Research Article

Jiwan Jung and Jungin Lee*

Joint distribution of the cokernels of random *p*-adic matrices II

https://doi.org/10.1515/forum-2023-0131
Received April 10, 2023

Abstract: In this paper, we study the combinatorial relations between the cokernels $\operatorname{cok}(A_n + px_iI_n)$ $(1 \le i \le m)$, where A_n is an $n \times n$ matrix over the ring of p-adic integers $\mathbb{Z}_p$, I_n is the $n \times n$ identity matrix and $x_1, \dots, x_m$ are elements of $\mathbb{Z}_p$ whose reductions modulo p are distinct. For a positive integer $m \le 4$ and given $x_1, \dots, x_m \in \mathbb{Z}_p$, we determine the set of m-tuples of finitely generated $\mathbb{Z}_p$-modules $(H_1, \dots, H_m)$ for which

$$(\operatorname{cok}(A_n + px_1I_n), \dots, \operatorname{cok}(A_n + px_mI_n)) = (H_1, \dots, H_m)$$

for some matrix A_n. We also prove that if A_n is an $n \times n$ Haar random matrix over $\mathbb{Z}_p$ for each positive integer n, then the joint distribution of $\operatorname{cok}(A_n + px_iI_n)$ $(1 \le i \le m)$ converges as $n \to \infty$.

Keywords: Random p-adic matrices, moments

MSC 2020: 15B52, 60B20

Communicated by: Freydoon Shahidi

1 Introduction

Friedman and Washington [4] computed the distribution of the cokernel of a random matrix over the ring of p-adic integers $\mathbb{Z}_p$. They proved that if $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ is a Haar random matrix (equidistributed with respect to the Haar measure) for each positive integer n and H is a finite abelian p-group, then

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{cok}(A_n) \cong H) = \frac{\prod_{k=1}^{\infty}(1 - p^{-k})}{|\operatorname{Aut}(H)|}. \tag{1.1}$$

Here $\mathrm{M}_{m\times n}(R)$ denotes the set of $m \times n$ matrices over a commutative ring R, $\mathrm{M}_n(R) := \mathrm{M}_{n\times n}(R)$ and $\mathbb{P}(\cdot)$ denotes the probability of an event. The study of the distributions of the cokernels for much larger classes of random p-adic matrices was initiated by the work of Wood [12] which proved universality for random symmetric matrices over $\mathbb{Z}_p$. Precisely, Wood proved that if $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ is an ε-balanced random symmetric matrix for each positive integer n, then the distribution of $\operatorname{cok}(A_n)$ always converges to the same distribution as $n \to \infty$.

Definition 1.1. For a real number $0 < \varepsilon < 1$, a random variable $x \in \mathbb{Z}_p$ is *ε-balanced* if $\mathbb{P}(x \equiv r \pmod{p}) \le 1 - \varepsilon$ for every $r \in \mathbb{Z}/p\mathbb{Z}$. A random matrix $A \in \mathrm{M}_n(\mathbb{Z}_p)$ is *ε-balanced* if its entries are independent and ε-balanced. A random symmetric matrix $A \in \mathrm{M}_n(\mathbb{Z}_p)$ is *ε-balanced* if its upper triangular entries are independent and ε-balanced.

Theorem 1.2 ([12, Corollary 9.2]). *Let $0 < \varepsilon < 1$ be a real number, H be a finite abelian p-group and $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ be an ε-balanced random symmetric matrix for each n. Then we have*

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{cok}(A_n) \cong H) = \frac{\#\{\textit{symmetric, bilinear, perfect } \phi : H \times H \to \mathbb{C}^*\}}{|H||\operatorname{Aut}(H)|} \prod_{k=1}^{\infty}(1 - p^{1-2k}).$$

***Corresponding author: Jungin Lee,** Department of Mathematics, Ajou University, Suwon 16499, Republic of Korea, e-mail: jileemath@ajou.ac.kr. https://orcid.org/0000-0003-0390-119X
Jiwan Jung, Department of Mathematics, Pohang University of Science and Technology, Pohang 37673, Republic of Korea, e-mail: guinipig123@postech.ac.kr

One of the key ingredients of the proof of Theorem 1.2 is the use of moments for random finitely generated abelian groups. For a given finite abelian group H, the *H-moment* of a random finitely generated abelian group X is defined by the expected value $\mathbb{E}(\#\operatorname{Sur}(X,H))$ of the number of surjective homomorphisms from X to H. If the moments of a random finitely generated abelian group X are not too large, then the distribution of X is uniquely determined by its moments [12, Theorem 8.3]. Theorem 1.2 follows from this result and a sophisticated computation of the moments of the cokernels of ε-balanced matrices.

Starting from the work of Wood, several universality results for the cokernels of random p-adic matrices were proved [3, 6–10, 13, 15]. All of these results were obtained by computing the (mixed) moments of the cokernels and determining the (joint) distribution of the cokernels from the moments. As an example, we provide a theorem of Nguyen and Wood [10] which proves universality for ε_n-balanced matrices over $\mathbb{Z}_p$, where ε_n does not decrease too fast as $n \to \infty$.

