Cohen–Lenstra distributions via random matrices over complete discrete valuation rings with finite residue fields

Gilyoung Cheong and Yifeng Huang

Abstract Let $(R, \mathfrak{m})$ be a complete discrete valuation ring with the finite residue field $R/\mathfrak{m} = \mathbb{F}_q$. Given a monic polynomial $P(t) \in R[t]$ whose reduction modulo $\mathfrak{m}$ gives an irreducible polynomial $\overline{P}(t) \in \mathbb{F}_q[t]$, we initiate an investigation of the distribution of $\operatorname{coker}(P(A))$, where $A \in \mathrm{Mat}_n(R)$ is randomly chosen with respect to the Haar probability measure on the additive group $\mathrm{Mat}_n(R)$ of $n \times n$ R-matrices. In particular, we provide a generalization of two results of Friedman and Washington about these random matrices. We use some concrete combinatorial connections between $\mathrm{Mat}_n(R)$ and $\mathrm{Mat}_n(\mathbb{F}_q)$ to translate our problems about a Haar-random matrix in $\mathrm{Mat}_n(R)$ into problems about a random matrix in $\mathrm{Mat}_n(\mathbb{F}_q)$ with respect to the uniform distribution. Our results over $\mathbb{F}_q$ are about the distribution of the $\overline{P}$-part of a random matrix $\overline{A} \in \mathrm{Mat}_n(\mathbb{F}_q)$ with respect to the uniform distribution, and one of them generalizes a result of Fulman. We heuristically relate our results to a celebrated conjecture of Cohen and Lenstra, which predicts that given an odd prime p, any finite abelian p-group (i.e., $\mathbb{Z}_p$-module) H occurs as the p-part of the class group of a random imaginary quadratic field extension of $\mathbb{Q}$ with a probability inversely proportional to $|\operatorname{Aut}_{\mathbb{Z}}(H)|$. We review three different heuristics for the conjecture of Cohen and Lenstra, and they are all related to special cases of our main conjecture, which we prove as our main theorems.

1. Introduction

In number theory, an influential conjecture of Cohen and Lenstra [2] states that given an odd prime p, a fixed finite abelian p-group H occurs as the p-part $\mathrm{Cl}_K[p^\infty]$ of the class group Cl_K of a random imaginary quadratic field extension K of $\mathbb{Q}$ with a probability inversely proportional to the size $|\operatorname{Aut}_{\mathbb{Z}}(H)|$ of the automorphism group of H.

CONJECTURE 1.1 (Cohen–Lenstra)
Given the notations above, we must have

$$\lim_{N\to\infty} \mathrm{Prob}_{K\in\mathbf{IQ}_{\le N}}\left(\mathrm{Cl}_K[p^\infty] \simeq H\right) = \frac{1}{|\operatorname{Aut}_{\mathbb{Z}}(H)|}\prod_{i=1}^{\infty}(1-p^{-i}),$$

Illinois Journal of Mathematics, Vol. 65, No. 2 (2021), 385–415
DOI 10.1215/00192082-8939615, © 2021 by the University of Illinois at Urbana–Champaign
Received June 1, 2020. Received in final form November 15, 2020.
First published online March 25, 2021.
2020 Mathematics Subject Classification: Primary 05E15; Secondary 11C20.

where $\mathbf{IQ}_{\leq N}$ *is the set of isomorphism classes of imaginary quadratic fields over* $\mathbb{Q}$ *whose absolute discriminant is at most* N *and the probability is given uniformly at random in this set.*

Let $n \in \mathbb{Z}_{\geq 1}$ be the size of a finite set S of some maximal ideals of $\mathcal{O}_K$, the ring of integers of a quadratic extension K of $\mathbb{Q}$, that generate Cl_K, as it is a finite abelian group. Then considering the exact sequence

$$\mathcal{O}_K^{S,\times} \to \mathcal{I}_K^S \to \mathrm{Cl}_K \to 0,$$

where $\mathcal{O}_K^{S,\times} := \{x \in K^\times : x\mathcal{O}_K$ can be written as a product of positive/negative powers of ideals in $S\}$ and $\mathcal{I}_K^S$ is the abelian group of fractional ideals that can be written as a product of positive/negative powers of ideals in S, the fact that $\mathcal{O}_K^{S,\times}$ is a finitely generated abelian group of rank $n = |S|$ (by [14, Corollary 11.7, Chapter I]) lets us have the following exact sequence:

$$\mathbb{Z}^n \to \mathbb{Z}^n \to \mathrm{Cl}_K \to 0.$$

Applying $(-) \otimes_{\mathbb{Z}} \mathbb{Z}_p$, we have the exact sequence

$$\mathbb{Z}_p^n \to \mathbb{Z}_p^n \to \mathrm{Cl}_K[p^\infty] \to 0,$$

so a heuristic approach to examine Conjecture 1.1 is to compute the cokernel of a "random" $\mathbb{Z}_p$-linear map $\mathbb{Z}_p^n \to \mathbb{Z}_p^n$. Friedman and Washington ([9, Proposition 1]) proved that

$$\lim_{n\to\infty} \mathrm{Prob}_{A\in \mathrm{Mat}_n(\mathbb{Z}_p)}\big(\mathrm{coker}(A) \simeq H\big) = \frac{1}{|\mathrm{Aut}_{\mathbb{Z}}(H)|}\prod_{i=1}^{\infty}(1-p^{-i}), \tag{1.1}$$

where the probability measure on $\mathrm{Mat}_n(\mathbb{Z}_p)$ is given by the Haar measure with the total measure 1.

One of our main theorems is a generalization of this result.

THEOREM 1.2 (cf. Theorem C)
Fix any prime p *(allowing* $p = 2$*). Let* $P_1(t), \ldots, P_r(t) \in \mathbb{Z}_p[t]$ *be any monic polynomials such that the reduction modulo* p *gives distinct irreducible polynomials* $\overline{P}_1(t), \ldots, \overline{P}_r(t) \in \mathbb{F}_p[t]$*, where* $r \in \mathbb{Z}_{\geq 1}$*. Suppose that* $\deg(P_r) = 1$*. Given any finite abelian* p*-group* H*, we have*

$$\lim_{n\to\infty} \mathrm{Prob}_{A\in \mathrm{Mat}_n(\mathbb{Z}_p)} \begin{pmatrix} \mathrm{coker}\big(P_1(A)\big) = \cdots = \mathrm{coker}\big(P_{r-1}(A)\big) = 0 \\ \textit{and } \mathrm{coker}\big(P_r(A)\big) \simeq H \end{pmatrix}$$
$$= \frac{1}{|\mathrm{Aut}_{\mathbb{Z}}(H)|}\prod_{j=1}^{r}\prod_{i=1}^{\infty}(1-p^{-i\deg(P_j)}).$$

Next, we briefly review another heuristic due to Friedman and Washington regarding an analogous statement to Conjecture 1.1, replacing $\mathbb{Q}$ with $\mathbb{F}_q(t)$. Note that any quadratic extension K of $\mathbb{Q}$ can be written as the form $K = \mathbb{Q}(\sqrt{d})$ for some square-free integer d. The extension K of $\mathbb{Q}$ is imaginary if and only if $d < 0$, and this is

equivalent to requiring that it has one place above infinity. In the case of a quadratic extension K of $\mathbb{F}_q(t)$, we assume q is odd and restrict to the case $K = \mathbb{F}_q(t)(\sqrt{d(t)})$ for some square-free $d(t) \in \mathbb{F}_q[t]$ of degree $2g+1$ with $g \in \mathbb{Z}_{\geq 1}$. In this case, the smooth, projective, and geometrically irreducible curve C_K over $\mathbb{F}_q$ corresponding to K has genus g. As a double cover over $\mathbb{P}^1_{\mathbb{F}_q}$, the curve C_K has one $\mathbb{F}_q$-point $\mathfrak{p}$ above $\infty = [0:1] \in \mathbb{P}^1(\mathbb{F}_q)$. This implies that we have an isomorphism $\mathrm{Cl}_K \simeq \mathrm{Pic}^0(C_K)$, given by $[D] \mapsto [D] - \deg(D)[\mathfrak{p}]$, where $\mathrm{Pic}^0(C_K)$ is the abelian group of the degree 0 divisor classes on C_K. Friedman and Washington ([9, Section 5]) observed that for a prime $p \nmid q$, the p-part of $\mathrm{Pic}^0(C_K)$ occurs as the cokernel of $A - \mathrm{id}$ of the p-adic Tate module of $\mathrm{Pic}^0(C_K \times_{\mathbb{F}_q} \overline{\mathbb{F}_q})$, where A is the automorphism of the Tate module induced by the Frobenius and id is the identity. The p-adic Tate module of $\mathrm{Pic}^0(C_K \times_{\mathbb{F}_q} \overline{\mathbb{F}_q})$ is known to be a free $\mathbb{Z}_p$-module with rank $2g$, where g is the genus of C_K (e.g., [13, p. 34]), so we have the exact sequence

$$\mathbb{Z}_p^{2g} \xrightarrow{A-\mathrm{id}} \mathbb{Z}_p^{2g} \to \mathrm{Cl}_K[p^\infty] \to 0,$$

where $A \in \mathrm{GL}_{2g}(\mathbb{Z}_p)$. As a supporting heuristic to a function field version of Conjecture 1.1, Friedman and Washington ([9, Section 4]) proved that

$$\lim_{n\to\infty} \mathrm{Prob}_{A \in \mathrm{GL}_n(\mathbb{Z}_p)}\big(\mathrm{coker}(A - \mathrm{id}) \simeq H\big) = \frac{1}{|\mathrm{Aut}_{\mathbb{Z}}(H)|} \prod_{i=1}^{\infty}(1 - p^{-i}), \tag{1.2}$$

where the probability is given by restricting the Haar measure on $\mathrm{Mat}_n(\mathbb{Z}_p)$ to $\mathrm{GL}_n(\mathbb{Z}_p)$ and then normalizing it so that we get the total measure 1. This is also a special case of our Theorem 1.2 by taking $r = 2$ with $P_1(t) = t$ and $P_2(t) = t - 1$ in the statement. (See Corollary 2.5 and its proof for the details.)

