples of cycle indices of finite group actions that are not conjugation actions, yet to be found. Utilizing Lemma II.11 in such situations may be useful to deal with some new enumeration questions. However, these are not the main foci of this thesis, so we will not investigate them here.

CHAPTER III

Cycle Indices of Permutation Groups and Their Applications to Pólya Enumeration Theorems

The results in this chapter are from [Che2020]. The main goal of this chapter is to prove Theorems I.1 and I.3 and their generalizations. We start by discussing combinatorial origin of Theorem I.3.

3.1 Pólya enumeration in combinatorics

Consider a finite set $X = \{x_1, \ldots, x_r\}$ of colors. A combinatorialist may ask about how to count the number of ways to color n vertices (which we write as $1, 2, \ldots, n$) of a graph with colors drawn from X. The graph may have symmetries, so we want to count the colorings of n vertices modulo the action of the group G of symmetries of the graph. This group G is a subgroup of S_n, and each coloring corresponds to an orbit $\boldsymbol{x} = [x_{i_1}, \ldots, x_{i_n}] \in X^n/G = \mathrm{Hom}_{\mathbf{Set}}([n], X)/G$ under the G-action on $[n] := \{1, 2, \ldots, n\}$. We denote by $e_i := e_i(\boldsymbol{x})$ the number of x_i appearing in $\boldsymbol{x}$. Note that $e_1 + \cdots + e_r = n$. Given any $(k_1, \ldots, k_r) \in (\mathbb{Z}_{\geqslant 0})^r$ such that $\sum_{i=1}^r k_i = n$, we may write $N_{(k_1,\ldots,k_r)}$ to mean the number of $\boldsymbol{x} \in X^n/G$ such that $e_i(\boldsymbol{x}) = k_i$ for all $1 \leqslant i \leqslant r$. We note that our counting problem is equivalent to computing the following degree n homogeneous polynomial:

$$P_{X^n/G}(\boldsymbol{t}) = P_{X^n/G}(t_1, \ldots, t_r) := \sum_{\substack{(k_1,\ldots,k_r)\in(\mathbb{Z}_{\geqslant 0})^r, \\ k_1+\cdots+k_r=n}} N_{(k_1,\ldots,k_r)} t_1^{k_1} \cdots t_r^{k_r} \in \mathbb{Z}[t_1, \ldots, t_n].$$

A classical theorem of Redfield [Red1927], which was also independently found by Pólya [Pol1937], computes the polynomial $P_{X^n/G}(\boldsymbol{t})$ in terms of the subgroup $G \leqslant S_n$. This theorem is often called the **Pólya enumeration theorem**:

Proposition III.1 (Pólya enumeration)**.** *Given the notation above, we have*

$$P_{X^n/G}(\boldsymbol{t}) = Z_G(\boldsymbol{t}, \boldsymbol{t}^2, \ldots, \boldsymbol{t}^n),$$

where $\boldsymbol{t}^j := t_1^j + \cdots + t_r^j$ *and*

$$Z_G(x_1, \ldots, x_n) = \frac{1}{|G|} \sum_{g\in G} x_1^{m_1(g)} \cdots x_n^{m_n(g)}$$

is the cycle index of G*, defined as in the introduction.*

Remark III.2. Note that a special case of Proposition III.1 obtained by taking $t_1 = t_2 = \cdots = t_r = 1$ says

$$|X^n/G| = \frac{1}{|G|} \sum_{g\in G} |X|^{m(g)},$$

where $m(g) := m_1(g) + \cdots + m_n(g)$, the number of cycles in the cycle decomposition of g in S_n. This can be easily obtained by applying Burnside's lemma because we can compute the size of the set $(X^n)^g$ of elements of X^n fixed by $g \in G$ as $|(X^n)^g| = |X|^{m(g)}$. We will see that Proposition III.1 follows from Theorem III.13, a more general formula.

Remark III.3. Applying the factorization formula for cyclic indices of symmetric groups in Lemma II.12, Proposition III.1 implies that

$$\sum_{n=0}^{\infty} P_{X^n/S_n}(\boldsymbol{t})u^n = \sum_{n=0}^{\infty} Z_{S_n}(\boldsymbol{t}, \boldsymbol{t}^2, \dots, \boldsymbol{t}^n)u^n = \exp\left(\sum_{p=1}^{\infty} \frac{(t_1^p + \cdots + t_{|X|}^p)u^p}{p}\right)$$
$$= \exp\left(\sum_{p=1}^{\infty} \frac{(t_1 u)^p}{p}\right) \cdots \exp\left(\sum_{p=1}^{\infty} \frac{(t_{|X|} u)^p}{p}\right) = \frac{1}{(1-t_1 u)\cdots(1-t_{|X|}u)}.$$

In particular, if taking $t_i = 1$ for all i, we have

$$\sum_{n=0}^{\infty} |X^n/S_n| u^n = \left(\frac{1}{1-u}\right)^{|X|}.$$

Remark III.4. We note that Theorem I.3 is an analogue of the Pólya enumeration theorem (Proposition III.1). We will see that these are special cases to Theorem III.9.

3.2 Cheah's result on Hodge numbers

In this section, we introduce an analogue of the Pólya enumeration theorem (Proposition III.1) in complex algebraic geometry. When X is a smooth projective variety over $\mathbb{C}$ of dimension d, we get a complex manifold structure on X. With respect to its analytic topology, the variety X (or more precisely, its set $X(\mathbb{C})$ of complex points) is compact, so Macdonald's results, introduced in Remark I.4, are also valid in this case. Moreover, we have the Hodge decomposition

$$H^i(X) = \bigoplus_{p+q=i} H^{p,q}(X),$$

where $H^{p,q}(X) := H^q(X, \Omega_X^p)$, whose coefficients are in $\mathbb{C}$, so it is natural to ask if Macdonald's results generalize to the Hodge numbers $h^{p,q}(X) = \dim_{\mathbb{C}}(H^{p,q}(X))$. Indeed, Cheah [Che1994] showed the following:

Proposition III.5 (Cheah)**.** *Keeping the above notation, we have*

$$\sum_{n=0}^{\infty} \chi_t(\mathrm{Sym}^n(X), x, y)u^n = \prod_{i=0}^{2d} \prod_{p+q=i} \left(\frac{1}{1 - x^p y^q t^i u}\right)^{(-1)^i h^{p,q}(X)},$$

where

$$\chi_t(Y, x, y) := \sum_{i=0}^{\infty} \sum_{p+q=i} x^p y^q (-t)^i h^{p,q}(Y).$$

Remark III.6. We note that $\mathrm{Sym}^n(X)$ is not necessarily smooth, but we have

$$H^\bullet(\mathrm{Sym}^n(X)) \hookrightarrow H^\bullet(X^n),$$

and it turns out that

$$h^{p,q}(\mathrm{Sym}^n(X)) = \dim_{\mathbb{C}}(H^\bullet(\mathrm{Sym}^n(X)) \cap H^{p,q}(X^n)).$$

This equality can be taken as definition for our purpose. We can understand the Hodge numbers of X^n/G for any subgroup $G \leqslant S_n$ in a similar manner.

Proposition III.5 follows from applying Corollary II.12 to the following formula regarding any permutation group $G \leqslant S_n$, which is another analogue of the Pólya enumeration theorem (Proposition III.1):

Proposition III.7 (Cheah)**.** *Keeping the above notation, we have*

$$\chi_t(X^n/G, x, y) = Z_G(\chi_t(X, x, y), \chi_{t^2}(X, x^2, y^2), \ldots, \chi_{t^n}(X, x^n, y^n)).$$

Cheah's proof essentially reruns Macdonald's proof in [Mac1962A], while remembering the tri-grading structure on $H^\bullet(X^n)$. The three gradings are associated to variables u, x, and y in the above formula. We will see that Proposition III.7 also follows from Theorem III.13, our general formula.

3.3 Generalized Pólya enumeration

In this section, we prove Theorem III.9, a generalized Pólya enumeration theorem, which is the main theorem of this chapter. (The following section will deal with its applications.) Throughout this section, we work over a field k. Let $V = \bigoplus_{i \geqslant 0} V_i$ be a graded vector space over k. Given $n \in \mathbb{Z}_{\geqslant 0}$, consider the n-fold tensor product $V^{\otimes n}$ of V over k, where $V^{\otimes 0} = k$. We have

$$V^{\otimes n} = \bigoplus_{r \geqslant 0} (V^{\otimes n})_r,$$

where

$$(V^{\otimes n})_r = \bigoplus_{i_1 + \cdots + i_n = r} V_{i_1} \otimes \cdots \otimes V_{i_n}.$$

This makes $V^{\otimes n}$ a graded vector space over k. Given any subgroup $G \leqslant S_n$, we consider the action of G on $V^{\otimes n}$ according to the **Koszul rule**. That is, we define

$$g \cdot (v_1 \otimes \cdots \otimes v_n) := (-1)^{Q_g(\deg(v_1), \ldots, \deg(v_n))} v_{g^{-1}(1)} \otimes \cdots \otimes v_{g^{-1}(n)},$$

for homogeneous $v_1, \ldots, v_n \in V$ (i.e., $v_i \in V_{\deg(v_i)}$) and $g \in G$, where $Q_g(x_1, \ldots, x_n) = \sum_{1 \leqslant i < j \leqslant n} \epsilon_{ij}(g) x_i x_j \in \mathbb{Z}[x_1, \ldots, x_n]$ is defined by

$$\epsilon_{ij}(g) := \begin{cases} 1 & \text{if } g(i) > g(j) \text{ and} \\ 0 & \text{if } g(i) < g(j). \end{cases}$$

It is important to note that this action respects the grading of $V^{\otimes n}$. In particular, it can be thought of as a family of k-linear maps $\{G \to \mathrm{GL}_k((V^{\otimes n})_r)\}_{r \in \mathbb{Z}_{\geqslant 0}}$.

We will consider traces of linear endomorphisms, so assume that each homogeneous piece V_i of V is finite-dimensional. Let $\phi \in \mathrm{End}_k(V)$ be graded (with degree 0) meaning that $\phi = \bigoplus_{i \geqslant 0} \phi_i$, where $\phi_i \in \mathrm{End}_k(V_i)$. This means that if $v \in V$ is a homogeneous element, then $\phi(v) \in V$ is a homogeneous element of degree $\deg(v)$ so that $\phi(v) = \phi_{\deg(v)}(v)$. We consider the **Lefschetz series**

$$L_t(\phi) := \sum_{i \geqslant 0} (-t)^i \mathrm{Tr}(\phi_i) \in k[\![t]\!]$$

of ϕ in u. We observe that given another graded endomorphism $\psi = \bigoplus_{i \geqslant 0} \psi_i$ on V and a constant $c \in k$, we have

$$L_t(\phi + c\psi) = L_t(\phi) + cL_t(\psi).$$

We also get the induced endomorphism $\phi^{\otimes n} \in \mathrm{End}_k(V^{\otimes n})$ given by

$$\phi^{\otimes n}(v_1 \otimes \cdots \otimes v_n) := \phi(v_1) \otimes \cdots \otimes \phi(v_n)$$

for homogeneous $v_1, \ldots, v_n \in V$, which hence respects the grading of $V^{\otimes n}$ so that we can write

$$\phi^{\otimes n} = \bigoplus_{r \geqslant 0} (\phi^{\otimes n})_r,$$

where

$$(\phi^{\otimes n})_r := \bigoplus_{i_1 + \cdots + i_n = r} \phi_{i_1} \otimes \cdots \otimes \phi_{i_n} \in \mathrm{End}_k((V^{\otimes n})_r) = \mathrm{End}_k\left(\bigoplus_{i_1 + \cdots + i_n = r} V_{i_1} \otimes \cdots \otimes V_{i_n} \right).$$

Given any $g \in G \leqslant S_n$ and homogeneous $v_1, \ldots, v_n \in V$, we define

$$\begin{aligned}(g \cdot \phi^{\otimes n})(v_1 \otimes \cdots \otimes v_n) &:= g(\phi(v_1) \otimes \cdots \otimes \phi(v_n)) \\ &= (-1)^{Q_g(\deg(v_1), \ldots, \deg(v_n))} \phi(v_{g^{-1}(1)}) \otimes \cdots \otimes \phi(v_{g^{-1}(n)}) \\ &= (-1)^{Q_g(\deg(v_1), \ldots, \deg(v_n))} \phi_{\deg(v_{g^{-1}(1)})}(v_{g^{-1}(1)}) \otimes \cdots \otimes \phi_{\deg(v_{g^{-1}(n)})}(v_{g^{-1}(n)}).\end{aligned}$$

This extends to a k-linear endomorphism $g\phi^{\otimes n}$ on $V^{\otimes n}$. It is important to note that we have the following commutativity although it is immediate from definitions:

Lemma III.8. *Keeping the notation above, we have*

$$(g\phi^{\otimes n})(v_1 \otimes \cdots \otimes v_n) = \phi^{\otimes n}(g(v_1 \otimes \cdots \otimes v_n)).$$

We now state the main theorem of this chapter:

Theorem III.9 (Generalized Pólya enumeration). *Let $\phi = \bigoplus_{i \geqslant 0} \phi_i$ be a graded endomorphism on a graded vector space $V = \bigoplus_{i \geqslant 0} V_i$ over k, where each V_i is finite-dimensional. If the ambient field k is of characteristic that does not divide $|G|$, then*

$$L_t(\phi^{\otimes n}|_{(V^{\otimes n})^G}) = Z_G(L_t(\phi), L_{t^2}(\phi^2), \ldots, L_{t^n}(\phi^n)).$$

Corollary III.10. *Keeping the notation as in Theorem III.9, assume further that*

- $V_i = 0$ *for* $i > 2d$*;*
- *the characteristic of* k *is* 0.

Then

$$\sum_{n=0}^{\infty} L_t(\phi^{\otimes n}|_{(V^{\otimes n})^{S_n}}) u^n = \frac{\det(\mathrm{id}_{V_1} - \phi_1 t u) \cdots \det(\mathrm{id}_{V_{2d-1}} - \phi_{2d-1} t^{2d-1} u)}{\det(\mathrm{id}_{V_0} - \phi_0 u) \cdots \det(\mathrm{id}_{V_{2d}} - \phi_{2d} t^{2d} u)}.$$

Proof. Both sides are invariant under taking any field extension of k, so we may assume that k is algebraically closed. In particular, the field k is now infinite, so we may assume that t is an element of k. By Corollary II.12 and Theorem III.9, we have

$$\begin{aligned}
\sum_{n=0}^{\infty} L_t(\phi^{\otimes n}|_{(V^{\otimes n})^{S_n}}) u^n &= \sum_{n=0}^{\infty} Z_{S_n}(L_t(\phi), L_{t^2}(\phi^2), \ldots, L_{t^n}(\phi^n)) u^n \\
&= \exp\left(\sum_{r=1}^{\infty} \frac{L_{t^r}(\phi^r) u^r}{r} \right) \\
&= \exp\left(\sum_{r=1}^{\infty} \sum_{i=0}^{2d} \frac{(-t^r)^i \mathrm{Tr}(\phi_i^r) u^r}{r} \right) \\
&= \prod_{i=0}^{2d} \exp\left(\sum_{r=1}^{\infty} \frac{(-1)^i \mathrm{Tr}((\phi_i t^i)^r) u^r}{r} \right) \\
&= \prod_{i=0}^{2d} \exp\left(\sum_{r=1}^{\infty} \frac{\mathrm{Tr}((\phi_i t^i)^r) u^r}{r} \right)^{(-1)^i}.
\end{aligned}$$

Hence, the result follows from the fact that

$$\det(\mathrm{id} - uA) = \exp\left(\sum_{r=1}^{\infty} \frac{\mathrm{Tr}(A^r)u^r}{r}\right)^{-1}$$

for any linear map A on a finite-dimensional vector space (e.g., [Mus, Lemma 4.12]). □

Theorem III.9 will be deduced from the following:

Theorem III.11 (Trace formula on $V^{\otimes n}$). *Let $\phi = \bigoplus_{i \geqslant 0} \phi_i$ be a graded endomorphism on a graded vector space $V = \bigoplus_{i \geqslant 0} V_i$ over k, where each V_i is finite-dimensional. For any $g \in S_n$, we have*

$$L_t(g\phi^{\otimes n}) = L_t(\phi)^{m_1(g)} L_{t^2}(\phi^2)^{m_2(g)} \cdots L_{t^n}(\phi^n)^{m_n(g)} \in k[\![t]\!].$$

Proof. Since the desired identity is only regarding traces of (homogeneous parts of) endomorphisms $g\phi^{\otimes n}$ and $\phi, \phi^2, \ldots, \phi^n$, we may assume that k is algebraically closed. Both sides of the identity are power series in $k[\![t]\!]$, so it is enough to show that for any $r \in \mathbb{Z}_{\geqslant 0}$, their coefficients of t^r match. This lets us reduce the problem to the case $V = V_0 \oplus \cdots \oplus V_r$ and $\phi = \phi_1 \oplus \cdots \oplus \phi_r$ essentially because

$$(V^{\otimes n})_r = \bigoplus_{i_1 + \cdots + i_n = r} V_{i_1} \otimes \cdots \otimes V_{i_r},$$

where the right-hand side only consists of tensor products of $V_0, \ldots, V_r$. In particular, we are now dealing with the case where $d = \dim_k(V) = \dim_k(V_0) + \cdots + \dim_k(V_r)$ is finite.

Without any loss of generality, we may assume that $d \geqslant 1$. Considering $\phi \in \mathrm{End}_k(V) = \mathrm{Mat}_d(k) = \mathbb{A}^{d^2}(k)$, we note that the desired equality for the coefficients of t^r cuts out a closed subset in $\mathbb{A}^{d^2}(k)$, with respect to the Zariski topology (on the set $\mathbb{A}^{d^2}(k)$ of closed points of $\mathbb{A}^{d^2}$ over k) as we can use the Kronecker product for the matrix form of $\phi^{\otimes n}$. The matrices with distinct eigenvalues form a Zariski open subset in $\mathrm{Mat}_d(k) = \mathbb{A}^{d^2}(k)$ because we can understand them as points of the locus whose discriminant of the characteristic polynomial is nonzero. This open locus is nonempty because k has at least d elements as it is infinite now that we are in the setting where k is algebraically closed. Thus, such matrices are dense in $\mathrm{Mat}_d(k) = \mathbb{A}^{d^2}(k)$, as the affine space is irreducible. This means that it is enough to show the desired statement for ϕ with d distinct eigenvalues, and this means that each ϕ_i is diagonalizable.

