Generalizations of results of Friedman and Washington on cokernels of random p-adic matrices

Gilyoung Cheong, Nathan Kaplan [*]

Department of Mathematics, University of California, Irvine, 340 Rowland Hall, Irvine, CA 92697, United States of America

A R T I C L E   I N F O

A B S T R A C T

Let p be prime and X be a Haar-random $n \times n$ matrix over $\mathbb{Z}_p$, the ring of p-adic integers. Let $P_1(t), \dots, P_l(t) \in \mathbb{Z}_p[t]$ be monic polynomials of degree at most 2 whose images modulo p are distinct and irreducible in $\mathbb{F}_p[t]$, where $\mathbb{F}_p$ denotes the finite field of p elements. For each j, let G_j be a finite module over $\mathbb{Z}_p[t]/(P_j(t))$. We show that as n goes to infinity, the probabilities that $\mathrm{cok}(P_j(X)) \simeq G_j$ are independent, and each probability can be described in terms of a Cohen–Lenstra distribution. We also show that for any fixed n, the probability that $\mathrm{cok}(P_j(X)) \simeq G_j$ for each j is a constant multiple of the probability that $\mathrm{cok}(P_j(\bar{X})) \simeq G_j/pG_j$ for each j, where $\bar{X}$ is an $n \times n$ uniformly random matrix over $\mathbb{F}_p$. These results generalize work of Friedman and Washington and prove new cases of a conjecture of Cheong and Huang.

© 2022 Elsevier Inc. All rights reserved.

1. Introduction

Throughout this paper, let p be a prime. For a commutative ring R, let $\mathrm{Mat}_n(R)$ denote the set of $n \times n$ matrices with entries in R and let I_n denote the $n \times n$ iden-

[*] Corresponding author.
E-mail addresses: gilyounc@uci.edu (G. Cheong), nckaplan@math.uci.edu (N. Kaplan).

tity matrix. The Haar measure on the additive group $\mathrm{Mat}_n(\mathbb{Z}_p) = \mathbb{Z}_p^{n^2}$, with respect to its compact p-adic topology, allows one to choose a random matrix $X \in \mathrm{Mat}_n(\mathbb{Z}_p)$. Let $\mathrm{cok}(X)$ denote the cokernel of X. In [5], Friedman and Washington proved that the probability that $\mathrm{cok}(X)$ is isomorphic to a fixed finite abelian p-group G converges to $|\mathrm{Aut}(G)|^{-1} \prod_{i=1}^{\infty}(1 - p^{-i})$ as $n \to \infty$. In particular, this probability is inversely proportional to the size of the automorphism group of G. For odd p, this probability is the one given in an influential conjecture of Cohen and Lenstra on the distribution of p-parts of class groups of imaginary quadratic fields, first introduced in [2]. Motivated by function field analogues of the Cohen–Lenstra conjecture, Friedman and Washington also proved that

$$\lim_{n \to \infty} \operatorname*{Prob}_{X \in \mathrm{GL}_n(\mathbb{Z}_p)} (\mathrm{cok}(X - I_n) \simeq G) = \frac{1}{|\mathrm{Aut}(G)|} \prod_{i=1}^{\infty}(1 - p^{-i}),$$

that is,

$$\lim_{n \to \infty} \operatorname*{Prob}_{X \in \mathrm{Mat}_n(\mathbb{Z}_p)} \begin{pmatrix} \mathrm{cok}(X) = 0, \\ \mathrm{cok}(X - I_n) \simeq G \end{pmatrix} =$$

$$\left(\lim_{n \to \infty} \operatorname*{Prob}_{X \in \mathrm{Mat}_n(\mathbb{Z}_p)} (\mathrm{cok}(X) = 0) \right) \left(\lim_{n \to \infty} \operatorname*{Prob}_{X \in \mathrm{Mat}_n(\mathbb{Z}_p)} (\mathrm{cok}(X - I_n) \simeq G) \right).$$

Our first main theorem is a generalization of these results. For a commutative ring R and an R-module G, let $\mathrm{Aut}_R(G)$ denote the group of R-linear automorphisms of G.

Theorem 1.1. *Let $P_1(t), \ldots, P_l(t) \in \mathbb{Z}_p[t]$ be monic polynomials of degree at most 2 whose images modulo p are distinct and irreducible in $\mathbb{F}_p[t]$. For each j, let G_j be a finite module over $\mathbb{Z}_p[t]/(P_j(t))$. We have*

$$\lim_{n \to \infty} \operatorname*{Prob}_{X \in \mathrm{Mat}_n(\mathbb{Z}_p)} \begin{pmatrix} \mathrm{cok}(P_j(X)) \simeq G_j \\ \text{for } 1 \leqslant j \leqslant l \end{pmatrix}$$

$$= \prod_{j=1}^{l} \frac{1}{|\mathrm{Aut}_{\mathbb{Z}_p[t]/(P_j(t))}(G_j)|} \left(\prod_{i=1}^{\infty} \left(1 - p^{-i \deg(P_j)} \right) \right).$$

There are explicit formulas for the sizes of the automorphism groups appearing in this result. We give one such formula in Lemma 3.7 and another in the discussion directly following it.

Theorem 1.1 may be surprising to the reader because if we take $l = 2$ with $P_1(t) = t$ and $P_2(t) = t - 1$, then for any n, many events regarding the matrices $P_1(X) = X$ and $P_2(X) = X - I_n$ are dependent as the entries of X completely determine the entries of $X - I_n$ and vice versa. Nevertheless, Theorem 1.1 shows that, for example, the event $\mathrm{cok}(X) \simeq \mathbb{Z}/p\mathbb{Z}$ becomes independent from the event $\mathrm{cok}(X - I_n) \simeq \mathbb{Z}/p\mathbb{Z}$ as $n \to \infty$. Theorem 1.1 also proves many new cases of a conjecture of Cheong and Huang [1,

Conjecture 2.3]. We note that the conjecture needs to be slightly modified from their version, as explained below. In [1, Theorem C], Cheong and Huang proved Theorem 1.1 when $G_1 = \cdots = G_{l-1} = 0$ and $\deg(P_l) = 1$, so our result is a significant improvement of theirs.

Conjecture 1.2 *(cf. [1, Conjecture 2.3]). The conclusion of Theorem 1.1 holds without specifying any conditions on the degrees of $P_1(t), \ldots, P_l(t) \in \mathbb{Z}_p[t]$.*

Remark 1.3. Conjecture 1.2 is stated slightly differently in [1, Conjecture 2.3]. In that version, each module G_j over $\mathbb{Z}_p[t]/(P_j(t))$ is only assumed to be a finite abelian p-group. We note that $\mathrm{cok}(P_j(X))$ has a $\mathbb{Z}_p[t]/(P_j(t))$-module structure where the action of $\bar{t}$ is given via left multiplication by X. This implies that some finite abelian p-groups do not arise as $\mathrm{cok}(P_j(X))$ for any X. For example, if $\deg(P_j) > 1$, then $\mathrm{cok}(P_j(\bar{X}))$ is a vector space over $\mathbb{F}_p[t]/(P_j(t))$, so $\dim_{\mathbb{F}_p}(\mathrm{cok}(P_j(\bar{X})))$ is a multiple of $\deg(P_j)$, where $\bar{X} \in \mathrm{Mat}_n(\mathbb{F}_p)$ is the image of X modulo p. Therefore, we see that $\mathrm{cok}(P_j(X))$, considered as a finite abelian p-group, cannot be isomorphic to $\mathbb{Z}/p\mathbb{Z}$. As noted in [1, Remark 2.2] or [2, Example 5.9], there is a *Cohen–Lenstra distribution* on the set of isomorphism classes of finite modules over any DVR whose residue field is finite, that is, a distribution in which each module appears with frequency inversely proportional to its number of automorphisms. One may check that $\mathbb{Z}_p[t]/(P_j(t))$ is indeed a DVR with its unique maximal ideal generated by p and its residue field is isomorphic to $\mathbb{F}_p[t]/(P_j(t))$. We see that Conjecture 1.2 is a natural correction of [1, Conjecture 2.3]. This change affects only Conjecture 2.3 in [1], not any theorems in that paper.

Let G be a finite module over $R = \mathbb{Z}_p[t]/(P_j(t))$. Since R is a PID, we have

$$G \simeq \mathbb{Z}_p[t]/(P_j(t)^{\lambda_1}) \times \cdots \times \mathbb{Z}_p[t]/(P_j(t)^{\lambda_r}),$$

for some partition $\lambda = (\lambda_1, \ldots, \lambda_r)$. In this case we say G has *type* λ. Using this correspondence between finite R-modules and partitions, we can check that any finite R-modules G and G' are isomorphic as modules over R if and only if they are isomorphic as finite abelian p-groups. We will use this observation in our proofs without mentioning it again.

Theorem 1.1 follows from the following stronger result that holds for any fixed $n \in \mathbb{Z}_{\geqslant 1}$, which is also a generalization of a result of Friedman and Washington in [5]. Let $P(t) \in \mathbb{Z}_p[t]$ be a monic polynomial whose reduction modulo p is irreducible in $\mathbb{F}_p[t]$ and let G be a finite module over $\mathbb{Z}_p[t]/(P(t))$. Define

$$r_{p^{\deg(P)}}(G) := \dim_{\mathbb{F}_{p^{\deg(P)}}}(G/pG),$$

where we identify $\mathbb{F}_{p^{\deg(P)}} = \mathbb{F}_p[t]/(P(t))$.

Theorem 1.4. *Let $P_1(t), \ldots, P_l(t) \in \mathbb{Z}_p[t]$ be monic polynomials of degree at most 2 whose images modulo p are distinct and irreducible in $\mathbb{F}_p[t]$ and let $q_j := p^{\deg(P_j)}$. For each j, let G_j be a finite module over $\mathbb{Z}_p[t]/(P_j(t))$. We have*

$$
\operatorname*{Prob}_{X \in \operatorname{Mat}_n(\mathbb{Z}_p)} \left(\begin{array}{c} \operatorname{cok}(P_j(X)) \simeq G_j \\ \text{for } 1 \leqslant j \leqslant l \end{array} \right) =
$$

$$
\left(\prod_{j=1}^{l} \frac{q_j^{r_{q_j}(G_j)^2} \prod_{i=1}^{r_{q_j}(G_j)} (1 - q_j^{-i})^2}{|\operatorname{Aut}_{\mathbb{Z}_p[t]/(P_j(t))}(G_j)|} \right) \operatorname*{Prob}_{\bar{X} \in \operatorname{Mat}_n(\mathbb{F}_p)} \left(\begin{array}{c} \operatorname{cok}(P_j(\bar{X})) \simeq G_j/pG_j \\ \text{for } 1 \leqslant j \leqslant l \end{array} \right).
$$

Remark 1.5. Theorem 1.4 is trivial when $n < \sum_{j=1}^{l} \dim_{\mathbb{F}_p}(G_j/pG_j)$ since each side of the equality is 0. This follows from the discussion of the basics of the $\mathbb{F}_q[t]$-module structure of a matrix $\bar{X} \in \operatorname{Mat}_n(\mathbb{F}_q)$ given at the start of Section 3.3 and the fact that $\operatorname{cok}(P_j(X))$ (mod p) $\simeq \operatorname{cok}(P_j(\bar{X}))$.

Theorem 1.4 follows from the following enumerative result for matrices in $\operatorname{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})$ with a fixed reduction modulo p.

Theorem 1.6. *Assume the notation and hypotheses in Theorem 1.4. Fix any $\bar{X} \in \operatorname{Mat}_n(\mathbb{F}_p)$ such that for each $1 \leqslant j \leqslant l$, we have*

$$
\dim_{\mathbb{F}_{q_j}}\big(\operatorname{cok}(P_j(\bar{X}))\big) = r_{q_j}(G_j).
$$

Choose any $N \in \mathbb{Z}_{\geqslant 0}$ such that $p^N G_j = 0$ for $1 \leqslant j \leqslant l$. Then

$$
\#\left\{ \begin{array}{c} X \in \operatorname{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z}): \\ \operatorname{cok}(P_j(X)) \simeq G_j \\ \text{for } 1 \leqslant j \leqslant l \\ \text{and } X \equiv \bar{X} \pmod{p} \end{array} \right\} = p^{Nn^2} \prod_{j=1}^{l} \frac{q_j^{r_{q_j}(G_j)^2} \prod_{i=1}^{r_{q_j}(G_j)} (1 - q_j^{-i})^2}{|\operatorname{Aut}_{\mathbb{Z}_p[t]/(P_j(t))}(G_j)|}.
$$

In particular, the left-hand side does not depend on the choice of $\bar{X} \in \operatorname{Mat}_n(\mathbb{F}_p)$.

Conjecture 1.7. *The conclusion of Theorem 1.4 holds without specifying any conditions on the degrees of $P_1(t), \ldots, P_l(t)$.*

Conjecture 1.8. *The conclusion of Theorem 1.6 holds without specifying any conditions on the degrees of $P_1(t), \ldots, P_l(t)$.*

Remark 1.9. Conjecture 1.7 implies Conjecture 1.2 in the same way that Theorem 1.4 implies Theorem 1.1, and Conjecture 1.8 implies Conjecture 1.7 in the same way that Theorem 1.6 implies to Theorem 1.4. When this paper was nearly completed, we were surprised during personal communication with Jungin Lee that Conjecture 1.2 can be

proven with a different method. This argument now appears in Lee's preprint [6]. However, Lee does not prove Theorem 1.4 or Theorem 1.6, and Conjectures 1.7 and 1.8 remain open.