The two heuristic results (1.1) and (1.2) involve different mathematical objects in their motivations. The fact that these numerical results are the same was referred to as "blurring" by Friedman and Washington ([9, Section 4]) for their own heuristic reason ([9, Section 1]). As mentioned above, one contribution of our work is to explain further what is behind this blurring phenomenon (i.e., Theorem 1.2). It is worth noting that our theorem contains more than (1.1) and (1.2). For instance, if p is chosen that -1 is not a square in $\mathbb{F}_p$, Theorem 1.2 implies that

$$\lim_{n\to\infty} \mathrm{Prob}_{A \in \mathrm{GL}_n(\mathbb{Z}_p)} \begin{pmatrix} \mathrm{coker}(A^2 + \mathrm{id}) = 0, \\ \mathrm{coker}(A - \mathrm{id}) \simeq H \end{pmatrix}$$
$$= \frac{1}{|\mathrm{Aut}_{\mathbb{Z}}(H)|} \Big(\prod_{i=1}^{\infty}(1 - p^{-i})\Big)\Big(\prod_{j=1}^{\infty}(1 - p^{-2j})\Big).$$

Furthermore, our paper contains much more than Theorem 1.2, and the main theorems can be found as Theorems A, B, and C in Section 2. We speculate that an even more general phenomenon is behind our main theorems, which we state as Conjecture 2.3.

REMARK 1.3

Despite the suggestive heuristic, Conjecture 1.1 is notorious for its difficulty, and it

is wide open except for the case $p = 3$. (Some progress for $p = 3$ in terms of the surjection moment method due to Davenport and Heilbronn is explained in [3, Section 8.5].) On the other hand, there has been a breakthrough for an analogous statement replacing $\mathbb{Q}$ with $\mathbb{F}_q(t)$ (for large g and q such that $q \not\equiv 0, 1 \mod p$) due to Ellenberg, Venkatesh, and Westerland ([3, Theorem 1.2]), using more geometric methods. Our work is not directly related to proving Conjecture 1.1, but it connects different results used as heuristic evidence for the conjecture.

It is interesting that Theorem 1.2 resembles the distribution given by (1.1) and (1.2) on the set of finite abelian p-groups, called the **Cohen–Lenstra distribution** (e.g., [3, Section 8.1]), and this motivates a more general definition of the Cohen–Lenstra distribution, which we will discuss in Section 2. This computation is also in accordance with the philosophy of "universality" described by Wood [19], which essentially states that the distributions we construct with random matrices tend to follow the Cohen–Lenstra distribution and its variants. Indeed, Wood dealt with various probability measures on $\mathrm{Mat}_n(\mathbb{Z}_p)$ extensively generalizing the Haar measure case and showed that, asymptotically in n, the cokernel of a random $A \in \mathrm{Mat}_n(\mathbb{Z}_p)$ with respect to any of such measures follows the Cohen–Lenstra distribution ([19, Theorem 1.2]). Our paper will stick with the Haar measure and its pushforwards given by the polynomial maps $P_1, \dots, P_r : \mathrm{Mat}_n(\mathbb{Z}_p) \to \mathrm{Mat}_n(\mathbb{Z}_p)$, in the sense of Theorem 1.2.

1.1. Organization for the rest of this paper

In Section 2, we give an even more general conjecture (Conjecture 2.3). Unlike in the introduction, our discussion will be for a general complete discrete valuation ring R with the finite residue field. The reader may choose to assume $R = \mathbb{Z}_p$ or $R = \mathbb{F}_q[\![t]\!]$, as the general case does not take any more effort. Some of our main theorems are special cases of this conjecture. We separated the main theorems as Theorems A, B, and C because their proofs are different. Theorems A and B can be equivalently stated as statements about a random matrix in $\mathrm{Mat}_n(\mathbb{F}_q)$, with respect to the uniform distribution. These equivalent statements are given in Theorems 2.8 and 2.10 introduced in Section 2.2. The reader interested only in matrices over finite fields can focus on this section. In Section 3, we will see that these statements over $\mathbb{F}_q$ are related to another heuristic for Conjecture 1.1 due to Cohen and Lenstra [2]. Section 4 is technical but important: we explain how to reduce the problems of computing the desired probabilities given by the Haar measure on $\mathrm{Mat}_n(R)$ into some combinatorial problems over finite local rings, providing crucial lemmas we use throughout the paper. In Section 5, we explain how to reduce Theorems A, B, and C into Theorems 2.8 and 2.10. In Section 6, we use an argument due to Boreico [1] to explain that Theorems A and B conversely imply Theorems 2.8 and 2.10. This section can be skipped if the reader is interested only in proofs of our main theorems. In Section 8, we give a proof for Theorems 2.8 and 2.10, and Section 7 introduces a combinatorial tool called "cycle index" and some of its properties we use in Section 8.

2. Main conjecture and theorems

Instead of $\mathbb{Z}_p$, we will work more generally with any complete discrete valuation ring (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 [9, Proposition 1], and the proof given there works for the general R.

PROPOSITION 2.1 (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

$$\operatorname{Prob}_{A \in \operatorname{Mat}_n(R)}\big(\operatorname{coker}(A) \simeq H\big) = \begin{cases} |\operatorname{Aut}_R(H)|^{-1}\big[\prod_{i=1}^{n}(1-q^{-i})\big]\big[\prod_{j=n-l_H+1}^{n}(1-q^{-j})\big] & \text{if } n \geq l_H, \\ 0 & \text{if } n < l_H, \end{cases}$$

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

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

Our paper generalizes the limiting distribution (i.e., the probability when n goes to infinity) in Proposition 2.1 as Theorem C. We also propose a more general conjecture in Conjecture 2.3.

Notations
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 2.2
It turns out that for any DVR $(R, \mathfrak{m})$ with $R/\mathfrak{m} = \mathbb{F}_q$, the assignment

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

defines a probability measure on the finest σ-algebra on $\mathbf{Mod}_R^{<\infty}$ (e.g., Remark 7.4). 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., Section 8 of [3]). Since R is a principal ideal domain (PID), for any finite length R-module H, we have a unique partition $\lambda = (\lambda_1, \ldots, \lambda_l)$, with the convention $\lambda_1 \geq \cdots \geq \lambda_l$, such that

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

In this case, we will write $\lambda(H) := \lambda$. A result of Macdonald ([12, (1.6), p. 181]) states that the number $|\operatorname{Aut}_R(H)|$ depends only on $q = |R/\mathfrak{m}|$ and λ so that we may write $w(q,\lambda) = |\operatorname{Aut}_R(H)|$. Using this and Lemma 7.3 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 non-negative integers. We will not name this more general distribution because it will appear only in our conjecture, not in any of our theorems, but we think that Cohen and Lenstra were aware of this, given the context of [2]. Fulman and Kaplan [8] discussed other similar distributions defined on $\mathcal{P}$ that come up in various combinatorial contexts.

2.1. Main conjecture and theorems

We first introduce our main conjecture about a random matrix $A \in \operatorname{Mat}_n(R)$, 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 $A \in \operatorname{Mat}_n(R)$ and $\overline{A} \in \operatorname{Mat}_n(\mathbb{F}_q)$, where the latter is given by the uniform distribution on $\operatorname{Mat}_n(\mathbb{F}_q)$.

CONJECTURE 2.3

Let $(R, \mathfrak{m})$ be a complete DVR such that $R/\mathfrak{m} = \mathbb{F}_q$ and $P_1(t), \dots, P_r(t) \in R[t]$ 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 $r \in \mathbb{Z}_{\geq 0}$. Fix any R-modules $H_1, \dots, H_r$ of finite length. We must have

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

Note that the limiting distribution $n \to \infty$ given by Proposition 2.1 is a special case of Conjecture 2.3. More cases of Conjecture 2.3 are proven as Theorems B and C. We now present our main theorems: Theorems A, B, and C.

THEOREM A

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

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

where $b_n(d)$, for $d \in \mathbb{Z}_{\geq 0}$, 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

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

REMARK 2.4

It will turn out that $b_n(d)$ given above are positive rational numbers explicitly given as

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

for any degree d monic irreducible polynomial $\overline{P}(t) \in \mathbb{F}_q[t]$. This will appear in the proof of Theorem 2.8, which is a step to prove Theorem A. To check why $b_n(d)$ ought to be given this way, apply Lemma 4.3 with $N = 0$ and $r = 1$ to the statement of Theorem A.

THEOREM B

Let $(R, \mathfrak{m})$ be a complete DVR such that $R/\mathfrak{m} = \mathbb{F}_q$ and $P_1(t), \ldots, P_r(t) \in R[t]$ 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 $r \in \mathbb{Z}_{\geq 0}$. We have

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

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 $1 \leq i \leq r$, 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 $P_2(A) \in S_2$.) Both Theorems A and B are corollaries of some statements (Theorems 2.8 and 2.10) about matrices over $\mathbb{F}_q$.

Our last theorem, introduced in the introduction for the specific case $R = \mathbb{Z}_p$, has a similar feature (and so does Conjecture 2.3).

THEOREM C

Let $(R, \mathfrak{m})$ *be a complete DVR such that* $R/\mathfrak{m} = \mathbb{F}_q$ *and* $P_1(t), \dots, P_r(t) \in R[t]$ *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* $r \in \mathbb{Z}_{\geq 1}$. *Suppose that* $\deg(P_r) = 1$. *Given any* R*-module* H *of finite length, we have*

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

Note that Theorem C generalizes the limiting distribution given in Proposition 2.1, a result of Friedman and Washington [9]. Theorem C also generalizes another result of the same authors ([9, (9), p. 234]), as we mentioned in the introduction, which we discuss as Corollary 2.5. Finally, Theorem C generalizes Theorem B by summing over all possible H up to isomorphisms.

The proof of the following corollary uses Lemma 4.3, which we introduce much later for the natural organization.

COROLLARY 2.5 (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*

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

Proof

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

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

we have

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

because $\operatorname{coker}(\overline{A}) = 0$ if and only if $\overline{A}$ is an automorphism of $(R/\mathfrak{m}^{N+1})^n$. Thus, applying Lemma 4.3 and Theorem C with $P_1(t) = t$ and $P_2(t) = t - 1$ for $r = 2$, we obtain the result by letting $n \to \infty$. □

REMARK 2.6

Our proof for Theorem C uses Lemma 5.2 due to Friedman and Washington [9], which appears in the original proof of Corollary 2.5. The condition $\deg(P_r) = 1$ in Theorem C is necessary is because it is needed in the proof 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

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

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 $0 \le l \le n$ 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 2.1 even for all $n \ge 0$, not just $n \to \infty$. This is not the proof given by Friedman and Washington [9] (as one can check Proposition 1 in their paper). However, Lemma 5.2 is from their paper, so it seems quite evident that Friedman and Washington were aware of this argument.