Thus, we may find $\eta_i \in \mathrm{GL}_{d_i}(k) = \mathrm{GL}(V_i)$ such that $\eta_i\phi_i\eta_i^{-1}$ is a diagonal matrix whose diagonal entries are the eigenvalues of ϕ_i, where $d_i = \dim_k(V_i)$. Then $\eta_i\phi_i^m\eta_i^{-1}$ for any $m \in \mathbb{Z}_{\geqslant 1}$ is a diagonal matrix whose diagonal entries consist of m-th powers of the eigenvalues of ϕ_i. Writing $\eta = \eta_1 \oplus \cdots \oplus \eta_r \in \mathrm{GL}_d(k)$, we see $\eta\phi\eta^{-1} = \eta_1\phi_1\eta_1^{-1} \oplus \cdots \oplus \eta_r\phi_r\eta_r^{-1}$ is a diagonal matrix, and so is

$$(\eta\phi\eta^{-1})^m = \eta\phi^m\eta^{-1} = \eta_1\phi_1^m\eta_1^{-1} \oplus \cdots \oplus \eta_r\phi_r^m\eta_r^{-1}.$$

Note that η respects the grading of V and $\eta^{\otimes n}$ commutes with the action of g by Lemma III.8. Since $(\eta\phi\eta^{-1})^{\otimes n} = \eta^{\otimes n}\phi^{\otimes n}(\eta^{-1})^{\otimes n}$, we have

$$(g(\eta\phi\eta^{-1})^{\otimes n})_r = (\eta^{\otimes n}g\phi^{\otimes n}(\eta^{-1})^{\otimes n})_r = (\eta^{\otimes n})_r(g\phi^{\otimes n})_r((\eta^{-1})^{\otimes n})_r.$$

Since

$$\eta^{\otimes n}(\eta^{-1})^{\otimes n}(v_1 \otimes \cdots \otimes v_n) = (\eta\eta^{-1}v_1) \otimes \cdots \otimes (\eta\eta^{-1}v_n) = v_1 \otimes \cdots \otimes v_n$$

for any homogeneous $v_1, \ldots, v_n \in V$, we see that $(\eta^{\otimes n})_r$ and $((\eta^{-1})^{\otimes n})_r$ are k-linear endomorphisms on $(V^{\otimes n})_r$ that are mutual inverses. Thus, replacing ϕ with $\eta\phi\eta^{-1}$, or equivalently ϕ_i with $\eta_i\phi_i\eta_i^{-1}$ for each i, will not affect the desired identity, so our problem is reduced to the case where each ϕ_i is diagonal.

Let $v_{i,1}, \ldots, v_{i,d_i} \in V_i$ be homogeneous elements of V forming an eigenbasis of V_i for ϕ_i as we vary $i \in \mathbb{Z}_{\geqslant 0}$. We shall denote the corresponding eigenvalues as $\alpha_{i,j} \in k$ so that $\phi(v_{i,j}) = \phi_i(v_{i,j}) = \alpha_{i,j}v_{i,j}$. To compute the coefficient of t^r on the left-hand side of the desired identity, fix any element

$$w_1 \otimes \cdots \otimes w_n \in (V^{\otimes n})_r = \bigoplus_{i_1+\cdots+i_n=r} V_{i_1} \otimes \cdots \otimes V_{i_n},$$

where $w_j = v_{i_j,h_j}$ for some h_j so that $\deg(w_j) = i_j$ and $\phi(w_j) = \phi_{i_j}(w_j) = \alpha_{i_j,h_j}w_j$. We have

$$\begin{aligned}(g\phi^{\otimes n})(w_1 \otimes \cdots \otimes w_n) &= \phi^{\otimes n}(g(w_1 \otimes \cdots \otimes w_n)) \\ &= (-1)^{Q_g(i_1,\ldots,i_n)}\phi(w_{g^{-1}(1)}) \otimes \cdots \otimes \phi(w_{g^{-1}(n)}) \\ &= (-1)^{Q_g(i_1,\ldots,i_n)}\alpha_{i_{g^{-1}(1)},h_{g^{-1}(1)}}w_{g^{-1}(1)} \otimes \cdots \otimes \alpha_{i_{g^{-1}(n)},h_{g^{-1}(n)}}w_{g^{-1}(n)} \\ &= \alpha_{i_{1,h_1}} \cdots \alpha_{i_n,h_n}(-1)^{Q_g(i_1,\ldots,i_n)}w_{g^{-1}(1)} \otimes \cdots \otimes w_{g^{-1}(n)},\end{aligned}$$

so the vector $w_1 \otimes \cdots \otimes w_n$ can possibly contribute a nonzero amount to $\mathrm{Tr}(g\phi^{\otimes n})_r$ precisely when $w_j = w_{g^{-1}(j)}$ for all $1 \leqslant j \leqslant n$. Consider the cycle decomposition of g in S_n:

$$g = (1 \ \cdots \ \lambda_1)(\lambda_1 + 1 \ \cdots \lambda_1 + \lambda_2) \cdots (\lambda_1 + \cdots + \lambda_{l-1} + 1 \ \cdots \ \lambda_1 + \cdots + \lambda_l),$$

where $\lambda_1 + \cdots + \lambda_l = n$. In this situation, saying that $w_j = w_{g^{-1}(j)}$ for all $1 \leqslant j \leqslant n$ is equivalent to saying

- $y_1 := w_1 = \cdots = w_{\lambda_1}$,
- $y_2 := w_{\lambda_1+1} = \cdots = w_{\lambda_1+\lambda_2}$,

  $\vdots$
- $y_l := w_{\lambda_1+\cdots+\lambda_{l-1}+1} = \cdots = w_{\lambda_1+\cdots+\lambda_l}$,

while $y_1, \ldots, y_l$ may or may not be distinct. This also shows that

- $e_1 := \deg(y_1) = i_1 = \cdots = i_{\lambda_1}$,
- $e_2 := \deg(y_2) = i_{\lambda_1+1} = \cdots = i_{\lambda_1+\lambda_2}$,

  $\vdots$
- $e_l := \deg(y_l) = i_{\lambda_1+\cdots+\lambda_{l-1}+1} = \cdots = i_{\lambda_1+\cdots+\lambda_l}$

and

- $\alpha_1 := \alpha_{i_1,h_1} = \cdots = \alpha_{i_{\lambda_1},h_{\lambda_1}}$,
- $\alpha_2 := \alpha_{i_{\lambda_1+1},h_{\lambda_1+1}} = \cdots = \alpha_{i_{\lambda_1+\lambda_2},h_{\lambda_1+\lambda_2}}$,

  $\vdots$
- $\alpha_l := \alpha_{i_{\lambda_1+\cdots+\lambda_{l-1}+1},h_{\lambda_1+\cdots+\lambda_{l-1}+1}} = \cdots = \alpha_{i_n,h_n}$.

Note that $y_j \in V_{e_j}$ and $\phi(y_j) = \phi_{e_j}(y_j) = \alpha_j y_j$. We also note that $\lambda_1 e_1 + \cdots + \lambda_l e_l = r$ because $(V_{e_1})^{\otimes\lambda_1} \otimes \cdots \otimes (V_{e_l})^{\otimes\lambda_l}$ is a direct summand of $(V^{\otimes n})_r$ in the decomposition of $V^{\otimes n}$ that gives the grading for the tensor product.

To compute the sign, we note that

$$Q_{\sigma\tau}(\boldsymbol{x}) = Q_\sigma(\boldsymbol{x}) + Q_\tau(\boldsymbol{x})$$

for any disjoint permutations $\sigma, \tau \in S_n$ and that

$$Q_{(\lambda+1\ \lambda+2\ \cdots\ \lambda+r)}(\boldsymbol{x}) = (x_{\lambda+1} + x_{\lambda+2} + \cdots + x_{\lambda+r-1})x_{\lambda+r}.$$

Thus, for this particular $g \in S_n$, we have

$$\begin{aligned} Q_g(i_1, \ldots, i_n) &= Q_{(1\ \cdots\ \lambda_1)}(i_1, \ldots, i_n) + \cdots + Q_{(\lambda_1+\cdots+\lambda_{l-1}+1\ \cdots\ \lambda_1+\cdots+\lambda_l)}(i_1, \ldots, i_n) \\ &= (i_1 + \cdots + i_{\lambda_1-1})i_{\lambda_1} + \cdots + (i_{\lambda_1+\cdots+\lambda_{l-1}+1} + \cdots + i_{\lambda_1+\cdots+\lambda_l-1})i_{\lambda_1+\cdots+\lambda_l} \\ &= (\lambda_1 - 1)e_1 \cdot e_1 + \cdots + (\lambda_l - 1)e_l \cdot e_l \\ &= (\lambda_1 - 1)e_1^2 + \cdots + (\lambda_l - 1)e_l^2. \end{aligned}$$

This implies that

$$\begin{aligned} Q_g(i_1, \ldots, i_n) &\equiv (\lambda_1 + 1)e_1 + \cdots + (\lambda_l + 1)e_l \\ &= r + e_1 + \cdots + e_l, \end{aligned}$$

where the congruence is taken modulo 2. Hence, we have computed the sign:

$$(-1)^{Q_g(i_1,\ldots,i_n)} = (-1)^{r+e_1+\cdots+e_l}.$$

This implies that the vector $w_1 \otimes \cdots \otimes w_n = y_1^{\otimes\lambda_1} \otimes \cdots \otimes y_l^{\otimes\lambda_l}$ contributes

$$(-1)^{r+e_1+\cdots+e_l}\alpha_{i_1,h_1} \cdots \alpha_{i_n,h_n} = (-1)^{r+e_1+\cdots+e_l}\alpha_1^{\lambda_1} \cdots \alpha_l^{\lambda_l}$$

to $\mathrm{Tr}(g\phi^{\otimes n})_r$. We keep fixing the partition $[\lambda_1, \ldots, \lambda_l] \vdash n$, which is an equivalent datum to the cycle decomposition of g in S_n. Write $B_i := \{v_{i,1}, \ldots, v_{i,d_i}\}$, the chosen eigenbasis for V_i. So far, we have seen that

$$\mathrm{Tr}(g\phi^{\otimes n})_r = \sum_{\lambda_1 e_1+\cdots+\lambda_l e_l=r}\ \sum_{(y_1,\ldots,y_l)\in B_{e_1}\times\cdots\times B_{e_l}} (-1)^{r+e_1+\cdots+e_l}\alpha_1^{\lambda_1} \cdots \alpha_l^{\lambda_l}.$$

We note that α_i appearing in the computation above is the eigenvalue for $y_i \in B_{e_i}$, so to remember this dependence, let us write $\alpha_{y_i} := \alpha_i$ in the following computation. We now compute

$$\begin{aligned}
L_t(g\phi^{\otimes n}) &= \sum_{r\geqslant 0}(-t)^r \mathrm{Tr}(g\phi^{\otimes n})_r \\
&= \sum_{r\geqslant 0}\ \sum_{\lambda_1e_1+\cdots+\lambda_le_l=r}\ \sum_{(y_1,\ldots,y_l)\in B_{e_1}\times\cdots\times B_{e_l}} (-1)^{e_1+\cdots+e_l}\alpha_{y_1}^{\lambda_1}\cdots\alpha_{y_l}^{\lambda_l}t^r \\
&= \sum_{r\geqslant 0}\ \sum_{\lambda_1e_1+\ldots+\lambda_le_l=r}\ \sum_{(y_1,\ldots,y_l)\in B_{e_1}\times\cdots\times B_{e_l}} (-1)^{e_1+\ldots+e_l}\alpha_{y_1}^{\lambda_1}\cdots\alpha_{y_l}^{\lambda_l}t^{\lambda_1e_1+\cdots+\lambda_le_l} \\
&= \sum_{r\geqslant 0}\ \sum_{\lambda_1e_1+\cdots+\lambda_le_l=r}\ \sum_{(y_1,\ldots,y_l)\in B_{e_1}\times\cdots\times B_{e_l}} \alpha_{y_1}^{\lambda_1}\cdots\alpha_{y_l}^{\lambda_l}(-t^{\lambda_1})^{e_1}\cdots(-t^{\lambda_l})^{e_l} \\
&= \sum_{r\geqslant 0}\ \sum_{\lambda_1e_1+\cdots+\lambda_le_l=r} \left(\sum_{y_1\in B_{e_1}}\alpha_{y_1}^{\lambda_1}(-t^{\lambda_1})^{e_1}\right)\cdots\left(\sum_{y_l\in B_{e_l}}\alpha_{y_l}^{\lambda_l}(-t^{\lambda_l})^{e_l}\right) \\
&= \sum_{r\geqslant 0}\ \sum_{\lambda_1e_1+\cdots+\lambda_le_l=r} \mathrm{Tr}(\phi_{e_1}^{\lambda_1})(-t^{\lambda_1})^{e_1}\cdots\mathrm{Tr}(\phi_{e_l}^{\lambda_l})(-t^{\lambda_l})^{e_l} \\
&= \sum_{e_1,\ldots,e_l\geqslant 0} \mathrm{Tr}(\phi_{e_1}^{\lambda_1})(-t^{\lambda_1})^{e_1}\cdots\mathrm{Tr}(\phi_{e_l}^{\lambda_l})(-t^{\lambda_l})^{e_l} \\
&= \left(\sum_{e_1\geqslant 0}\mathrm{Tr}(\phi_{e_1}^{\lambda_1})(-t^{\lambda_1})^{e_1}\right)\cdots\left(\sum_{e_l\geqslant 0}\mathrm{Tr}(\phi_{e_l}^{\lambda_l})(-t^{\lambda_l})^{e_l}\right) \\
&= \left(\sum_{i\geqslant 0}\mathrm{Tr}(\phi_{i}^{\lambda_1})(-t^{\lambda_1})^{i}\right)\cdots\left(\sum_{i\geqslant 0}\mathrm{Tr}(\phi_{i}^{\lambda_l})(-t^{\lambda_l})^{i}\right) \\
&= \left(\sum_{i\geqslant 0}\mathrm{Tr}(\phi_{i})(-t)^{i}\right)^{m_1(g)}\left(\sum_{i\geqslant 0}\mathrm{Tr}(\phi_{i}^{2})(-t^2)^{i}\right)^{m_2(g)}\cdots\left(\sum_{i\geqslant 0}\mathrm{Tr}(\phi_{i}^{n})(-t^n)^{i}\right)^{m_n(g)} \\
&= L_t(\phi)^{m_1(g)}L_{t^2}(\phi^2)^{m_2(g)}\cdots L_{t^n}(\phi^n)^{m_n(g)},
\end{aligned}$$

as desired. □

We will use the following Lemma in the proof of Theorem III.9:

Lemma III.12. *Let G be any finite group k-linearly acting on a finite-dimensional*

k-vector space W, where k is a field whose characteristic does not divide $|G|$. For any endomorphism $\psi : W \to W$ with $\psi(W^G) \subset W^G$, we have

$$\mathrm{Tr}(\psi \circ e_G) = \mathrm{Tr}(\psi|_{W^G}),$$

where $e_G := |G|^{-1} \sum_{g \in G} g : W \to W$.

Proof. Fix any basis $w_1, \ldots, w_r, w_{r+1}, \ldots, w_n$ for W such that $w_1, \ldots, w_r$ is a basis for $W^G = e_G(W)$. Since $e_G^2 = e_G$, we know that the minimal polynomial $P(t)$ of e_G divides $t(t-1)$. Hence, the matrix of e_G is diagonalizable with all of its eigenvalues being 0 or 1. This implies that we may find $\alpha \in \mathrm{GL}(W)$ such that the matrix of $\alpha e_G \alpha^{-1}$ is of the form $\mathrm{diag}(1, 1, \ldots, 1, 0, 0, \ldots, 0)$. The rank of $\alpha e_G \alpha^{-1}$ is $r = \dim_k(e_G(W)) = \dim_k(W^G)$ and $\alpha e_G \alpha^{-1}(\alpha w) = \alpha e_G w = \alpha w$ for all $w \in W^G$. This implies that $\alpha e_G \alpha^{-1}(\alpha w_i) = 0$ for $r + 1 \leqslant i \leqslant n = \dim_k(W)$. Since $\alpha \psi \alpha^{-1}(\alpha(W^G)) \subset \alpha(W^G)$, we have

$$\mathrm{Tr}((\alpha\psi\alpha^{-1})(\alpha e_G \alpha^{-1})) = \mathrm{Tr}((\alpha\psi\alpha^{-1})|_{\alpha(W^G)}) = \mathrm{Tr}(\psi|_{W^G}).$$

Since the left-hand side is $\mathrm{Tr}((\alpha\psi\alpha^{-1})(\alpha e_G\alpha^{-1})) = \mathrm{Tr}(\alpha\psi e_G\alpha^{-1}) = \mathrm{Tr}(\psi e_G)$, we are done. □

Proof of Theorem III.9. Using Lemma III.8, we have

$$\phi^{\otimes n} \circ e_G = \frac{1}{|G|} \sum_{g \in G} g\phi^{\otimes n} \in \mathrm{End}_k(V^{\otimes n}).$$

Hence, to finish the proof, it is enough to show that

$$L_t(\phi^{\otimes n}|_{(V^{\otimes n})^G}) = L_t(\phi^{\otimes n} \circ e_G)$$

because then we may apply Lemma III.11. To show this, it is enough to show

$$\mathrm{Tr}((\phi^{\otimes n})_r|_{(V^{\otimes n})^G_r}) = \mathrm{Tr}((\phi^{\otimes n})_r \circ e_G)$$

for any given $r \in \mathbb{Z}_{\geqslant 0}$, but we know this from Lemma III.12. This finishes the proof. □

3.4 Generalized Pólya enumeration in cohomological settings

Before discussing applications of Theorem III.9, our generalized Pólya enumeration theorem, we discuss a formal axiomatic setting where the theorem applies. Then we show how a version of Theorem III.9 in such a setting implies Theorem I.3, Proposition III.1, Proposition III.7, and so on.

Let $\mathcal{C}$ be a category where any finite products exist. Fix a field k, and suppose that we have a functor

$$H^\bullet : \mathcal{C}^{\mathrm{op}} \to \mathbf{GrVec}_k$$

from the opposite category $\mathcal{C}^{\mathrm{op}}$ of $\mathcal{C}$ to the category $\mathbf{GrVec}_k$ of $\mathbb{Z}_{\geqslant 0}$-graded vector spaces over k whose morphisms are k-linear graded maps (of degree 0). Given any object X in $\mathcal{C}$, we may write

$$H^\bullet(X) = \bigoplus_{i=0}^{\infty} H^i(X),$$

where each $H^i(X)$ is a vector space over k. Given any morphism $F : X \to Y$ in $\mathcal{C}$, the induced k-linear map $F^* : H^\bullet(Y) \to H^\bullet(X)$ can be decomposed as $F^* = \bigoplus_{i=0}^{\infty} F_i^*$ with a k-linear map $F_i^* : H^i(Y) \to H^i(X)$ for each $i \in \mathbb{Z}_{\geqslant 0}$ by definition. In addition, we assume the following axioms:

Axiom 1. Given any object X in $\mathcal{C}$, we assume that there is a **cup product**, namely a k-bilinear map $\cup : H^i(X) \times H^j(X) \to H^{i+j}(X)$ defined for each $i, j \in \mathbb{Z}_{\geqslant 0}$ such that

$$a \cup b = (-1)^{ij} b \cup a$$

for all $a \in H^i(X)$ and $b \in H^j(X)$.

Axiom 2. Assuming Axiom 1, given any objects X and Y in $\mathcal{C}$, we assume the **Künneth formula**: that is, we assume that the k-linear map

$$H^\bullet(X) \otimes_k H^\bullet(Y) \to H^\bullet(X \times Y)$$

given by $a \otimes b \mapsto p_X^*(a) \cup p_Y^*(b)$ for any homogeneous elements $a \in H^\bullet(X)$ and $b \in H^\bullet(Y)$ is an isomorphism.

Axiom 3. Given any object X in $\mathcal{C}$, the k-vector space $H^i(X)$ is finite-dimensional for $i \in \mathbb{Z}_{\geqslant 0}$.