Friedman and Washington prove the special case of Theorem 1.6 where $l = 1$ and $\deg(P_1) = 1$. Our proof of Theorem 1.6 is based on theirs but involves additional inputs related to the Smith normal form and the minors of a matrix. We study the conditions on the entries of a matrix over $\mathbb{Z}/p^{N+1}\mathbb{Z}$ that determine whether or not its cokernel is isomorphic to a particular finite module G. We then apply elementary operations for block submatrices, which we summarize in Lemma 3.4, so that we can apply the $l = 1$ case multiple times to prove Theorem 1.6.

There are several approaches to understanding the distribution of $\mathrm{cok}(X)$ for $X \in \mathrm{Mat}_n(\mathbb{Z}_p)$ that have appeared since the original result of Friedman and Washington. One approach that plays a major role in other work on cokernels of families of random p-adic matrices is the method of *moments* where one studies the expected number of surjections from $\mathrm{cok}(X)$ to a fixed finite abelian p-group. See [9], [3, Section 8], and [10,11] for more on this perspective. Evans gives a Markov chain approach to this problem in [4]. Van Peski gives a new approach to this result in his work on cokernels of products of p-adic random matrices in [8]. It is not immediately clear how to adapt any of these approaches to study cases of Theorem 1.1 where $l > 1$, or where $l = 1$ and $\deg(P_1) = 2$.

2. Theorem 1.6 implies Theorem 1.4 and Theorem 1.4 implies Theorem 1.1

We begin this section by recalling two key lemmas from [1].

Lemma 2.1 *([1], Lemma 4.3). Let $l \in \mathbb{Z}_{\geqslant 1}$ and $G_1, \ldots, G_l$ be finite abelian p-groups. Choose any $N \in \mathbb{Z}_{\geqslant 0}$ such that $p^N G_1 = \cdots = p^N G_l = 0$. For any monic polynomials $f_1(t), \ldots, f_l(t) \in \mathbb{Z}_p[t]$ and $n \in \mathbb{Z}_{\geqslant 1}$, we have*

$$\Prob_{X \in \mathrm{Mat}_n(\mathbb{Z}_p)} \left(\begin{array}{c} \mathrm{cok}(f_j(X)) \simeq G_j \\ \text{for } 1 \leqslant j \leqslant l \end{array} \right) = \Prob_{X \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})} \left(\begin{array}{c} \mathrm{cok}(f_j(X)) \simeq G_j \\ \text{for } 1 \leqslant j \leqslant l \end{array} \right).$$

The next result follows from [1, Theorem 2.10] and [1, Lemma 5.3].

Lemma 2.2. *Let $l \in \mathbb{Z}_{\geqslant 1}$, $r_1, \ldots, r_l \in \mathbb{Z}_{\geqslant 0}$, and $P_1(t), \ldots, P_l(t) \in \mathbb{F}_p[t]$ be distinct irreducible polynomials. We have*

$$\lim_{n \to \infty} \Prob_{\bar{X} \in \mathrm{Mat}_n(\mathbb{F}_p)} \left(\begin{array}{c} \dim_{\mathbb{F}_p[t]/(P_j(t))}(\mathrm{cok}(P_j(\bar{X}))) = r_j \\ \text{for } 1 \leqslant j \leqslant l \end{array} \right)$$

$$= \prod_{j=1}^{l} \left(\frac{p^{-r_j^2 \deg(P_j)} \prod_{i=1}^{\infty}(1 - p^{-i \deg(P_j)})}{\prod_{i=1}^{r_j}(1 - p^{-i \deg(P_j)})^2} \right).$$

Proof that Theorem 1.6 implies Theorem 1.4 and Theorem 1.4 implies Theorem 1.1.
Throughout the proof, we write $R_j := \mathbb{Z}_p[t]/(P_j(t))$ and $q_j := p^{\deg(P_j)}$ so that $\mathbb{F}_{q_j} = \mathbb{F}_p[t]/(P_j(t))$. By applying Lemma 2.1, we see that it is enough to prove the desired statements with $\mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})$ in place of $\mathrm{Mat}_n(\mathbb{Z}_p)$. Moreover, as explained in Remark 1.5, we may assume that $n \geqslant \sum_{j=1}^{l} \dim_{\mathbb{F}_p}(\mathrm{cok}(P_j(\bar{X})))$.

Theorem 1.6 implies that

$$\# \left\{ \begin{array}{c} X \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z}) : \\ \mathrm{cok}(P_j(X)) \simeq G_j \\ \text{for } 1 \leqslant j \leqslant l \end{array} \right\} =$$

$$p^{Nn^2} \left(\prod_{j=1}^{l} \frac{q_j^{r_{q_j}(G_j)^2} \prod_{i=1}^{r_{q_j}(G_j)}(1 - q_j^{-i})^2}{|\mathrm{Aut}_{R_j}(G_j)|} \right) \cdot \# \left\{ \begin{array}{c} \bar{X} \in \mathrm{Mat}_n(\mathbb{F}_p) : \\ \mathrm{cok}(P_j(\bar{X})) \simeq G_j/pG_j \\ \text{for } 1 \leqslant j \leqslant l \end{array} \right\}.$$

Dividing by $p^{(N+1)n^2} = \#\mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})$ and noting that $\#\mathrm{Mat}_n(\mathbb{F}_p) = p^{n^2}$, we have

$$\Pr_{X \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})} \left(\begin{array}{c} \mathrm{cok}(P_j(X)) \simeq G_j \\ \text{for } 1 \leqslant j \leqslant l \end{array} \right)$$

$$= \left(\prod_{j=1}^{l} \frac{q_j^{r_{q_j}(G_j)^2} \prod_{i=1}^{r_{q_j}(G_j)}(1 - q_j^{-i})^2}{|\mathrm{Aut}_{R_j}(G_j)|} \right) \frac{\# \left\{ \begin{array}{c} \bar{X} \in \mathrm{Mat}_n(\mathbb{F}_p) : \\ \mathrm{cok}(P_j(\bar{X})) \simeq G_j/pG_j \\ \text{for } 1 \leqslant j \leqslant l \end{array} \right\}}{\#\mathrm{Mat}_n(\mathbb{F}_p)}$$

$$= \left(\prod_{j=1}^{l} \frac{q_j^{r_{q_j}(G_j)^2} \prod_{i=1}^{r_{q_j}(G_j)}(1 - q_j^{-i})^2}{|\mathrm{Aut}_{R_j}(G_j)|} \right) \Pr_{\bar{X} \in \mathrm{Mat}_n(\mathbb{F}_p)} \left(\begin{array}{c} \mathrm{cok}(P_j(\bar{X})) \simeq G_j/pG_j \\ \text{for } 1 \leqslant j \leqslant l \end{array} \right),$$

so Theorem 1.4 follows.

Next, assume Theorem 1.4. Applying Lemma 2.2 with $r_j = r_{q_j}(G_j)$ shows that

$$\lim_{n \to \infty} \Pr_{\bar{X} \in \mathrm{Mat}_n(\mathbb{F}_p)} \left(\begin{array}{c} \mathrm{cok}(P_j(\bar{X})) \simeq G_j/pG_j \\ \text{for } 1 \leqslant j \leqslant l \end{array} \right) = \prod_{j=1}^{l} \left(\frac{q_j^{-r_{q_j}(G_j)^2} \prod_{i=1}^{\infty}(1 - q_j^{-i})}{\prod_{i=1}^{r_{q_j}(G_j)}(1 - q_j^{-i})^2} \right).$$

Starting from the statement of Theorem 1.4, applying Lemma 2.1 and then taking $n \to \infty$ implies that

$$\lim_{n \to \infty} \Pr_{X \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})} \left(\begin{array}{c} \mathrm{cok}(P_j(X)) \simeq G_j \\ \text{for } 1 \leqslant j \leqslant l \end{array} \right)$$

$$= \prod_{j=1}^{l} \frac{q_j^{r_{q_j}(G_j)^2} \prod_{i=1}^{r_{q_j}(G_j)}(1 - q_j^{-i})^2}{|\mathrm{Aut}_{R_j}(G_j)|} \cdot \frac{q_j^{-r_{q_j}(G_j)^2} \prod_{i=1}^{\infty}(1 - q_j^{-i})}{\prod_{i=1}^{r_{q_j}(G_j)}(1 - q_j^{-i})^2}$$

$$= \prod_{j=1}^{l} \frac{1}{|\mathrm{Aut}_{R_j}(G_j)|} \prod_{i=1}^{\infty} (1 - q_j^{-i}),$$

so Theorem 1.1 follows. $\square$

3. Proof of Theorem 1.6 when $l = 1$

In this section we prove Theorem 1.6 when $l = 1$.

3.1. Useful lemmas

When $l = 1$ and $\deg(P_1) = 1$, we consider the following more general version of Theorem 1.6.

Lemma 3.1. *Let $(R, \mathfrak{m})$ be a complete DVR with finite residue field $R/\mathfrak{m} = \mathbb{F}_q$, let G be a finite R-module, and choose any $N \in \mathbb{Z}_{\geqslant 0}$ such that $\mathfrak{m}^N G = 0$. For any $\alpha \in R/\mathfrak{m}^{N+1}$, $n \in \mathbb{Z}_{\geqslant 0}$, and $\bar{X} \in \mathrm{Mat}_n(\mathbb{F}_q)$ satisfying $\mathrm{cok}(\bar{X} - \bar{\alpha} I_n) \simeq G/\mathfrak{m} G$, where $\bar{\alpha} \in \mathbb{F}_q = R/\mathfrak{m}$ is the image of α modulo $\mathfrak{m}$, we have*

$$\# \left\{ \begin{array}{l} X \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1}): \\ R^n/(X - \alpha I_n)R^n \simeq G \\ \text{and } X \equiv \bar{X} \pmod{\mathfrak{m}} \end{array} \right\} = q^{Nn^2} \frac{q^{r_q(G)^2} \prod_{i=1}^{r_q(G)} (1 - q^{-i})^2}{|\mathrm{Aut}_R(G)|},$$

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

Lemma 3.1 can be deduced from the arguments introduced by Friedman and Washington in [5] although they only discuss the case $R = \mathbb{Z}_p$. In this section, we give a different proof of this result. We need to apply this more general version of Lemma 3.1 in our proof of Theorem 1.6 when at least one of the polynomials $P_j(t)$ has degree 2.

The following lemma, which we learned from personal communication with Jungin Lee, is crucial to our proof of Theorem 1.6 when at least one of the polynomials $P_j(t)$ has degree 2.

Lemma 3.2 *(Lee). Given $m \in \mathbb{Z}_{\geqslant 0}$, let $P(t) \in (\mathbb{Z}/p^m\mathbb{Z})[t]$ be a monic polynomial of degree d. Consider*

$$R := (\mathbb{Z}/p^m\mathbb{Z})[t]/(P(t)) = \mathbb{Z}/p^m\mathbb{Z} \oplus \bar{t}(\mathbb{Z}/p^m\mathbb{Z}) \oplus \cdots \oplus \bar{t}^{d-1}(\mathbb{Z}/p^m\mathbb{Z}).$$

Fix $X \in \mathrm{Mat}_n(\mathbb{Z}/p^m\mathbb{Z})$. The map

$$\psi \colon \frac{(\mathbb{Z}/p^m\mathbb{Z})^n}{P(X)(\mathbb{Z}/p^m\mathbb{Z})^n} \to \mathrm{cok}_R(X - \bar{t} I_n) := \frac{R^n}{(X - \bar{t} I_n)R^n}$$

defined by $\psi([v]) = [v]$, where $v \in (\mathbb{Z}/p^m\mathbb{Z})^n$, is an R-linear isomorphism.

Proof. Since $P(\bar{t}) = 0$ in $R = (\mathbb{Z}/p^m\mathbb{Z})[t]/(P(t))$, we have $P(x) = (x - \bar{t})Q(x)$ for some $Q(x) \in R[x]$. For $w \in (\mathbb{Z}/p^m\mathbb{Z})^n$, we have

$$P(X)w = (X - \bar{t}I_n)Q(X)w$$

in R^n, so ψ is well-defined. Since

$$\psi(\bar{t}[v]) = \psi([Xv]) = [Xv] = [\bar{t}v] = \bar{t}[v],$$

we see that ψ is R-linear.