REMARK 2.7

Given our discussion, the known cases for Conjecture 2.3 to the best of our knowledge are the following:

- any $r \ge 0$ with $H_1 = \cdots = H_r = 0$ (Theorem B);
- any $r \ge 1$ with $\deg(P_r) = 1$, while $H_1 = \cdots H_{r-1} = 0$ and any H_r (Theorem C).

2.2. Random matrices over finite fields

Among our three theorems, A and B can be rephrased as statements about $\overline{A} \in \mathrm{Mat}_n(\mathbb{F}_q)$, chosen uniformly at random. In this section, we will write A instead of $\overline{A}$ for convenience. Given any module M over a commutative ring R and an ideal I of R, we define the I**-part** of M as

$$M[I^\infty] := \{x \in M : I^N x = 0 \text{ for some } N \in \mathbb{Z}_{\ge 1}\}.$$

For any $A \in \mathrm{Mat}_n(\mathbb{F}_q)$ and $P = P(t) \in \mathbb{F}_q[t]$, we will write $A[P^\infty]$ to mean the (P)-part of the $\mathbb{F}_q[t]$-module given by the action of A on $\mathbb{F}_q^n$. (See Section 7.1 for details.) Theorem A will be deduced from the following.

THEOREM 2.8

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

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

where $b_n(d)$, for $d \in \mathbb{Z}_{\geq 0}$, 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

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

REMARK 2.9

Note that given q, n, and H, the conclusion of Theorem 2.8 depends only 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 $n \geq 0$, Theorem 2.8 implies that

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

Likewise, Theorem B will be deduced from the following.

THEOREM 2.10

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 $1 \leq j \leq r$. Then

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

As an immediate corollary, we see how random matrices in $\mathrm{GL}_n(\mathbb{F}_q)$ are related to Cohen–Lenstra distributions as $n \to \infty$. This is originally due to Fulman in his thesis [5], but a partial result to this was also observed by Washington prior to Fulman ([17, Theorem 1(b)]). Washington's result can be obtained by taking $P(t) = t - 1$ in the following corollary and applying Lemma 5.3, which is due to Cohen and Lenstra.

COROLLARY 2.11 ([7, p. 2])
Fix any monic irreducible polynomial $P(t) \in \mathbb{F}_q[t] \smallsetminus \{t\}$ *and a* P^∞*-torsion* $\mathbb{F}_q[t]$*-module* H *of finite length. Then*

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

Proof
Applying Theorem 2.10 by taking $P_1(t) = t$ and $P_2(t) = P(t)$ with $H_1 = 0$ and $H_2 = H$, we get

$$\begin{aligned}
&\lim_{n\to\infty} \mathrm{Prob}_{A\in \mathrm{GL}_n(\mathbb{F}_q)}\big(A[P^\infty] \simeq H\big)\\
&\quad= \lim_{n\to\infty} \frac{|\{A \in \mathrm{GL}_n(\mathbb{F}_q) : A[P^\infty] \simeq H\}|}{|\mathrm{Mat}_n(\mathbb{F}_q)|}\frac{|\mathrm{Mat}_n(\mathbb{F}_q)|}{|\mathrm{GL}_n(\mathbb{F}_q)|}\\
&\quad= \frac{\lim_{n\to\infty} \mathrm{Prob}_{A\in \mathrm{Mat}_n(\mathbb{F}_q)}(A[t^\infty] = 0 \text{ and } A[P^\infty] \simeq H)}{\prod_{i=1}^{\infty}(1-q^{-i})}\\
&\quad= \frac{1}{|\operatorname{Aut}_{\mathbb{F}_q[t]}(H)|}\prod_{i=1}^{\infty}\frac{(1-q^{-i})(1-q^{-i\deg(P)})}{(1-q^{-i})}\\
&\quad= \frac{1}{|\operatorname{Aut}_{\mathbb{F}_q[t]}(H)|}\prod_{i=1}^{\infty}(1-q^{-i\deg(P)}),
\end{aligned}$$

as desired. □

REMARK 2.12
Thanks to Nathan Kaplan, we have noticed that Boreico has independently obtained Theorem 2.10 in his thesis ([1, Theorem 3.8.18]) prior to our paper. Boreico's proof differs from ours, but he also sketches our proof and discusses the same corollary (i.e., Corollary 2.11). We believe that providing our proof for Theorem 2.10 is still valuable for clarity and details. We recommend that the interested reader take a look at his alternative proof of Theorem 2.10 (i.e., [1, Theorem 3.8.18]) which uses more direct linear algebraic and measure theoretic arguments. Boreico's proof also inspired us to find many connections between our results over $\mathbb{F}_q$ and random matrices over an arbitrary complete DVR whose residue field at its maximal ideal is $\mathbb{F}_q$. A part of his proof is presented in this paper as Lemma 6.1. We use this to get Corollary 6.3, which will enable us to see that Theorems A and B imply Theorems 2.8 and 2.10.

REMARK 2.13
The referee pointed out that there is a stronger version of Corollary 2.11 in another paper of Fulman [6, Theorem 4] and suggested that a variation Fulman's proof in [6] may also lead to a valid proof of Theorem 2.10. Indeed, it turned out that this is the case. We briefly explain how to modify Fulman's proof in [6] to prove Theorem 2.10 for the sake of completeness, but the reader may skip this part unless necessary. Mimicking

the step where Fulman multiplies $1-u$ to the identity in Lemma 7.2, we multiply the left-hand side and the right-hand side of the identity,

$$\prod_{i=0}^{\infty}(1-q^{-i}u) = \prod_{P\in|\mathbb{A}^1_{\mathbb{F}_q}|}\sum_{\nu\in\mathcal{P}}\frac{u^{|\nu|\deg(P)}}{|\operatorname{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|},$$

which can be deduced from Lemma 7.3 to those of the identity given by Lemma 7.1, respectively. From here, imitating the proof of [6, Theorem 4], it is not difficult to achieve a valid proof of Theorem 2.10. The proof we provide in this paper has many similar features to this, although the two proofs are not identical.

3. Philosophy of Cohen and Lenstra

Notations

Given a ring R and integer $N \geq 1$, we denote by $\mathbf{Mod}_R^{\leq N}$ the set of isomorphism classes of R-modules whose size is less than or equal to to N and $\mathbf{Mod}_R^{=N}$ the set of isomorphism classes of R-modules whose size is equal to N.

Conjecture 1.1 was motivated by the numerical observation of Cohen and Lenstra that most class groups of imaginary quadratic field extensions of $\mathbb{Q}$ are cyclic and that "the scarcity of noncylic groups can be attributed to the fact that they have many automorphisms" (as in the first page of [2]). For instance, note that

$$\left|\operatorname{Aut}_{\mathbb{Z}}\big(\mathbb{Z}/(5)\oplus\mathbb{Z}/(5)\big)\right| = 480,$$

while

$$\left|\operatorname{Aut}_{\mathbb{Z}}\big(\mathbb{Z}/(25)\big)\right| = 20,$$

even though the groups $\mathbb{Z}/(5)\oplus\mathbb{Z}/(5)$ and $\mathbb{Z}/(25)$ have the same size. More specifically, their speculation predicts that, for $N \gg 0$, the probability we choose $\mathbb{Z}/(25)$ as the class group of a random number field from $\mathbf{IQ}_{\leq N}$ (as in the introduction) should be about $480/20 = 24$ times larger than the probability we choose $\mathbb{Z}/(5)\oplus\mathbb{Z}/(5)$ similarly. Cohen and Lenstra made a hypothesis that the limiting distribution in N of the class group of a random $K \in \mathbf{IQ}_{\leq N}$ would be similar to that of a random finite abelian group A, whose probability of occurrence is proportional to $1/|\operatorname{Aut}_{\mathbb{Z}}(A)|$. They showed that for any finite abelian p-group H, we have

$$\lim_{N\to\infty}\operatorname{Prob}_{A\in\mathbf{Mod}_{\mathbb{Z}}^{\leq N}}\big(A[p^\infty]\simeq H\big) = \frac{1}{|\operatorname{Aut}_{\mathbb{Z}}(H)|}\prod_{i=1}^{\infty}(1-p^{-i}),$$

where we used the following definition with $S = \mathbf{Mod}_{\mathbb{Z}}^{\leq N}$.

DEFINITION 3.1

Given a nonempty finite subset S of the isomorphism classes of a category $\mathcal{C}$, all of whose automorphism groups are finite, we define

$$\operatorname{Prob}_{s\in S}(s \text{ satisfies } \mathscr{P}) := \frac{\sum_{s\in S,\ s \text{ satisfies } \mathscr{P}} 1/|\operatorname{Aut}_{\mathcal{C}}(s)|}{\sum_{s\in S} 1/|\operatorname{Aut}_{\mathcal{C}}(s)|},$$

where $\mathscr{P}$ is any property on S.

This provides another heuristic philosophy behind Conjecture 1.1, which historically predates Proposition 2.1. This philosophy still works if we replace $\mathbb{Z}$ by $\mathbb{F}_q[t]$. Under the conjugate action $\mathrm{GL}_n(\mathbb{F}_q) \curvearrowright \mathrm{Mat}_n(\mathbb{F}_q)$, the set $\mathrm{Mat}_n(\mathbb{F}_q)/\mathrm{GL}_n(\mathbb{F}_q)$ of orbits parametrizes the set $\mathbf{Mod}^{=q^n}_{\mathbb{F}_q[t]}$ of the isomorphism classes of $\mathbb{F}_q[t]$-modules of $\mathbb{F}_q$-dimension n because each matrix $\overline{A} \in \mathrm{Mat}_n(\mathbb{F}_q)$ gives $\mathbb{F}_q^n$ an $\mathbb{F}_q[t]$-module structure, which we denote as $\overline{A} \curvearrowright \mathbb{F}_q^n$, by $t \cdot v := \overline{A}v$ for $v \in \mathbb{F}_q^n$ and two matrices define isomorphic $\mathbb{F}_q[t]$-module structures if and only if they are in the same orbit under the conjugate action of $\mathrm{GL}_n(\mathbb{F}_q)$. Noting that

$$\mathrm{Aut}_{\mathbb{F}_q[t]}(\overline{A} \curvearrowright \mathbb{F}_q^n) = \mathrm{Stab}_{\mathrm{GL}_n(\mathbb{F}_q)}(\overline{A}),$$

by an application of the orbit-stabilizer theorem, we have

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

Therefore, Theorems 2.8 and 2.10 can be reinterpreted as the computations on explicit probability distributions on $\mathbf{Mod}^{=q^n}_{\mathbb{F}_q[t]}$. Cohen and Lenstra considered a similar distribution on $\mathbf{Mod}^{\leq q^n}_{\mathbb{F}_q[t]}$ instead of $\mathbf{Mod}^{=q^n}_{\mathbb{F}_q[t]}$ in Theorem 2.10. Their proof works for many Dedekind domains R including $\mathbb{Z}$ and $\mathbb{F}_q[t]$, but it requires that there are finitely many finite length R-modules M with $|M| \leq N$ for any $N > 0$ (up to isomorphisms) and the zeta function $\zeta_R(s)$ of R must have only one simple pole at $s = 1$.