The reader may immediately note that Axiom 1 is only meaningful due to Axiom 2 since otherwise one can always give trivial bilinear maps for a cup product of $H^\bullet(X)$. Note that these two axioms give

$$H^\bullet(X)^{\otimes n} \simeq H^\bullet(X^n)$$

defined by

$$v_1 \otimes \cdots \otimes v_n \mapsto p_1^*(v_1) \cup \cdots \cup p_n^*(v_n),$$

for any homogeneous $v_1, \ldots, v_n \in H^\bullet(X)$, where $p_1, \ldots, p_n$ are the projection maps $X^n \to X$. If G is any subgroup of S_n, then G acts on X^n by permuting coordinates. The induced action of G on $H^\bullet(X^n)$ is precisely given by

$$g \cdot (p_1^*(v_1) \cup \cdots \cup p_n^*(v_n)) = p_{g(1)}^*(v_1) \cup \cdots \cup p_{g(n)}^*(v_n).$$

for $g \in G$. If $\phi = \bigoplus_{i=0}^{\infty} \phi_i : H^\bullet(X) \to H^\bullet(X)$ is any k-linear graded endomorphism, then it induces a k-linear graded map $\phi_{X^n} : H^\bullet(X^n) \to H^\bullet(X^n)$ given by

$$p_1^*(v_1) \cup \cdots \cup p_n^*(v_n) \mapsto p_1^*(\phi(v_1)) \cup \cdots \cup p_n^*(\phi(v_n)),$$

using Axiom 2: $H^\bullet(X^n) \simeq H^\bullet(X)^{\otimes n}$. Under this isomorphism, the map ϕ_{X^n} corresponds to $\phi^{\otimes n}$. This map is compatible with the G-action we discussed above, so ϕ induces a k-linear graded map $\phi_{X^n}|_{H^\bullet(X^n)^G} : H^\bullet(X^n)^G \to H^\bullet(X^n)^G$ on the G-invariant subspaces. Moreover, we note that the corresponding G-action on $H^\bullet(X)^{\otimes n}$ to the one on $H^\bullet(X^n)$ is given by

$$g \cdot (v_1 \otimes \cdots \otimes v_n) = (-1)^{Q_g(\deg(v_1), \ldots, \deg(v_n))} v_{g^{-1}(1)} \otimes \cdots \otimes v_{g^{-1}(n)},$$

where $Q_g(x_1, \ldots, x_n)$ is defined in the previous section. This is the same G-action given by the Kozsul sign rule, so we may apply Theorem III.9 to obtain the following:

Theorem III.13. *Keeping the notation and assuming Axioms 1, 2, and 3 above, suppose that the characteristic of k does not divide $|G|$. Then*

$$L_t(\phi_{X^n}|_{H^\bullet(X^n)^G}) = Z_G(L_t(\phi), L_{t^2}(\phi^2), \ldots, L_{t^n}(\phi^n)).$$

Corollary III.10 implies the following:

Corollary III.14. *Keeping the same assumptions as in Theorem III.13, assume further that*

- *$H^i(X) = 0$ for $i > 2d$;*

- *the characteristic of k is 0.*

Then

$$\sum_{n=0}^{\infty} L_t(\phi_{X^n}|_{H^\bullet(X^n)^{S_n}})u^n = \frac{\det(\mathrm{id}_{V_1} - \phi_1 tu)\cdots\det(\mathrm{id}_{V_{2d-1}} - \phi_{2d-1}t^{2d-1}u)}{\det(\mathrm{id}_{V_0} - \phi_0 u)\cdots\det(\mathrm{id}_{V_{2d}} - \phi_{2d}t^{2d}u)}.$$

Continuing our discussion, if $F : X \to X$ is an endomorphism in $\mathcal{C}$, then

$$\begin{aligned} F^*_{X^n}(p_1^*(v_1) \cup \cdots \cup p_n^*(v_n)) &= p_1^*(F^*(v_1)) \cup \cdots \cup p_n^*(F^*(v_n)) \\ &= (F \circ p_1)^*(v_1) \cup \cdots \cup (F \circ p_n)^*(v_n) \\ &= (p_1 \circ F^n)^*(v_1) \cup \cdots \cup (p_n \circ F^n)^*(v_n) \\ &= (F^n)^*(p_1^*(v_1) \cup \cdots \cup p_n^*(v_n)), \end{aligned}$$

for any homogenous $v_1, \ldots, v_n \in H^\bullet(X)$, so $F^*_{X^n} = (F^n)^*$, where $F^n : X^n \to X^n$ is induced by $F : X \to X$. Thus,

- if the quotient map $X^n \to X^n/G$ exists in $\mathcal{C}$ so that we have $H^\bullet(X^n/G) \to H^\bullet(X^n)^G \hookrightarrow H^\bullet(X^n)$, and

- if we furthermore assume that this gives an isomorphism $H^\bullet(X^n/G) \simeq H^\bullet(X^n)^G$,

then the map $(F^n/G)^*$ corresponds to $(F^n)^*|_{H^\bullet(X^n)^G}$, where F^n/G is the induced endomorphism on X^n/G. Thus, Theorem III.13 tells us:

Theorem III.15. *Keeping the notation and the assumptions above, if the characteristic of the ambient field k does not divide $|G|$, then we have*

$$L_t((F^n/G)^*) = Z_G(L_t(F^*), L_{t^2}(F^*)^2, \ldots, L_{t^n}(F^*)^n).$$

Corollary III.14 implies:

Corollary III.16. *Keeping the notation and the assumptions above, assume further that*

- $H^i(X) = 0$ *for* $i > 2d$*;*
- *the characteristic of* k *is* 0.

Then

$$\sum_{n=0}^{\infty} L_t((F^n/S_n)^*)u^n = \frac{\det(\mathrm{id}_{H^1(X)} - F_1^* tu) \cdots \det(\mathrm{id}_{H^{2d-1}(X)} - F_{2d-1}^* t^{2d-1}u)}{\det(\mathrm{id}_{H^0(X)} - F_0^* u) \cdots \det(\mathrm{id}_{H^{2d}(X)} - F_{2d}^* t^{2d}u)}.$$

3.5 Proofs of Theorems I.1, I.3, and their analogues

We first prove Theorems I.1 and I.3 in the case of compact complex manifolds. We also prove Propositions III.5 and III.7 as well as Proposition III.1. These proofs can be taken as examples from general theorems in the previous sections.

Example III.17. Let X be a compact complex manifold of dimension d and be $H^\bullet(X)$ the singular cohomology of X with rational coefficients. The quotient map $X^n \to X^n/G$ induces an isomorphism $H^\bullet(X^n/G) \simeq H^\bullet(X^n)^G$ as proven in [Mac1962J]. In this case, Theorem III.15 with $\mathcal{C}$ being the category of compact complex manifolds proves the first case of Theorem I.3. Likewise, Corollary III.16 proves the first case of Theorem I.1. Furthermore, if X is a complex projective variety, then taking the cohomology for complex coefficients, Theorem III.13 with $\phi = \bigoplus_{p,q \in \mathbb{Z}_{\geqslant 0}} x^p y^q \mathrm{id}_{H^{p,q}(X)}$

proves Proposition III.7 and Corollary III.14 proves Proposition III.5. For Proposition III.1 where X is a finite set, we give it the discrete topology and the trivial 0-dimensional complex manifold structure. Since X is finite, it is compact, and applying Theorem III.13 with $\phi = \operatorname{diag}(t_1, \ldots, t_r) \circlearrowleft H^0(X) = \mathbb{Q}x_1 \oplus \cdots \oplus \mathbb{Q}x_r$ recovers Proposition III.1.

We next prove Theorems I.1 and I.3 in the case of quasi-projective varieties over finite fields.

Example III.18. Let X be a quasi-projective variety over $\mathbb{F}_q$ of dimension d and $H^\bullet(X)$ be the compactly supported l-adic étale cohomology of X, given a prime l. Standard theorems about the étale cohomology that go into the proof of the rationality of the zeta series $\boldsymbol{Z}_X(t)$ (which can be found in [Mil1980], for example) let us use Theorem III.13 and Corollary III.14 with $\mathcal{C}$ being the category of quasi-projective $\mathbb{F}_q$-varieties. If $l \nmid |G|$, then one can modify the proof of [HN1975, Proposition 3.2.1] to show that the quotient map $X^n \to X^n/G$ induces an isomorphism $H^\bullet(X^n/G) \simeq H^\bullet(X^n)^G$, so Theorem III.15 proves the second case of Theorem I.3. Likewise, Corollary III.16 proves the second case of Theorem I.1.

3.6 Point counting over finite fields

In this section, we discuss some concrete consequences of Theorem I.3 for point counting over $\mathbb{F}_q$. Take

- $\mathcal{C}$ to be the category of quasi-projective varieties over $\mathbb{F}_q$;

- $H^\bullet(X)$ the compactly supported l-adic étale cohomology for a prime l not dividing q and $|G|$;
- $F = \mathrm{Fr}_{q,X}$ the Frobenius endomorphism on X.

in Theorem I.3. Then F^n/G is the Frobenius endomorphism $\mathrm{Fr}_{q,X^n/G}$ on X^n/G, so Theorem I.3 implies that

$$L_t(\mathrm{Fr}^*_{q,X^n/G}) = Z_G(L_t(\mathrm{Fr}^*_{q,X}), L_{t^2}((\mathrm{Fr}^*_{q,X})^2), \ldots, L_{t^n}((\mathrm{Fr}^*_{q,X})^n).$$

Now, we apply the Grothendieck-Lefschetz trace formula $L_1((\mathrm{Fr}^*_{q,Y})^r) = |Y(\mathbb{F}_{q^r})|$ to see the following:

Corollary III.19. *Let X be a quasi-projective variety over $\mathbb{F}_q$ and G a subgroup of S_n, acting on X^n by permuting coordinates. Then*

$$|(X^n/G)(\mathbb{F}_q)| = Z_G(|X(\mathbb{F}_q)|, |X(\mathbb{F}_{q^2})|, \ldots, |X(\mathbb{F}_{q^n})|).$$

Example III.20. Applying Corollary III.19 for $G = S_n$ for $n \in \mathbb{Z}_{\geqslant 0}$ and Corollary II.12, we have

$$\sum_{n=0}^{\infty} |\mathrm{Sym}^n(X)(\mathbb{F}_q)| u^n = \exp\left(\sum_{r=1}^{\infty} \frac{|X(\mathbb{F}_{q^r})|}{r} u^r\right) = \boldsymbol{Z}_X(u).$$

Example III.21. In particular, when $X = \mathbb{A}^1$, the affine line over $\mathbb{F}_q$, we get

$$|(\mathbb{A}^n/G)(\mathbb{F}_q)| = q^n.$$

When q is odd, we have

$$\mathbb{A}^n/A_n = \mathrm{Spec}(\mathbb{F}_q[x_1, \ldots, x_n]^{A_n}) \simeq \mathrm{Spec}\left(\frac{\mathbb{F}_q[t_1, \ldots, t_n, y]}{(y^2 - \Delta_n(t_1, \ldots, t_n))}\right),$$

where A_n is the alternating group of n letters, which acts on $\mathbb{A}^n$ by permuting coordinates, and $\Delta_n(t_1, \ldots, t_n)$ is the discriminant of $x^n + t_1x^{n-1} + \cdots + t_{n-1}x + t_n$. Thus, applying the result above, we see that there are precisely q^n solutions to the equation

$$y^2 = \Delta_n(t_1, \ldots, t_n)$$

over $\mathbb{F}_q$. Thus, for $n \geqslant 2$, if we consider the set map

$$\Delta_n : \mathbb{F}_q^n \to \mathbb{F}_q$$

given by the discriminant, then we see that

$$|\Delta_n^{-1}(\{\text{quadratic residues in } \mathbb{F}_q^\times\})| = |\Delta_n^{-1}(\{\text{quadratic non-residues in } \mathbb{F}_q^\times\})|,$$

since $|\Delta_n^{-1}(0)| = q^{n-1}$, which is given by the fact that there are precisely $q^n - q^{n-1}$ degree n monic square-free polynomials in $\mathbb{F}_q[x]$. That is, if we let A to be the left-hand side and B the right-hand side of the desired identity, we have

$$1 \cdot q^{n-1} + 2 \cdot A + 0 \cdot B = |(\mathbb{A}^n/A_n)(\mathbb{F}_q)| = q^n$$

so that $A = (q^n - q^{n-1})/2$ and $B = |(\mathbb{A}^n/A_n)(\mathbb{F}_q)| - |\Delta_n^{-1}(0)| - A = (q^n - q^{n-1})/2$. This identity was previously found in [CKS2018] using a more explicit method.

CHAPTER IV

Cycle Indices of Conjugate Actions of General Linear Groups on Matrices over Finite Fields and Their Applications

The results in this chapter are based on [CH2018], a joint paper of the author and Yifeng Huang.

4.1 Matrices over finite fields

Given a finite field $\mathbb{F}_q$, consider the set $\mathrm{Mat}_n(\mathbb{F}_q)$ of $n \times n$ matrices over $\mathbb{F}_q$. It is natural to ask how many matrices $A \in \mathrm{Mat}_n(\mathbb{F}_q)$ satisfy a certain property, or, in other words, what the proportion of such matrices is. For instance, from an elementary counting argument, we know that the proportion of matrices that are invertible is

$$\frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{Mat}_n(\mathbb{F}_q)|} = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})}{q^n} = (1 - q^{-1})(1 - q^{-2}) \cdots (1 - q^{-n}).$$

To put it another way, this is the probability that a random matrix A in $\mathrm{Mat}_n(\mathbb{F}_q)$ does not have 0 as an eigenvalue. Recall from Example II.4 that for any $A \in \mathrm{Mat}_n(\mathbb{F}_q)$, we can decompose its characteristic polynomial $f_A(t)$ into a partition of powers of its irreducible factors:

$$(P(t)^{\lambda_{P,1}(A)}, \ldots, P(t)^{\lambda_{P,l_{A,P}}(A)})_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|}$$

or

$$(A \circlearrowright \mathbb{F}_q^n) \simeq \bigoplus_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} \left(\frac{\mathbb{F}_q[t]}{(P(t))^{\lambda_{P,1}(A)}} \oplus \cdots \oplus \frac{\mathbb{F}_q[t]}{(P(t))^{\lambda_{P,l_{A,P}}(A)}} \right),$$

which classifies the $\mathbb{F}_q[t]$-module structure given by the action of matrix A on $\mathbb{F}_q^n$. (In particular, we have $f_A(t) = \prod_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} P(t)^{\lambda_{P,1}(A) + \cdots + \lambda_{P,l_{A,P}}(A)}$.) The (P)-part (or simply P-part) of the matrix A is

$$A[P^\infty] \simeq \frac{\mathbb{F}_q[t]}{(P(t))^{\lambda_{P,1}(A)}} \oplus \cdots \oplus \frac{\mathbb{F}_q[t]}{(P(t))^{\lambda_{P,l_{A,P}}(A)}},$$

and recall that the modules of the form on the right-hand side of the above are called $(P)^\infty$-torsion (or simply P^∞-torsion) modules. The proportion we computed above is that of matrices whose t-part is trivial.

Then what is the probability that a random matrix $A \in \mathrm{Mat}_n(\mathbb{F}_q)$ has a specified t-part, other than the zero module? It turns out that given any t^∞-torsion $\mathbb{F}_q[t]$-module H (of $\mathbb{F}_q$-dimension $\leqslant n$), we have

$$\mathrm{Prob}_{A \in \mathrm{Mat}_n(\mathbb{F}_q)}(A[t^\infty] \simeq H) = \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H)|} \prod_{i=1}^{n} (1 - q^{-i}).$$

When $n \to \infty$, we prove a more general result, which was stated as Theorem I.7 in the introduction:

Theorem IV.1. *Fix any distinct monic irreducible polynomials $P_1(t), \ldots, P_r(t) \in \mathbb{F}_q[t]$ and P_j^∞-torsion $\mathbb{F}_q[t]$-module H_j of finite length for $1 \leqslant j \leqslant r$. Then*

$$\lim_{n \to \infty} \underset{A \in \mathrm{Mat}_n(\mathbb{F}_q)}{\mathrm{Prob}} \left(\begin{array}{c} A[P_j^\infty] \simeq H_j \\ \text{for } 1 \leqslant j \leqslant r \end{array} \right) = \prod_{j=1}^{r} \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_j)|} \prod_{i=1}^{\infty} (1 - q^{-i \deg(P_j)}).$$

The following lemma will be used in the proof of Lemma IV.3:

Lemma IV.2 ((1.6) on p.181 in [Mac1995])**.** *Let $(R, \mathfrak{m})$ be a DVR (discrete valuation ring) with the finite residue field $R/\mathfrak{m} = \mathbb{F}_q$. Given a partition λ, we have*

$$|\mathrm{Aut}_R(H_{\mathfrak{m},\lambda})| = q^{|\lambda|+2n(\lambda)} \prod_{d=1}^{\infty} \prod_{i=1}^{m_d(\lambda)} (1 - q^{-i}),$$

where $m_d(\lambda)$ is the number of parts of λ with length d and

$$n(\lambda) := 0 \cdot \lambda_1 + 1 \cdot \lambda_2 + 2 \cdot \lambda_3 + \cdots + (l-1) \cdot \lambda_l.$$

Recall from Example II.4 that we denote by $|\mathbb{A}^1_{\mathbb{F}_q}|$ the set of closed points of $\mathbb{A}^1_{\mathbb{F}_q} = \mathrm{Spec}(\mathbb{F}_q[t])$ or, equivalently, the set of monic irrducible polynomials in $\mathbb{F}_q[t]$. The following is a key lemma that will be used in our proof of Theorem IV.1:

Lemma IV.3 (Proposition 19 in [Sto1988])**.** *For any $P \in |\mathbb{A}^1_{\mathbb{F}_q}|$, we have*

$$\sum_{\nu \in \mathcal{P}} \frac{y^{|\nu|}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|} = \prod_{i=1}^{\infty} \frac{1}{1 - q^{-i\deg(P)}y} \in \mathbb{Q}[\![y]\!],$$

where

$$H_{P,\nu} := \mathbb{F}_q[t]/(P(t))^{\nu_1} \oplus \cdots \oplus \mathbb{F}_q[t]/(P(t))^{\nu_l}$$

for any given partition $\nu = [\nu_1, \ldots, \nu_l]$.