Suppose $\psi([v]) = 0$ in $R^n/(X - \bar{t}I_n)R^n$. Let $v \in (\mathbb{Z}/p^m\mathbb{Z})^n$ be any representative of $[v]$. There exist $w_0, \ldots, w_{d-1} \in (\mathbb{Z}/p^m\mathbb{Z})^n$ such that when considered as an element of R^n,

$$
\begin{aligned}
v &= (X - \bar{t}I_n)(w_0 + \bar{t}w_1 + \cdots + \bar{t}^{d-1}w_{d-1}) \\
&= Xw_0 + \bar{t}Xw_1 + \cdots + \bar{t}^{d-1}Xw_{d-1} - (\bar{t}w_0 + \bar{t}^2 w_1 + \cdots + \bar{t}^d w_{d-1}) \\
&= Xw_0 + \bar{t}(Xw_1 - w_0) + \bar{t}^2(Xw_2 - w_1) + \cdots + \bar{t}^{d-1}(Xw_{d-1} - w_{d-2}) - \bar{t}^d w_{d-1}.
\end{aligned}
$$

Writing $P(t) = t^d + a_{d-1}t^{d-1} + \cdots + a_1 t + a_0$, this implies that as an element of R^n,

$$
\begin{aligned}
v =& Xw_0 + a_0 w_{d-1} + \bar{t}(Xw_1 - w_0 + a_1 w_{d-1}) + \bar{t}^2(Xw_2 - w_1 + a_2 w_{d-1}) + \\
& \cdots + \bar{t}^{d-1}(Xw_{d-1} - w_{d-2} + a_{d-1}w_{d-1}).
\end{aligned}
$$

Since $v \in (\mathbb{Z}/p^m\mathbb{Z})^n$, the decomposition $R = \mathbb{Z}/p^m\mathbb{Z} \oplus \bar{t}(\mathbb{Z}/p^m\mathbb{Z}) \oplus \cdots \oplus \bar{t}^{d-1}(\mathbb{Z}/p^m\mathbb{Z})$ implies that as elements of $(\mathbb{Z}/p^m\mathbb{Z})^n$,

$$
\begin{aligned}
v &= Xw_0 + a_0 w_{d-1}, \\
w_0 &= Xw_1 + a_1 w_{d-1}, \\
w_1 &= Xw_2 + a_2 w_{d-1}, \\
&\cdots \\
w_{d-2} &= Xw_{d-1} + a_{d-1}w_{d-1}.
\end{aligned}
$$

Therefore, as an element of $(\mathbb{Z}/p^m\mathbb{Z})^n$,

$$
\begin{aligned}
v &= Xw_0 + a_0 w_{d-1} \\
&= X^2 w_1 + a_1 Xw_{d-1} + a_0 w_{d-1} \\
&= X^3 w_2 + a_2 X^2 w_{d-1} + a_1 Xw_{d-1} + a_0 w_{d-1} \\
&\quad \cdots \\
&= X^{d-1} w_{d-2} + a_{d-2}X^{d-2}w_{d-1} + \cdots + a_1 Xw_{d-1} + a_0 w_{d-1}
\end{aligned}
$$

$$= X^d w_{d-1} + a_{d-1} X^{d-1} w_{d-1} + a_{d-2} X^{d-2} w_{d-1} + \cdots + a_1 X w_{d-1} + a_0 w_{d-1}$$
$$= (X^d + a_{d-1} X^{d-1} + a_{d-2} X^{d-2} + \cdots + a_1 X + a_0) w_{d-1} = P(X) w_{d-1}.$$

This means $[v] = 0$ in $(\mathbb{Z}/p^m\mathbb{Z})^n / P(X)(\mathbb{Z}/p^m\mathbb{Z})^n$, and we conclude that ψ is injective. Given any $v_0 + \bar{t}v_1 + \cdots + \bar{t}^{d-1} v_{d-1} \in R^n$, where each $v_i \in (\mathbb{Z}/p^m\mathbb{Z})^n$, we have

$$[v_0 + X v_1 + \cdots + X^{d-1} v_{d-1}] = [v_0 + \bar{t}v_1 + \cdots + \bar{t}^{d-1} v_{d-1}]$$

in $R^n/(X - \bar{t}I_n)R^n$. This shows that ψ is surjective. $\square$

3.2. Proof of Theorem 1.6 when $l = 1$

We now use Lemma 3.1 to prove Theorem 1.6 when $l = 1$. Let $P(t) \in \mathbb{Z}_p[t]$ be a monic polynomial of degree at most 2 whose reduction modulo p is irreducible in $\mathbb{F}_p[t]$. Let $q := p^{\deg(P)}$. We want to show that for any finite module G over $\mathbb{Z}_p[t]/(P(t))$, $N \in \mathbb{Z}_{\geq 0}$ such that $p^{N+1}G = 0$, and $\bar{X} \in \mathrm{Mat}_n(\mathbb{F}_p)$ with $r_q(G) := \dim_{\mathbb{F}_q}(G/pG) = \dim_{\mathbb{F}_q}(\mathrm{cok}(P(\bar{X})))$, we have

$$\#\left\{ \begin{array}{c} X \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z}): \\ \mathrm{cok}(P(X)) \simeq G \\ \text{and } X \equiv \bar{X} \pmod{p} \end{array} \right\} = p^{Nn^2} \frac{q^{r_q(G)^2} \prod_{i=1}^{r_q(G)} (1 - q^{-i})^2}{|\mathrm{Aut}_{\mathbb{Z}_p[t]/(P(t))}(G)|}.$$

Proof. Lemma 3.1 with $R = \mathbb{Z}_p$ gives the result we need for $\deg(P) = 1$, so we suppose that $\deg(P) = 2$. In this case, we have $q = p^2$. For ease of notation, we write $P(t)$ for the image of $P(t)$ in $(\mathbb{Z}/p^{N+1}\mathbb{Z})[t]$. Suppose $A \in \mathrm{Mat}_n(\mathbb{F}_p)$ satisfies

$$\dim_{\mathbb{F}_q}(\mathrm{cok}(P(A))) = r_q(G).$$

For the rest of the proof, let $R = (\mathbb{Z}/p^{N+1}\mathbb{Z})[t]/(P(t))$. Lemma 3.2 implies that

$$\#\left\{ \begin{array}{c} X \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z}): \\ \mathrm{cok}(P(X)) \simeq G \\ \text{and } X \equiv A \pmod{p} \end{array} \right\} = \#\left\{ \begin{array}{c} X \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z}): \\ \mathrm{cok}_R(X - \bar{t}I_n) \simeq G \\ \text{and } X \equiv A \pmod{p} \end{array} \right\}.$$

We claim that the size of this set is independent of the choice of A.

The decomposition $R = (\mathbb{Z}/p^{N+1}\mathbb{Z}) \oplus \bar{t}(\mathbb{Z}/p^{N+1}\mathbb{Z})$ gives a decomposition $\mathrm{Mat}_n(R) = \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z}) \oplus \bar{t}\mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})$. This decomposition shows that

$$c_{N,n} := \#\left\{ \begin{array}{c} Z = X + \bar{t}Y \in \mathrm{Mat}_n(R): \\ \mathrm{cok}_R(Z) \simeq G \\ \text{and } Z \equiv A - \bar{t}I_n \pmod{p} \end{array} \right\} = \#\left\{ \begin{array}{c} (X, Y) \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})^2: \\ \mathrm{cok}_R(X + \bar{t}Y) \simeq G, \\ X \equiv A \text{ and } Y \equiv -I_n \pmod{p} \end{array} \right\}.$$

We explicitly compute $c_{N,n}$, which turns out to be independent of A. We have

$$c_{N,n} = \# \left\{ \begin{array}{c} (X, Y) \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})^2 : \\ \mathrm{cok}_R(X + \bar{t}Y) \simeq G, \\ X \equiv A \text{ and } Y \equiv -I_n \pmod{p} \end{array} \right\}$$

$$= \sum_{pM \in p\mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})} \# \left\{ \begin{array}{c} X \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z}) : \\ \mathrm{cok}_R(X + \bar{t}(pM - I_n)) \simeq G. \\ \text{and } X \equiv A \pmod{p} \end{array} \right\}.$$

For any $pM \in p\mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})$, we have a bijection

$$\left\{ \begin{array}{c} X' \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z}) : \\ \mathrm{cok}_R(X' + \bar{t}(pM - I_n)) \simeq G \\ \text{and } X' \equiv A \pmod{p} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} X \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z}) : \\ \mathrm{cok}_R(X - \bar{t}I_n) \simeq G \\ \text{and } X \equiv A \pmod{p} \end{array} \right\}$$

given by $X' \mapsto X = -X'(pM - I_n)^{-1}$. Since $|p\mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})| = p^{Nn^2}$, we have

$$c_{N,n} = p^{Nn^2} \cdot \# \left\{ \begin{array}{c} X \in \mathrm{Mat}_n(\mathbb{Z}/(p^{N+1})) : \\ \mathrm{cok}_R(X - \bar{t}I_n) \simeq G, \\ \text{and } X \equiv A \pmod{p} \end{array} \right\},$$

and so

$$c_{N,n} p^{-Nn^2} = \# \left\{ \begin{array}{c} X \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z}) : \\ \mathrm{cok}(P(X)) \simeq G \\ \text{and } X \equiv A \pmod{p} \end{array} \right\}.$$

Moreover, Lemma 3.1 implies

$$c_{N,n} = p^{2Nn^2} \frac{q^{r_q(G)^2} \prod_{i=1}^{r_q(G)} (1 - q^{-i})^2}{|\mathrm{Aut}_{\mathbb{Z}_p[t]/(P(t))}(G)|},$$

because $q = p^2$. Therefore,

$$\# \left\{ \begin{array}{c} X \in \mathrm{Mat}_n(\mathbb{Z}/(p^{N+1})) : \\ \mathrm{cok}(P(X)) \simeq G \\ \text{and } X \equiv A \pmod{p} \end{array} \right\} = c_{N,n} p^{-Nn^2} = p^{Nn^2} \frac{q^{r_q(G)^2} \prod_{i=1}^{r_q(G)} (1 - q^{-i})^2}{|\mathrm{Aut}_{\mathbb{Z}_p[t]/(P(t))}(G)|}. \quad \square$$

3.3. Outline of the proof of Lemma 3.1

In the rest of this section, we prove Lemma 3.1. Without loss of generality, we may assume $\alpha = 0$. We show that given

- a finite R-module G,

- $N \in \mathbb{Z}_{\geqslant 0}$ such that $\mathfrak{m}^N G = 0$, and
- $\bar{X} \in \mathrm{Mat}_n(\mathbb{F}_q)$ such that $\mathrm{cok}(\bar{X}) \simeq G/\mathfrak{m}G$ as $\mathbb{F}_q$-vector spaces,

we have

$$\#\left\{\begin{array}{c} X \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1}): \\ \mathrm{cok}(X) \simeq G \\ \text{and } X \equiv \bar{X} \pmod{\mathfrak{m}} \end{array}\right\} = q^{Nn^2} \frac{q^{r_q(G)^2} \prod_{i=1}^{r_q(G)}(1-q^{-i})^2}{|\mathrm{Aut}_R(G)|}. \tag{1}$$

In order to give the outline of our argument, we recall some linear algebra related to $\bar{X} \in \mathrm{Mat}_n(\mathbb{F}_q)$. We can give $\mathbb{F}_q^n$ an $\mathbb{F}_q[t]$-module structure by defining the t-action as left multiplication by $\bar{X}$ on the $n \times 1$ matrices over $\mathbb{F}_q$. With this structure in mind, we may write $\bar{X}$ to also mean the corresponding $\mathbb{F}_q[t]$-module, namely the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$ together with the action of $\bar{X}$. Given any irreducible polynomial $P(t) \in \mathbb{F}_q[t]$, we have

$$\mathrm{cok}(P(\bar{X})) \simeq \ker(P(\bar{X})) \simeq \bar{X}[P^\infty]/P\bar{X}[P^\infty]$$

as $\mathbb{F}_q$-vector spaces, where $\bar{X}[P^\infty]$ denotes the P-part of the $\mathbb{F}_q[t]$-module $\bar{X}$. For ease of notation, throughout the proof we let $r = r_q(G)$. Since $\mathrm{cok}(\bar{X}) \simeq G/\mathfrak{m}G \simeq \mathbb{F}_q^r$, we have

$$\bar{X}[t^\infty] \simeq \mathbb{F}_q[t]/(t^{m_1}) \times \cdots \times \mathbb{F}_q[t]/(t^{m_r})$$

as $\mathbb{F}_q[t]$-modules, where $m_1 \geqslant m_2 \geqslant \cdots \geqslant m_r \geqslant 1$. In other words, the matrix $\bar{X}$ has r Jordan blocks corresponding to the eigenvalue 0 with sizes $m_1, \ldots, m_r$.

Our argument is divided into three main steps:

1. We prove that it is enough to show that (1) holds for $\bar{X} \in \mathrm{Mat}_n(\mathbb{F}_q)$ of the special form

$$\bar{X} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & \mathrm{id} & 0 \\ 0 & 0 & \bar{M} \end{bmatrix},$$

where
   - $\mathrm{id} = I_{m_1+\cdots+m_r-r}$, the $(m_1+\cdots+m_r-r) \times (m_1+\cdots+m_r-r)$ identity matrix, and
   - $\bar{M} \in \mathrm{GL}_{n-(m_1+\cdots+m_r)}(\mathbb{F}_q)$.
2. For $\bar{X}$ of this form, we prove that the left-hand side of (1) is

$$q^{N(n^2-r^2)} \cdot \#\{uA \in u\mathrm{Mat}_r(R/\mathfrak{m}^{N+1}): \mathrm{cok}(uA) \simeq G\},$$

where u is a uniformizer of R (i.e., a generator for its maximal ideal, so $\mathfrak{m} = (u) = uR$).