PROPOSITION 3.2 ([2, Example 5.9, $u = 0$])
Let R be a number ring or the coordinate ring of an affine open subset of a smooth, geometrically connected, and projective curve over $\mathbb{F}_q$ obtained by subtracting an $\mathbb{F}_q$-point. Fix finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ of R. For $1 \leq j \leq r$, say H_j is an $\mathfrak{m}_j^\infty$-torsion R-module of finite length and $q_j := |R/\mathfrak{m}_j|$. We have

$$\lim_{N \to \infty} \mathrm{Prob}_{A \in \mathbf{Mod}^{\leq N}_R} \begin{pmatrix} A[\mathfrak{m}_j^\infty] \simeq H_j \\ \text{for } 1 \leq j \leq r \end{pmatrix} = \prod_{j=1}^{r} \frac{1}{|\mathrm{Aut}_R(H_j)|} \prod_{i=1}^{\infty} (1 - q_j^{-i}).$$

REMARK 3.3
Roughly speaking, Theorem B, Theorem C, Theorem 2.10, and Proposition 3.2 (for the case $R = \mathbb{F}_q[t]$) tell us about how distributions involving some global information about $\mathbb{A}^1_{\mathbb{F}_q} = \mathrm{Spec}(\mathbb{F}_q[t])$ can be obtained by their local information. As their invariants such as n or N go to infinity, their local events become independent.

REMARK 3.4
Using the notations in the proof of Corollary 2.11, we have

$$\lim_{n \to \infty} \mathrm{Prob}_{\overline{A} \in \mathrm{GL}_n(\mathbb{F}_q)}\left(\overline{A}[P^\infty] \simeq H\right) = \lim_{n \to \infty} \mathrm{Prob}_{A \in \mathbf{Mod}^{=q^n}_{\mathbb{F}_q[t]}} \begin{pmatrix} A[t^\infty] = 0 \text{ and} \\ A\left[P(t)^\infty\right] \simeq H \end{pmatrix}$$

$$= \lim_{n \to \infty} \mathrm{Prob}_{A \in \mathbf{Mod}^{\leq q^n}_{\mathbb{F}_q[t]}} \begin{pmatrix} A[t^\infty] = 0 \text{ and} \\ A\left[P(t)^\infty\right] \simeq H \end{pmatrix},$$

so Fulman's result about random matrices in $\mathrm{GL}_n(\mathbb{F}_q)$ can be naturally compared to a special case of Proposition 3.2. This provides a concrete reason why a random matrix in $\mathrm{GL}_n(\mathbb{F}_q)$ produces a Cohen–Lenstra distribution (as $n \to \infty$), resolving previous inquiries made by Fulman [7], Fulman–Kaplan [8], Lengler [11], and Washington [17]. In general, many algebraic objects, whose probability of occurrence is inversely proportional to the numbers of their automorphisms, seem to follow some version of Cohen-Lenstra distribution, and our results exemplify such phenomena. More broad examples on "universal" occurrences of Cohen–Lenstra distributions (or similar-looking distributions) can be found in the literature (e.g., [18] and [19]), and this seems to be an active area of research.

4. Converting Haar measure problems into problems over finite local rings

In this section, we explain how to reduce the problems of computing the probabilities in Theorems A, B, and C given by the Haar measure on $\mathrm{Mat}_n(R)$ into some combinatorial problems over finite local rings. This will be used in the next section when we show how Theorems 2.8 and 2.10 imply Theorems A and B.

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 $N \in \mathbb{Z}_{\geq 0}$ such that $\mathfrak{m}^N H = 0$.

LEMMA 4.1

Let $(R, \mathfrak{m})$ be a complete DVR with $R/\mathfrak{m} = \mathbb{F}_q$ and H a finite length R-module. Fix any $N \in \mathbb{Z}_{\geq 0}$ 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 may have

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

for some partition $\lambda = (\lambda_1, \ldots, \lambda_l)$. Since $\mathfrak{m}^N H = 0$, we have $1 \leq \lambda_i \leq N$ 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 $e \in \mathbb{Z}_{\geq 0}$. 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 $u_1\pi^{e_1}, \ldots, u_n\pi^{e_n}$, where $u_i \in R^\times$ and $0 \leq e_i \leq N$. The matrix $\overline{g_1}\overline{A}\overline{g_2} \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ is diagonal with nonzero entries $\overline{u_1\pi}^{e_1}, \ldots, \overline{u_n\pi}^{e_n} \in R/\mathfrak{m}^{N+1}$. We must have $(e_1, \ldots, e_n) = (\lambda_1, \ldots, \lambda_l, 0, \ldots, 0)$ because $\overline{g_1}, \overline{g_2} \in \mathrm{GL}_n(R/\mathfrak{m}^{N+1})$ so that

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

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

Therefore, we have

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

as desired. □

REMARK 4.2

The easiest case of Lemma 4.1 is when $N = 0$, which necessarily means $H = 0$. For this case, the lemma can be proven by a direct application of Nakayama's lemma. This special case is all we need for Theorems A and B, but the full version of Lemma 4.1 is needed for proving Theorem C. We will not directly use Lemma 4.1, but it will be used to prove the following lemma, which we will use to prove our main theorems. It describes how we may concretely think of certain events according to the Haar measure on $\mathrm{Mat}_n(R)$.

LEMMA 4.3

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

$$\begin{aligned}&\mathrm{Prob}_{A \in \mathrm{Mat}_n(R)} \begin{pmatrix} \operatorname{coker}\big(f_j(A)\big) \simeq H_j \\ \textit{for } 1 \leq j \leq r \end{pmatrix} \\ &\quad = \mathrm{Prob}_{\overline{A} \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})} \begin{pmatrix} \operatorname{coker}\big(f_j(\overline{A})\big) \simeq H_j \\ \textit{for } 1 \leq j \leq r \end{pmatrix}.\end{aligned}$$

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 $\operatorname{coker}(f(A)) \simeq H$ if and only if $\operatorname{coker}(f(A + \pi^{N+1}B)) \simeq H$ for all $B \in \mathrm{Mat}_n(R)$. Having this in mind, applying Lemma 4.1 lets us see that

$$\begin{aligned}&\mathrm{Prob}_{A \in \mathrm{Mat}_n(R)} \begin{pmatrix} \operatorname{coker}\big(f_j(A)\big) \simeq H_j \\ \text{for } 1 \leq j \leq r \end{pmatrix} \\ &\quad = \sum_{\overline{A} \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})} \mu_n\Big(\big(A + \mathfrak{m}^{N+1}\mathrm{Mat}_n(R)\big)\Big)\end{aligned}$$

$$\cap \left\{ \begin{array}{c} M \in \mathrm{Mat}_n(R) : \\ \mathrm{coker}\big(f_j(M)\big) \simeq H_j \text{ for } 1 \le j \le r \end{array} \right\} \Bigg)$$

$$= \frac{1}{|\mathrm{Mat}_n(R/\mathfrak{m}^{N+1})|} \left| \left\{ \begin{array}{c} \overline{A} \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1}) : \\ \mathrm{coker}\big(f_j(\overline{A})\big) \simeq H_j \text{ for } 1 \le j \le r \end{array} \right\} \right|$$

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

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

5. Reductions for Theorems A, B, and C

5.1. Theorems 2.8 and 2.10 imply Theorems A and B

In this section, we show that Theorems 2.8 and 2.10 imply Theorems A and B, respectively.

Proof that Theorems 2.8 and 2.10 imply Theorems A and B

We keep the notations in Theorem B. Taking $N = 0$ in Lemma 4.3, we have

$$\mathrm{Prob}_{A \in \mathrm{Mat}_n(R)} \left(\begin{array}{c} \mathrm{coker}\big(P_j(A)\big) = 0 \\ \text{for } 1 \le j \le r \end{array} \right) = \mathrm{Prob}_{\overline{A} \in \mathrm{Mat}_n(\mathbb{F}_q)} \left(\begin{array}{c} \mathrm{coker}\big(P_j(\overline{A})\big) = 0 \\ \text{for } 1 \le j \le r \end{array} \right).$$

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 2.10 (and, taking $r = 1$, $H_1 = H = 0$ in Theorem 2.8). □

REMARK 5.1

In the above proof, we used only the special cases of Theorems 2.8 and 2.10 when $H = 0$ and $H_1 = \cdots = H_r = 0$ to deduce Theorems A and B, respectively. However, we will see with Corollary 6.3 that it is also easy to deduce Theorems 2.8 and 2.10 from Theorems A and B. Underlying this is a formula due to Boreico [1] given as Lemma 6.1 in this paper.

5.2. Theorem 2.10 implies Theorem C

This section is devoted to showing that Theorem 2.10 implies Theorem C. The crucial lemma is the following result due to Friedman and Washington ([9, $\#_H(\bar{R})$, p. 236]).

LEMMA 5.2

Let $(R, \mathfrak{m})$ be a complete DVR with $R/\mathfrak{m} = \mathbb{F}_q$ and H a finite length R-module. Choose any $N \in \mathbb{Z}_{\ge 0}$ 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 $\operatorname{coker}(P(A)) \simeq H$ *is equal to*

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

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

We note that the reason we require $\deg(P) = 1$ is because we want the map $\operatorname{Mat}_n(R/\mathfrak{m}^{N+1}) \to \operatorname{Mat}_n(R/\mathfrak{m}^{N+1})$ given by $A \mapsto \bar{P}(A)$ bijective given in the proof of Lemma 5.2 ([9, p. 236]). 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 ([2, Theorem 6.3] with $u = 0$) as follows.