Proof. We use the proof presented in [CNY20]. Using the formula for $|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|$ from Lemma IV.2, we may reduce the problem to the case where $P(t) = t$. Then we can rewrite the left-hand side of the desired identity as

$$\sum_{n=0}^{\infty} \sum_{\lambda \vdash n} \frac{y^n}{|\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{F}_q)}(J_{0,\lambda})|},$$

where $J_{0,\lambda}$ is the Jordan canonical form given by the 0-Jordan blocks whose sizes are equal to the parts of the partition λ, and the action $\mathrm{GL}_n(\mathbb{F}_q) \circlearrowright \mathrm{Mat}_n(\mathbb{F}_q)$ is given by the conjugation. By the orbit-stabilizer theorem, we have

$$\frac{1}{|\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{F}_q)}(J_{0,\lambda})|} = \frac{|\mathrm{GL}_n(\mathbb{F}_q) \cdot J_{0,\lambda}|}{|\mathrm{GL}_n(\mathbb{F}_q)|}.$$

Recall that the $n \times n$ matrices all of whose eigenvalues are 0 are precisely the nilpotent matrices. Thus, we have

$$\begin{aligned}
\sum_{n=0}^{\infty} \sum_{\lambda \vdash n} \frac{y^n}{|\mathrm{Stab}_{\mathrm{GL}_n(\mathbb{F}_q)}(J_{0,\lambda})|} &= \sum_{n=0}^{\infty} \frac{|\mathrm{Nil}_n(\mathbb{F}_q)| y^n}{|\mathrm{GL}_n(\mathbb{F}_q)|} \\
&= 1 + \sum_{n=1}^{\infty} \frac{q^{n(n-1)} y^n}{(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})} \\
&= 1 + \sum_{n=1}^{\infty} \frac{(q^{-1}y)^n}{(1 - q^{-1})(1 - q^{-2}) \cdots (1 - q^{-n})} \\
&= \sum_{n=0}^{\infty} (q^{-1}y)^n \left(\sum_{j_1=0}^{\infty} q^{-j_1} \right) \left(\sum_{j_2=0}^{\infty} q^{-2j_2} \right) \cdots \left(\sum_{j_n=0}^{\infty} q^{-nj_n} \right) \\
&= \sum_{n=0}^{\infty} (q^{-1}y)^n \sum_{j_1=0}^{\infty} \sum_{j_2=0}^{\infty} \cdots \sum_{j_n=0}^{\infty} q^{-j_1 - 2j_2 - \cdots - nj_n} \\
&= \prod_{i=0}^{\infty} (1 + q^{-i}(q^{-1}y) + q^{-2i}(q^{-1}y)^2 + \cdots) \\
&= \prod_{i=0}^{\infty} \frac{1}{1 - q^{-(i+1)}y} \\
&= \prod_{i=1}^{\infty} \frac{1}{1 - q^{-i}y},
\end{aligned}$$

where for the second equality we used the elementary identity $|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$ and the Fine–Herstein theorem (e.g., [FH1958, Theorem 1]), which gives the number $|\mathrm{Nil}_n(\mathbb{F}_q)|$ of nilpotent matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$:

$$|\mathrm{Nil}_n(\mathbb{F}_q)| = q^{n(n-1)}.$$

For the sixth equality, we have used the fact that the coefficient of Y^n in the product

$$\prod_{i=0}^{\infty} (1 + X^i Y + X^{2i} Y^2 + \cdots)$$

is equal to

$$\sum_{j_1=0}^{\infty}\sum_{j_2=0}^{\infty}\cdots\sum_{j_n=0}^{\infty} X^{j_1+2j_2+\cdots+nj_n},$$

where X, Y are considered to be complex numbers varying within the open unit disk centered at 0 (i.e., $|X|, |Y| < 1$) so that we can take $X = q^{-1}$ and $Y = q^{-1}y$ with $|y| < q$ in our proof for the sixth equality in the chain of equalities above. Indeed, when we expand the given product, we have

$$\begin{aligned}\prod_{i=0}^{\infty}(1 + X^iY + X^{2i}Y^2 + \cdots) &= \sum_{m_0,m_1,m_2,\cdots\geqslant 0} X^{0\cdot m_0+1\cdot m_1+2\cdot m_2+\cdots}Y^{m_0+m_1+m_2+\cdots} \\ &= \sum_{n=0}^{\infty} Y^n \sum_{\substack{m_0,m_1,m_2,\cdots\geqslant 0 \\ m_0+m_1+m_2+\cdots=n}} X^{m_1+2m_2+\cdots},\end{aligned}$$

so it is enough to show that

$$\sum_{\substack{m_0,m_1,m_2,\cdots\geqslant 0 \\ m_0+m_1+m_2+\cdots=n}} X^{m_1+2m_2+\cdots} = \sum_{j_1=0}^{\infty}\sum_{j_2=0}^{\infty}\cdots\sum_{j_n=0}^{\infty} X^{j_1+2j_2+\cdots+nj_n}.$$

Note that we have a bijection

$$\{(m_0, m_1, m_2, \dots) \in \mathbb{Z}_{\geqslant 0}^{\infty} : m_0+m_1+m_2+\cdots = n\} \leftrightarrow \{(m_1, m_2, \dots) \in \mathbb{Z}_{\geqslant 0}^{\infty} : m_1+m_2+\cdots \leqslant n\}.$$

given by $(m_0, m_1, m_2, \dots) \mapsto (m_1, m_2, \dots)$. Thus, it remains to show the following:

$$\sum_{\substack{m_1,m_2,\cdots\geqslant 0 \\ m_1+m_2+\cdots\leqslant n}} X^{m_1+2m_2+\cdots} = \sum_{j_1=0}^{\infty}\sum_{j_2=0}^{\infty}\cdots\sum_{j_n=0}^{\infty} X^{j_1+2j_2+\cdots+nj_n}.$$

If $n = 0$, both sides are 1, so let $n \geqslant 1$. Let A_n be the set of partitions whose number of parts counting with multiplicity (i.e., the total column length of Young diagrams) is $\leqslant n$ and B_n the set of partitions whose parts (i.e., the row lengths of Young diagrams) are $\leqslant n$. Then we have a bijection $A_n \leftrightarrow B_n$ given by taking conjugation, so in particular, we have

$$\sum_{\lambda\in A_n} X^{|\lambda|} = \sum_{\lambda\in B_n} X^{|\lambda|}.$$

Now, noting that

$$\sum_{\lambda \in A_n} X^{|\lambda|} = \sum_{\substack{m_1, m_2, \cdots \geqslant 0 \\ m_1 + m_2 + \cdots \leqslant n}} X^{m_1 + 2m_2 + \cdots}$$

and

$$\sum_{\lambda \in B_n} X^{|\lambda|} = \sum_{j_1=0}^{\infty} \sum_{j_2=0}^{\infty} \cdots \sum_{j_n=0}^{\infty} X^{j_1 + 2j_2 + \cdots + nj_n},$$

we finish the proof. □

4.2 Proof of Theorem IV.1

We first give some definitions that will be used in our proof. Fix any subset $X \subset \mathbb{A}^1_{\mathbb{F}_q} = \mathrm{Spec}(\mathbb{F}_q[t])$, and denote by $|X|$ the set of closed points of $\mathbb{A}^1_{\mathbb{F}_q}$ inside X. We define the **cycle series of** X (**relative to** $\mathbb{A}^1_{\mathbb{F}_q}$) as follows:

$$\hat{\mathcal{Z}}(X, \boldsymbol{x}, u) = \prod_{P \in |X|} \sum_{\nu \in \mathcal{P}} \frac{x_{P,\nu} u^{|\nu| \deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|},$$

where each $P \in |\mathbb{A}^1_{\mathbb{F}_q}|$ simultaneously means a monic irreducible polynomial or the maximal ideal $(P(t))$ of $\mathbb{F}_q[t]$, or a closed point of $\mathbb{A}^1_{\mathbb{F}_q}$, generated by $P(t)$. Note that by Corollary II.13, we have

$$\hat{\mathcal{Z}}(\mathbb{A}^1_{\mathbb{F}_q}, \boldsymbol{x}, u) = \sum_{n=0}^{\infty} \mathcal{Z}_{[\mathrm{Mat}_n/\mathrm{GL}_n](\mathbb{F}_q)}(\boldsymbol{x}) u^n.$$

That is, the cycle series of the affine line $\mathbb{A}^1_{\mathbb{F}_q}$ is the generating function for the n-th cycle index of the conjugate action $\mathrm{GL}_n(\mathbb{F}_q) \circlearrowright \mathrm{Mat}_n(\mathbb{F}_q)$ for $n \in \mathbb{Z}_{\geqslant 0}$. Another important case is

$$\hat{\mathcal{Z}}(\{P\}, \boldsymbol{x}, u) = \sum_{\nu \in \mathcal{P}} \frac{x_{P,\nu} u^{|\nu| \deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|},$$

where $P \in |\mathbb{A}^1_{\mathbb{F}_q}|$. By definition, whenever we have finitely many $P_1, \ldots, P_r \in X$, we have

$$\hat{\mathcal{Z}}(X, \boldsymbol{x}, u) = \hat{\mathcal{Z}}(X \smallsetminus \{P_1, \ldots, P_r\}, \boldsymbol{x}, u) \hat{\mathcal{Z}}(\{P_1\}, \boldsymbol{x}, u) \cdots \hat{\mathcal{Z}}(\{P_r\}, \boldsymbol{x}, u).$$

Denote by $\hat{\mathcal{Z}}(X, u)$ what we get by taking all $x_{P,\nu} = 1$ in $\hat{\mathcal{Z}}(X, \boldsymbol{x}, u)$. Corollary II.14 implies that

$$\hat{\mathcal{Z}}(\mathbb{A}^1_{\mathbb{F}_q} \smallsetminus \{(t)\}, u) = 1 + u + u^2 + \cdots = \frac{1}{1-u}.$$

Finally, for any $P \in |\mathbb{A}^1_{\mathbb{F}_q}|$, Lemma IV.3 with $y = u^{\deg(P)}$ implies that

$$\hat{\mathcal{Z}}(\{P\}, u) = \sum_{\nu \in \mathcal{P}} \frac{u^{|\nu| \deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|} = \prod_{i=1}^{\infty} \frac{1}{1 - (q^{-i}u)^{\deg(P)}}.$$

We are now ready to give a proof of Theorem IV.1.

Proof of Theorem IV.1. We will use the notation given above. Taking $x_{P,\nu} = 1$ for all $P \notin \{P_1, \dots, P_r\}$, while still denoting by $\boldsymbol{x}$ the sequence of variables after such evaluations, we have

$$\begin{aligned}\hat{\mathcal{Z}}(\mathbb{A}^1_{\mathbb{F}_q}, \boldsymbol{x}, u) &= \hat{\mathcal{Z}}(\mathbb{A}^1_{\mathbb{F}_q} \smallsetminus \{P_1, \dots, P_r\}, u)\hat{\mathcal{Z}}(\{P_1\}, \boldsymbol{x}, u) \cdots \hat{\mathcal{Z}}(\{P_r\}, \boldsymbol{x}, u) \\ &= \frac{\hat{\mathcal{Z}}(\mathbb{A}^1_{\mathbb{F}_q} \smallsetminus \{(t)\}, u)\hat{\mathcal{Z}}(\{(t)\}, u)\hat{\mathcal{Z}}(\{P_1\}, \boldsymbol{x}, u) \cdots \hat{\mathcal{Z}}(\{P_r\}, \boldsymbol{x}, u)}{\hat{\mathcal{Z}}(\{P_1\}, u) \cdots \hat{\mathcal{Z}}(\{P_r\}, u)} \\ &= \left(\frac{1}{1-u}\right) \frac{\hat{\mathcal{Z}}(\{(t)\}, u)\hat{\mathcal{Z}}(\{P_1\}, \boldsymbol{x}, u) \cdots \hat{\mathcal{Z}}(\{P_r\}, \boldsymbol{x}, u)}{\hat{\mathcal{Z}}(\{P_1\}, u) \cdots \hat{\mathcal{Z}}(\{P_r\}, u)}.\end{aligned}$$

Without loss of generality, suppose that $\lambda^{(1)}, \dots, \lambda^{(m)}$ are nonempty, while $\lambda^{(m+1)}, \dots, \lambda^{(r)} = \varnothing$, for some $0 \leqslant m \leqslant r$. In the above identity, take $x_{P_j,\nu} = 0$ for nonempty ν not equal to $\lambda^{(j)}$ while $x_{P_j,\lambda^{(j)}} = 1$ for $1 \leqslant j \leqslant m$. We will still write $\boldsymbol{x}$ to mean the sequence of variables after evaluations, although this is now just a sequence in $\{0, 1\}$. We may compute the limit of the coefficient of u^n of the left-hand side as $n \to \infty$ by evaluating $u = 1$ without the factor $(1-u)^{-1}$ on the right-hand side, and since

$$\hat{\mathcal{Z}}(\{(t)\}, 1) = \lim_{n \to \infty} \frac{|\mathrm{Mat}_n(\mathbb{F}_q)|}{|\mathrm{GL}_n(\mathbb{F}_q)|},$$

we have

$$\begin{aligned}
&\lim_{n\to\infty} \mathrm{Prob}_{A\in \mathrm{Mat}_n(\mathbb{F}_q)}\left(\begin{array}{c} \mu_{P_j}(A) \in \{\varnothing, \lambda^{(j)}\} \text{ for } 1 \leqslant j \leqslant m, \\ \mu_{P_{m+1}}(A) = \cdots = \mu_{P_r}(A) = \varnothing \end{array}\right) \\
&= \frac{\hat{\mathcal{Z}}(\{P_1\}, \boldsymbol{x}, 1) \cdots \hat{\mathcal{Z}}(\{P_r\}, \boldsymbol{x}, 1)}{\hat{\mathcal{Z}}(\{P_1\}, 1) \cdots \hat{\mathcal{Z}}(\{P_r\}, 1)} \\
&= \left[\prod_{j=1}^{m}\left(1 + \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q}(H_{P,\lambda^{(j)}})|}\right)\prod_{i=1}^{\infty}(1 - q^{-i\deg(P_j)})\right] \cdot \left[\prod_{j=m+1}^{r}\prod_{i=1}^{\infty}(1 - q^{-i\deg(P_j)})\right].
\end{aligned}$$

To finish the proof, we proceed by induction on $m \geqslant 0$. Given partitions $\nu^{(1)}, \ldots, \nu^{(m)}$, write

$$P(\nu^{(1)}, \ldots, \nu^{(m)}) := \lim_{n\to\infty} \mathrm{Prob}_{A\in \mathrm{Mat}_n(\mathbb{F}_q)}\left(\begin{array}{c} \mu_{P_j}(A) = \nu^{(j)} \text{ for } 1 \leqslant j \leqslant m, \\ \mu_{P_{m+1}}(A) = \cdots = \mu_{P_r}(A) = \varnothing \end{array}\right),$$

as long as the limit on the right-hand side exists. Taking $m = 0$, what we have proved above implies that

$$P(\varnothing, \cdots, \varnothing) = \prod_{j=1}^{r}\prod_{i=1}^{\infty}(1 - q^{-i\deg(P_j)}),$$

which serves the base case for the induction. For the induction hypothesis, suppose that our statement is true when at most $m - 1 \geqslant 0$ partitions among $\lambda^{(1)}, \ldots, \lambda^{(r)}$ are nonempty. We know that

$$\begin{aligned}
&\sum_{\substack{\nu^{(1)}, \ldots, \nu^{(m)}: \\ \nu^{(j)} \in \{\varnothing, \lambda^{(j)}\} \\ \text{for } 1 \leqslant j \leqslant m}} P(\nu^{(1)}, \ldots, \nu^{(m)}) \\
&= \left[\prod_{j=1}^{m}\left(1 + \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\lambda^{(j)}})|}\right)\prod_{i=1}^{\infty}(1 - q^{-i\deg(P_j)})\right] \cdot \left[\prod_{j=m+1}^{r}\prod_{i=1}^{\infty}(1 - q^{-i\deg(P_j)})\right],
\end{aligned}$$

so

$$\begin{aligned}
P(\lambda^{(1)}, \dots, \lambda^{(m)}) &= \sum_{\substack{\nu^{(1)},\dots,\nu^{(m)}: \\ \nu^{(j)} \in \{\varnothing, \lambda^{(j)}\} \\ \text{for } 1 \leqslant j \leqslant m}} P(\nu^{(1)}, \dots, \nu^{(m)}) - \sum_{\substack{\nu^{(1)},\dots,\nu^{(m)}: \\ \nu^{(j)} \in \{\varnothing, \lambda^{(j)}\} \\ \text{for } 1 \leqslant j \leqslant m, \\ \text{not all } \nu^{(j)} \text{ are } \lambda^{(j)}}} P(\nu^{(1)}, \dots, \nu^{(m)}) \\
&= \left[\prod_{j=1}^{m} \left(1 + \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\lambda^{(j)}})|} \right) \prod_{i=1}^{\infty} (1 - q^{-i\deg(P_j)}) \right] \cdot \left[\prod_{j=m+1}^{r} \prod_{i=1}^{\infty} (1 - q^{-i\deg(P_j)}) \right] \\
&\quad - \sum_{\substack{\nu^{(1)},\dots,\nu^{(m)}: \\ \nu^{(j)} \in \{\varnothing, \lambda^{(j)}\} \\ \text{for } 1 \leqslant j \leqslant m, \\ \text{not all } \nu^{(j)} \text{ are } \lambda^{(j)}}} P(\nu^{(1)}, \dots, \nu^{(m)}) \\
&= \prod_{j=1}^{r} \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\lambda^{(j)}})|} \prod_{i=1}^{\infty} (1 - q^{-i\deg(P_j)}),
\end{aligned}$$

where we used the induction hypothesis for the last equality, which lets us see that all the terms in the sum are canceled out. This finishes the proof. □

The following result gives some ideas about what happens when n is fixed before tending to infinity:

Theorem IV.4. *Fix any monic irreducible polynomial $P = P(t) \in \mathbb{F}_q[t]$ and a P^∞-torsion $\mathbb{F}_q[t]$-module H of finite length. Write $h := \dim_{\mathbb{F}_q}(H)$. Then*

$$\operatorname*{Prob}_{A \in \mathrm{Mat}_n(\mathbb{F}_q)}(A[P^\infty] \simeq H) = \begin{cases} \frac{b_{n-h}(\deg(P))}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H)|} \prod_{i=1}^{n} (1 - q^{-i}) & \text{if } n \geqslant h \text{ and} \\ 0 & \text{if } n < h, \end{cases}$$

where $b_n(d)$, for $d \in \mathbb{Z}_{\geqslant 0}$, are given by

$$\sum_{n=0}^{\infty} b_n(d) u^n = \prod_{i=1}^{\infty} \frac{1 - (q^{-i}u)^d}{1 - q^{1-i}u} \in \mathbb{C}[\![u]\!].$$

Moreover, we have

$$\lim_{n \to \infty} b_n(d) = \prod_{i=1}^{\infty} \frac{1 - q^{-id}}{1 - q^{-i}}$$

so that

$$\lim_{n\to\infty} \mathrm{Prob}_{A\in \mathrm{Mat}_n(\mathbb{F}_q)}(A[P^\infty] \simeq H) = \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H)|}\prod_{i=1}^{\infty}(1 - q^{-i\deg(P)}).$$

Proof. In this proof, we will denote the polynomial P in the statement by P_0 instead. We may assume that

$$H = H_{P_0,\lambda} = \mathbb{F}_q[t]/(P_0(t))^{\lambda_1} \oplus \cdots \oplus \mathbb{F}_q[t]/(P_0(t))^{\lambda_l}$$

for some fixed partition $\lambda = (\lambda_1, \dots, \lambda_l) \in \mathcal{P}$. The case $\lambda = \varnothing$ (i.e., $H = 0$) turns out to be the most important. For this, it is enough to show that

$$b_n(\deg(P_0)) = \frac{|\{A \in \mathrm{Mat}_n(\mathbb{F}_q) : \mu_{P_0}(A) = \varnothing\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|}.$$

Let $y_n(P_0)$ be the expression on the right-hand side. Take $x_{P_0,\nu} = 0$ for all nonempty ν and $x_{P,\nu} = 1$ for all $P \neq P_0$ in Lemma II.13, which leads to

$$\begin{aligned}\sum_{n=0}^{\infty} y_n(P_0)u^n &= \prod_{\substack{P\in|\mathbb{A}^1_{\mathbb{F}_q}|,\\ P(t)\neq P_0(t)}} \sum_{\nu\in\mathcal{P}} \frac{u^{|\nu|\deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|} \\ &= \left(\sum_{\nu\in\mathcal{P}} \frac{u^{|\nu|\deg(P_0)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\nu})|}\right)^{-1} \left(\sum_{\nu\in\mathcal{P}} \frac{u^{|\nu|}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{t,\nu})|}\right) \prod_{\substack{P\in|\mathbb{A}^1_{\mathbb{F}_q}|,\\ P(t)\neq t}} \sum_{\nu\in\mathcal{P}} \frac{u^{|\nu|\deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|} \\ &= \left(\prod_{i=1}^{\infty} \frac{1-(q^{-i}u)^{\deg(P_0)}}{1-q^{-i}u}\right)\left(\frac{1}{1-u}\right) \\ &= \prod_{i=1}^{\infty} \frac{1-(q^{-i}u)^{\deg(P_0)}}{1-q^{1-i}u},\end{aligned}$$

where we applied Lemma II.14, with the evaluations $x_{P,\nu} = 1$, which gives

$$1 + u + u^2 + \cdots = \frac{1}{1-u},$$

and Lemma IV.3 as well. This shows that $y_n(P_0) = b_n(\deg(P_0))$ by the definition of $b_n(d)$ in the statement of Theorem IV.4.