3. We prove that

$$\#\{uA \in u\mathrm{Mat}_r(R/\mathfrak{m}^{N+1})\colon \mathrm{cok}(uA) \simeq G\} = \frac{q^{Nr^2+r^2}\prod_{i=1}^{r}(1-q^{-i})^2}{|\mathrm{Aut}_R(G)|}.$$

Remark 3.3. Friedman and Washington prove Lemma 3.1 in [5, p. 236]. Their proof is similar to the one outlined above. They reduce the statement to the count given in the third main step. Then they note that $\mathrm{cok}(uA') \simeq H$ if and only if $\mathrm{cok}(A') \simeq uH$. Finally, they compute

$$\#\{A' \in \mathrm{Mat}_r(R/\mathfrak{m}^{N+1})\colon \mathrm{cok}(A') \simeq uH\}$$

using [5, Proposition 1].

The final part of our argument is longer but works more directly with the entries of the matrices we consider. In particular, we describe conditions on a matrix over $R/\mathfrak{m}^{N+1}$ that determine whether or not its cokernel is isomorphic to a particular module G. We give a full proof of Lemma 3.1 because several of the pieces are important for the proof of the general case of Theorem 1.6. We also believe that the techniques in our proof may be useful for other problems about cokernels of families of random p-adic matrices.

We now carry out the first part of our three step strategy.

Proof of Lemma 3.1: Step (1). By switching rows and columns of $\bar{X}$, there exist $\bar{Q}_1, \bar{Q}_2 \in \mathrm{GL}_n(\mathbb{F}_q)$ such that

$$\bar{Q}_1\bar{X}\bar{Q}_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & \mathrm{id} & 0 \\ 0 & 0 & \bar{M} \end{bmatrix},$$

where

- id is the $(m_1 + \cdots + m_r - r) \times (m_1 + \cdots + m_r - r)$ identity matrix, and
- $\bar{M} \in \mathrm{GL}_{n-(m_1+\cdots+m_r)}(\mathbb{F}_q)$.[1]

Fix lifts $Q_1, Q_2 \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ of $\bar{Q}_1, \bar{Q}_2$, meaning $Q_i \equiv \bar{Q}_i \pmod{\mathfrak{m}}$ for $i \in \{1,2\}$. Since $\bar{Q}_1, \bar{Q}_2 \in \mathrm{GL}_n(\mathbb{F}_q)$, we have $Q_1, Q_2 \in \mathrm{GL}_n(R/\mathfrak{m}^{N+1})$. Fix a lift $M \in \mathrm{GL}_{n-(m_1+\cdots+m_r)}(R/\mathfrak{m}^{N+1})$ of $\bar{M}$.

For any lift $X \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ of $\bar{X}$, note that $Q_1XQ_2 \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ is a lift of $\bar{Q}_1\bar{X}\bar{Q}_2$. On the other hand, if $Y \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ is a lift of $\bar{Q}_1\bar{X}\bar{Q}_2$, then

---

[1] In [5, p. 234, (11)], these $\bar{Q}_1$ and $\bar{Q}_2$ are taken to be inverses of each other, but it is not possible to find such matrices in general. For example, the 2×2 matrix $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ is not similar to any matrix of the form $\begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix}$ with $d \neq 0$. Nevertheless, this is an easy fix.

$Q_1^{-1} Y Q_2^{-1} \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ is a lift of $\bar{X}$. This gives a bijection between the lifts of $\bar{X}$ to $\mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ and the lifts of $\bar{Q}_1 \bar{X} \bar{Q}_2$ to $\mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$. Hence, the number of lifts $X \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ of $\bar{X}$ is equal to the number of lifts $Y = Q_1 X Q_2 \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ of $\bar{Q}_1 \bar{X} \bar{Q}_2$. Since $\mathrm{cok}(Y) = \mathrm{cok}(Q_1 X Q_2) \simeq \mathrm{cok}(X)$, it is enough to count the lifts $Y = Q_1 X Q_2 \in \mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ of $\bar{Q}_1 \bar{X} \bar{Q}_2$ with $\mathrm{cok}(Y) \simeq G$. $\quad\square$

3.4. Elementary operations for block submatrices

Before we carry out the second main step of the proof of Lemma 3.1, we recall some material about elementary row and column operations for block submatrices. Let R be a commutative ring and $X \in \mathrm{Mat}_n(R)$. Each of the following three elementary row operations corresponds to left multiplication by a matrix in $\mathrm{GL}_n(R)$:

- Exchange the i-th row $X_{(i)}$ with the j-th row $X_{(j)}$ for any distinct $i, j \in [1, n]$;
- Multiply $X_{(i)}$ by a unit in R for any $i \in [1, n]$;
- Replace $X_{(i)}$ with $X_{(i)} + a X_{(j)}$ for any $a \in R$ and any distinct $i, j \in [1, n]$.

Likewise, each of the following three elementary column operations corresponds to right multiplication by a matrix in $\mathrm{GL}_n(R)$:

- Exchange the i-th column $X^{(i)}$ with the j-th column $X^{(j)}$ for any distinct $i, j \in [1, n]$;
- Multiply $X^{(i)}$ by a unit in R for any $i \in [1, n]$;
- Replace $X^{(i)}$ with $X^{(i)} + a X^{(j)}$ for any $a \in R$ and any distinct $i, j \in [1, n]$.

Note that elementary (row or column) operations do not change the isomorphism class of $\mathrm{cok}(X)$.

A key technique in the proof Lemma 3.1 is an analogous method for elementary operations with block submatrices of X. Let n be a positive integer and $n_1, \ldots, n_s \geqslant 1$ satisfy $n_1 + \cdots + n_s = n$. We subdivide $X \in \mathrm{Mat}_n(R)$ into block submatrices where $X_{[i,j]}$ is an $n_i \times n_j$ matrix over R:

$$
X = \begin{bmatrix}
X_{[1,1]} & X_{[1,2]} & \cdots & X_{[1,s-1]} & X_{[1,s]} \\
X_{[2,1]} & X_{[2,2]} & \cdots & X_{[2,s-1]} & X_{[2,s]} \\
\vdots & \vdots & \cdots & \vdots & \vdots \\
X_{[s-1,1]} & X_{[s-1,2]} & \cdots & X_{[s-1,s-1]} & X_{[s-1,s]} \\
X_{[s,1]} & X_{[s,2]} & \cdots & X_{[s,s-1]} & X_{[s,s]}
\end{bmatrix}.
$$

Lemma 3.4 (Elementary operations for block submatrices). *Keeping the notation as above, fix distinct $i, j \in [1, s]$. Any of the following three elementary block row operations on $X \in \mathrm{Mat}_n(R)$ corresponds to left multiplication of X by a matrix in $\mathrm{GL}_n(R)$:*

1. *Exchange the i-th (block) row $X_{[i]} = [X_{[i,1]}, \cdots, X_{[i,s]}]$ with the j-th row $X_{[j]} = [X_{[j,1]}, \cdots, X_{[j,s]}]$;*

2. *Multiply* $X_{[i]} = [X_{[i,1]}, \cdots, X_{[i,s]}]$ *on the left by any* $g \in \mathrm{GL}_{n_i}(R)$ *to get* $gX_{[i]} = [gX_{[i,1]}, \cdots, gX_{[i,s]}]$;

3. *For any* $n_i \times n_j$ *matrix* A, *replace* $X_{[i]}$ *with* $X_{[i]} + AX_{[j]} = [X_{[i,1]} + AX_{[j,1]}, \cdots, X_{[i,s]} + AX_{[j,s]}]$.

Likewise, any of the following three column block row operations on $X \in \mathrm{Mat}_n(R)$ *corresponds to right multiplication of* X *by a matrix in* $\mathrm{GL}_n(R)$:

1. *Exchange the i-th (block) column* $X^{[i]} = \begin{bmatrix} X_{[1,i]} \\ \vdots \\ X_{[s,i]} \end{bmatrix}$ *with the j-th column* $X^{[j]} = \begin{bmatrix} X_{[1,j]} \\ \vdots \\ X_{[s,j]} \end{bmatrix}$;

2. *Multiply* $X^{[i]} = \begin{bmatrix} X_{[1,i]} \\ \vdots \\ X_{[s,i]} \end{bmatrix}$ *on the right by any* $g \in \mathrm{GL}_{n_i}(R)$ *to get* $X^{[i]}g = \begin{bmatrix} X_{[1,i]}g \\ \vdots \\ X_{[s,i]}g \end{bmatrix}$;

3. *For an* $n_j \times n_i$ *matrix* A, *replace* $X^{[i]}$ *with* $X^{[i]} + X^{[j]}A = \begin{bmatrix} X_{[1,i]} + X_{[1,j]}A \\ \vdots \\ X_{[s,i]} + X_{[s,j]}A \end{bmatrix}$.

In particular, the operations above do not change the isomorphism class of $\mathrm{cok}(X)$.

Proof. We note that

$$[X_{[i,1]}, \cdots, X_{[i,s]}]^T = \begin{bmatrix} X_{[i,1]}^T \\ \vdots \\ X_{[i,s]}^T \end{bmatrix}.$$

Therefore, the column operations are given by taking the transposes of the row operations and it is enough to prove Lemma 3.4 for the block row operations.

The operations (1) and (3) follow directly from the corresponding ones from the usual elementary operations. The operation (2) corresponds to left multiplication by the block diagonal matrix with blocks $I_{n_1}, I_{n_2}, \ldots, I_{n_{i-1}}, g, I_{n_{i+1}}, \ldots, I_{n_s}$, that is, the matrix that comes from replacing the $[i, i]$-block of the identity matrix with g. This finishes the proof. $\square$

Proof of Lemma 3.1: Step (2). Suppose that $\bar{X} \in \mathrm{Mat}_n(\mathbb{F}_q)$ is of the form described in Step (1) of the outline of the proof given in Section 3.3. Recall that R is a complete DVR with maximal ideal $\mathfrak{m}$ and residue field $R/\mathfrak{m} = \mathbb{F}_q$. Let u be a uniformizer of R, so $\mathfrak{m} = (u)$.

Any lift of $\bar{X} \in \mathrm{Mat}_n(\mathbb{F}_q)$ to $\mathrm{Mat}_n(R/\mathfrak{m}^{N+1})$ is of the form

$$X = \begin{bmatrix} uA_1 & uA_2 & uA_3 \\ uA_4 & \mathrm{id} + uA_5 & uA_6 \\ uA_7 & uA_8 & M + uA_9 \end{bmatrix},$$

where $uA_1, uA_2, uA_3, uA_4, uA_5, uA_6, uA_7, uA_8, uA_9$ are matrices over $R/\mathfrak{m}^{N+1}$ all of whose entries are in (u) such that

- $uA_1 \in u\mathrm{Mat}_r(R/\mathfrak{m}^{N+1})$,
- $uA_5 \in u\mathrm{Mat}_{m_1+\cdots+m_r-r}(R/\mathfrak{m}^{N+1})$, $\mathrm{id} = I_{m_1+\cdots+m_r-r}$, and
- $uA_9 \in u\mathrm{Mat}_{n-(m_1+\cdots+m_r)}(R/\mathfrak{m}^{N+1})$.

Choose representatives $\alpha_1, \ldots, \alpha_q \in R/\mathfrak{m}^{N+1}$ for the equivalence classes in $(R/\mathfrak{m}^{N+1})/(\mathfrak{m}/\mathfrak{m}^{N+1}) \simeq R/\mathfrak{m} = \mathbb{F}_q$. The filtration $R/\mathfrak{m}^{N+1} \supset \mathfrak{m}/\mathfrak{m}^{N+1} \supset \cdots \supset \mathfrak{m}^N/\mathfrak{m}^{N+1}$ shows that each element of $R/\mathfrak{m}^{N+1}$ can be written uniquely as $a_0 + a_1 u + \cdots + a_N u^N$, where each a_i is equal to some α_j. So each entry of the matrix uA_k is of the form $a_1 u + a_2 u^2 + \cdots + a_N u^N$ where each a_i is equal to some α_j. There are q^{Nn^2} total possible choices for the entries of $uA_1, uA_2, uA_3, uA_4, uA_5, uA_6, uA_7, uA_8, uA_9$ over $R/\mathfrak{m}^{N+1}$ if we do not require any condition on $\mathrm{cok}(X)$. We count choices for which $\mathrm{cok}(X) \cong G$.