LEMMA 5.3 (Cohen and Lenstra)
Let $(R, \mathfrak{m})$ *be a complete DVR with* $R/\mathfrak{m} = \mathbb{F}_q$. *For any* $l \in \mathbb{Z}_{\geq 0}$, *we have*

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

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

Proof that Theorem 2.10 implies Theorem C
Let $l_H := \dim_{\mathbb{F}_q}(H/\mathfrak{m}H)$ and choose $N \in \mathbb{Z}_{\geq 0}$ such that $\mathfrak{m}^N H = 0$. We first note that

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

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

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

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

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

Applying Lemma 5.2 implies that

$$\left|\left\{\begin{array}{c} A \in \operatorname{Mat}_n(R/\mathfrak{m}^{N+1}): \\ \operatorname{coker}\left(P_j(A)\right) = 0 \text{ for } 1 \leq j \leq r-1, \\ \operatorname{coker}\left(P_r(A)\right) \simeq H \end{array}\right\}\right|$$

$$= \frac{q^{Nn^2+l_H^2} \prod_{i=1}^{l_H}(1-q^{-i})^2}{|\operatorname{Aut}_R(H)|} \left|\left\{\begin{array}{c} \overline{A} \in \operatorname{Mat}_n(\mathbb{F}_q): \\ \overline{A}[\overline{P}_j^{\infty}] = 0 \text{ for } 1 \leq j \leq r-1, \\ \dim_{\mathbb{F}_q}\left(\overline{A}[\overline{P}_r^{\infty}]/\overline{P}_r\overline{A}[\overline{P}_r^{\infty}]\right) = l_H \end{array}\right\}\right|,$$

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

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

Hence, applying Theorem 2.10 and Lemma 5.3, this leads to

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

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

6. Boreico's formula

We now introduce a formula due to Boreico, appearing in his proof of Theorem 2.8 (or [1, Theorem 3.8.18]). We will use this formula to see that Theorems 2.8 and 2.10 give no more information than Theorems A and B. Any reader who cares only about proofs of our main theorems (Theorems A, B, and C as well as Theorems 2.8 and 2.10) can skip this section because their proofs do not require Boreico's formula. However, the remark following Lemma 6.1 explains how this formula can be used to prove a special case of Theorem 2.8.

LEMMA 6.1 (Boreico)

Fix any distinct monic irreducible polynomials $\overline{P}_1(t),\dots,\overline{P}_r(t)\in\mathbb{F}_q[t]$. For $1\le j\le r$, fix a finite $\overline{P}_j^{\infty}$-torsion $\mathbb{F}_q[t]$-module H_j and let $h_j:=\dim_{\mathbb{F}_q}(H_j)$. If $n\ge h_1+\cdots+h_r$, then we have

$$\begin{aligned}
&\mathrm{Prob}_{\overline{A}\in\mathrm{Mat}_{n-(h_1+\cdots+h_r)}(\mathbb{F}_q)}\begin{pmatrix}\overline{A}[\overline{P}_j^{\infty}]=0\\ \textit{for } 1\le j\le r\end{pmatrix}\\
&\quad=\Big(\frac{|\mathrm{Aut}_{\mathbb{F}_q[x]}(H_1)|\cdots|\mathrm{Aut}_{\mathbb{F}_q[x]}(H_r)|}{\prod_{i=n-(h_1+\cdots+h_r)+1}^{n}(1-q^{-i})}\Big)\mathrm{Prob}_{\overline{A}\in\mathrm{Mat}_n(\mathbb{F}_q)}\begin{pmatrix}\overline{A}[\overline{P}_j^{\infty}]\simeq H_j\\ \textit{for } 1\le j\le r\end{pmatrix}.
\end{aligned}$$

REMARK 6.2

Lemma 6.1 reduces Theorem 2.10 to the special case where $H_1 = \cdots = H_r = 0$, and it can similarly reduce Theorem 2.8 into this special case. In particular, if $r = 1$ and $\overline{P}_1(t) = t$, then writing $H = H_1$ and $h = h_1 \leq n$, we can apply Lemma 6.1 to compute

$$\begin{aligned}
&\mathrm{Prob}_{\overline{A}\in \mathrm{Mat}_n(\mathbb{F}_q)}\big(\overline{A}[t^\infty] \simeq H\big) \\
&\quad = \frac{1}{|\operatorname{Aut}_{\mathbb{F}_q[t]}(H)|}\,\mathrm{Prob}_{\overline{A}\in \mathrm{Mat}_{n-h}(\mathbb{F}_q)}\big(\overline{A}[t^\infty] = 0\big)\prod_{i=n-h+1}^{n}(1-q^{-i}) \\
&\quad = \frac{1}{|\operatorname{Aut}_{\mathbb{F}_q[t]}(H)|}\,\frac{|\mathrm{GL}_{n-h}(\mathbb{F}_q)|}{|\mathrm{Mat}_{n-h}(\mathbb{F}_q)|}\prod_{i=n-h+1}^{n}(1-q^{-i}) \\
&\quad = \frac{1}{|\operatorname{Aut}_{\mathbb{F}_q[t]}(H)|}\prod_{i=1}^{n}(1-q^{-i}),
\end{aligned}$$

which proves a special case of Theorem 2.8.

We have seen that Theorems 2.8 and 2.10 imply Theorems A and B. The following corollary of the above formula immediately implies that the converse also holds.

COROLLARY 6.3

Let $(R, \mathfrak{m})$ be a complete DVR with $R/\mathfrak{m} = \mathbb{F}_q$ and $P_1(t), \ldots, P_r(t) \in R[t]$ monic polynomials such that the reduction modulo $\mathfrak{m}$ gives distinct irreducible polynomials $\overline{P}_1(x), \ldots, \overline{P}_r(x) \in \mathbb{F}_q[x]$. For $1 \leq j \leq r$, fix a finite $\overline{P}_j^\infty$-torsion $\mathbb{F}_q[t]$-module H_j and let $h_j := \dim_{\mathbb{F}_q}(H_j)$. If $n \geq h_1 + \cdots + h_r$, then we have

$$\begin{aligned}
&\mathrm{Prob}_{A\in \mathrm{Mat}_{n-(h_1+\cdots+h_r)}(R)}\begin{pmatrix}\operatorname{coker}\big(P_j(A)\big) = 0 \\ \textit{for } 1 \leq j \leq r\end{pmatrix} \\
&\quad = \Big(\frac{|\operatorname{Aut}_{\mathbb{F}_q[x]}(H_1)|\cdots|\operatorname{Aut}_{\mathbb{F}_q[x]}(H_r)|}{\prod_{i=n-(h_1+\cdots+h_r)+1}^{n}(1-q^{-i})}\Big)\,\mathrm{Prob}_{\overline{A}\in \mathrm{Mat}_n(\mathbb{F}_q)}\begin{pmatrix}\overline{A}[\overline{P_j}^\infty] \simeq H_j \\ \textit{for } 1 \leq j \leq r\end{pmatrix}.
\end{aligned}$$

Proof

This follows from applying Lemma 4.3 with $N = 0$ to Lemma 6.1. □

We now prove Lemma 6.1. This proof is due to Boreico ([1, p. 109]).

Proof of Lemma 6.1

In this proof, we write $A \in \mathrm{Mat}_n(\mathbb{F}_q)$ instead of $\overline{A}$ and P_j replacing $\overline{P}_j$ for the sake of convenience. Let $H := H_1 \oplus \cdots \oplus H_r$, and $h := \dim_{\mathbb{F}_q}(H) = h_1 + \cdots + h_r$. The key observation is that the number of $A \in \mathrm{Mat}_n(\mathbb{F}_q)$ such that $A[P_j^\infty] \simeq H_j$ for $1 \leq j \leq r$ is equal to the number of triples (V, ϕ, ψ), where

- V is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ with dimension h;
- $\phi \in \mathrm{End}_{\mathbb{F}_q}(V)$ such that $(\phi \curvearrowright V) \simeq H$ as $\mathbb{F}_q[t]$-modules;

- $\psi \in \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_q^n)$ such that $\psi|_V = \phi$ and

$$\bigoplus_{i=1}^{r} (\psi \curvearrowright \mathbb{F}_q^n)[P_j^\infty] \simeq (\phi \curvearrowright V)$$

as $\mathbb{F}_q[t]$-modules, where the direct sum is internally taken in $\mathbb{F}_q^n$. For any given (V, ϕ) with $(\phi \curvearrowright V) \simeq H$, the number of ψ satisfying the above conditions is equal to the number of matrices of the form

$$\begin{bmatrix} H & B \\ 0 & C \end{bmatrix},$$

where H also means the $h \times h$ rational canonical form of the $\mathbb{F}_q[t]$-module H, already fixed, while B is any $h \times (n-h)$ matrix and $C \in \mathrm{Mat}_{n-h}(\mathbb{F}_q)$ such that $P_1(C) \cdots P_r(C) \in \mathrm{GL}_{n-h}(\mathbb{F}_q)$. The number of such matrices is

$$q^{h(n-h)} \left| \left\{ C \in \mathrm{Mat}_{n-h}(\mathbb{F}_q) : C[P_j^\infty] = 0 \text{ for } 1 \le j \le r \right\} \right|.$$

It remains to count the number of (V, ϕ) described above. Given any $\mathbb{F}_q$-linear injection $\alpha : H \hookrightarrow \mathbb{F}_q^n$, we may get such a pair by taking $V = \alpha(H)$ and $\phi = \alpha t \alpha^{-1}|_V$, where t here means the $\mathbb{F}_q$-linear endomorphism of H given by the action of t. Every pair (V, ϕ) with $(\phi \curvearrowright V) \simeq H = (t \curvearrowright H)$ arises this way, and any two $\alpha, \beta \in \mathrm{Inj}_{\mathbb{F}_q}(H, \mathbb{F}_q^n)$ give rise to the same pair precisely when

- $\alpha(H) = \beta(H)$ (so that we call it V) and
- $\alpha t \alpha^{-1}|_V = \beta t \beta^{-1}|_V$.