Now, we may assume that the partition $\lambda = (\lambda_1, \ldots, \lambda_l)$ is nonempty (i.e., $l > 0$). We again recall that $x_{P,\varnothing} = 1$ by our definition. In Lemma II.13, take $x_{P,\nu} = 1$ on both sides for $P \neq P_0$ to get

$$\sum_{n=0}^{\infty} \sum_{A \in \mathrm{Mat}_n(\mathbb{F}_q)} \frac{x_{P_0, \mu_{P_0}(A)}}{|\mathrm{GL}_n(\mathbb{F}_q)|} u^n = \left(\sum_{\nu \in \mathcal{P}} \frac{x_{P_0,\nu} u^{|\nu| \deg(P_0)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\nu})|} \right) \left(\prod_{P \neq P_0} \sum_{\nu \in \mathcal{P}} \frac{u^{|\nu| \deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|} \right).$$

Next, we take $x_{P_0,\nu} = 0$ for all nonempty $\nu \neq \lambda$ and $x_{P_0,\lambda} = 1$. Then

$$\begin{aligned}
&1 + \sum_{n=1}^{\infty} \left(\frac{|\{A \in \mathrm{Mat}_n(\mathbb{F}_q) : \mu_{P_0}(A) = \lambda \text{ or } \varnothing\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} \right) u^n \\
&\quad = \left(1 + \frac{u^{|\lambda| \deg(P_0)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\lambda})|} \right) \left(\prod_{P \neq P_0} \sum_{\nu \in \mathcal{P}} \frac{u^{|\nu| \deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|} \right) \\
&\quad = \left(1 + \frac{u^{|\lambda| \deg(P_0)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\lambda})|} \right) \left(\prod_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} \sum_{\nu \in \mathcal{P}} \frac{u^{|\nu| \deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|} \right) \left(\sum_{\nu \in \mathcal{P}} \frac{u^{|\nu| \deg(P_0)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\nu})|} \right)^{-1}
\end{aligned}$$

$$\begin{aligned}
&= \left(1 + \frac{u^{|\lambda| \deg(P_0)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\lambda})|} \right) \left(\prod_{P(t) \neq t} \sum_{\nu \in \mathcal{P}} \frac{u^{|\nu| \deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|} \right) \\
&\qquad \cdot \left(\sum_{\nu \in \mathcal{P}} \frac{u^{|\nu|}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{(t),\nu})|} \right) \left(\sum_{\nu \in \mathcal{P}} \frac{u^{|\nu| \deg(P_0)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\nu})|} \right)^{-1} \\
&= \left(1 + \frac{u^{|\lambda| \deg(P_0)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\lambda})|} \right) \left(\frac{1}{1-u} \right) \left(\prod_{i=1}^{\infty} \frac{1 - (q^{-i}u)^{\deg(P_0)}}{1 - q^{-i}u} \right),
\end{aligned}$$

applying Lemma II.14 (again with the evaluations $x_{P,\nu} = 1$) and Lemma IV.3. Thus, we have

$$\begin{aligned}
&1 + \sum_{n=1}^{\infty} \left(\frac{|\{A \in \mathrm{Mat}_n(\mathbb{F}_q) : \mu_{P_0}(A) = \lambda \text{ or } \varnothing\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} \right) u^n \\
&\quad = (1 + cu^h)(1 + b_1 u + b_2 u^2 + b_3 u^3 + \cdots) \\
&\quad = 1 + b_1 u + b_2 u + \cdots + b_{h-1} u^{h-1} + (b_h + c) u^h + (b_{h+1} + cb_1) u^{h+1} + (b_{h+2} + cb_2) u^{h+2} + \cdots,
\end{aligned}$$

where

- $c = |\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\lambda})|^{-1} = |\mathrm{Aut}_{\mathbb{F}_q[t]}(H)|^{-1}$,
- $b_n = b_n(\deg(P_0))$, and
- $h = |\lambda| \deg(P_0) = \dim_{\mathbb{F}_q}(H)$.

Thus, continuing the previous computations, since we have established that

$$b_n = \frac{|\{A \in \mathrm{Mat}_n(\mathbb{F}_q) : \mu_{P_0}(A) = \varnothing\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|},$$

we have (as $b_0 = 1$)

$$\begin{aligned} &\frac{|\{A \in \mathrm{Mat}_n(\mathbb{F}_q) : \mu_{P_0}(A) = \lambda\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} \\ &= \begin{cases} cb_{n-h} = |\mathrm{Aut}_{\mathbb{F}_q[t]}(H)|^{-1} b_{n-h}(\deg(P_0)) & \text{if } n \geqslant h = |\lambda| \deg(P_0), \\ 0 & \text{if } n < h = |\lambda| \deg(P_0). \end{cases} \end{aligned}$$

By multiplying both sides by

$$\begin{aligned} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{Mat}_n(\mathbb{F}_q)|} &= \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})}{q^{n^2}} \\ &= (1 - q^{-1})(1 - q^{-2}) \cdots (1 - q^{-n}), \end{aligned}$$

we finish the proof. □

Remark IV.5. Note that given q, n, and H, the conclusion of Theorem IV.4 only depends on $\deg(P)$ rather than P itself. A special case where $\deg(P) = 1$ is interesting (i.e., $P(t) = t - a$ for some $a \in \mathbb{F}_q$). Since $b_n(1) = 1$ for all $n \geqslant 0$, Theorem IV.4 implies that

$$\underset{A \in \mathrm{Mat}_n(\mathbb{F}_q)}{\mathrm{Prob}}(A[(t-a)^\infty] \simeq H) = \begin{cases} \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H)|} \prod_{i=1}^n (1 - q^{-i}) & \text{if } n \geqslant \dim_{\mathbb{F}_q}(H) \text{ and} \\ 0 & \text{if } n < \dim_{\mathbb{F}_q}(H). \end{cases}$$

4.3 The distribution of the cokernel of a random $\mathbb{Z}_p$-matrix

Although it is already interesting to deal with matrices over $\mathbb{Z}_p$, in this section we work more generally with any complete DVR R with the maximal ideal $\mathfrak{m}$, or simply denoted as $(R, \mathfrak{m})$, whose residue field $R/\mathfrak{m}$ is finite so that we may write $R/\mathfrak{m} = \mathbb{F}_q$. For any such R, saying that an R-module has finite size is equivalent to saying that it is of finite length. Finite abelian p-groups are finite size $\mathbb{Z}_p$-modules, so they are finite length $\mathbb{Z}_p$-modules. The following statement with $R = \mathbb{Z}_p$ was given as [FW1987, Proposition 1], but the proof given there works for the general R. We use the Haar probability measure on $\mathrm{Mat}_n(R) = R^{n^2}$, the unique Haar measure on the additive topological group with total measure 1.

Proposition IV.6 (Friedman-Washington)**.** *Let $(R, \mathfrak{m})$ be a complete DVR with $R/\mathfrak{m} = \mathbb{F}_q$. Given any finite length R-module H, we have*

$$\underset{A \in \mathrm{Mat}_n(R)}{\mathrm{Prob}}(\mathrm{coker}(A) \simeq H) = \begin{cases} \dfrac{1}{|\mathrm{Aut}_R(H)|} \left(\prod_{i=1}^{n}(1-q^{-i})\right) \left(\prod_{j=n-l_H+1}^{n}(1-q^{-j})\right) & \text{if } n \geqslant l_H, \\ 0 & \text{if } n < l_H, \end{cases}$$

where $l_H := \dim_{\mathbb{F}_q}(H/\mathfrak{m}H)$. In particular, we have

$$\lim_{n \to \infty} \underset{A \in \mathrm{Mat}_n(R)}{\mathrm{Prob}}(\mathrm{coker}(A) \simeq H) = \frac{1}{|\mathrm{Aut}_R(H)|} \prod_{i=1}^{\infty}(1-q^{-i}).$$

We will generalize the limiting distribution (i.e., the probability when $n \to \infty$) in Proposition IV.6 as Theorem C. We also propose a more general conjecture in Conjecture IV.8. Given any ring R, we denote by $\mathbf{Mod}_R^{<\infty}$ the set of isomorphism classes of finite size R-modules. When $(R, \mathfrak{m})$ is a DVR with $R/\mathfrak{m} = \mathbb{F}_q$, this is the same as the set of isomorphism classes of finite length R-modules. When denoting an isomorphism class, we will interchangeably write a representative of it to denote the class.

Remark IV.7. It turns out that for any DVR $(R, \mathfrak{m})$ with $R/\mathfrak{m} = \mathbb{F}_q$, the assignment

$$\{H\} \mapsto \frac{1}{|\mathrm{Aut}_R(H)|}\prod_{i=1}^{\infty}(1-q^{-i})$$

defines a probability measure on the set of subsets of $\mathbf{Mod}_R^{<\infty}$ (by an application of Lemma IV.3). We call this the **Cohen-Lenstra distribution of** R, although the terminology is mostly used for the case $R = \mathbb{Z}_p$ in the literature (e.g., see [EVW2016, Section 8]). Since R is a PID (principal ideal domain), for any finite length R-module H, we have a unique partition $\lambda = (\lambda_1, \dots, \lambda_l)$, with the convention $\lambda_1 \geqslant \cdots \geqslant \lambda_l$, such that

$$H \simeq R/\mathfrak{m}^{\lambda_1} \oplus \cdots \oplus R/\mathfrak{m}^{\lambda_l}.$$

In this case, we will write $\lambda(H) := \lambda$. Recall that the number $|\mathrm{Aut}_R(H)|$ only depends on $q = |R/\mathfrak{m}|$ and λ so that we may write $w(q, \lambda) = |\mathrm{Aut}_R(H)|$ (e.g., see Lemma IV.2). Using this and Lemma IV.3 with $y = 1$, one may check that

$$\lambda \mapsto \frac{1}{w(q,\lambda)}\prod_{i=1}^{\infty}(1-q^{-i})$$

defines a probability distribution on the set $\mathcal{P}$ of partitions of nonnegative integers. We will not name this more general distribution. Fulman and Kaplan [FK2019] discussed other similar distributions defined on $\mathcal{P}$ that come up in various combinatorial contexts.

4.3.1 Main conjecture and theorems

We shall introduce our main conjecture about a random matrix $A \in \mathrm{Mat}_n(R)$, where $(R, \mathfrak{m})$ is a complete DVR such that $R/\mathfrak{m} = \mathbb{F}_q$. We will resolve special cases of this conjecture as Theorems B and C by understanding interplays between random matrices $A \in \mathrm{Mat}_n(R)$ and $\overline{A} \in \mathrm{Mat}_n(\mathbb{F}_q)$, where the latter is given by the uniform distribution on $\mathrm{Mat}_n(\mathbb{F}_q)$.

Conjecture IV.8. *Let $(R, \mathfrak{m})$ be a complete DVR such that $R/\mathfrak{m} = \mathbb{F}_q$ and $P_1(t), \dots, P_r(t) \in R[t]$ are monic polynomials such that the reduction modulo $\mathfrak{m}$ gives distinct irreducible polynomials $\overline{P}_1(t), \dots, \overline{P}_r(t) \in \mathbb{F}_q[t]$, where $r \in \mathbb{Z}_{\geqslant 0}$. Fix any R-modules $H_1, \dots, H_r$ of finite length. We must have*

$$\lim_{n\to\infty} \mathrm{Prob}_{A\in\mathrm{Mat}_n(R)} \begin{pmatrix} \mathrm{coker}(P_j(A)) \simeq H_j \\ \textit{for } 1 \leqslant j \leqslant r \end{pmatrix} = \prod_{j=1}^{r} \frac{1}{w(q^{\deg(P_j)}, \lambda(H_j))} \prod_{i=1}^{\infty} (1 - q^{-i\deg(P_j)}).$$

Note that the limiting distribution $n \to \infty$ given by Proposition IV.6 is a special case of Conjecture IV.8. More cases of Conjecture IV.8 are proven as Theorems B and C. We now present our main theorems of this section: Theorems A, B, and C.

Theorem A. Let $(R, \mathfrak{m})$ be a complete DVR such that $R/\mathfrak{m} = \mathbb{F}_q$ and $P(t) \in R[t]$ is a monic polynomial such that the reduction modulo $\mathfrak{m}$ gives an irreducible polynomial $\overline{P}(t) \in \mathbb{F}_q[t]$. We have

$$\underset{A\in\mathrm{Mat}_n(R)}{\mathrm{Prob}} (\mathrm{coker}(P(A)) = 0) = b_n(\deg(P)) \prod_{i=1}^{n} (1 - q^{-i}),$$

where $b_n(d)$, for $d \in \mathbb{Z}_{\geqslant 0}$, are given by

$$\sum_{n=0}^{\infty} b_n(d) u^n = \prod_{i=1}^{\infty} \frac{1 - (q^{-i}u)^d}{1 - q^{1-i}u} \in \mathbb{C}[\![u]\!].$$

Moreover, we have

$$\lim_{n\to\infty} b_n(d) = \prod_{i=1}^{\infty} \frac{1 - q^{-id}}{1 - q^{-i}},$$

so in particular, we have

$$\lim_{n\to\infty}\operatorname*{Prob}_{A\in\mathrm{Mat}_n(R)}(\mathrm{coker}(P(A))=0)=\prod_{i=1}^{\infty}(1-q^{-i\deg(P)}).$$

Proof. By an application of Nakayama's lemma (or taking $N=0$ in Lemma IV.14 which we introduce later), we have

$$\operatorname*{Prob}_{A\in\mathrm{Mat}_n(R)}\begin{pmatrix}\mathrm{coker}(P_j(A))=0\\ \text{for } 1\leqslant j\leqslant r\end{pmatrix}=\operatorname*{Prob}_{A\in\mathrm{Mat}_n(\mathbb{F}_q)}\begin{pmatrix}\mathrm{coker}(P_j(\overline{A}))=0\\ \text{for } 1\leqslant j\leqslant r\end{pmatrix}.$$

Moreover, we note that for any $\overline{A}\in\mathrm{Mat}_n(\mathbb{F}_q)$, we have $\mathrm{coker}(P_j(\overline{A}))=0$ if and only if $P_j(\overline{A})=\overline{P}_j(\overline{A})$ is invertible in $\mathrm{Mat}_n(\mathbb{F}_q)$. This is the same as saying $A[\overline{P}_j^{\infty}]=0$, so this finishes the proof by taking $H_1=\cdots=H_r=0$ in Theorem IV.4. □

Remark IV.9. Using the proof of Theorem IV.4, we can check that $b_n(d)$ given above are positive rational numbers explicitly given as

$$b_n(d)=\frac{|\{\overline{A}\in\mathrm{Mat}_n(\mathbb{F}_q):\mathrm{coker}(\overline{P}(\overline{A}))=0\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|}=\frac{|\{\overline{A}\in\mathrm{Mat}_n(\mathbb{F}_q):\overline{P}(\overline{A})\in\mathrm{GL}_n(\mathbb{F}_q)\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|},$$

for any degree d monic irreducible polynomial $\overline{P}(t)\in\mathbb{F}_q[t]$.

Theorem B. Let $(R,\mathfrak{m})$ be a complete DVR such that $R/\mathfrak{m}=\mathbb{F}_q$ and $P_1(t),\ldots,P_r(t)\in R[t]$ are monic polynomials such that the reduction modulo $\mathfrak{m}$ gives distinct irreducible polynomials $\overline{P}_1(t),\ldots,\overline{P}_r(t)\in\mathbb{F}_q[t]$, where $r\in\mathbb{Z}_{\geqslant 0}$. We have

$$\lim_{n\to\infty}\operatorname*{Prob}_{A\in\mathrm{Mat}_n(R)}\begin{pmatrix}\mathrm{coker}(P_j(A))=0\\ \text{for } 1\leqslant j\leqslant r\end{pmatrix}=\prod_{j=1}^{r}\prod_{i=1}^{\infty}(1-q^{-i\deg(P_j)}).$$

That is, Theorem B generalizes the limiting result in Theorem A by saying that the events, each of which says that $\mathrm{coker}(P_i(A)) = 0$, for $1 \leqslant i \leqslant r$ are asymptotically independent as n goes to infinity. This is surprising because many events regarding $P_1(A)$ and $P_2(A)$ are dependent. (For example, we may take $P_1(t) = t$ and $P_2(t) = t - 1$ with any subset $S_1 \subset \mathrm{Mat}_n(R)$ and $S_2 = \{A - \mathrm{id} : A \in S_1\}$. Then $P_1(A) \in S_1$ if and only if $P_2(A) \in S_2$.)

The following was stated in the introduction as Theorem I.9 for the case $R = \mathbb{Z}_p$:

Theorem C. Let $(R, \mathfrak{m})$ be a complete DVR such that $R/\mathfrak{m} = \mathbb{F}_q$ and $P_1(t), \dots, P_r(t) \in R[t]$ are monic polynomials such that the reduction modulo $\mathfrak{m}$ gives distinct irreducible polynomials $\overline{P}_1(t), \dots, \overline{P}_r(t) \in \mathbb{F}_q[t]$, where $r \in \mathbb{Z}_{\geqslant 1}$. Suppose that $\deg(P_r) = 1$. Given any R-module H of finite length, we have

$$\lim_{n \to \infty} \underset{A \in \mathrm{Mat}_n(R)}{\mathrm{Prob}} \left(\begin{array}{c} \mathrm{coker}(P_1(A)) = \cdots = \mathrm{coker}(P_{r-1}(A)) = 0 \\ \text{and } \mathrm{coker}(P_r(A)) \simeq H \end{array} \right) = \frac{1}{|\mathrm{Aut}_R(H)|} \prod_{j=1}^{r} \prod_{i=1}^{\infty} (1 - q^{-i \deg(P_j)}).$$

Note that Theorem C generalizes the limiting distribution given in Proposition IV.6, a result of Friedman and Washington. Theorem C also generalizes another result of the same authors [FW1987, (9) on p.234], which we discuss as Corollary IV.10. Finally, Theorem C generalizes Theorem B by summing over all possible H up to isomorphisms.