First, we freely choose $u\boldsymbol{A} := (uA_2, uA_3, uA_4, uA_5, uA_6, uA_7, uA_8, uA_9)$. There are $q^{N(n^2-r^2)}$ possible choices for $u\boldsymbol{A}$. We claim that given $u\boldsymbol{A}$ and uA_1 there exist $P_{1,u\boldsymbol{A}}$ and $P_{2,u\boldsymbol{A}} \in \mathrm{GL}_n(R/\mathfrak{m}^{N+1})$, depending on $u\boldsymbol{A}$ but not uA_1, such that

$$P_{1,u\boldsymbol{A}} X P_{2,u\boldsymbol{A}} = \begin{bmatrix} uA_{uA_1,p\boldsymbol{A}} & 0 & 0 \\ 0 & \mathrm{id} + uB_{u\boldsymbol{A}} & 0 \\ 0 & 0 & M + uA_9 \end{bmatrix}, \qquad (2)$$

where

$$uB_{u\boldsymbol{A}} = u(A_5 - uA_6(M + uA_9)^{-1}A_8),$$

and $uA_{uA_1,u\boldsymbol{A}}$ depends on uA_1 and $u\boldsymbol{A}$. We prove the existence of these matrices $P_{1,u\boldsymbol{A}}, P_{2,u\boldsymbol{A}}$ by describing (block) row and column operations that we can apply to X, using Lemma 3.4. Since $\mathrm{id} + uB_{p\boldsymbol{A}}$ and $M + uA_9$ are invertible modulo $\mathfrak{m}$, they are also invertible as matrices over $R/\mathfrak{m}^{N+1}$. Therefore,

$$\mathrm{cok}(X) \simeq \mathrm{cok}(P_{1,u\boldsymbol{A}} X P_{2,u\boldsymbol{A}}) \simeq \mathrm{cok}(uA_{A_1,u\boldsymbol{A}}).$$

The sequence of (block) row and column operations that we apply to X makes it clear that the map taking uA_1 to $uA_{uA_1,u\boldsymbol{A}}$ is a bijection from $u\mathrm{Mat}_r(R/\mathfrak{m}^{N+1})$ to itself. Therefore, the number of choices of $uA_1, uA_2, \ldots, uA_9$ for which $\mathrm{cok}(uA_{uA_1,u\boldsymbol{A}}) \simeq G$ is equal to

$$q^{N(n^2-r^2)} \cdot \#\{uA \in u\mathrm{Mat}_r(R/\mathfrak{m}^{N+1}) \colon \mathrm{cok}(uA) \simeq G\}.$$

Given a choice of $u\boldsymbol{A}$, we now describe the (block) row and column operations taking X to the matrix on the right-hand side of (2). Applying Lemma 3.4, subtract

$$uA_6(M + uA_9)^{-1}[uA_7, uA_8, M + uA_9]$$
$$= [u^2 A_6(M + uA_9)^{-1}A_7, u^2 A_6(M + uA_9)^{-1}A_8, uA_6]$$

from the second block row of X to get

$$\begin{bmatrix} uA_1 & uA_2 & uA_3 \\ u(A_4 - uA_6(M + uA_9)^{-1}A_7) & \mathrm{id} + u(A_5 - uA_6(M + uA_9)^{-1}A_8) & 0 \\ uA_7 & uA_8 & M + uA_9 \end{bmatrix}.$$

Next, subtract

$$uA_3(M + uA_9)^{-1}[uA_7, uA_8, M + uA_9]$$
$$= [u^2 A_3(M + uA_9)^{-1}A_7, u^2 A_3(M + uA_9)^{-1}A_8, uA_3]$$

from the first block row to get

$$\begin{bmatrix} u(A_1 - uA_3(M + uA_9)^{-1}A_7) & u(A_2 - uA_3(M + uA_9)^{-1}A_8) & 0 \\ u(A_4 - uA_6(M + uA_9)^{-1}A_7) & \mathrm{id} + u(A_5 - uA_6(M + uA_9)^{-1}A_8) & 0 \\ uA_7 & uA_8 & M + uA_9 \end{bmatrix}.$$

Now subtract

$$uA_8(M + uA_9)^{-1} \begin{bmatrix} 0 \\ 0 \\ M + uA_9 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ uA_8 \end{bmatrix}$$

from the second block column and then subtract

$$uA_7(M + uA_9)^{-1} \begin{bmatrix} 0 \\ 0 \\ M + uA_9 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ uA_7 \end{bmatrix}$$

from the first block column to get

$$\begin{bmatrix} u(A_1 - uA_3(M + uA_9)^{-1}A_7) & u(A_2 - uA_3(M + uA_9)^{-1}A_8) & 0 \\ u(A_4 - uA_6(M + uA_9)^{-1}A_7) & \mathrm{id} + u(A_5 - uA_6(M + uA_9)^{-1}A_8) & 0 \\ 0 & 0 & M + uA_9 \end{bmatrix}.$$

Since $\mathrm{id} + u(A_5 - uA_6(M + uA_9)^{-1}A_8)$ is invertible over $R/\mathfrak{m}^{N+1}$, we may apply similar arguments to get rid of the blocks directly above it and directly to the left of it. This gives a matrix of the desired form where $uA_{uA_1,u\boldsymbol{A}}$ is the upper left block.

It is clear that changing the entries of uA_1 changes the entries of $u(A_1 - uA_3(R + uA_9)^{-1}A_7)$, and therefore also changes the entries of $uA_{uA_1, uA}$. What we have described above is a bijection from $u\mathrm{Mat}_r(R/\mathfrak{m}^{N+1})$ to itself, defined by taking uA_1 to $uA_{uA_1, uA}$. This completes the proof of Step (2). $\square$

3.5. Counting matrices with a given cokernel

Before completing the proof of Step (3) of the outline given in Section 3.3, which finishes the proof of Lemma 3.1, we recall some additional facts.

Lemma 3.5. *Let R be a PID and $X \in \mathrm{Mat}_n(R)$ have rank r over the fraction field of R. There exist $P, Q \in \mathrm{GL}_n(R)$ such that $PXQ = S$ is a diagonal matrix whose diagonal entries $(s_1, s_2, \ldots, s_r, 0, \ldots, 0)$ satisfy $s_i \mid s_{i+1}$ for all $1 \leqslant i \leqslant r - 1$. Since $\mathrm{cok}(X) \simeq \mathrm{cok}(PXQ) = \mathrm{cok}(S)$, we have*

$$\mathrm{cok}(X) \cong R/s_1R \oplus R/s_2R \oplus \cdots \oplus R/s_rR \oplus R^{n-r}.$$

Moreover, these s_i are uniquely determined up to multiplication by a unit of R, and

$$s_1 \cdots s_i = \gcd(i \times i \text{ minors of } X).$$

We call these $s_1, \ldots, s_r$ the invariant factors *of $\mathrm{cok}(X)$.*

The following formula for the number of $\bar{X} \in \mathrm{Mat}_n(\mathbb{F}_q)$ of given rank is well-known.

Lemma 3.6. *For any integers $n \geqslant 1$ and $0 \leqslant r \leqslant n$, the number of rank r matrices in $\mathrm{Mat}_n(\mathbb{F}_q)$ is*

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

We will use the following formula for the number of automorphisms of a finite module over a complete DVR whose residue field is finite. See for example [5, p. 236] for a proof.

Lemma 3.7. *Let $(R, \mathfrak{m})$ be a complete DVR with a finite residue field $R/\mathfrak{m} = \mathbb{F}_q$. Suppose*

$$G \simeq (R/\mathfrak{m}^{e_1})^{r_1} \times \cdots \times (R/\mathfrak{m}^{e_k})^{r_k}$$

for integers $e_1 > e_2 > \cdots > e_k \geqslant 1$ and $r_1, \ldots, r_k \geqslant 1$. Then

$$|\mathrm{Aut}_R(G)| = \prod_{i=1}^k q^{-r_i^2} |\mathrm{GL}_{r_i}(\mathbb{F}_q)| \prod_{1 \leqslant i,j \leqslant k} q^{\min(e_i, e_j) r_i r_j}.$$

We give an alternate expression for $|\mathrm{Aut}_R(G)|$ from [7, p. 181]. We will not need it in this paper, but in some circumstances it is more convenient to use than the expression in Lemma 3.7. Suppose $(R, \mathfrak{m})$ and $\mathbb{F}_q$ are as in the statement of the lemma and G is a finite R-module of type λ. Let $m_i(\lambda)$ be the number of parts of λ of size i and $\lambda'_i = m_i(\lambda) + m_{i+1}(\lambda) + \cdots$. Then,

$$|\mathrm{Aut}_R(G)| = q^{\sum_{i \geqslant 1}(\lambda'_i)^2} \prod_{i \geqslant 1} \prod_{j=1}^{m_i(\lambda)} (1 - q^{-j}).$$

This expression is equivalent to the one from [7, p. 181] since $n(\lambda) = \sum_{i \geqslant 1} \binom{\lambda'_i}{2}$.

For clarity, we state Step (3) of the proof outline given in Section 3.3 as a separate result.

Lemma 3.8. *Let $(R, \mathfrak{m})$ be a complete DVR with a finite residue field $R/\mathfrak{m} = \mathbb{F}_q$ and let u be a uniformizer of R. Let G be a finite R-module with $r_q(G) := \dim_{\mathbb{F}_q}(G/\mathfrak{m}G) = r$ and $N \in \mathbb{Z}_{\geqslant 0}$ satisfy $\mathfrak{m}^N G = 0$. We have*

$$\#\{uA \in u\mathrm{Mat}_r(R/\mathfrak{m}^{N+1}) \colon \mathrm{cok}(uA) \simeq G\} = \frac{q^{Nr^2 + r^2} \prod_{i=1}^{r}(1 - q^{-i})^2}{|\mathrm{Aut}_R(G)|}.$$

As mentioned in Remark 3.3, this result is proven by Friedman and Washington [5, p. 236]. We give a different proof here that more directly considers the conditions on the entries of a matrix that determine whether or not its cokernel is isomorphic to a particular module G.

Proof. As in the proof of Step (2) of Lemma 3.1, choose representatives $\alpha_1, \ldots, \alpha_q \in R/\mathfrak{m}^{N+1}$ for the equivalence classes of $R/\mathfrak{m}$. Every element of $R/\mathfrak{m}^{N+1}$ can be expressed uniquely as $a_0 + a_1 u + a_2 u^2 + \cdots + a_N u^N$, where each a_i is equal to some α_j. Let $uA \in \mathrm{Mat}_r(R/\mathfrak{m}^{N+1})$ and express each entry of uA in this form. We have

$$uA = uA_1 + u^2 A_2 + \cdots + u^N A_N,$$

where each A_i is an $r \times r$ matrix with entries in $\{\alpha_1, \ldots, \alpha_q\}$.

We would like to use Lemma 3.5 to describe the conditions on a matrix in $\mathrm{Mat}_r(R/\mathfrak{m}^{N+1})$ that determine whether or not its cokernel is isomorphic to G. However, Lemma 3.5 only applies for matrices with entries in a PID. Therefore, we take lifts of our matrices to R. Choose $u\tilde{A} \in u\mathrm{Mat}_r(R)$ to be a fixed lift of $uA \in \mathrm{Mat}_r(R/\mathfrak{m}^{N+1})$. We see that for any i, j, the (i, j) entry of $u\tilde{A}$ is congruent to the (i, j) entry of uA modulo $\mathfrak{m}^{N+1}$. Consider the projection map $\pi \colon R \to R/\mathfrak{m}^{N+1}$ and suppose $\alpha'_1, \ldots, \alpha'_q$ satisfy $\pi(\alpha'_i) = \alpha_i$. Note that $\alpha'_1, \ldots, \alpha'_q$ are representatives of the equivalences classes of $R/\mathfrak{m}$. Expressing each entry of $u\tilde{A}$ in terms of its u-adic digit expansion, we can write

$$u\tilde{A} = uA_1 + u^2 A_2 + \cdots + u^N A_N + u^{N+1} A_{N+1} + \cdots$$

where each A_i is an $r \times r$ matrix with entries in $\{\alpha_1', \ldots, \alpha_q'\}$. For ease of notation, we identify A_i with its image in $\mathrm{Mat}_n(\mathbb{F}_q)$ under the map defined by reducing each entry modulo $\mathfrak{m}$. When we refer to the rank of the matrix A_i we always mean the rank of this matrix in $\mathrm{Mat}_n(\mathbb{F}_q)$.

We now apply Lemma 3.5 to $u\tilde{A}$ to determine the conditions on the entries of $A_1, A_2, A_3, \ldots$ that imply $\mathrm{cok}(u\tilde{A}) \simeq G$. Since $u^N G = 0$, Lemma 3.5 implies that $\mathrm{cok}(uA) \simeq G$ if and only if $\mathrm{cok}(u\tilde{A}) \simeq G$. Therefore, these conditions are independent of the choice of $A_{N+1}, A_{N+2}, \ldots$. We count choices of $A_1, \ldots, A_N$ for which $\mathrm{cok}(u\tilde{A}) \simeq G$, completing the proof.

Since R is a PID with unique maximal ideal $\mathfrak{m} = (u)$, by the classification of modules over a PID there are unique integers $e_1 > e_2 > \cdots > e_k \geqslant 1$ and $r_1, \ldots, r_k \geqslant 1$ such that

$$G \simeq (R/\mathfrak{m}^{e_1})^{r_1} \times \cdots \times (R/\mathfrak{m}^{e_k})^{r_k} = (R/u^{e_1}R)^{r_1} \times \cdots \times (R/u^{e_k}R)^{r_k}.$$

Since $r = r_q(G)$, we have $r_1 + \cdots + r_k = r$. By assumption, $u^N G = 0$, which is equivalent to $N \geqslant e_1$.