The second condition can be restated as $\alpha^{-1}|_V \beta \in \mathrm{Aut}_{\mathbb{F}_q[t]}(H)$. By taking $\eta = \alpha^{-1}|_V \beta$, we see that $\alpha, \beta \in \mathrm{Inj}_{\mathbb{F}_q}(H, \mathbb{F}_q^n)$ give the same pair (V, ϕ) if and only if there is $\eta \in \mathrm{Aut}_{\mathbb{F}_q[t]}(H)$ such that $\beta = \alpha\eta$. Thus, the set $\mathrm{Inj}_{\mathbb{F}_q}(H, \mathbb{F}_q^n)/\mathrm{Aut}_{\mathbb{F}_q[t]}(H)$ of orbits under the right action $\mathrm{Inj}_{\mathbb{F}_q}(H, \mathbb{F}_q^n) \circlearrowleft \mathrm{Aut}_{\mathbb{F}_q[t]}(H)$, given by the pre-composition, parametrizes the pairs (V, ϕ) such that V is an h-dimensional subspace of $\mathbb{F}_q^n$ and $(\phi \curvearrowright V) \simeq H$. This is a free action, so by Burnside's lemma, we have

$$\begin{aligned} \left| \mathrm{Inj}_{\mathbb{F}_q}(H, \mathbb{F}_q^n)/\mathrm{Aut}_{\mathbb{F}_q[t]}(H) \right| &= \frac{|\mathrm{Inj}_{\mathbb{F}_q}(H, \mathbb{F}_q^n)|}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H)|} \\ &= \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H)|}(q^n - 1)(q^n - q) \cdots (q^n - q^{h-1}) \end{aligned}$$

because we have assumed that $n \ge h$. Combining altogether, we have

$$\begin{aligned} &\left| \left\{ \begin{matrix} A \in \mathrm{Mat}_n(\mathbb{F}_q) : \\ A[P_j^\infty] = H_j \text{ for } 1 \le j \le r \end{matrix} \right\} \right| \\ &\quad = \frac{q^{h(n-h)}(q^n - 1)(q^n - q) \cdots (q^n - q^{h-1})}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H)|} \left| \left\{ \begin{matrix} C \in \mathrm{Mat}_{n-h}(\mathbb{F}_q) : \\ C[P_j^\infty] = 0 \text{ for } 1 \le j \le r \end{matrix} \right\} \right|. \end{aligned}$$

Dividing by $q^{n^2} = |\operatorname{Mat}_n(\mathbb{F}_q)|$, we get

$$\begin{aligned}
&\operatorname{Prob}_{A\in\operatorname{Mat}_n(\mathbb{F}_q)}\begin{pmatrix} A[P_j^\infty] = H_j \\ \text{for } 1\le j\le r\end{pmatrix} \\
&\quad= \frac{q^{-(n-h)(n-h)}\prod_{i=n-h+1}^{n}(1-q^{-i})}{|\operatorname{Aut}_{\mathbb{F}_q[t]}(H)|}\left|\begin{Bmatrix} C\in\operatorname{Mat}_{n-h}(\mathbb{F}_q): \\ C[P_j^\infty]=0 \text{ for } 1\le j\le r\end{Bmatrix}\right| \\
&\quad= \frac{\prod_{i=n-h+1}^{n}(1-q^{-i})}{|\operatorname{Aut}_{\mathbb{F}_q[t]}(H)|}\operatorname{Prob}_{C\in\operatorname{Mat}_{n-h}(\mathbb{F}_q)}\begin{pmatrix} C[P_j^\infty]=0 \\ \text{for } 1\le j\le r\end{pmatrix}.
\end{aligned}$$

Since $\operatorname{Aut}_{\mathbb{F}_q[t]}(H)\simeq\operatorname{Aut}_{\mathbb{F}_q[t]}(H_1)\times\cdots\times\operatorname{Aut}_{\mathbb{F}_q[t]}(H_r)$, this finishes the proof. □

7. Useful lemmas for Theorems 2.8 and 2.10

Our main tool in proving Theorems 2.8 and 2.10 is a generating function that encodes information about similarity classes in $\operatorname{Mat}_n(\mathbb{F}_q)$.

7.1. Cycle index

Every matrix $A\in\operatorname{Mat}_n(\mathbb{F}_q)$ gives rise to an $\mathbb{F}_q[t]$-module structure on $\mathbb{F}_q^n$, and up to an $\mathbb{F}_q[t]$-isomorphism, it is

$$H_{P_1,\lambda^{(1)}}\oplus\cdots\oplus H_{P_r,\lambda^{(r)}},$$

where $P_i(t)\in\mathbb{F}_q[t]$ are monic irreducible polynomials and $\lambda^{(i)}=(\lambda_1^{(i)},\dots,\lambda_{l_i}^{(i)})$ are nonempty partitions with

$$H_{P_i,\lambda^{(i)}} := \mathbb{F}_q[t]/\big(P_i(t)^{\lambda_{i,1}}\big)\oplus\cdots\oplus\mathbb{F}_q[t]/\big(P_i(t)^{\lambda_{i,l_i}}\big)$$

as long as $n\ge 1$. For $n=0$, we have $r=0$, corresponding to the empty partition, and this is consistent with the fact that we have only the zero module for this case. Up to a permutation, these $H_{P_i,\lambda^{(i)}}$ characterize the similarity class of A. For any monic irreducible $P=P(t)\in\mathbb{F}_q[t]$, we denote by $\mu_P(A)$ the partition associated to the P-part of A or equivalently to the isomorphism class of the $\mathbb{F}_q[t]$-module $A\curvearrowright\mathbb{F}_q^n$. More specifically, with the above notation, we have

$$\mu_{P_i}(A)=\lambda^{(i)}=(\lambda_1^{(i)},\dots,\lambda_{l_i}^{(i)})$$

and $\mu_P(A)=\emptyset$ when $P\ne P_i$ for all i. We write $|\mathbb{A}^1_{\mathbb{F}_q}|$ to mean the set of all monic irreducible polynomials in $\mathbb{F}_q[t]$. As the notation suggests, $|\mathbb{A}^1_{\mathbb{F}_q}|$ can be seen as the set of closed points of the affine line $\mathbb{A}^1_{\mathbb{F}_q}=\operatorname{Spec}(\mathbb{F}_q[t])$ over $\mathbb{F}_q$. For each nonempty partition ν and $P\in|\mathbb{A}^1_{\mathbb{F}_q}|$, we consider a unique formal variable $x_{P,\nu}$. For the empty partition $\emptyset$, we put $x_{P,\emptyset}:=1$. As in Section 2, we write $\mathcal{P}$ to mean the set of all partitions of non-negative integers, where the only partition for 0 is $\emptyset$.

From the structure theorem about finitely generated modules over $\mathbb{F}_q[t]$, which is a PID, and the Chinese remainder theorem, we note that for any two matrices $A,B\in$

$\mathrm{Mat}_n(\mathbb{F}_q)$, the following are equivalent:

(1) A and B are similar;
(2) A and B are in the same orbit under the conjugate action $\mathrm{GL}_n(\mathbb{F}_q) \curvearrowright \mathrm{Mat}_n(\mathbb{F}_q)$;
(3) A and B give the isomorphic $\mathbb{F}_q[t]$-module structures on $\mathbb{F}_q^n$;
(4) $\mu_P(A) = \mu_P(B)$ for all $P \in |\mathbb{A}^1_{\mathbb{F}_q}|$;
(5) $\prod_{P\in|\mathbb{A}^1_{\mathbb{F}_q}|} x_{P,\mu_P(A)} = \prod_{P\in|\mathbb{A}^1_{\mathbb{F}_q}|} x_{P,\mu_P(B)}$.

We define the n**th cycle index of the conjugate action** $\mathrm{GL}_n(\mathbb{F}_q) \curvearrowright \mathrm{Mat}_n(\mathbb{F}_q)$ to be the polynomial

$$\mathcal{Z}\big(\mathrm{Mat}_n(\mathbb{F}_q), \boldsymbol{x}\big) := \frac{1}{|\mathrm{GL}_n(\mathbb{F}_q)|} \sum_{A\in\mathrm{Mat}_n(\mathbb{F}_q)} \prod_{P\in|\mathbb{A}^1_{\mathbb{F}_q}|} x_{P,\mu_P(A)} \in \mathbb{Q}[\boldsymbol{x}],$$

where $\boldsymbol{x} := (x_{P,\nu})$ is the sequence of formal variables $x_{P,\nu}$. We define the n**th cycle index of the group** $\mathrm{GL}_n(\mathbb{F}_q)$ by the analogous definition for the restricted conjugation action $\mathrm{GL}_n(\mathbb{F}_q) \curvearrowright \mathrm{GL}_n(\mathbb{F}_q)$:

$$\mathcal{Z}\big(\mathrm{GL}_n(\mathbb{F}_q), \boldsymbol{x}\big) := \frac{1}{|\mathrm{GL}_n(\mathbb{F}_q)|} \sum_{A\in\mathrm{GL}_n(\mathbb{F}_q)} \prod_{P\in|\mathbb{A}^1_{\mathbb{F}_q}|} x_{P,\mu_P(A)} \in \mathbb{Q}[\boldsymbol{x}].$$

Notice that the irreducible polynomial $P(t) = t$ will not occur in the product above because for any $A \in \mathrm{Mat}_n(\mathbb{F}_q)$, saying that $A \in \mathrm{GL}_n(\mathbb{F}_q)$ is equivalent to saying $\mu_t(A) = \emptyset$ (i.e., A has no t-part).

7.2. Useful lemmas

We will introduce three lemmas useful for proving Theorems 2.8 and 2.10. The first one is due to Stong, who introduced the cycle index of the conjugate action $\mathrm{GL}_n(\mathbb{F}_q) \curvearrowright \mathrm{Mat}_n(\mathbb{F}_q)$.

LEMMA 7.1 ([16, Lemma 1])
We have

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

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

The result above proves the following lemma due to Kung, who introduced the cycle index of $\mathrm{GL}_n(\mathbb{F}_q)$.

LEMMA 7.2 ([10, Lemma 1])
We have

$$\sum_{n=0}^{\infty} \mathcal{Z}\big(\mathrm{GL}_n(\mathbb{F}_q), \boldsymbol{x}\big)u^n = \sum_{n=0}^{\infty} \sum_{A \in \mathrm{GL}_n(\mathbb{F}_q)} \Big(\frac{\prod_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} x_{P,\mu_P(A)}}{|\mathrm{GL}_n(\mathbb{F}_q)|}\Big)u^n$$

$$= \prod_{\substack{P \in |\mathbb{A}^1_{\mathbb{F}_q}|, \\ P(t) \neq t}} \sum_{\nu \in \mathcal{P}} \frac{x_{P,\nu} u^{|\nu| \deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|}$$

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

Proof
If we take $x_{t,\nu} = 0$ for all nonempty partitions ν in the expression

$$\mathcal{Z}\big(\mathrm{Mat}_n(\mathbb{F}_q), \boldsymbol{x}\big) = \frac{1}{|\mathrm{GL}_n(\mathbb{F}_q)|} \sum_{A \in \mathrm{Mat}_n(\mathbb{F}_q)} \prod_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} x_{P,\mu_P(A)},$$

we get $\mathcal{Z}(\mathrm{GL}_n(\mathbb{F}_q), \boldsymbol{x})$ because any square matrix is invertible if and only if it does not have 0 eigenvalue (or equivalently, if it does not have any invariant factor divisible by t). Thus, Lemma 7.1 implies the result. □

The following is the third lemma we need, due to Stong. This lemma serves a crucial role in the proofs of Theorems 2.8 and 2.10. Stong's proof relies on the fact that there are $q^{n(n-1)}$ nilpotent matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$, a famous result of Fine and Herstein [4].