The proof of the following corollary uses Lemma IV.14, which we introduce later:

Corollary IV.10 (Friedman and Washington)**.** *Let $(R, \mathfrak{m})$ be any complete DVR with $R/\mathfrak{m} = \mathbb{F}_q$ and H any R-module of finite length. We have*

$$\lim_{n\to\infty} \operatorname*{Prob}_{A\in\mathrm{GL}_n(R)}(\mathrm{coker}(A - \mathrm{id}) \simeq H) = \frac{1}{|\mathrm{Aut}_R(H)|}\prod_{i=1}^{\infty}(1-q^{-i}).$$

Proof. Choose any $N \in \mathbb{Z}_{\geqslant 0}$ such that $\mathfrak{m}^N H = 0$. Since

$$\frac{|\mathrm{GL}_n(R/\mathfrak{m}^{N+1})|}{|\mathrm{Mat}_n(R/\mathfrak{m}^{N+1})|} = \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{Mat}_n(\mathbb{F}_q)|} = \prod_{i=1}^{n}(1-q^{-i}),$$

we have

$$\begin{aligned}\operatorname*{Prob}_{\overline{A}\in\mathrm{Mat}_n(R/\mathfrak{m}^{N+1})}\begin{pmatrix}\mathrm{coker}(\overline{A}) = 0,\\ \mathrm{coker}(\overline{A}-\mathrm{id}) \simeq H\end{pmatrix} &= \frac{|\mathrm{GL}_n(R/\mathfrak{m}^{N+1})|}{|\mathrm{Mat}_n(R/\mathfrak{m}^{N+1})|}\operatorname*{Prob}_{\overline{A}\in\mathrm{GL}_n(R/\mathfrak{m}^{N+1})}(\mathrm{coker}(\overline{A}-\mathrm{id}) \simeq H)\\ &= \operatorname*{Prob}_{A\in\mathrm{GL}_n(R)}(\mathrm{coker}(A-\mathrm{id}) \simeq H)\prod_{i=1}^{n}(1-q^{-i}),\end{aligned}$$

applying Lemma IV.14, noting that $\mathrm{coker}(\overline{A}) = 0$ if and only if $\overline{A}$ is an automorphism of $(R/\mathfrak{m}^{N+1})^n$. Thus, Theorem C, with $P_1(t) = t$ and $P_2(t) = t - 1$ for $r = 2$, admits the result by letting $n \to \infty$. □

Remark IV.11. Our proof for Theorem C uses Lemma IV.15 due to Friedman and Washington, which appears in the original proof of Corollary IV.10. The condition $\deg(P_r) = 1$ in Theorem C is necessary is because it is needed in the proof of this lemma, and for now, we are unable to drop this condition. In fact, our proof will show more generally that given the same hypothesis as in Theorem C, we have

$$\begin{aligned}&\mathrm{Prob}_{A\in\mathrm{Mat}_n(R)}\begin{pmatrix}\mathrm{coker}(P_1(A)) = \cdots = \mathrm{coker}(P_{r-1}(A)) = 0\\ \text{and } \mathrm{coker}(P_r(A)) \simeq H\end{pmatrix}\\ &= \frac{q^{l_H^2}\prod_{i=1}^{l_H}(1-q^{-i})^2}{|\mathrm{Aut}_R(H)|}\mathrm{Prob}_{\overline{A}\in\mathrm{Mat}_n(\mathbb{F}_q)}\begin{pmatrix}\mathrm{coker}(P_j(\overline{A})) = 0 \text{ for } 1 \leqslant j \leqslant r-1,\\ \dim_{\mathbb{F}_q}(\mathrm{coker}(P_r(\overline{A})) = l_H\end{pmatrix},\end{aligned}$$

where $l_H = \dim_{\mathbb{F}_q}(H/\mathfrak{m}H)$. By taking $r = 1$ and $P_1(t) = t$ and using the fact that the number of matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ with corank $0 \leqslant l \leqslant n$ is equal to

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

we can deduce Proposition IV.6 even for all $n \geqslant 0$, not just $n \to \infty$. This is not the proof given by Friedman and Washington [FW1987] (as one can check Proposition 1 in their paper). However, Lemma IV.15 is from their paper, so it seems very likely that Friedman and Washington were aware of this argument.

4.3.2 Useful lemmas

For the results that follow, we recall that given a finite length module H over a complete DVR $(R, \mathfrak{m})$ with $R/\mathfrak{m} = \mathbb{F}_q$, there exists $N \in \mathbb{Z}_{\geqslant 0}$ such that $\mathfrak{m}^N H = 0$.

Lemma IV.12. *Let $(R, \mathfrak{m})$ be a complete DVR with $R/\mathfrak{m} = \mathbb{F}_q$ and H a finite length R-module. Fix any $N \in \mathbb{Z}_{\geqslant 0}$ such that $\mathfrak{m}^N H = 0$. For any $A \in \mathrm{Mat}_n(R)$, we have $\mathrm{coker}(A) \simeq H$ if and only if $\mathrm{coker}(\overline{A}) \simeq H$, where $\overline{A} \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ is the image of A modulo $\mathfrak{m}^{N+1}$.*

Proof. If $\mathrm{coker}(A) \simeq H$, then $\mathrm{coker}(\overline{A}) \simeq H/\mathfrak{m}^{N+1}H \simeq H$ because $\mathfrak{m}^{N+1}H = \mathfrak{m}\mathfrak{m}^N H = 0$. Conversely, let $\mathrm{coker}(\overline{A}) \simeq H$. Since R is a PID, we can write

$$H \simeq R/\mathfrak{m}^{\lambda_1} \oplus \cdots \oplus R/\mathfrak{m}^{\lambda_l}$$

for some partition $\lambda = (\lambda_1, \ldots, \lambda_l)$. Since $\mathfrak{m}^N H = 0$, we have $1 \leqslant \lambda_i \leqslant N$ for all i. The fact that R is a PID lets us choose $g_1, g_2 \in \mathrm{GL}_n(R)$ such that $g_1 A g_2$ is a diagonal matrix (i.e., a Smith normal form of A). Since $(R, \mathfrak{m})$ is a DVR, choosing a generator π of $\mathfrak{m}$, each diagonal entry of $g_1 A g_2$ is either 0 or of the form $u\pi^e$, where u is a unit of R and $e \in \mathbb{Z}_{\geqslant 0}$. There should not be any 0 in the diagonal entries modulo $\mathfrak{m}^{N+1}$ because $\mathrm{coker}(\overline{A}) \simeq H$ is annihilated by $\mathfrak{m}^N$. (This is why our conclusion is about A modulo $\mathfrak{m}^{N+1}$ instead of $\mathfrak{m}^N$.) Thus, the diagonal entries of $g_1 A g_2$ are of the form $u_1\pi^{e_1}, \dots, u_n\pi^{e_n}$, where $u_i \in R^\times$ and $0 \leqslant e_i \leqslant N$. The matrix $\overline{g_1}\overline{A}\overline{g_2} \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ is diagonal with nonzero entires $\overline{u_1\pi^{e_1}}, \dots, \overline{u_n\pi^{e_n}} \in R/\mathfrak{m}^{N+1}$. We must have $(e_1, \dots, e_n) = (\lambda_1, \dots, \lambda_l, 0, \dots, 0)$ because $\overline{g_1}, \overline{g_2} \in \mathrm{GL}_n(R/\mathfrak{m}^{N+1})$ so that

$$\begin{aligned} R/\mathfrak{m}^{e_1} \oplus \cdots \oplus R/\mathfrak{m}^{e_n} &\simeq \mathrm{coker}(\overline{g_1}\overline{A}\overline{g_2}) \\ &\simeq \mathrm{coker}(\overline{A}) \\ &\simeq H \\ &\simeq R/\mathfrak{m}^{\lambda_1} \oplus \cdots \oplus R/\mathfrak{m}^{\lambda_l}. \end{aligned}$$

Therefore, we have

$$\begin{aligned} \mathrm{coker}(A) &\simeq R/\mathfrak{m}^{e_1} \oplus \cdots \oplus R/\mathfrak{m}^{e_n} \\ &\simeq R/\mathfrak{m}^{\lambda_1} \oplus \cdots \oplus R/\mathfrak{m}^{\lambda_l} \\ &\simeq H, \end{aligned}$$

as desired. □

Remark IV.13. The easiest case of Lemma IV.12 is when $N = 0$, which necessarily means $H = 0$. In this case, the lemma can be proven by a direct application of Nakayama's lemma. This special case is all we need for Theorem A and Theorem B, but the full version of Lemma IV.12 is needed for proving Theorem C. We will not directly use Lemma IV.12, but it will be used to prove the following lemma, which we will use to prove our theorems. It describes how we may concretely think of certain events according to the Haar measure on $\mathrm{Mat}_n(R)$.

Lemma IV.14. *Let $(R, \mathfrak{m})$ be a complete DVR with $R/\mathfrak{m} = \mathbb{F}_q$ and $H_1, \dots, H_r$ finite length R-modules, where $r \in \mathbb{Z}_{\geqslant 1}$. Choose any $N \in \mathbb{Z}_{\geqslant 0}$ such that $\mathfrak{m}^N H_1 = \cdots = \mathfrak{m}^N H_r = 0$. For any monic polynomials $f_1(t), \dots, f_r(t) \in R[t]$, we have*

$$\mathrm{Prob}_{A \in \mathrm{Mat}_n(R)} \left(\begin{array}{c} \mathrm{coker}(f_j(A)) \simeq H_j \\ \text{for } 1 \leqslant j \leqslant r \end{array} \right) = \mathrm{Prob}_{\overline{A} \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})} \left(\begin{array}{c} \mathrm{coker}(f_j(\overline{A})) \simeq H_j \\ \text{for } 1 \leqslant j \leqslant r \end{array} \right).$$

Proof. Consider the projection $\mathrm{Mat}_n(R) \twoheadrightarrow \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ given modulo $\mathfrak{m}^{N+1}$. Denoting this map by $A \mapsto \overline{A}$, the Haar measure on $\mathrm{Mat}_n(R)$ assigns $1/|\mathrm{Mat}_n(R/\mathfrak{m}^{N+1})|$ to the fiber $A + \mathfrak{m}^{N+1}\mathrm{Mat}_n(R)$ of any $\overline{A} \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$. Moreover, for any monic polynomial $f(t) \in R[t]$, a generator π of $\mathfrak{m}$, and any $B \in \mathrm{Mat}_n(R)$, we have $f(A + \pi^{N+1}B) = f(A) + \pi^{N+1}C$ for some $C \in \mathrm{Mat}_n(R)$. Thus, for any R-module H with $\mathfrak{m}^N H = 0$, we have $\mathrm{coker}(f(A)) \simeq H$ if and only if $\mathrm{coker}(f(A + \pi^{N+1}B)) \simeq H$ for all $B \in \mathrm{Mat}_n(R)$. Having this in mind, applying Lemma IV.12 lets us see that

$$\begin{aligned}
&\mathrm{Prob}_{A \in \mathrm{Mat}_n(R)} \left(\begin{array}{c} \mathrm{coker}(f_j(A)) \simeq H_j \\ \text{for } 1 \leqslant j \leqslant r \end{array} \right) \\
&= \sum_{\overline{A} \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})} \mu_n \left((A + \mathfrak{m}^{N+1}\mathrm{Mat}_n(R)) \cap \left\{ \begin{array}{c} M \in \mathrm{Mat}_n(R) : \\ \mathrm{coker}(f_j(M)) \simeq H_j \text{ for } 1 \leqslant j \leqslant r \end{array} \right\} \right) \\
&= \frac{1}{|\mathrm{Mat}_n(R/\mathfrak{m}^{N+1})|} \left| \left\{ \begin{array}{c} \overline{A} \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1}) : \\ \mathrm{coker}(f_j(\overline{A})) \simeq H_j \text{ for } 1 \leqslant j \leqslant r \end{array} \right\} \right| \\
&= \mathrm{Prob}_{\overline{A} \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})} \left(\begin{array}{c} \mathrm{coker}(f_j(\overline{A})) \simeq H_j \\ \text{for } 1 \leqslant j \leqslant r \end{array} \right),
\end{aligned}$$

where μ_n denotes the Haar (probability) measure on $\mathrm{Mat}_n(R)$. This finishes the proof. □

Lemma IV.15 (Friedman and Washington)**.** *Let $(R, \mathfrak{m})$ be a complete DVR with $R/\mathfrak{m} = \mathbb{F}_q$ and H a finite length R-module. Choose any $N \in \mathbb{Z}_{\geqslant 0}$ such that $\mathfrak{m}^N H = 0$. Fix any monic polynomial $P(t) \in R[t]$ of degree 1. For any $\overline{A} \in \mathrm{Mat}_n(\mathbb{F}_q)$, the number of lifts $A \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ of $\overline{A}$ such that $\mathrm{coker}(P(A)) \simeq H$ is equal to*

$$\begin{cases} q^{Nn^2+l_H^2}|\mathrm{Aut}_R(H)|^{-1}\prod_{i=1}^{l_H}(1-q^{-i})^2 & \text{if } \dim_{\mathbb{F}_q}(\mathrm{coker}(P(\overline{A}))) = l_H, \\ 0 & \text{if } \dim_{\mathbb{F}_q}(\mathrm{coker}(P(\overline{A}))) \neq l_H, \end{cases}$$

where $l_H := \dim_{\mathbb{F}_q}(H/\mathfrak{m}H)$.

We note that the reason that we require $\deg(P) = 1$ is because we want the map $\mathrm{Mat}_n(R/\mathfrak{m}^{N+1}) \to \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ given by $A \mapsto \bar{P}(A)$ bijective given in the proof of Lemma IV.15 (p.236 of [FW1987]), which we do not repeat in this thesis. This is also why we need the condition $\deg(P_r) = 1$ in Theorem C. We will use another lemma due to Cohen and Lenstra (Theorem 6.3 in [CL1983] with $u = 0$) as follows.

Lemma IV.16 (Cohen and Lenstra)**.** *Let $(R, \mathfrak{m})$ be a complete DVR with $R/\mathfrak{m} = \mathbb{F}_q$. For any $l \in \mathbb{Z}_{\geqslant 0}$, we have*

$$\operatorname*{Prob}_{H \in \boldsymbol{Mod}_R^{<\infty}}(\dim_{\mathbb{F}_q}(H/\mathfrak{m}H) = l) = \frac{q^{-l^2}\prod_{i=1}^{\infty}(1-q^{-i})}{\prod_{i=1}^{l}(1-q^{-i})^2}$$

with respect to the Cohen–Lenstra distribution on $\boldsymbol{Mod}_R^{<\infty}$.

We are now ready to prove Theorem C.

Proof of Theorem C. Let $l_H := \dim_{\mathbb{F}_q}(H/\mathfrak{m}H)$ and choose $N \in \mathbb{Z}_{\geqslant 0}$ such that $\mathfrak{m}^N H = 0$. We first note that

$$\dim_{\mathbb{F}_q}(\operatorname{coker}(P_r(\overline{A}))) = \dim_{\mathbb{F}_q}(\ker(P_r(\overline{A}))) = \dim_{\mathbb{F}_q}(\overline{A}[\overline{P}_r^{\infty}]/\overline{P}_r\overline{A}[\overline{P}_r^{\infty}]).$$

By Nakayama's lemma, we observe that the preimage of the set

$$\left\{\begin{matrix} \overline{A} \in \operatorname{Mat}_n(\mathbb{F}_q) : \\ \overline{A}[\overline{P}_j^{\infty}] = 0 \text{ for } 1 \leqslant j \leqslant r-1 \end{matrix}\right\} = \left\{\begin{matrix} \overline{A} \in \operatorname{Mat}_n(\mathbb{F}_q) : \\ \operatorname{coker}(P_j(\overline{A})) = 0 \text{ for } 1 \leqslant j \leqslant r-1 \end{matrix}\right\}$$

under the projection $\operatorname{Mat}_n(R/\mathfrak{m}^{N+1}) \twoheadrightarrow \operatorname{Mat}_n(\mathbb{F}_q)$ modulo $\mathfrak{m}$ is precisely

$$\left\{\begin{matrix} A \in \operatorname{Mat}_n(R/\mathfrak{m}^{N+1}) : \\ \operatorname{coker}(P_j(A)) = 0 \text{ for } 1 \leqslant j \leqslant r-1 \end{matrix}\right\}.$$

Applying Lemma IV.15 implies that

$$\begin{aligned} &\left|\left\{\begin{matrix} A \in \operatorname{Mat}_n(R/\mathfrak{m}^{N+1}) : \\ \operatorname{coker}(P_j(A)) = 0 \text{ for } 1 \leqslant j \leqslant r-1, \\ \operatorname{coker}(P_r(A)) \simeq H \end{matrix}\right\}\right| \\ &= \frac{q^{Nn^2+l_H^2}\prod_{i=1}^{l_H}(1-q^{-i})^2}{|\operatorname{Aut}_R(H)|}\left|\left\{\begin{matrix} \overline{A} \in \operatorname{Mat}_n(\mathbb{F}_q) : \\ \overline{A}[\overline{P}_j^{\infty}] = 0 \text{ for } 1 \leqslant j \leqslant r-1, \\ \dim_{\mathbb{F}_q}(\overline{A}[\overline{P}_r^{\infty}]/\overline{P}_r\overline{A}[\overline{P}_r^{\infty}]) = l_H \end{matrix}\right\}\right|, \end{aligned}$$

so dividing by $q^{(N+1)n^2} = |\operatorname{Mat}_n(R/\mathfrak{m}^{N+1})|$, we have

$$\begin{aligned} &\operatorname{Prob}_{A \in \operatorname{Mat}_n(R/\mathfrak{m}^{N+1})}\left(\begin{matrix} \operatorname{coker}(P_j(A)) = 0 \text{ for } 1 \leqslant j \leqslant r-1, \\ \operatorname{coker}(P_r(A)) \simeq H \end{matrix}\right) \\ &= \frac{q^{l_H^2}\prod_{i=1}^{l_H}(1-q^{-i})^2}{q^{n^2}|\operatorname{Aut}_R(H)|}\left|\left\{\begin{matrix} \overline{A} \in \operatorname{Mat}_n(\mathbb{F}_q) : \\ \overline{A}[\overline{P}_j^{\infty}] = 0 \text{ for } 1 \leqslant j \leqslant r-1, \\ \dim_{\mathbb{F}_q}(\overline{A}[\overline{P}_r^{\infty}]/\overline{P}_r\overline{A}[\overline{P}_r^{\infty}]) = l_H \end{matrix}\right\}\right| \\ &= \frac{q^{l_H^2}\prod_{i=1}^{l_H}(1-q^{-i})^2}{|\operatorname{Aut}_R(H)|}\operatorname{Prob}_{\overline{A} \in \operatorname{Mat}_n(\mathbb{F}_q)}\left(\begin{matrix} \overline{A}[\overline{P}_j^{\infty}] = 0 \text{ for } 1 \leqslant j \leqslant r-1, \\ \dim_{\mathbb{F}_q}(\overline{A}[\overline{P}_r^{\infty}]/\overline{P}_r\overline{A}[\overline{P}_r^{\infty}]) = l_H \end{matrix}\right). \end{aligned}$$

Hence, applying Theorem IV.1 and Lemma IV.16, this leads to

$$\begin{aligned}
&\lim_{n\to\infty} \mathrm{Prob}_{A\in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})}\begin{pmatrix} \mathrm{coker}(P_j(A)) = 0 \text{ for } 1 \leqslant j \leqslant r-1, \\ \mathrm{coker}(P_r(A)) \simeq H \end{pmatrix} \\
&= \frac{q^{l_H^2}\prod_{i=1}^{l_H}(1-q^{-i})^2}{|\mathrm{Aut}_R(H)|} \cdot \frac{q^{-l_H^2}\prod_{i=1}^{\infty}(1-q^{-i})}{\prod_{i=1}^{l_H}(1-q^{-i})^2} \cdot \prod_{j=1}^{r-1}\prod_{i=1}^{\infty}(1-q^{-i\deg(P_j)}) \\
&= \frac{1}{|\mathrm{Aut}_R(H)|}\prod_{j=1}^{r}\prod_{i=1}^{\infty}(1-q^{-i\deg(P_j)}),
\end{aligned}$$

noting that $\deg(P_r) = 1$. This finishes the proof. □

CHAPTER V

Distributions of Torsion Sheaves on Curves over Finite Fields

The contents of this chapter come from a joint work in progress with Haoyang Guo and Yifeng Huang. One of the main goals of this chapter is to provide a proof of Theorem I.9, which will be restated as Theorem V.1.

5.1 Motivation and results

In the beginning of Chapter IV, we saw how the proportion of the $n \times n$ matrices over $\mathbb{F}_q$ with finitely many specified local conditions converges to the corresponding probability given by a Cohen–Lenstra distribution when $n \to \infty$. To understand this, we needed an easy but important observation that a matrix $A \in \mathrm{Mat}_n(\mathbb{F}_q)$ can be seen as an $\mathbb{F}_q[t]$-module with $\mathbb{F}_q$-dimension n.