The invariant factors of $\mathrm{cok}(u\tilde{A})$ are only determined up to multiplication by a unit, so we can assume each one is of the form u^m for some $m \geqslant 1$. We order the invariant factors by these exponents since $u^{m_1} \mid u^{m_2}$ if and only if $m_1 \leqslant m_2$. By Lemma 3.5, the smallest invariant factor of $\mathrm{cok}(u\tilde{A})$ is equal to the greatest common divisor of the 1×1 minors of $u\tilde{A}$. Therefore, u^{e_k} is the smallest invariant factor of $\mathrm{cok}(u\tilde{A})$ if and only if $A_1 = A_2 = \cdots = A_{e_k - 1} = 0$ and A_{e_k} is nonzero.

Our next goal is to count the invariant factors of this smallest size.

Claim: Suppose that $A_1 = A_2 = \cdots = A_{e_k - 1} = 0$. Then $\mathrm{cok}(u\tilde{A})$ has exactly r_k invariant factors u^{e_k} if and only if A_{e_k} has rank r_k.

Proof of Claim. The rank of A_{e_k} is the largest m such that there exists a nonzero $m \times m$ minor of A_{e_k}. Suppose $i \in [1, r]$. By Lemma 3.5 applied to $u\tilde{A}$, we have $s_1 \cdots s_i = \gcd(i \times i \text{ minors of } u\tilde{A})$. As explained above, since $A_1 = A_2 = \cdots = A_{e_k - 1} = 0$, if $A_{e_k} \neq 0$, then $u^{e_k} = s_1$ is the smallest invariant factor of $\mathrm{cok}(u\tilde{A})$. Since $s_1 \mid \cdots \mid s_i$, we see that $(u^{e_k})^i \mid s_1 \cdots s_i$.

If there exists a nonzero $r_k \times r_k$ minor of A_{e_k}, then there is an $r_k \times r_k$ minor of $u\tilde{A}$ equal to $(u^{e_k})^{r_k}$ times a unit in R. This implies $\gcd(r_k \times r_k \text{ minors of } u\tilde{A}) = (u^{e_k})^{r_k}$, and therefore $\mathrm{cok}(u\tilde{A})$ has at least r_k invariant factors equal to u^{e_k}.

By the same reasoning, if there is a nonzero $(r_k + 1) \times (r_k + 1)$ minor of A_{e_k}, then $\mathrm{cok}(u\tilde{A})$ has at least $r_k + 1$ invariant factors equal to u^{e_k}. Therefore, $\mathrm{cok}(u\tilde{A})$ has exactly r_k invariant factors equal to u^{e_k} if and only if $A_{e_k} \in \mathrm{Mat}_r(\mathbb{F}_q)$ has rank r_k. $\quad \square$

Given $A_1 = A_2 = \cdots = A_{e_k - 1} = 0$ and A_{e_k} with rank r_k, we find the constraints on $A_{e_k + 1}, A_{e_k + 2}, \ldots$ that determine whether $\mathrm{cok}(u\tilde{A})$ has no invariant factors between u^{e_k} and $u^{e_{k-1}}$ and exactly r_{k-1} invariant factors equal to $u^{e_{k-1}}$. Since A_{e_k} has rank r_k, there exist $P_{A_{e_k}}, Q_{A_{e_k}} \in \mathrm{GL}_r(\mathbb{F}_q)$ such that

$$P_{A_{e_k}} A_{e_k} Q_{A_{e_k}} = \begin{bmatrix} 0 & 0 \\ 0 & I_{r_k} \end{bmatrix}.$$

Let $P'_{A_{e_k}}$ be an arbitrary lift of $P_{A_{e_k}}$ to $\mathrm{GL}_r(R)$ and $Q'_{A_{e_k}}$ be an arbitrary lift of $Q_{A_{e_k}}$ to $\mathrm{GL}_r(R)$. We have

$$\mathrm{cok}(u\tilde{A}) \simeq \mathrm{cok}(P'_{A_{e_k}} u\tilde{A} Q'_{A_{e_k}}) = \mathrm{cok}\left(u^{e_k} A'_{e_k} + u^{e_k+1} A'_{e_k+1} + \cdots\right),$$

where $A'_j = P'_{A_{e_k}} A_j Q'_{A_{e_k}}$.

We claim that the next smallest size of an invariant factor of $\mathrm{cok}(u\tilde{A})$ after u^{e_k} is $u^{e_{k-1}}$ if and only if $A'_{e_k+1}, \ldots, A'_{e_{k-1}-1}$ have all of their entries in the top left $(r-r_k) \times (r-r_k)$ corner equal to 0 and $A'_{e_{k-1}}$ has a nonzero entry in its top left $(r-r_k) \times (r-r_k)$ corner.

Suppose $j \in [e_k+1, e_{k-1}-1]$. If A'_j has a nonzero entry in its top left $(r-r_k) \times (r-r_k)$ corner, then there is an $(r_k+1) \times (r_k+1)$ minor of $u\tilde{A}$ equal to $u^j(u^{e_k})^{r_k}$ times a unit in R. Lemma 3.5 now implies that the next smallest invariant factor of $\mathrm{cok}(u\tilde{A})$ after u^{e_k} has size at most u^j.

Now suppose $A'_{e_k+1}, \ldots, A'_{e_{k-1}-1}$ have all of their entries in the top left $(r-r_k) \times (r-r_k)$ corner equal to 0. Every $(r_k+1) \times (r_k+1)$ minor of $P'_{A_{e_k}} u\tilde{A} Q'_{A_{e_k}}$ is divisible by $u^{e_{k-1}}(u^{e_k})^{r_k}$. Lemma 3.5 implies that the next smallest invariant factor of $\mathrm{cok}(u\tilde{A})$ after u^{e_k} is at least $u^{e_{k-1}}$. If there is a nonzero entry in the top left $(r-r_k) \times (r-r_k)$ corner of $A'_{e_{k-1}}$, then there is an $(r_k+1) \times (r_k+1)$ minor of $u\tilde{A}$ equal to $u^{e_{k-1}}(u^{e_k})^{r_k}$ times a unit in R. If every entry in the top left $(r-r_k) \times (r-r_k)$ corner of $A'_{e_{k-1}}$ is 0, then every $(r_k+1) \times (r_k+1)$ minor of $u\tilde{A}$ is divisible by $u^{e_{k-1}+1}(u^{e_k})^{r_k}$. Thus, this next smallest invariant factor of $\mathrm{cok}(u\tilde{A})$ is equal to $u^{e_{k-1}}$ if and only if there is a nonzero entry in the top left $(r-r_k) \times (r-r_k)$ corner of $A'_{e_{k-1}}$.

Suppose that the second smallest invariant factor of $\mathrm{cok}(u\tilde{A})$ is equal to $u^{e_{k-1}}$. We now determine the number of invariant factors of this size. For any t, the greatest common divisor of the $(r_k+t) \times (r_k+t)$ minors of $P'_{A_{e_k}} u\tilde{A} Q'_{A_{e_k}}$ is divisible by $(u^{e_k})^{r_k}(u^{e_{k-1}})^t$. By Lemma 3.5, there are at least t invariant factors of $\mathrm{cok}(u\tilde{A})$ equal to $u^{e_{k-1}}$ if and only if there is an $(r_k+t) \times (r_k+t)$ minor of $P'_{A_{e_k}} u\tilde{A} Q'_{A_{e_k}}$ equal to $(u^{e_k})^{r_k}(u^{e_{k-1}})^t$ times a unit in R.

Consider the top left $(r-r_k) \times (r-r_k)$ corner of $A'_{e_{k-1}}$. Suppose it has rank t. This matrix has a nonzero $t \times t$ minor, but each of its $(t+1) \times (t+1)$ minors is 0. Therefore, there is a $(r_k+t) \times (r_k+t)$ minor of $P'_{A_{e_k}} u\tilde{A} Q'_{A_{e_k}}$ equal to $(u^{e_k})^{r_k}(u^{e_{k-1}})^t$ times a unit in R, but no $(r_k+t+1) \times (r_k+t+1)$ minor of $P'_{A_{e_k}} u\tilde{A} Q'_{A_{e_k}}$ is equal to $(u^{e_k})^{r_k}(u^{e_{k-1}})^{t+1}$ times a unit in R. We conclude that $\mathrm{cok}(u\tilde{A})$ has exactly r_{k-1} invariant factors equal to $u^{e_{k-1}}$ if and only if $t = r_{k-1}$. As above, we multiply by appropriate $P'_{A_{e_{k-1}}}, Q'_{A_{e_{k-1}}} \in \mathrm{GL}_r(R)$. We then repeat this argument for the remaining invariant factors of G.

When considering the matrix that determines the number of invariant factors of $\mathrm{cok}(u\tilde{A})$ equal to u^{e_1}, we need the top left $r_1 \times r_1$ piece of an $(r_1+r_2) \times (r_1+r_2)$ submatrix to have rank r_1. There are no conditions on the remaining $2r_1 r_2 + r_2^2$ entries of this submatrix. Similarly, when we consider the matrix that determines the number of

invariant factors of $\mathrm{cok}(u\tilde{A})$ equal to u^{e_2}, we need the top left $(r_1 + r_2) \times (r_1 + r_2)$ piece of an $(r_1 + r_2 + r_3) \times (r_1 + r_2 + r_3)$ submatrix to have rank r_2. There are no conditions on the remaining $2(r_1 + r_2)r_3 + r_3^2$ entries of this submatrix. Continuing in this way, we see that the total number of choices of $uA \in \mathrm{Mat}_r(R/\mathfrak{m}^{N+1})$ for which $\mathrm{cok}(u\tilde{A}) \simeq G$ is equal to

$$\left(\prod_{i=0}^{k-1} \# \left\{ \begin{array}{c} X \in \mathrm{Mat}_{r-(r_k+r_{k-1}+\cdots+r_{k-i+1})}(\mathbb{F}_q): \\ \mathrm{rank}(X) = r_{k-i} \end{array} \right\} \right) \left(q^{\sum_{i=1}^{k}(N-e_i)(r_i^2 + 2r_i \sum_{1\leqslant j<i} r_j)} \right).$$

We have

$$q^{\sum_{i=1}^{k}(N-e_i)(r_i^2 + 2r_i \sum_{1\leqslant j<i} r_j)} = q^{Nr^2 - \sum_{i=1}^{k} e_i r_i^2 - 2\sum_{1\leqslant j<i\leqslant k} e_i r_i r_j}$$

$$= \frac{q^{Nr^2}}{\prod_{1\leqslant i,j\leqslant k} q^{\min(e_i,e_j)r_i r_j}}$$

since $r = r_1 + \cdots + r_k$.

Applying Lemma 3.6 shows that

$$\prod_{i=0}^{k-1} \# \left\{ \begin{array}{c} X \in \mathrm{Mat}_{r-(r_k+r_{k-1}+\cdots+r_{k-i+1})}(\mathbb{F}_q): \\ \mathrm{rank}(X) = r_{k-i} \end{array} \right\}$$

$$= q^{r^2} \frac{(1-q^{-1})^2(1-q^{-2})^2 \cdots (1-q^{-r})^2}{((1-q^{-1})(1-q^{-2})\cdots(1-q^{-r_1}))\cdots((1-q^{-1})(1-q^{-2})\cdots(1-q^{-r_k}))}$$

$$= q^{r^2} \frac{\prod_{i=1}^{r}(1-q^{-i})^2}{q^{-(r_1^2+\cdots+r_k^2)}|\mathrm{GL}_{r_1}(\mathbb{F}_q)|\cdots|\mathrm{GL}_{r_k}(\mathbb{F}_q)|}.$$

Therefore, we have

$$\left(\prod_{i=0}^{k-1} \# \left\{ \begin{array}{c} X \in \mathrm{Mat}_{r-(r_k+r_{k-1}+\cdots+r_{k-i+1})}(\mathbb{F}_q): \\ \mathrm{rank}(X) = r_{k-i} \end{array} \right\} \right) \left(q^{\sum_{i=1}^{k}(N-e_i)(r_i^2 + 2r_i \sum_{1\leqslant j<i} r_j)} \right)$$

$$= \frac{q^{Nr^2+r^2} \prod_{i=1}^{r}(1-q^{-i})^2}{\prod_{i=1}^{k} q^{-r_i^2} |\mathrm{GL}_{r_i}(\mathbb{F}_q)| \prod_{1\leqslant i,j\leqslant k} q^{\min(e_i,e_j)r_i r_j}}$$

$$= \frac{q^{Nr^2+r^2} \prod_{i=1}^{r}(1-q^{-i})^2}{|\mathrm{Aut}_R(G)|},$$

where in the last step we applied Lemma 3.7. □

4. The proof of Theorem 1.6

In this section, we use the special case of Theorem 1.6 where $l = 1$ to prove Theorem 1.6 in general. We first recall some notation and assumptions. We are given

- monic polynomials $P_1(t), \ldots, P_l(t) \in \mathbb{Z}_p[t]$ of degree at most 2 whose images in $\mathbb{F}_p[t]$ are distinct and irreducible and a finite module G_j over $\mathbb{Z}_p[t]/(P_j(t))$ for each $1 \leqslant j \leqslant l$,
- $N \in \mathbb{Z}_{\geqslant 0}$ such that $p^N G_j = 0$ for each $1 \leqslant j \leqslant l$, and
- $\bar{X} \in \mathrm{Mat}_n(\mathbb{F}_p)$ such that for each $1 \leqslant j \leqslant l$,

$$\dim_{\mathbb{F}_{q_j}}\bigl(\mathrm{cok}(P_j(\bar{X}))\bigr) = r_{q_j}(G_j),$$

where $q_j = p^{\deg(P_j)}$.