LEMMA 7.3 ([16, Proposition 19])
For any $P \in |\mathbb{A}^1_{\mathbb{F}_q}|$, *we have*

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

REMARK 7.4
Using [12, (1.6), p. 181], Lemma 7.3 implies that for any DVR $(R, \mathfrak{m})$ with $R/\mathfrak{m} = \mathbb{F}_q$, we have

$$\sum_{H \in \mathbf{Mod}_R^{<\infty}} \frac{y^{\dim_{\mathbb{F}_q}(H)}}{|\mathrm{Aut}_R(H)|} = \prod_{i=1}^{\infty} \frac{1}{1 - q^{-i} y} \in \mathbb{Q}[\![y]\!].$$

Hence, taking $y = 1$, this proves that the assignment $\{H\} \mapsto |\mathrm{Aut}_R(H)|^{-1} \times \prod_{i=1}^{\infty}(1 - q^{-i})$ is indeed a probability measure on $\mathbf{Mod}_R^{<\infty}$.

8. Proofs of Theorems 2.8 and 2.10

In this section, we provide proofs of Theorems 2.8 and 2.10. By the results of Section 5, this will finish the proofs of Theorems A, B, and C.

8.1. Proof of Theorem 2.8

We first deal with the sequence $(b_n(d))_{n\in\mathbb{Z}_{\geq 0}}$ appearing in Theorem A and Theorem 2.8 as well as some convergences of relevant infinite products of formal power series. Such a product needs to be treated with care because its expansion leads to a power series whose coefficients are given by infinite sums.

First, fix $0 \leq t < 1$. The sequence

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

is decreasing in n, while it is bounded below by 0. Thus, the sequence converges in $\mathbb{R}$. Since $0 \leq t < 1$, an application of [15, Theorem 15.4] ensures that the limit of this product as $n \to \infty$ is nonzero. In particular, taking $t = q^{-1}$, we see $\prod_{i=1}^{\infty}(1-q^{-i}) > 0$ makes sense, and so does

$$\prod_{i=1}^{\infty}\frac{1-q^{-di}}{1-q^{-i}} := \frac{\prod_{i=1}^{\infty}(1-q^{-di})}{\prod_{i=1}^{\infty}(1-q^{-i})}$$

for any $d \in \mathbb{Z}_{\geq 1}$. The power series $\sum_{i=1}^{\infty} q^{-i}u$ has radius of convergence q at $u = 0$. Hence, by taking $f_i(u) = 1 - q^{-i}u$ in [15, Theorem 15.6], we see that the product

$$\prod_{i=1}^{\infty} f_i(u) = \prod_{i=1}^{\infty}(1-q^{-i}u)$$

converges uniformly on any compact subsets of $\{u \in \mathbb{C} : |u| < q\}$. The power series $\sum_{i=1}^{\infty} q^{-di}u^d$ also has radius of convergence q at $u = 0$, so we may apply the same theorem to deduce that the product

$$\prod_{i=1}^{\infty}\left(1-(q^{-i}u)^d\right)$$

converges uniformly on any compact subsets of $\{u \in \mathbb{C} : |u| < q\}$. This implies that both products are holomorphic in $\{u \in \mathbb{C} : |u| < q\}$, and hence so is their ratio (as none of them vanishes in the specified open disc of $\mathbb{C}$ with radius q). Thus, we may rewrite it as a power series

$$\prod_{i=1}^{\infty}\frac{1-(q^{-i}u)^d}{1-q^{-i}u} = a_0(d) + a_1(d)u + a_2(d)u^2 + \cdots,$$

whose radius of convergence is q at $u = 0$. Thus, we can evaluate both sides at $u = 1 < q$ to have

$$\prod_{i=1}^{\infty}\frac{1-q^{-id}}{1-q^{-i}} = a_0(d) + a_1(d) + a_2(d) + \cdots.$$

Since the only holomorphic function in the open disc with a limit point in its zero set (in the open disc) must be the zero function, we must have the same identity

$$\prod_{i=1}^{\infty}\frac{1-(q^{-i}u)^d}{1-q^{-i}u} = a_0(d) + a_1(d)u + a_2(d)u^2 + \cdots$$

in $\mathbb{C}[\![u]\!]$ as well, where we take u to be formal. Therefore, in $\mathbb{C}[\![u]\!]$, we have

$$\begin{aligned} &b_0(d) + b_1(d)u + b_2(d)u^2 + \cdots \\ &\quad = \frac{1}{1-u} \prod_{i=1}^{\infty} \frac{1-(q^{-i}u)^d}{1-q^{-i}u} \\ &\quad = (1+u+u^2+\cdots)\big(a_0(d) + a_1(d)u + a_2(d)u^2 + \cdots\big) \\ &\quad = a_0(d) + \big(a_0(d)+a_1(d)\big)u + \big(a_0(d)+a_1(d)+a_2(d)\big)u^2 + \cdots. \end{aligned}$$

This implies that $b_n(d) = a_0(d) + a_1(d) + \cdots + a_n(d)$, so

$$\lim_{n\to\infty} b_n(d) = a_0(d) + a_1(d) + \cdots = \prod_{i=1}^{\infty} \frac{1-q^{-id}}{1-q^{-i}},$$

and this proves the last parts of Theorem A and Theorem 2.8. Thus, we need only to show the statement of Theorem 2.8 before we take the limit $n \to \infty$ to finish its proof.

Proof of Theorem 2.8
In this proof, we will denote the polynomial P in the statement by P_0 instead. We may assume that

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

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

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

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 7.1, which leads to

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

where we applied Lemma 7.2, with the evaluations $x_{P,\nu} = 1$, which gives

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

and Lemma 7.3 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 A and Theorem 2.8.

Now, we may assume that the partition $\lambda = (\lambda_1, \ldots, \lambda_l)$ is nonempty (i.e., $l > 0$). We again recall that $x_{P,\emptyset} = 1$ by our definition. In Lemma 7.1, take $x_{P,\nu} = 1$ on both sides for $P \neq P_0$ to get

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

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

$$1 + \sum_{n=1}^{\infty} \Big(\frac{|\{A \in \mathrm{Mat}_n(\mathbb{F}_q) : \mu_{P_0}(A) = \lambda \text{ or } \emptyset\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} \Big) u^n$$
$$= \Big(1 + \frac{u^{|\lambda| \deg(P_0)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\lambda})|} \Big) \Big(\prod_{P \neq P_0} \sum_{\nu \in \mathcal{P}} \frac{u^{|\nu| \deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|} \Big)$$
$$= \Big(1 + \frac{u^{|\lambda| \deg(P_0)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\lambda})|} \Big) \Big(\prod_{P \in |\mathbb{A}^1_{\mathbb{F}_q}|} \sum_{\nu \in \mathcal{P}} \frac{u^{|\nu| \deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|} \Big)$$
$$\times \Big(\sum_{\nu \in \mathcal{P}} \frac{u^{|\nu| \deg(P_0)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\nu})|} \Big)^{-1}$$
$$= \Big(1 + \frac{u^{|\lambda| \deg(P_0)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\lambda})|} \Big) \Big(\prod_{P(t) \neq t} \sum_{\nu \in \mathcal{P}} \frac{u^{|\nu| \deg(P)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P,\nu})|} \Big)$$
$$\times \Big(\sum_{\nu \in \mathcal{P}} \frac{u^{|\nu|}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{(t),\nu})|} \Big) \Big(\sum_{\nu \in \mathcal{P}} \frac{u^{|\nu| \deg(P_0)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\nu})|} \Big)^{-1}$$
$$= \Big(1 + \frac{u^{|\lambda| \deg(P_0)}}{|\mathrm{Aut}_{\mathbb{F}_q[t]}(H_{P_0,\lambda})|} \Big) \Big(\frac{1}{1-u} \Big) \Big(\prod_{i=1}^{\infty} \frac{1 - (q^{-i}u)^{\deg(P_0)}}{1 - q^{-i}u} \Big),$$

applying Lemma 7.2 (again with the evaluations $x_{P,\nu} = 1$) and Lemma 7.3. Thus, we have

$$1 + \sum_{n=1}^{\infty} \Big(\frac{|\{A \in \mathrm{Mat}_n(\mathbb{F}_q) : \mu_{P_0}(A) = \lambda \text{ or } \emptyset\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} \Big) u^n$$
$$= (1 + cu^h)(1 + b_1 u + b_2 u^2 + b_3 u^3 + \cdots)$$

$$= 1 + b_1 u + b_2 u + \cdots + b_{h-1} u^{h-1} + (b_h + c) u^h + (b_{h+1} + c b_1) u^{h+1} + (b_{h+2} + c b_2) u^{h+2} + \cdots,$$

where

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

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

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

we have (as $b_0 = 1$)

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

By multiplying both sides by

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

we finish the proof. □

8.2. Proof of Theorem 2.10

Before the proof, we give some definitions that will enable us to write a clearer proof. Fix any subset $X \subset \mathbb{A}^1_{\mathbb{F}_q} = \operatorname{Spec}(\mathbb{F}_q[t])$. We define the **cycle index of** X (**relative to** $\mathbb{A}^1_{\mathbb{F}_q}$) as follows:

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

where each $P \in |\mathbb{A}^1_{\mathbb{F}_q}|$ simultaneously means a monic irreducible polynomial or the maximal ideal $(P(t))$ of $\mathbb{F}_q[t]$ generated by it (i.e., a closed point of $\mathbb{A}^1_{\mathbb{F}_q}$). Note that by Lemma 7.1, we have

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

That is, the cycle index of the affine line $\mathbb{A}^1_{\mathbb{F}_q}$ is the generating function for the nth cycle index of the conjugate action $\operatorname{GL}_n(\mathbb{F}_q) \curvearrowright \operatorname{Mat}_n(\mathbb{F}_q)$ for all $n \in \mathbb{Z}_{\geq 0}$. Another important example is

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

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

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

Denote by $\hat{\boldsymbol{Z}}(X, u)$ what we get by taking all $x_{P,\nu} = 1$ in $\hat{\boldsymbol{Z}}(X, \boldsymbol{x}, u)$. Lemma 7.2 implies that

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

Finally, Lemma 7.3 implies that for any $P \in |\mathbb{A}^1_{\mathbb{F}_q}|$, we have

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

We are now ready to give the proof of Theorem 2.10.