Now, it is natural to ask, by considering the proportion of the $\mathbb{F}_q$-matrices as the proportion of $\mathbb{F}_q[t]$-modules, whether we can generalize our observation to R-modules for a more general (commutative Noetherian) ring R, other than $\mathbb{F}_q[t]$. In algebraic geometry, finitely generated R-modules correspond to coherent sheaves over

$\mathscr{O}_{\mathrm{Spec}(R)}$ (also known as $\mathscr{O}_{\mathrm{Spec}(R)}$-modules). Hence, it is also natural to ask whether we can generalize our discussion to prove that the proportion of coherent sheaves on a scheme with finitely specified local conditions gives rise to a Cohen–Lenstra distribution, when a certain invariant tends to infinity. We will require some nice conditions on the scheme to make our plan work.

To figure out a valid generalization, first, we reconsider what the probability

$$\underset{A\in\mathrm{Mat}_n(\mathbb{F}_q)}{\mathrm{Prob}}(A \text{ satsifies } \mathscr{P})$$

means, where $\mathscr{P}$ is a property of matrices that is constant on any orbit $|[A]|$ of the conjugation action $\mathrm{GL}_n(\mathbb{F}_q) \circlearrowright \mathrm{Mat}_n(\mathbb{F}_q)$. We have

$$\begin{aligned}
\underset{A\in\mathrm{Mat}_n(\mathbb{F}_q)}{\mathrm{Prob}}(A \text{ satsifies } \mathscr{P}) &= \frac{|\{A \in \mathrm{Mat}_n(\mathbb{F}_q) : A \text{ satsifies } \mathscr{P}\}|}{|\mathrm{Mat}_n(\mathbb{F}_q)|} \\
&= \frac{\displaystyle\sum_{\substack{[A]\in\mathrm{Mat}_n(\mathbb{F}_q)/\mathrm{GL}_n(\mathbb{F}_q),\\ A \text{ satsifies } \mathscr{P}}} |[A]|}{\displaystyle\sum_{[A]\in\mathrm{Mat}_n(\mathbb{F}_q)/\mathrm{GL}_n(\mathbb{F}_q)} |[A]|} \\
&= \frac{\displaystyle\sum_{\substack{[A]\in\mathrm{Mat}_n(\mathbb{F}_q)/\mathrm{GL}_n(\mathbb{F}_q),\\ A \text{ satsifies } \mathscr{P}}} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(A)|}}{\displaystyle\sum_{[A]\in\mathrm{Mat}_n(\mathbb{F}_q)/\mathrm{GL}_n(\mathbb{F}_q)} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(A)|}} \\
&= \frac{\displaystyle\sum_{\substack{[A]\in\mathrm{Mat}_n(\mathbb{F}_q)/\mathrm{GL}_n(\mathbb{F}_q),\\ A \text{ satsifies } \mathscr{P}}} \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(A)|}}{\displaystyle\sum_{[A]\in\mathrm{Mat}_n(\mathbb{F}_q)/\mathrm{GL}_n(\mathbb{F}_q)} \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(A)|}}.
\end{aligned}$$

Using the natural bijection from $\mathrm{Mat}_n(\mathbb{F}_q)/\mathrm{GL}_n(\mathbb{F}_q)$ to the set $\mathbf{Mod}_{\mathbb{F}_q[t]}^{=q^n}$ of isomorphism classes of $\mathbb{F}_q[t]$-modules with size q^n, we have

$$\operatorname*{Prob}_{A \in \mathrm{Mat}_n(\mathbb{F}_q)}(A \text{ satsifies } \mathscr{P}) = \frac{\displaystyle\sum_{\substack{[A] \in \mathbf{Mod}_{\mathbb{F}_q[t]}^{=q^n}, \\ A \text{ satsifies } \mathscr{P}}} \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(A)|}}{\displaystyle\sum_{[A] \in \mathbf{Mod}_{\mathbb{F}_q[t]}^{=q^n}} \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(A)|}}.$$

We note that the right-hand side is more intrinsic than the left-hand side. That is, we do not need to use matrices to consider the $\mathbb{F}_q[t]$-modules. More generally, given any category $\mathcal{C}$ whose objects have finite automorphism groups, for any nonempty finite set S consisting of some isomorphism classes of objects of $\mathcal{C}$, we define

$$\operatorname*{Prob}_{[A] \in S}(A \text{ satsifies } \mathscr{P}) := \frac{\displaystyle\sum_{\substack{[A] \in S, \\ A \text{ satsifies } \mathscr{P}}} \frac{1}{|\mathrm{Aut}_{\mathcal{C}}(A)|}}{\displaystyle\sum_{[A] \in S} \frac{1}{|\mathrm{Aut}_{\mathcal{C}}(A)|}},$$

where $\mathscr{P}$ is a property of objects in $\mathcal{C}$ that is constant on its isomorphism classes. Hence, the above discussion gives

$$\operatorname*{Prob}_{A \in \mathrm{Mat}_n(\mathbb{F}_q)}(A \text{ satsifies } \mathscr{P}) = \operatorname*{Prob}_{A \in \mathbf{Mod}_{\mathbb{F}_q[t]}^{=q^n}}(A \text{ satsifies } \mathscr{P}).$$

What we have shown in Theorem IV.1 can be rephrased as:

$$\lim_{n \to \infty} \operatorname*{Prob}_{A \in \mathbf{Mod}_{\mathbb{F}_q[t]}^{=q^n}} \left(\begin{array}{c} A[P_j^\infty] \simeq H_j \\ \text{for } 1 \leqslant j \leqslant r \end{array} \right) = \prod_{j=1}^{r} \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_j)|} \prod_{i=1}^{\infty} (1 - q^{-i \deg(P_j)}),$$

where $P_1(t), \dots, P_r(t) \in \mathbb{F}_q[t]$ are distinct monic irreducible polynomials with P_j^∞-torsion $\mathbb{F}_q[t]$-module H_j of finite length for $1 \leqslant j \leqslant r$. The generalization of Theorem IV.1 is as follows, which we stated as Theorem I.9 in the introduction:

Theorem V.1. *Let X be a smooth, projective, and geometrically irreducible curve over $\mathbb{F}_q$ minus finitely many closed points. Given any distinct closed points $p_1, \dots, p_r$*

of X, let H_j be a finite length module over $\mathscr{O}_{X,p_j}$ for $1 \leqslant j \leqslant r$. Then

$$\lim_{n\to\infty} \operatorname*{Prob}_{[\mathcal{F}]\in \boldsymbol{Mod}_{\mathscr{O}_X}^{=q^n}} \left(\begin{array}{c} \mathcal{F}_{p_j} \simeq H_j \\ \\ \textit{for } 1 \leqslant j \leqslant r \end{array} \right) = \prod_{j=1}^{r} \frac{1}{|\mathrm{Aut}_{\mathscr{O}_{X,p_j}}(H_j)|} \prod_{i=1}^{\infty} (1 - q^{-i\deg(p_j)}),$$

where $\boldsymbol{Mod}_{\mathscr{O}_X}^{=q^n}$ is the set of isomorphism classes of torsion coherent $\mathscr{O}_X$-modules $\mathcal{F}$ with $\sum_{p\in|X|} \dim_{\mathbb{F}_q}(\mathcal{F}_p) = n$, denoting by $|X|$ to mean the set of closed points of X.

5.2 Classification of finite length modules

Let R be a finitely generated $\mathbb{F}_q$-algebra, and suppose that R is also a Dedekind domain. We first classify finite length modules over R. (This should be well-known, but we could not find a reasonable source.) Let M be any R-module of finite length. Then $n = \dim_{\mathbb{F}_q}(M)$ is finite, and thus $|M| = q^n$ is finite as well. Without loss of generality, let $M \neq 0$. This implies that the annihilator ideal J of M in R is not the unit ideal. We also note that $J \neq 0$. To see this, suppose otherwise that $J = 0$. We are assuming M has q^n elements, so write $M = \{m_1, \dots, m_{q^n}\}$. Since $J = 0$ and R is a domain, this implies that there exists at least one m_i whose annihilator is 0. Since R has infinitely many elements under our hypothesis, we can take infinitely many distinct elements $a_1, a_2, a_3, \dots$ to construct infinitely many distinct elements $a_1m_i, a_2m_i, a_3m_i, \dots$ in M. We can do this since for any $a_j \neq a_k$, we have $(a_j - a_k)m_i \neq 0$. However, this contradicts the fact that M is of finite size. Thus, we conclude that $J \neq 0$. Since R is a Dedekind domain, we have a unique decomposition for J:

$$J = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

where $\mathfrak{p}_i$ are distinct maximal ideals of R and $e_i \geqslant 1$ with $r \geqslant 1$. We note that M is also a module over the ring

$$R/J \simeq R/\mathfrak{p}_1^{e_1} \times \cdots \times R/\mathfrak{p}_r^{e_r}.$$

Thus, for any maximal ideal $\mathfrak{m} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, the localization $M_{\mathfrak{m}}$ is a module defined over $(R/J)_{\mathfrak{m}} = 0$, so we have $M_{\mathfrak{m}} = 0$. On the other hand $M_{\mathfrak{p}_i}$ is a module defined over $(R/J)_{\mathfrak{p}_i} \simeq R/\mathfrak{p}_i^{e_i}$ so that

$$M_{\mathfrak{p}_i} \simeq R/\mathfrak{p}_i^{\lambda_{i,1}} \oplus \cdots \oplus R/\mathfrak{p}_i^{\lambda_{i,l_i}}.$$

Thus, we have

$$M \simeq M_{\mathfrak{p}_1} \oplus \cdots \oplus M_{\mathfrak{p}_r} \simeq \bigoplus_{i=1}^{r} (R/\mathfrak{p}_i^{\lambda_{i,1}} \oplus \cdots \oplus R/\mathfrak{p}_i^{\lambda_{i,l_i}}).$$

Hence, we get a complete classification of R-modules of finite length (or finite $\mathbb{F}_q$-dimension). For convenience, given a maximal ideal $\mathfrak{p}$ and a partition $\lambda = (\lambda_1, \ldots, \lambda_l)$, we write

$$H_{\mathfrak{p},\lambda} := R/\mathfrak{p}^{\lambda_1} \oplus \cdots \oplus R/\mathfrak{p}^{\lambda_l},$$

and what we proved is that any R-module of finite length is of the form

$$H_{\mathfrak{p}_1,\lambda^{(1)}} \oplus \cdots \oplus H_{\mathfrak{p}_r,\lambda^{(r)}}$$

for some maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of R and some partitions $\lambda^{(1)}, \ldots, \lambda^{(r)}$.

Remark V.2. Note that given any finite length R-module, the above discussion also implies that we have

- $\mathrm{Supp}_R(M) = \{\mathfrak{p} \in \mathrm{Spec}(R) : M_{\mathfrak{p}} \neq 0\} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ and
- $M \simeq M_{\mathfrak{p}_1} \oplus \cdots \oplus M_{\mathfrak{p}_r}$ given by $m \mapsto (m/1, \ldots, m/1)$.

5.3 Cycle indices to count torsion coherent sheaves

Let X be as in Theorem V.1, namely a smooth, projective, and geometrically irreducible curve over $\mathbb{F}_q$ minus finitely many closed points. Let $\mathcal{F}$ be any torsion coherent $\mathscr{O}_X$-module. Due to the discussion from the previous section, we know that the support of $\mathcal{F}$ c sists of finitely many points, say $p_1, \dots, p_r \in X$, and these points are closed points because X is an integral curve. Given any closed point p of X and a nonempty partition λ, we consider a formal variable $x_{p,\lambda}$. We define $x_{p,\varnothing} := 1$. For any isomorphism class $[\mathcal{F}]$ of a torsion cohrent sheaf $\mathcal{F}$ on X, we consider its support $\{p_1, \dots, p_r\}$ and recall that we have $\mathcal{F}_{p_i} \simeq H_{p_i,\lambda^{(i)}}$ for some partition $\lambda^{(i)}$. We define $x_{[\mathcal{F}]} := x_{p_1,\lambda^{(1)}} \cdots x_{p_r,\lambda^{(r)}}$. We define the n-th **cycle index** of X to be

$$\mathcal{Z}(X, n, \boldsymbol{x}) := \sum_{[\mathcal{F}] \in \mathbf{Mod}_X^{=q^n}} \frac{x_{[\mathcal{F}]}}{|\mathrm{Aut}_{\mathscr{O}_X}(\mathcal{F})|}.$$

By the orbit-stabilizer theorem, we observe that this generalizes the cycle index $\mathcal{Z}_{[\mathrm{Mat}_n/\mathrm{GL}_n](\mathbb{F}_q)}(\boldsymbol{x})$ of the conjugation action $\mathrm{GL}_n(\mathbb{F}_q) \circlearrowright \mathrm{Mat}_n(\mathbb{F}_q)$ as follows:

$$\mathcal{Z}(\mathbb{A}^1_{\mathbb{F}_q}, n, \boldsymbol{x}) = \mathcal{Z}_{[\mathrm{Mat}_n/\mathrm{GL}_n](\mathbb{F}_q)}(\boldsymbol{x}).$$

To prove Theorem V.1, we need an analogue for Corollary II.13. For this, we need the following lemma:

Lemma V.3. *Keeping the notation above, we have a group isomorphism*

$$\mathrm{Aut}_{\mathscr{O}_X}(\mathcal{F}) \simeq \mathrm{Aut}_{\mathscr{O}_{X,p_1}}(\mathcal{F}_{p_1}) \times \cdots \times \mathrm{Aut}_{\mathscr{O}_{X,p_r}}(\mathcal{F}_{p_r})$$

given by the localizations: $\phi \mapsto (\phi_{p_1}, \dots, \phi_{p_r})$.

Moreover, given any torsion coherent $\mathscr{O}_{X,p_i}$*-module* M_i *for* $1 \leqslant i \leqslant r$*, we have a torsion coherent* $\mathscr{O}_X$*-module* $\mathcal{G}$ *such that* $\mathcal{G}_{x_i} = M_i$ *for* $1 \leqslant i \leqslant r$ *and* $\mathcal{G}_y = 0$ *for any* $y \notin \{x_1, \dots, x_r\}$.

Proof. Given $\phi, \psi \in \operatorname{Aut}_{\mathscr{O}_X}(\mathcal{F})$, if $\phi_{p_i} = \psi_{p_i}$ for $1 \leqslant i \leqslant r$, then $\phi_x = \psi_x$ for all $x \in X$, since $\{x_1, \dots, x_r\}$ is the support of $\mathcal{F}$. This implies that $\phi = \psi$, so the map is injective.

To show surjectivity, we will use more specific assumptions about the scheme X. Fix $\phi_i \in \operatorname{Aut}_{\mathscr{O}_{X,p_i}}(\mathcal{F}_{x_i})$ for $1 \leqslant i \leqslant r$. Since X is quasi-compact, we may cover it with finitely many nonempty affine opens $U_1, \dots, U_l$. Say among $p_1, \dots, p_r$, we have $p_{i_{j,1}}, \dots, p_{i_{j,r_j}} \in U_j$. From the previous section, we know that

$$\mathcal{F}(U_j) \simeq \mathcal{F}_{p_{i_{j,1}}} \times \cdots \times \mathcal{F}_{p_{i_{j,r_j}}}$$

given by the localizations, and we know each $U_i \cap U_j$ is affine because X is separated, so these isomorphisms are compatible with taking intersections among $U_1, \dots, U_l$. Now, if we denote by ϕ_{U_j} the $\mathscr{O}_X(U_j)$-linear automorphism of $\mathcal{F}(U_j)$ corresponding to $\phi_{i_{j,1}} \times \cdots \times \phi_{i_{j,r_j}}$. In particular, we have $(\phi_{U_j})_{p_{i_{j,k}}} = \phi_{i_{j,k}}$, so the maps ϕ_{U_j} are compatible with taking intersections among $U_1, \dots, U_l$. Hence, we may glue them to get an $\mathscr{O}_X$-linear map $\phi : \mathcal{F} \to \mathcal{F}$. By checking the localizations at $p_1, \dots, p_r$, we see ϕ is an automorphism, which shows the surjectivity of $\operatorname{Aut}_{\mathscr{O}_X}(\mathcal{F}) \to \prod_{i=1}^{r} \operatorname{Aut}_{\mathscr{O}_{X,p_i}}(\mathcal{F}_{p_i})$.

It remains to show that we can glue any given torsion coherent modules M_i defined over $\mathscr{O}_{X,p_i}$ for $1 \leqslant i \leqslant r$ to an $\mathscr{O}_X$-module. We use the same $U_1, \dots, U_l$ given above. Define

$$\mathcal{G}(U_j) := M_{i_{j,1}} \times \cdots \times M_{i_{j,r_j}},$$

which is an $\mathscr{O}_X(U_j)$-module. Since any finite intersections among $U_1, \dots, U_l$ are affine, we may analogously define $\mathcal{G}(U_{i_1} \cap \cdots \cap U_{i_k})$ and get restriction maps among them. Hence, we may glue these modules to construct an $\mathscr{O}_X$-module $\mathcal{G}$ on X. □

We now provide an analogue of Theorem II.13. We omit its proof as it is a direct corollary of Lemma V.3.

Lemma V.4. *Let X be as in Theorem V.1. Then*

$$\begin{aligned}\sum_{n=0}^{\infty} \mathscr{Z}(X, n, \boldsymbol{x}) u^n &= \sum_{n=0}^{\infty} \sum_{[\mathcal{F}] \in \boldsymbol{Mod}_X^{=q^n}} \frac{x_{[\mathcal{F}]}}{|\mathrm{Aut}_{\mathscr{O}_X}(\mathcal{F})|} u^n \\ &= \prod_{p \in |X|} \sum_{\nu \in \mathcal{P}} \frac{x_{p,\nu} u^{|\nu| \deg(p)}}{|\mathrm{Aut}_{\mathscr{O}_{X,p}}(\mathcal{F}_p)|},\end{aligned}$$

where $|X|$ is the set of closed points of X.

5.4 Proof of Theorem I.9 (Theorem V.1)

In this section, we use the cycle indices for X introduced in the previous section to prove Theorem V.1. For this, we will also need a generalization of Lemma IV.3:

Lemma V.5. *Let $(R, \mathfrak{p})$ be any DVR with the finite residue field $R/\mathfrak{p} = \mathbb{F}_q$. Then*

$$\sum_{\nu \in \mathcal{P}} \frac{y^{|\nu|}}{|\mathrm{Aut}_R(H_{\mathfrak{p},\nu})|} = \prod_{i=1}^{\infty} \frac{1}{1 - q^{-i \deg(\mathfrak{p})} y} \in \mathbb{Q}[\![y]\!].$$

Proof. By an application of Lemma IV.2, we have

$$|\mathrm{Aut}_R(H_{\mathfrak{p},\nu})| = |\mathrm{Aut}_{\mathbb{F}_{q^{\deg(\mathfrak{p})}}[\![t]\!]}(H_{(t),\nu})|,$$

so we are done by applying Lemma IV.3. □

Given X as in Theorem V.1, we may write $X = C \smallsetminus \{x_1, \dots, x_m\}$, where C is a smooth, projective, and geometrically irreducible curve over $\mathbb{F}_q$ and $x_1, \dots, x_m$ are finitely many closed points of X. (We allow the case $m = 0$.) By the rationality of zeta series $\boldsymbol{Z}_C(u)$ of C, we may write

$$\boldsymbol{Z}_C(u) = \frac{f_C(u)}{(1-u)(1-qu)},$$

where $f_C(u) \in \mathbb{Z}[u]$ is of degree $2g$, denoting by g the genus of C (e.g., see [Ras, Theorem 2.7]). This implies that we have

$$\boldsymbol{Z}_X(u) = (1-u^{d_1})\cdots(1-u^{d_m})\boldsymbol{Z}_C(u) = \frac{(1-u^{d_1})\cdots(1-u^{d_m})f_C(u)}{(1-u)(1-qu)},$$

where $d_i = \deg(x_i)$. We will use this form of $\boldsymbol{Z}_X(u)$ in our proofs.