We count lifts $X \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})$ of $\bar{X}$ such that for each $1 \leqslant j \leqslant l$ we have $\mathrm{cok}(P_j(X)) \simeq G_j$.

Proof of Theorem 1.6. We use an argument similar to two steps of the proof outline given for Lemma 3.1 in Section 3.3. There exists $\bar{Q} \in \mathrm{GL}_n(\mathbb{F}_p)$ such that

$$\bar{Q}^{-1}\bar{X}\bar{Q} = \begin{bmatrix} J_1 & 0 & \cdots & 0 & 0 \\ 0 & J_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & J_l & 0 \\ 0 & 0 & \cdots & 0 & M \end{bmatrix},$$

where each eigenvalue of J_j over $\overline{\mathbb{F}}_p$ is a root of $P_j(t)$ and M is a square matrix over $\mathbb{F}_p$ with no eigenvalue over $\overline{\mathbb{F}}_p$ that is a root of any of $P_1(t), \ldots, P_l(t)$. Note that if G_j is trivial, then J_j is the empty matrix.

Fix a lift $Q \in \mathrm{GL}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})$ of $\bar{Q} \in \mathrm{GL}_n(\mathbb{F}_p)$. Given a lift $X \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})$ of $\bar{X} \in \mathrm{Mat}_n(\mathbb{F}_p)$, the matrix $Q^{-1}XQ$ is a lift of $\bar{Q}^{-1}\bar{X}\bar{Q}$. On the other hand, if $Y \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})$ is a lift of $\bar{Q}^{-1}\bar{X}\bar{Q}$, then QYQ^{-1} is a lift of $\bar{X}$. Note that $P_j(Q^{-1}XQ) = Q^{-1}P_j(X)Q$. As in Step (1) of the proof of Lemma 3.1 described in Section 3.3, taking advantage of this bijection between the lifts of $\bar{X}$ and the lifts of $\bar{Q}^{-1}\bar{X}\bar{Q}$, it is enough to prove Theorem 1.6 for the case where

$$\bar{X} = \begin{bmatrix} J_1 & 0 & \cdots & 0 & 0 \\ 0 & J_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & J_l & 0 \\ 0 & 0 & \cdots & 0 & M \end{bmatrix}.$$

Fix $j \in [1, l]$ and let $R_j := (\mathbb{Z}/p^{N+1}\mathbb{Z})[t]/(P_j(t))$. Over $R_j/pR_j = \mathbb{F}_p[t]/(P_j(t))$, the matrix $J_j - \bar{t}\,\mathrm{id}$ is not invertible, while for any $k \neq j$, the matrix $J_k - \bar{t}\,\mathrm{id}$ is invertible. The matrix $M - \bar{t}\,\mathrm{id}$ is also invertible.

Any lift $X \in \mathrm{Mat}_n(\mathbb{Z}/p^{N+1}\mathbb{Z})$ of $\bar{X}$ is of the form

$$
X = \begin{bmatrix}
pA_{11} + J_1 & pA_{12} & \cdots & pA_{1l} & pA_{1,l+1} \\
pA_{21} & pA_{22} + J_2 & \cdots & pA_{2l} & pA_{2,l+1} \\
\vdots & \vdots & \cdots & \vdots & \vdots \\
pA_{l1} & pA_{l2} & \cdots & pA_{ll} + J_l & pA_{l,l+1} \\
pA_{l+1,1} & pA_{l+1,2} & \cdots & pA_{l+1,l} & pA_{l+1,l+1} + M
\end{bmatrix},
$$

where the pA_{st} are matrices over $\mathbb{Z}/p^{N+1}\mathbb{Z}$ all of whose entries are 0 modulo p, and each of $J_1, \ldots, J_l, M$ is the unique lift to $\mathbb{Z}/p^{N+1}\mathbb{Z}$ with entries in $\{0, 1, \ldots, p-1\}$ of the corresponding matrix over $\mathbb{F}_p$. Let $n_1, \ldots, n_l, n_{l+1} \in \mathbb{Z}_{\geqslant 0}$ so that $pA_{ii} \in p\mathrm{Mat}_{n_i}(\mathbb{Z}/p^{N+1}\mathbb{Z})$ for $1 \leqslant i \leqslant l+1$. In particular, $n = n_1 + \cdots + n_l + n_{l+1}$.

A key idea in this argument is to work with expansions of elements of $\mathbb{Z}/p^{N+1}\mathbb{Z}$ in terms of powers of p, and to use these expansions of elements to give similar expansions for matrices. Each entry of pA_{st} is of the form $a_1 p + a_2 p^2 + \cdots + a_{N-1}p^{N-1} + a_N p^N$, where $a_i \in \{0, 1, \ldots, p-1\}$. Without any constraints there are p^{Nn^2} total lifts X of $\bar{X}$. Recall that by Lemma 3.2, we have $\mathrm{cok}(P_j(X)) \simeq \mathrm{cok}_{R_j}(X - \bar{t}I_n)$.

We choose a sequence of (block) row and column operations from Lemma 3.4 to transform the matrix $X - \bar{t}I_n$, which is equal to

$$
\begin{bmatrix}
pA_{11} + J_1 - \bar{t}\mathrm{id} & pA_{12} & \cdots & pA_{1l} & pA_{1,l+1} \\
pA_{21} & pA_{22} + J_2 - \bar{t}\mathrm{id} & \cdots & pA_{2l} & pA_{2,l+1} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
pA_{l1} & pA_{l2} & \cdots & pA_{ll} + J_l - \bar{t}\mathrm{id} & pA_{l,l+1} \\
pA_{l+1,1} & pA_{l+1,2} & \cdots & pA_{l+1,l} & pA_{l+1,l+1} + M - \bar{t}\mathrm{id}
\end{bmatrix} \tag{3}
$$

into the block diagonal matrix whose blocks are given by

$$
pA_{11} + J_1 - \bar{t}\mathrm{id} + p^2 B_1^{(j)} + \bar{t}p^2 C_1^{(j)}, \ldots, pA_{ll} + J_l - \bar{t}\mathrm{id} + p^2 B_l^{(j)} + \bar{t}p^2 C_l^{(j)}, pA_{l+1,l+1} + M - \bar{t}\mathrm{id},
$$

where $p^2 B_i^{(j)}, p^2 C_i^{(j)} \in p^2\mathrm{Mat}_{n_i}(\mathbb{Z}/p^{N+1}\mathbb{Z})$ depend on pA_{st} with $1 \leqslant s, t \leqslant l+1$ except they do not depend on pA_{ii}. We conclude that $X - \bar{t}I_n$ and this block diagonal matrix have isomorphic cokernels over R_j.

Suppose $i, j \in [1, l]$ are distinct. Since $J_i - \bar{t}\mathrm{id}$ is invertible over R_j/pR_j, we see that $pA_{ii} + J_i - \bar{t}\mathrm{id} + p^2 B_i^{(j)} + \bar{t}p^2 C_i^{(j)}$ is invertible over R_j. Similarly, $pA_{l+1,l+1} + M - \bar{t}\mathrm{id}$ is invertible over R_j. This implies

$$
\begin{aligned}
\mathrm{cok}(P_j(X)) &\simeq \mathrm{cok}_{R_j}(X - \bar{t}I_n) \\
&\simeq \mathrm{cok}_{R_j}(pA_{jj} + J_j - \bar{t}\mathrm{id} + p^2 B_j^{(j)} + \bar{t}p^2 C_j^{(j)}) \\
&= \mathrm{cok}_{R_j}(J_j + pA_{jj} + p^2 B_j^{(j)} - \bar{t}(\mathrm{id} - p^2 C_j^{(j)})).
\end{aligned}
$$

Multiplying by an invertible matrix does not change the isomorphism class of the cokernel, so

$$\mathrm{cok}_{R_j}(J_j + pA_{jj} + p^2 B_j^{(j)} - \bar{t}(\mathrm{id} - p^2 C_j^{(j)}))$$

$$\simeq \mathrm{cok}_{R_j}((\mathrm{id} - p^2 C_j^{(j)})^{-1}(J_j + pA_{jj} + p^2 B_j^{(j)}) - \bar{t}\mathrm{id})$$

$$\simeq \mathrm{cok}\big(P_j\big((\mathrm{id} - p^2 C_j^{(j)})^{-1}(J_j + pA_{jj} + p^2 B_j^{(j)})\big)\big).$$

Fix any choices for $\{pA_{st} : 1 \leqslant s, t \leqslant l+1, \ s \neq t\}$ and also fix a choice of $pA_{l+1,l+1}$. Note that there are $p^{N(n^2 - (n_1^2 + \cdots + n_l^2))}$ total possible choices for these matrices. The matrices $p^2 B_i^{(j)}, p^2 C_i^{(j)} \in p^2\mathrm{Mat}_{n_i}(\mathbb{Z}/p^{N+1}\mathbb{Z}))$ play an important role in our proof. Given choices for the pA_{st} above and for $pA_{l+1,l+1}$ we can think of $p^2 B_i^{(j)}$ and $p^2 C_i^{(j)}$ as being functions of $(pA_{11}, \ldots, pA_{i-1,i-1}, pA_{i+1,i+1}, \ldots, pA_{ll})$. We usually do not usually include this dependence in the notation for $p^2 B_i^{(j)}$ and $p^2 C_i^{(j)}$ because it would make things much harder to read, but in a few cases we include this additional notation for emphasis.

Consider the function Φ_N that takes $(pA_{11}, pA_{22}, \ldots, pA_{ll})$ to

$$\left((\mathrm{id} - p^2 C_1^{(1)})^{-1}(J_1 + pA_{11} + p^2 B_1^{(1)}), \cdots, (\mathrm{id} - p^2 C_l^{(l)})^{-1}(J_l + pA_{ll} + p^2 B_l^{(l)})\right).$$

So Φ_N is a map from $p\mathrm{Mat}_{n_1}(\mathbb{Z}/p^{N+1}\mathbb{Z}) \times \cdots \times p\mathrm{Mat}_{n_l}(\mathbb{Z}/p^{N+1}\mathbb{Z})$ to

$$\left\{ \begin{array}{c} Y_1 \in \mathrm{Mat}_{n_1}(\mathbb{Z}/p^{N+1}\mathbb{Z}): \\ Y_1 \equiv J_1 \pmod{p} \end{array} \right\} \times \cdots \times \left\{ \begin{array}{c} Y_l \in \mathrm{Mat}_{n_l}(\mathbb{Z}/p^{N+1}\mathbb{Z}): \\ Y_l \equiv J_l \pmod{p} \end{array} \right\}.$$

Claim: Φ_N is a bijection.

Assuming the claim for now, we complete the proof of Theorem 1.6. By the discussion above, $\mathrm{cok}(P_j(X)) \simeq G_j$ for each j if and only if $\mathrm{cok}\big(P_j\big((\mathrm{id} - p^2 C_j^{(j)})^{-1}(J_j + pA_{jj} + p^2 B_j^{(j)})\big)\big) \simeq G_j$ for each j. Since Φ_N is a bijection, the number of choices for $(pA_{11}, \ldots, pA_{ll})$ such that $\mathrm{cok}(P_j(X)) \simeq G_j$ for each j is equal to

$$\# \left\{ \begin{array}{c} (Y_1, \ldots, Y_l) \in \mathrm{Mat}_{n_1}(\mathbb{Z}/p^{N+1}\mathbb{Z}) \times \cdots \times \mathrm{Mat}_{n_l}(\mathbb{Z}/p^{N+1}\mathbb{Z}) : \\ \mathrm{cok}(P_j(Y_j)) \simeq G_j \text{ and } Y_j \equiv J_j \pmod{p} \text{ for } 1 \leqslant j \leqslant l \end{array} \right\}.$$

It is clear that this is equal to

$$\prod_{j=1}^{l} \# \left\{ \begin{array}{c} Y_j \in \mathrm{Mat}_{n_j}(\mathbb{Z}/p^{N+1}\mathbb{Z}) : \\ \mathrm{cok}(P_j(Y_j)) \simeq G_j \text{ and } Y_j \equiv J_j \pmod{p} \end{array} \right\}.$$

By the $l = 1$ case of Theorem 1.6, this is equal to

$$\prod_{j=1}^{l} p^{Nn_j^2} \frac{q_j^{r_{q_j}(G_j)^2} \prod_{i=1}^{r_{q_j}(G_j)} (1 - q_j^{-i})^2}{|\mathrm{Aut}_{\mathbb{Z}_p[t]/(P_j(t))}(G_j)|}.$$

Multiplying by $p^{N(n^2 - (n_1^2 + \cdots + n_l^2))}$ to account for all possible choices of $\{pA_{st} : 1 \leqslant s, t \leqslant l+1, \ s \neq t\}$ and $pA_{l+1,l+1}$ completes the proof of Theorem 1.6.