Proof of Theorem 2.10
We will use the notations and the arguments 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

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

Without loss of generality, suppose that $\lambda^{(1)}, \dots, \lambda^{(m)}$ are nonempty, while $\lambda^{(m+1)}, \dots, \lambda^{(r)} = \emptyset$, for some $0 \le m \le r$. 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 $1 \le j \le m$. We will still write $\boldsymbol{x}$ to mean the sequence of variables after evaluations, although this is now just a sequence in $\{0, 1\}$. Arguing as in Section 8.1, 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

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

we have

$$\begin{aligned}
&\lim_{n \to \infty} \operatorname{Prob}_{A \in \operatorname{Mat}_n(\mathbb{F}_q)} \begin{pmatrix} \mu_{P_j}(A) \in \{\emptyset, \lambda^{(j)}\} \text{ for } 1 \le j \le m, \\ \mu_{P_{m+1}}(A) = \cdots = \mu_{P_r}(A) = \emptyset \end{pmatrix} \\
&\quad = \frac{\hat{\boldsymbol{Z}}(\{P_1\}, \boldsymbol{x}, 1) \cdots \hat{\boldsymbol{Z}}(\{P_r\}, \boldsymbol{x}, 1)}{\hat{\boldsymbol{Z}}(\{P_1\}, 1) \cdots \hat{\boldsymbol{Z}}(\{P_r\}, 1)}
\end{aligned}$$

$$= \Big[\prod_{j=1}^{m}\Big(1+\frac{1}{|\operatorname{Aut}_{\mathbb{F}_q}(H_{P,\lambda^{(j)}})|}\Big)\prod_{i=1}^{\infty}(1-q^{-i\deg(P_j)})\Big]$$

$$\cdot\Big[\prod_{j=m+1}^{r}\prod_{i=1}^{\infty}(1-q^{-i\deg(P_j)})\Big].$$

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

$$P(\nu^{(1)},\ldots,\nu^{(m)}) := \lim_{n\to\infty} \operatorname{Prob}_{A\in\operatorname{Mat}_n(\mathbb{F}_q)}\begin{pmatrix}\mu_{P_j}(A)=\nu^{(j)} \text{ for } 1\leq j\leq m,\\ \mu_{P_{m+1}}(A)=\cdots=\mu_{P_r}(A)=\emptyset\end{pmatrix},$$

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

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

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

$$\sum_{\substack{\nu^{(1)},\ldots,\nu^{(m)}:\\ \nu^{(j)}\in\{\emptyset,\lambda^{(j)}\}\\ \text{for } 1\leq j\leq m}} P(\nu^{(1)},\ldots,\nu^{(m)})$$

$$= \Big[\prod_{j=1}^{m}\Big(1+\frac{1}{|\operatorname{Aut}_{\mathbb{F}_q}(H_{P,\lambda^{(j)}})|}\Big)\prod_{i=1}^{\infty}(1-q^{-i\deg(P_j)})\Big]$$

$$\cdot\Big[\prod_{j=m+1}^{r}\prod_{i=1}^{\infty}(1-q^{-i\deg(P_j)})\Big],$$

so

$$P(\lambda^{(1)},\ldots,\lambda^{(m)}) = \sum_{\substack{\nu^{(1)},\ldots,\nu^{(m)}:\\ \nu^{(j)}\in\{\emptyset,\lambda^{(j)}\}\\ \text{for } 1\leq j\leq m}} P(\nu^{(1)},\ldots,\nu^{(m)})$$

$$- \sum_{\substack{\nu^{(1)},\ldots,\nu^{(m)}:\\ \nu^{(j)}\in\{\emptyset,\lambda^{(j)}\}\\ \text{for } 1\leq j\leq m,\\ \text{not all } \nu^{(j)} \text{ are } \lambda^{(j)}}} P(\nu^{(1)},\ldots,\nu^{(m)})$$

$$= \Big[\prod_{j=1}^{m}\Big(1+\frac{1}{|\operatorname{Aut}_{\mathbb{F}_q}(H_{P,\lambda^{(j)}})|}\Big)\prod_{i=1}^{\infty}(1-q^{-i\deg(P_j)})\Big]$$

$$\cdot\Big[\prod_{j=m+1}^{r}\prod_{i=1}^{\infty}(1-q^{-i\deg(P_j)})\Big]$$

$$- \sum_{\substack{\nu^{(1)},\dots,\nu^{(m)}: \\ \nu^{(j)} \in \{\emptyset, \lambda^{(j)}\} \\ \text{for } 1 \le j \le m, \\ \text{not all } \nu^{(j)} \text{ are } \lambda^{(j)}}} P(\nu^{(1)}, \dots, \nu^{(m)})$$

$$= \prod_{j=1}^{r} \frac{1}{|\operatorname{Aut}_{\mathbb{F}_q}(H_{P,\lambda^{(j)}})|} \prod_{i=1}^{\infty} (1 - q^{-i \deg(P_j)}),$$

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. □

Acknowledgments. We would like to thank our advisor Michael Zieve for various supports, including the financial support for relevant travel through NSF grant DMS-1162181 for Cheong and DMS-1601844 for Huang. We thank Karen Smith and the University of Michigan, for nominating and granting Rackham one-term dissertation fellowships to both of us. Huang thanks Gopal Prasad for the Prasad Family Fellowship. Cheong was supported by the University of Michigan and the University of California–Irvine for travel relevant to this work. We thank Sasha Barvinok, Kwun Chung, Ofir Gorodetsky, Mel Hochster, Zhan Jiang, Hendrik Lenstra, Eric Rains, and Brad Rodgers for helpful conversations. We thank Jordan Ellenberg for bringing our attention to [19]. We deeply appreciate Jason Fulman, Haoyang Guo, Nathan Kaplan, Jeff Lagarias, Yuan Liu, and Melanie Matchett Wood for constructive advice regarding previous drafts of this paper. Finally, we would like to thank the referee, who devoted much time and effort in reading our paper in the finest details, for extremely thorough and insightful comments.

References

[1] I. Boreico, Statistics of random integral matrices, Ph.D. dissertation, Stanford University, 2016. MR 4172218.

[2] H. Cohen and H. W. Lenstra Jr., "Heuristics on class groups of number fields" in *Number Theory, Noordwijkerhout 1983, (Noordwijkerhout, 1983)*, Lecture Notes Math. **1068** Springer, Berlin, 33–62. MR 0756082. DOI 10.1007/BFb0099440.

[3] J. S. Ellenberg, A. Venkatesh, and C. Westerland, *Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields*, Ann. of Math. (2) **183** (2016), no. 3, 729–786. MR 3488737. DOI 10.4007/annals.2016.183.3.1.

[4] N. J. Fine and I. N. Herstein, *The probability that a matrix be nilpotent*, Illinois J. Math. **2** (1958), no. 4A, 499–504. MR 0096677.

[5] J. Fulman, Probability in the classical groups over finite fields: Symmetric functions, stochastic algorithms and cycle indices, Ph.D. dissertation, Harvard University, 1997. MR 2695900.

[6] J. Fulman, *Random matrix theory over finite fields*, Bull. Amer. Math. Soc. (N.S.) **39** (2001), no. 1, 51–85. MR 1864086. DOI 10.1090/S0273-0979-01-00920-X.

[7] J. Fulman, *Cohen–Lenstra heuristics and random matrix theory over finite fields*, J. Group Theory **17** (2014), no. 4, 619–648. MR 3228936. DOI 10.1515/jgt-2014-0005.

[8] J. Fulman and N. Kaplan, *Random partitions and Cohen–Lenstra heuristics*, Ann. Comb. **23** (2019), no. 2, 295–315. MR 3962859. DOI 10.1007/s00026-019-00425-y.

[9] E. Friedman and L. C. Washington, "On the distribution of divisor class groups of curves over a finite field" in *Théorie des Nombres (Quebec, PQ, 1987)*, de Gruyter, Berlin, 1989, 227–239. MR 1024565.

[10] J. Kung, *The cycle structure of a linear transformation over a finite field*, Linear Algebra Appl. **36** (1981), 141–155. MR 0604337. DOI 10.1016/0024-3795(81)90227-5.

[11] J. Lengler, *The Cohen–Lenstra heuristic: Methodology and results*, J. Algebra **323** (2010), no. 10, 2960–2976. MR 2609186. DOI 10.1016/j.jalgebra.2010.01.016.

[12] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, 2nd ed., Oxford Math. Monogr., Oxford Univ. Press, New York, 1995. MR 1354144.

[13] J. S. Milne, *Abelian Varieties*, https://www.jmilne.org/math/CourseNotes, 2008.

[14] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. **322**, Springer, Berlin, 1999. MR 1697859. DOI 10.1007/978-3-662-03983-0.

[15] W. Rudin, *Real and Complex Analysis*, 3rd ed., McGraw-Hill, New York, 1987. MR 0924157.

[16] R. Stong, *Some asymptotic results on finite vector spaces*, Adv. in Appl. Math. **9** (1988), no. 2, 167–199. MR 0937520. DOI 10.1016/0196-8858(88)90012-7.

[17] L. C. Washington, *Some remarks on Cohen–Lenstra heuristics*, Math. Comp. **47** (1986), no. 176, 741–747. MR 0856717. DOI 10.2307/2008187.

[18] M. W. Wood, *The distribution of sandpile groups of random graphs*, J. Amer. Math. Soc, **30** (2017), no. 4, 915–958. MR 3671933. DOI 10.1090/jams/866.

[19] M. W. Wood, *Random integral matrices and the Cohen–Lenstra heuristics*, Amer. J. Math. **141** (2019), no. 2, 383–398. MR 3928040. DOI 10.1353/ajm.2019.0008.

Cheong: Department of Mathematics, University of Michigan, Ann Arbor, Michicgan, USA; gcheong@umich.edu

Huang: Department of Mathematics, University of Michigan, Ann Arbor, Michigan, USA; huangyf@umich.edu