Lemma V.6. *Keeping the notation as above, we have*

$$\lim_{n\to\infty} \sum_{[\mathcal{F}]\in \boldsymbol{Mod}_X^{=q^n}} \frac{1}{|\mathrm{Aut}_{\mathscr{O}_X}(\mathcal{F})|} = \frac{(1-q^{-d_1})\cdots(1-q^{-d_m})f_C(q^{-1})}{1-q^{-1}} \prod_{i=2}^{\infty} \zeta_X(i),$$

where $\zeta_X(s) = \boldsymbol{Z}_X(q^{-s})$ is the zeta function of X. In particular, this quantity is nonzero.

Proof. Taking $x_{p,\nu} = 1$ for all p, ν in Lemma V.4 and applying Lemma V.5, we have

$$\begin{aligned}
\sum_{n=0}^{\infty} \sum_{[\mathcal{F}]\in \mathbf{Mod}_X^{=q^n}} \frac{1}{|\mathrm{Aut}_{\mathscr{O}_X}(\mathcal{F})|}u^n &= \prod_{p\in|X|}\sum_{\nu\in\mathcal{P}} \frac{u^{|\nu|\deg(p)}}{|\mathrm{Aut}_{\mathscr{O}_{X,p}}(\mathcal{F}_p)|} \\
&= \prod_{p\in|X|}\prod_{i=1}^{\infty} \frac{1}{1-(q^{-i}u)^{\deg(p)}} \\
&= \prod_{i=1}^{\infty}\prod_{p\in|X|} \frac{1}{1-(q^{-i}u)^{\deg(p)}} \\
&= \frac{(1-(q^{-1}u)^{d_1})\cdots(1-(q^{-1}u)^{d_m})f_C(q^{-1}u)}{(1-q^{-1}u)(1-u)} \prod_{i=2}^{\infty} \boldsymbol{Z}_X(q^{-i}u),
\end{aligned}$$

so

$$\begin{aligned}
\lim_{n\to\infty} \sum_{[\mathcal{F}]\in \mathbf{Mod}_X^{=q^n}} \frac{1}{|\mathrm{Aut}_{\mathscr{O}_X}(\mathcal{F})|} &= \frac{(1-q^{-d_1})\cdots(1-q^{-d_m})f_C(q^{-1})}{1-q^{-1}} \prod_{i=2}^{\infty} \boldsymbol{Z}_X(q^{-i}) \\
&= \frac{(1-q^{-d_1})\cdots(1-q^{-d_m})f_C(q^{-1})}{1-q^{-1}} \prod_{i=2}^{\infty} \zeta_X(i),
\end{aligned}$$

as desired. The fact that this quantity is nonzero follows from the fact that every root of $f_C(u)$ are of the size $q^{-k/2}$ for some integer k. □

We now give a proof of Theorem V.1.

Proof. Let l be the number of nonzero modules among $H_1, \dots, H_r$. We may assume that $H_j = H_{p_j,\lambda^{(j)}}$ for some partitions $\lambda^{(1)}, \dots, \lambda^{(r)}$ so that l is also the number of nonempty partitions among them. We argue by induction on l. First, consider the case where $l = 0$. Given any coherent torsion $\mathscr{O}_X$-module $\mathcal{F}$ and a closed point p of X, we write $\mu_p(\mathcal{F})$ to mean the partition associated to the $\mathscr{O}_{X,p}$-module $\mathcal{F}_p$. In particular, we have $\mu_p(\mathcal{F}) = \varnothing$ if and only if $\mathcal{F}_p = 0$.

Taking $x_{p,\nu} = 1$ for any $p \notin \{p_1, \dots, p_r\}$ and $x_{p_j,\nu} = 0$ for all $1 \leqslant j \leqslant n$ and nonempty ν in Lemma V.4 and applying Lemma V.5 we get

$$\begin{aligned}
&\sum_{n=0}^{\infty} \sum_{\substack{[\mathcal{F}] \in \mathbf{Mod}_X^{=q^n}, \\ \mu_{p_1}(\mathcal{F}) = \cdots = \mu_{p_l}(\mathcal{F}) = \varnothing}} \frac{1}{|\mathrm{Aut}_{\mathscr{O}_X}(\mathcal{F})|} u^n \\
&\quad = \left(\prod_{p \in |X|} \sum_{\nu \in \mathcal{P}} \frac{u^{|\nu| \deg(p)}}{|\mathrm{Aut}_{\mathscr{O}_{X,p}}(\mathcal{F}_p)|} \right) \left(\prod_{j=1}^{r} \sum_{\nu \in \mathcal{P}} \frac{u^{|\nu| \deg(p_j)}}{|\mathrm{Aut}_{\mathscr{O}_{X,p_j}}(\mathcal{F}_{p_j})|} \right)^{-1} \\
&\quad = \left(\prod_{j=1}^{r} \prod_{i=1}^{\infty} (1 - (q^{-i}u)^{\deg(p_j)}) \right) \left(\prod_{p \in |X|} \prod_{i=1}^{\infty} \frac{1}{1 - (q^{-i}u)^{\deg(p)}} \right) \\
&\quad = \left(\prod_{j=1}^{r} \prod_{i=1}^{\infty} (1 - (q^{-i}u)^{\deg(p_j)}) \right) \left(\prod_{i=1}^{\infty} \prod_{p \in |X|} \frac{1}{1 - (q^{-i}u)^{\deg(p)}} \right) \\
&\quad = \left(\prod_{j=1}^{r} \prod_{i=1}^{\infty} (1 - (q^{-i}u)^{\deg(p_j)}) \right) \left(\prod_{i=1}^{\infty} \boldsymbol{Z}_X(q^{-i}u) \right) \\
&\quad = \left(\prod_{j=1}^{r} \prod_{i=1}^{\infty} (1 - (q^{-i}u)^{\deg(p_j)}) \right) \frac{(1 - (q^{-1}u)^{d_1}) \cdots (1 - (q^{-1}u)^{d_m}) f_C(q^{-1}u)}{(1 - q^{-1}u)(1 - u)} \prod_{i=2}^{\infty} \boldsymbol{Z}_X(q^{-i}u).
\end{aligned}$$

Hence, we have

$$\lim_{n\to\infty} \operatorname*{Prob}_{[\mathcal{F}]\in\mathbf{Mod}_X^{=q^n}} \left(\begin{array}{c} \mu_{p_j}(\mathcal{F}) = \varnothing \\ \text{for } 1 \leqslant j \leqslant r \end{array} \right) \sum_{[\mathcal{F}]\in\mathbf{Mod}_X^{=q^n}} \frac{1}{|\mathrm{Aut}_{\mathscr{O}_X}(\mathcal{F})|}$$

$$= \left(\prod_{j=1}^{r} \prod_{i=1}^{\infty} (1 - q^{-i\deg(p_j)}) \right) \frac{(1-q^{-d_1})\cdots(1-q^{-d_m}) f_C(q^{-1})}{1-q^{-1}} \prod_{i=2}^{\infty} \boldsymbol{Z}_X(q^{-i}),$$

so applying Lemma V.6, we have

$$\lim_{n\to\infty} \operatorname*{Prob}_{[\mathcal{F}]\in\mathbf{Mod}_X^{=q^n}} \left(\begin{array}{c} \mu_{p_j}(\mathcal{F}) = \varnothing \\ \text{for } 1 \leqslant j \leqslant r \end{array} \right) = \prod_{j=1}^{r} \prod_{i=1}^{\infty} (1 - q^{-i\deg(p_j)}).$$

For induction hypothesis, suppose that we know the result for $l = 0, 1, \ldots, k-1$, and consider the case where $l = k$. We may assume that $\lambda^{(1)}, \ldots, \lambda^{(k)}$ are nonempty, while $\lambda^{(k+1)} = \cdots = \lambda^{(r)} = \varnothing$. We take

- $x_{p,\nu} = 1$ for any $p \notin \{p_1, \ldots, p_r\}$,
- $x_{p_j,\nu} = 0$ for all $1 \leqslant j \leqslant k$ and $\nu \neq \varnothing, \lambda^{(j)}$, and
- $x_{p_j,\lambda^{(j)}} = 1$ for all $1 \leqslant j \leqslant k$ and $\nu \neq \lambda^{(j)}$

to get

$$\sum_{n=0}^{\infty} \sum_{\substack{[\mathcal{F}]\in\mathbf{Mod}_X^{=q^n}, \\ \mu_{p_j}(\mathcal{F})\in\{\varnothing,\lambda^{(j)}\} \text{ for } 1\leqslant j\leqslant k, \\ \mu_{p_{k+1}}(\mathcal{F})=\cdots=\mu_{p_r}(\mathcal{F})=\varnothing}} \frac{1}{|\mathrm{Aut}_{\mathscr{O}_X}(\mathcal{F})|} u^n$$

$$= \left(\prod_{j=1}^{r} \left(1 + \frac{u^{|\lambda^{(j)}|\deg(p_j)}}{|\mathrm{Aut}_{\mathscr{O}_{X,p_j}}(H_{p_j,\nu})|} \right) \right) \left(\prod_{p\in|X|} \sum_{\nu\in\mathcal{P}} \frac{u^{|\nu|\deg(p)}}{|\mathrm{Aut}_{\mathscr{O}_{X,p}}(\mathcal{F}_p)|} \right) \left(\prod_{j=1}^{r} \sum_{\nu\in\mathcal{P}} \frac{u^{|\nu|\deg(p_j)}}{|\mathrm{Aut}_{\mathscr{O}_{X,p_j}}(\mathcal{F}_{p_j})|} \right)^{-1}$$

$$= \left(\prod_{j=1}^{r} \left(1 + \frac{u^{|\lambda^{(j)}|\deg(p_j)}}{|\mathrm{Aut}_{\mathscr{O}_{X,p_j}}(H_{p_j,\nu})|} \right) \prod_{i=1}^{\infty} (1 - (q^{-i}u)^{\deg(p_j)}) \right) \left(\prod_{p\in|X|} \prod_{i=1}^{\infty} \frac{1}{1-(q^{-i}u)^{\deg(p)}} \right)$$

$$\begin{aligned}
&= \left(\prod_{j=1}^{r}\left(1+\frac{u^{|\lambda^{(j)}|\deg(p_j)}}{|\mathrm{Aut}_{\mathscr{O}_{X,p_j}}(H_{p_j,\nu})|}\right)\prod_{i=1}^{\infty}(1-(q^{-i}u)^{\deg(p_j)})\right)\left(\prod_{i=1}^{\infty}\prod_{p\in|X|}\frac{1}{1-(q^{-i}u)^{\deg(p)}}\right)\\
&= \left(\prod_{j=1}^{r}\left(1+\frac{u^{|\lambda^{(j)}|\deg(p_j)}}{|\mathrm{Aut}_{\mathscr{O}_{X,p_j}}(H_{p_j,\nu})|}\right)\prod_{i=1}^{\infty}(1-(q^{-i}u)^{\deg(p_j)})\right)\left(\prod_{i=1}^{\infty}\boldsymbol{Z}_X(q^{-i}u)\right)\\
&= \left(\prod_{j=1}^{r}\left(1+\frac{u^{|\lambda^{(j)}|\deg(p_j)}}{|\mathrm{Aut}_{\mathscr{O}_{X,p_j}}(H_{p_j,\nu})|}\right)\prod_{i=1}^{\infty}(1-(q^{-i}u)^{\deg(p_j)})\right)\\
&\qquad\qquad \cdot \frac{(1-(q^{-1}u)^{d_1})\cdots(1-(q^{-1}u)^{d_m})f_C(q^{-1}u)}{(1-q^{-1}u)(1-u)}\prod_{i=2}^{\infty}\boldsymbol{Z}_X(q^{-i}u).
\end{aligned}$$

This implies that

$$\begin{aligned}
&\lim_{n\to\infty}\operatorname*{Prob}_{[\mathcal{F}]\in\mathbf{Mod}_X^{=q^n}}\begin{pmatrix}\mu_{p_j}(\mathcal{F})\in\{\varnothing,\lambda^{(j)}\}\text{ for }1\leqslant j\leqslant m,\\ \mu_{p_{m+1}}(\mathcal{F})=\cdots=\mu_{p_r}(\mathcal{F})=\varnothing\end{pmatrix}\sum_{[\mathcal{F}]\in\mathbf{Mod}_X^{=q^n}}\frac{1}{|\mathrm{Aut}_{\mathscr{O}_X}(\mathcal{F})|}\\
&= \left(\prod_{j=1}^{r}\left(1+\frac{1}{|\mathrm{Aut}_{\mathscr{O}_{X,p_j}}(H_{p_j,\nu})|}\right)\prod_{i=1}^{\infty}(1-q^{-i\deg(p_j)})\right)\\
&\qquad\qquad \cdot \frac{(1-q^{-d_1})\cdots(1-q^{-d_m})f_C(q^{-1})}{1-q^{-1}}\prod_{i=2}^{\infty}\boldsymbol{Z}_X(q^{-i}).
\end{aligned}$$

Hence, applying Lemma V.6, we have

$$\begin{aligned}
&\lim_{n\to\infty}\operatorname*{Prob}_{[\mathcal{F}]\in\mathbf{Mod}_X^{=q^n}}\begin{pmatrix}\mu_{p_j}(\mathcal{F})\in\{\varnothing,\lambda^{(j)}\}\text{ for }1\leqslant j\leqslant m,\\ \mu_{p_{m+1}}(\mathcal{F})=\cdots=\mu_{p_r}(\mathcal{F})=\varnothing\end{pmatrix}\\
&= \prod_{j=1}^{r}\left(1+\frac{1}{|\mathrm{Aut}_{\mathscr{O}_{X,p_j}}(H_{p_j,\nu})|}\right)\prod_{i=1}^{\infty}(1-q^{-i\deg(p_j)}).
\end{aligned}$$

By applying induction just as in the proof of Theorem IV.1, we are done. □

Bibliography

[Bor2016] I. Boreico, *Statistics of random integral matrices*, Ph.D. thesis, Stanford University (2016).

[CKS2018] J. Chan, S. Kwon, and M. Seaman, *On the distribution of discriminants over a finite field*, available at https://arxiv.org/abs/1812.06231

[Che1994] J. Cheah, *The cohomology of smooth nested Hilbert schemes of points*, Ph.D. thesis, the University of Chicago, (1994).

[Che2020] G. Cheong, *Pólya enumeration theorems in algebraic geometry*, available at https://arxiv.org/abs/2003.04825

[CNY20] G. Cheong, H. Nam, and M. Yu, *Large q convergence of random characteristic polynomials to random permutations and its applications*, available at https://arxiv.org/abs/2005.07846

[CH2018] G. Cheong and Y. Huang, *Cohen–Lenstra distributions via random matrices over complete discrete valuation rings with finite fields*, available at https://arxiv.org/abs/1812.11728

[CL1983] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Proceedings of the Journees Arithmetiques held at Noordwijkerhout, the

Netherlands, July 11–15, 1983, Lecture Notes in Mathematics **1068** (1983), Springer-Verlag, New York, 33–62.

[Del1971] P. Deligne, *Théorie de Hodge II*, Publications Mathématiques de l'I.H.E.S, **40** (1971), 5–58.

[Dwo1960] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, American Journal of Mathematics, **82** (1960), 631–648.

[EVW2016] J. S. Ellenberg, A. Venkatesh, and C. Westerland, *Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields*, Annals of Mathematics **183** (2016), 729–786.

[FH1958] N. J. Fine and I. N. Herstein, *The probability that a matrix be nilpotent*, Illinois Journal of Mathematics **2** (1958), 499–504.

[FW1987] E. Friedman and L. C. Washington, *On the distribution of divisor class groups of curves over a finite field*, Théorie des Nombres (Quebec, PQ, 1987), de Gruyter, Berlin (1989), 227–239.

[Ful1997] J. Fulman, *Probability in the classical groups over finite fields: symmetric functions, stochastic algorithms and cycle indices*, Ph.D. thesis, Harvard University (1997).

[FK2019] J. Fulman and N. Kaplan, *Random partitions and Cohen-Lenstra heuristics*, Annals of Combinatorics **23** (2019), 295–315.

[Gro1957] A. Grothendieck, *Sur quelques points d'algébre homologique*, Tohoku Mathematical Journal, **9** (1957), 119–221.

[HP1973] F. Harary and E. M. Palmer, *Graphical Enumeration*, Academic Press (1973).

[HN1975] G. Harder and M. S. Narasimhan, *On the cohomology groups of moduli spaces of vector bundles on curves*, Mathematische Annalen, **212** (1975), 215–248.

[Hat2002] A. Hatcher, *Algebraic Topology*, Cambridge University Press (2002).

[Kap2000] M. Kapranov, *The elliptic curve in the S-duality theory and Eisenstein series for Kac-Moody groups*, available at https://arxiv.org/abs/math/0001005

[Kun1981] J. Kung, *The cycle structure of a linear transformation over a finite field*, Linear Algebra and its Applications **36** (1981), 141–155.

[Mac1962A] I. G. Macdonald, *The Poincaré polynomial of a symmetric product*, Mathematical Proceedings of the Cambridge Philosophical Society, **58** (1962), 563–568.

[Mac1962J] I. G. Macdonald, *Symmetric products of an algebraic curve*, Topology, **1** (1962), 319–343.

[Mac1995] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, 2nd edition, Oxford (1995).

[Mil1980] J. S. Milne, *Étale Cohomology*, Princeton Mathematical Series, **33** (1980).

[Mus] M. Mustaţă, *Zeta functions in algebraic geometry*, lecture notes, available at http://www-personal.umich.edu/~mmustata/zeta_book.pdf

[Mus2] M. Mustaţă, *Singular cohomology as sheaf cohomology with constant coefficients*, lecture notes, available at http://www-personal.umich.edu/~mmustata/SingSheafcoho.pdf

[Pol1937] G. Pólya, *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen* (2nd ed.), Oxford (1995).

[PR1987] G. Pólya and R. C. Read, *Combinatorial Enumeration of Groups, Graphs, and Chemical Compounds*, Spring-Verlag (1987).

[Ras] S. Raskin, *The Weil conjectures for curves*, available at https://math.uchicago.edu/~may/VIGRE/VIGRE2007/REUPapers/FINALFULL/Raskin.pdf

[Red1927] J. H. Redfield, *The theory of group-reduced distributions*, American Journal of Mathematics, **49** (1927), 433–455.

[SL1966] L. Shepp and S. Lloyd, Ordered cycle lengths in a random permutation, Memoirs of the American Mathematical Society **121** (1966), 340-357.

[Sta1999] R. Stanley, *Enumerative Combinatorics: Volume 2*, Cambridge University Press (1999).

[Sto1988] R. Stong, *Some asymptotic results on finite vector spaces*, Advances in Applied Mathematics **9** (1988), 167–199.

[Vak2015] R. Vakil, Lecture notes for Arizona Winter School 2015.

[VW2015] R. Vakil and M. M. Wood, *Discriminants in the Grothendieck ring*, Duke Mathematical Journal, **164** (2015), No. 6.