We now need only prove that Φ_N is a bijection. Since Φ_N is a map between finite sets of the same size, we need only prove that it is surjective. We define a sequence of maps $\Phi_1, \ldots, \Phi_{N-1}, \Phi_N$ and prove that each one is a bijection. Let $k \in [1, N]$. Our next goal is to define the map Φ_k.

- For each element of $\{pA_{st} \colon 1 \leqslant s, t \leqslant l + 1, \ s \neq t\}$, let $pA_{st}^{[k]}$ be the matrix over $\mathbb{Z}/p^{k+1}\mathbb{Z}$ such that $pA_{st} \equiv pA_{st}^{[k]} \pmod{p^{k+1}}$.
- Let $pA_{l+1,l+1}^{[k]}$ be the matrix over $\mathbb{Z}/p^{k+1}\mathbb{Z}$ such that $pA_{l+1,l+1} \equiv pA_{l+1,l+1}^{[k]} \pmod{p^{k+1}}$.

For each $j \in [1, l]$, choose a matrix $pA_{jj} \in \mathrm{Mat}_{n_j}(\mathbb{Z}/p^{k+1}\mathbb{Z})$. We construct a matrix analogous to the one given in (3) using $pA_{11}, \ldots, pA_{ll}, pA_{l+1,l+1}^{[k]}$ and the elements of $\{pA_{st}^{[k]} \colon 1 \leqslant s, t \leqslant l + 1, \ s \neq t\}$. We then apply the same sequence of (block) row and column operations that we applied to the matrix in (3). This gives a block diagonal matrix whose blocks are given by

$$pA_{11} + J_1 - \bar{t}\mathrm{id} + p^2 B_1^{(j,k)} + \bar{t}p^2 C_1^{(j,k)}, \ldots, pA_{ll} + J_l - \bar{t}\mathrm{id} + p^2 B_l^{(j,k)} + \bar{t}p^2 C_l^{(j,k)},$$

$$pA_{l+1,l+1} + M - \bar{t}\mathrm{id},$$

where $p^2 B_i^{(j,k)}, p^2 C_i^{(j,k)} \in p^2 \mathrm{Mat}_{n_i}(\mathbb{Z}/p^{k+1}\mathbb{Z})$ are functions of the collection of matrices $(pA_{11}, \ldots, pA_{i-1,i-1}, pA_{i+1,i+1}, \ldots, pA_{ll})$. A key thing to note is that for any $1 \leqslant k' \leqslant k \leqslant N$, if $pA_{jj} \equiv pA_{jj}' \pmod{p^{k'+1}}$ for each $j \in [1, l]$, then

$$p^2 B_i^{(j,k)}(pA_{11}, \ldots, pA_{i-1,i-1}, pA_{i+1,i+1}, \ldots, pA_{ll})$$

$$\equiv \quad p^2 B_i^{(j,k')}(pA_{11}', \ldots, pA_{i-1,i-1}', pA_{i+1,i+1}', \ldots, pA_{ll}') \pmod{p^{k'+1}}.$$

An analogous result holds for the matrices $p^2 C_i^{(j,k)}$ and $p^2 C_i^{(j,k')}$.

We define a map

$$\Phi_k \colon p\mathrm{Mat}_{n_1}(\mathbb{Z}/p^{k+1}\mathbb{Z}) \times \cdots \times p\mathrm{Mat}_{n_l}(\mathbb{Z}/p^{k+1}\mathbb{Z}) \to$$

$$\left\{ \begin{array}{c} Y_1 \in \mathrm{Mat}_{n_1}(\mathbb{Z}/p^{k+1}\mathbb{Z}) \colon \\ Y_1 \equiv J_1 \pmod{p} \end{array} \right\} \times \cdots \times \left\{ \begin{array}{c} Y_l \in \mathrm{Mat}_{n_l}(\mathbb{Z}/p^{k+1}\mathbb{Z}) \colon \\ Y_l \equiv J_l \pmod{p} \end{array} \right\}$$

that takes $(pA_{11}, pA_{22}, \ldots, pA_{ll})$ to

$$\left((\mathrm{id} - p^2 C_1^{(1,k)})^{-1}(J_1 + pA_{11} + p^2 B_1^{(1,k)}), \cdots, (\mathrm{id} - p^2 C_l^{(l,k)})^{-1}(J_l + pA_{ll} + p^2 B_l^{(l,k)}) \right).$$

Now that we have defined $\Phi_1, \ldots, \Phi_N$, we see that they are compatible with reducing the inputs modulo powers of p. More precisely, for any $1 \leqslant k' \leqslant k \leqslant N$, if $pA_{jj} \equiv pA_{jj}' \pmod{p^{k'+1}}$ for every $j \in [1, l]$, then

$$\Phi_k(pA_{11}, pA_{22}, \ldots, pA_{ll}) \equiv \Phi_{k'}(pA'_{11}, pA'_{22}, \ldots, pA'_{ll}) \pmod{p^{k'+1}}.$$

We now prove that Φ_1 is a bijection. We have

$$(\mathrm{id} - p^2 C_j^{(j,1)})^{-1}(J_j + pA_{jj} + p^2 B_j^{(j,1)}) \equiv J_j + pA_{jj} \pmod{p^2},$$

so it is clear that Φ_1 is a bijection.

We now assume that Φ_{k-1} is a bijection and prove that Φ_k is a surjection. Choose $(Y_1, \ldots, Y_l)$ such that for each j, we have $Y_j \in \mathrm{Mat}_{n_j}(\mathbb{Z}/p^{k+1}\mathbb{Z})$ with $Y_j \equiv J_j \pmod{p}$. Such a matrix can be written uniquely as

$$Y_j = J_j + pS_j^{[1]} + p^2 S_j^{[2]} + \cdots + p^k S_j^{[k]},$$

where each $S_j^{[i]}$ is an $n_j \times n_j$ matrix with entries in $\{0, 1, \ldots, p-1\}$. Define $Y'_j \in \mathrm{Mat}_{n_j}(\mathbb{Z}/p^k\mathbb{Z})$ by

$$Y'_j = J_j + pS_j^{[1]} + p^2 S_j^{[2]} + \cdots + p^{k-1} S_j^{[k-1]},$$

so $Y_j \equiv Y'_j \pmod{p^k}$.

Since Φ_{k-1} is a bijection, there exists $(pA'_{11}, \ldots, pA'_{ll}) \in p\mathrm{Mat}_{n_1}(\mathbb{Z}/p^k\mathbb{Z}) \times \cdots \times p\mathrm{Mat}_{n_l}(\mathbb{Z}/p^k\mathbb{Z})$ such that for each $j \in [1, l]$,

$$(\mathrm{id} - p^2 C_j^{(j,k-1)})^{-1}(J_j + pA'_{jj} + p^2 B_j^{(j,k-1)}) = J_j + pS_j^{[1]} + p^2 S_j^{[2]} + \cdots + p^{k-1} S_j^{[k-1]} = Y'_j.$$

There are unique $n_j \times n_j$ matrices $T_j^{[k']}$ with entries in $\{0, 1, \ldots, p-1\}$ such that

$$pA'_{jj} = pT_j^{[1]} + p^2 T_j^{[2]} + \cdots + p^{k-1} T_j^{[k-1]}.$$

Let $pA_j^*(T_j^{[k]}) \in p\mathrm{Mat}_{n_j}(\mathbb{Z}/p^{k+1}\mathbb{Z})$ be defined by

$$pA_j^*(T_j^{[k]}) = \left(pT_j^{[1]} + p^2 T_j^{[2]} + \cdots + p^{k-1} T_j^{[k-1]} \right) + p^k T_j^{[k]},$$

where $T_j^{[k]}$ is an $n_j \times n_j$ matrix with entries in $\{0, 1, \ldots, p-1\}$.

We claim that there exist $T_1^{[k]}, \ldots, T_l^{[k]}$ such that

$$\Phi_k\left(pA_1^*(T_1^{[k]}), \ldots, pA_l^*(T_l^{[k]}) \right) = (Y_1, \ldots, Y_l).$$

For any choice of $(T_1^{[k]}, \ldots, T_l^{[k]})$, since for each $j \in [1, l]$ we have $pA_j^*(T_j^{[k]}) \equiv pA'_{jj} \pmod{p^k}$, we see that

$$\Phi_k(pA_1^*(T_1^{[k]}), \ldots, pA_l^*(T_l^{[k]})) \equiv \Phi_{k-1}(pA'_{11}, \ldots, pA'_{ll}) = (Y'_1, \ldots, Y'_l) \pmod{p^k}.$$

For each j there exists an $n_j \times n_j$ matrix S_j^* with entries in $\{0, 1, \dots, p-1\}$ such that

$$(\mathrm{id} - p^2 C_j^{(j,k)})^{-1}(J_j + pA_j^*(T_j^{[k]}) + p^2 B_j^{(j,k)})$$
$$= J_j + pS_j^{[1]} + p^2 S_j^{[2]} + \cdots + p^{k-1} S_j^{[k-1]} + p^k S_j^* \in \mathrm{Mat}_{n_j}(\mathbb{Z}/p^{k+1}\mathbb{Z}).$$

The crucial observation is that because of the factor of p^2,

$$p^2 B_j^{(j,k)}(pA_1^*(T_1^{[k]}), \dots, pA_l^*(T_l^{[k]})) \quad \text{and} \quad p^2 C_j^{(j,k)}(pA_1^*(T_1^{[k]}), \dots, pA_l^*(T_l^{[k]}))$$

depend on $pA_1^*(T_1^{[k]}), \dots, pA_l^*(T_l^{[k]})$ but they do not depend on $T_1^{[k]}, \dots, T_l^{[k]}$. That is, once we have fixed choices for $(T_i^{[1]}, \dots, T_i^{[k-1]})$ for each i, the matrices $p^2 B_j^{(j,k)}, p^2 C_j^{(j,k)}$ are determined. Therefore, we see that each S_j^* depends only on a choice of $T_j^{[k]}$ and not on the choices for $T_i^{[k]}$ where $i \neq j$.

By definition, a different choice of $T_j^{[k]}$ gives a different matrix $pA_j^*(T_j^{[k]})$. It is now clear that a different matrix $pA_j^*(T_j^k)$ gives a different matrix S_j^*. That is, the map taking $T_j^{[k]}$ to

$$(\mathrm{id} - p^2 C_j^{(j,k)})^{-1}(J_j + pA_j^*(T_j^{[k]}) + p^2 B_j^{(j,k)}) \in \left\{ \begin{array}{c} Y_j^* \in \mathrm{Mat}_{n_j}(\mathbb{Z}/p^{k+1}\mathbb{Z}) \colon \\ Y_j^* \equiv Y_j' \pmod{p^k} \end{array} \right\}$$

is injective. Since this is an injective map between finite sets of the same size, it is a bijection. We conclude that there is a choice of $(T_1^{[k]}, \dots, T_l^{[k]})$ such that for each $j \in [1, l]$, we have

$$(\mathrm{id} - p^2 C_j^{(j,k)})^{-1}(J_j + pA_j^*(T_j^{[k]}) + p^2 B_j^{(j,k)}) = Y_j.$$

Therefore, Φ_k is a surjection and so, a bijection. Continuing in this way, we conclude that Φ_N is a bijection. $\square$

Acknowledgments

References

[1] G. Cheong, Y. Huang, Cohen–Lenstra distributions via random matrices over complete discrete valuation rings with finite residue fields, Ill. J. Math. 65 (2) (2021) 385–415.
[2] H. Cohen, H.W. Lenstra Jr., Heuristics on class groups of number fields, in: Proceedings of the Journees Arithmetiques Held at Noordwijkerhout, the Netherlands, July 11–15, 1983, in: Lecture Notes in Mathematics, vol. 1068, Springer-Verlag, New York, 1983, pp. 33–62.

[3] J. Ellenberg, A. Venkatesh, C. Westerland, Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields, Ann. Math. (2) 183 (3) (2016) 729–786.

[4] S. Evans, Elementary divisors and determinants of random matrices over a local field, Stoch. Process. Appl. 102 (1) (2002) 89–102.

[5] E. Friedman, 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, pp. 227–239.

[6] J. Lee, Joint distribution of the cokernels of random p-adic matrices, preprint, 17 pp., https://arxiv.org/abs/2201.09572, 2022.

[7] I.G. Macdonald, Symmetric Functions and Hall Polynomials, second edition, Oxford University Press, New York, 1995.

[8] R. Van Peski, Limits and fluctuations of p-adic random matrix products, Sel. Math. New Ser. 27 (2021) 98, https://doi.org/10.1007/s00029-021-00709-3.

[9] M.M. Wood, Asymptotics for number fields and class groups, in: Directions in Number Theory, in: Assoc. Women Math. Ser., vol. 3, Springer, Cham, 2016, pp. 291–339.

[10] M.M. Wood, The distribution of sandpile groups of random graphs, J. Am. Math. Soc. 30 (4) (2017) 915–958.

[11] M.M. Wood, Random integral matrices and the Cohen–Lenstra heuristics, Am. J. Math. 141 (2) (2019) 383–398.