Theorem 1.3 ([10, Theorem 4.1]). *Let $u \geq 0$ be an integer, H a finite abelian p-group and $(\varepsilon_n)_{n\geq 1}$ a sequence of real numbers such that $0 < \varepsilon_n < 1$ for each n and for every $\Delta > 0$, we have $\varepsilon_n \geq \frac{\Delta \log n}{n}$ for sufficiently large n. Let $A_n \in \mathrm{M}_{n\times(n+u)}(\mathbb{Z}_p)$ be an ε_n-balanced random matrix for each n. Then we have*

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{cok}(A_n) \cong H) = \frac{\prod_{k=1}^{\infty}(1-p^{-k-u})}{|H|^u|\operatorname{Aut}(H)|}. \tag{1.2}$$

On the other hand, there had been recent progress on generalization of the cokernel condition. Friedman and Washington [4] proved that if A_n is a Haar random matrix in $\mathrm{GL}_n(\mathbb{Z}_p)$ for each n and H is a finite abelian p-group, then

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{cok}(A_n - I_n) \cong H) = \frac{\prod_{k=1}^{\infty}(1-p^{-k})}{|\operatorname{Aut}(H)|} \tag{1.3}$$

where I_n denotes the $n \times n$ identity matrix. As a natural generalization of this result, Cheong and Huang [1] predicted the limiting joint distribution of the cokernels $\operatorname{cok}(P_i(A_n))$ ($1 \leq i \leq m$) where $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ is a Haar random matrix for each n and $P_1(t), \dots, P_m(t) \in \mathbb{Z}_p[t]$ are monic polynomials whose reductions modulo p are distinct and irreducible. This conjecture was settled by the second author [5, Theorem 2.1]. (Cheong and Kaplan [2, Theorem 1.1] independently proved the conjecture under the assumption that $\deg(P_i) \leq 2$ for each i.) Recently, Cheong and Yu [3] generalized this to the case that A_n is ε-balanced for each n.

Theorem 1.4 ([3, Corollary 1.8]). *Let $0 < \varepsilon < 1$ be a real number and $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ an ε-balanced matrix for each $n \geq 1$. Let $P_1(t), \dots, P_m(t) \in \mathbb{Z}_p[t]$ be monic polynomials whose reductions modulo p in $\mathbb{F}_p[t]$ are distinct and irreducible. Also let H_i be a finite module over $R_i := \mathbb{Z}_p[t]/(P_i(t))$ for each i. Then we have*

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{cok}(P_i(A_n)) \cong H_i \text{ for } 1 \leq i \leq m) = \prod_{i=1}^{m} \frac{\prod_{k=1}^{\infty}(1-p^{-k\deg(P_i)})}{|\operatorname{Aut}_{R_i}(H_i)|}. \tag{1.4}$$

We remark that each R_i is a discrete valuation ring with a finite residue field $R_i/pR_i \cong \mathbb{F}_{p^{\deg(P_i)}}$ and the cokernel $\operatorname{cok}(P_i(A_n))$ has a natural R_i-module structure defined by $t \cdot x := A_n x$. There are other ways to generalize the cokernel condition. For example, Van Peski [11, Theorem 1.4] computed the joint distribution of

$$\operatorname{cok}(A_1), \operatorname{cok}(A_2A_1), \dots, \operatorname{cok}(A_r \cdots A_1)$$

for a fixed $n \geq 1$ and Haar random matrices $A_1, \dots, A_r \in \mathrm{M}_n(\mathbb{Z}_p)$ by using explicit formulas for certain skew Hall-Littlewood polynomials. Nguyen and Van Peski [8, Theorem 1.2] generalized this to the case where $A_1, \dots, A_r$ are ε-balanced.

In Theorem 1.4, the distribution of the cokernels $\operatorname{cok}(P_i(A_n))$ ($1 \leq i \leq m$) becomes asymptotically independent as $n \to \infty$. Here the condition that the reductions modulo p of $P_1(t), \dots, P_m(t)$ are distinct is essential. If two polynomials $P_1(t), P_2(t) \in \mathbb{Z}_p[t]$ have the same reduction modulo p, then $\operatorname{cok}(P_1(A))$ and $\operatorname{cok}(P_2(A))$ have the same p-rank so they cannot be asymptotically independent. (The p-rank of a finite abelian p-group G is given by $r_p(G) := \operatorname{rank}_{\mathbb{F}_p}(G/pG)$.) Nevertheless, we can still consider their joint distribution. In the previous work of the second author [7], the joint distribution in the simplest case ($P_1(t) = t$ and $P_2(t) = t + p$) was computed. Denote $c_r(p) := \prod_{k=1}^{r}(1-p^{-k})$ and $c_\infty(p) := \prod_{k=1}^{\infty}(1-p^{-k})$.

Theorem 1.5 ([7, Theorem 3.11]). *Let $(\varepsilon_n)_{n\geq 1}$ be a sequence of real numbers such that for every $\Delta > 0$, we have $\varepsilon_n \geq \frac{\Delta \log n}{n}$ for sufficiently large n. Let $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ be an ε_n-balanced random matrix for each n. Then we have*

$$\lim_{n\to\infty} \mathbb{P}(\operatorname{cok}(A_n) \cong H_1 \text{ and } \operatorname{cok}(A_n + pI_n) \cong H_2) = \begin{cases} 0, & r_p(H_1) \neq r_p(H_2), \\ \dfrac{p^{r^2} c_\infty(p) c_r(p)^2}{|\mathrm{Aut}(H_1)||\mathrm{Aut}(H_2)|}, & r_p(H_1) = r_p(H_2) = r, \end{cases}$$

for every finite abelian p-groups H_1 and H_2.

It is very hard to compute the joint distribution of the cokernels $\operatorname{cok}(P_i(A))$ $(1 \leq i \leq m)$ in general, even in the case that each A_n is equidistributed. Thus we propose the following easier problem.

Problem 1.6. *Let $P_1(t), \dots, P_m(t) \in \mathbb{Z}_p[t]$ be monic polynomials whose reductions modulo p are irreducible, let $R_i = \mathbb{Z}_p[t]/(P_i(t))$, let $\mathcal{M}_{R_i}$ be the set of finitely generated R_i-modules and let $\mathcal{M} = \prod_{i=1}^m \mathcal{M}_{R_i}$. For a given $(H_1, \dots, H_m) \in \mathcal{M}$, determine whether there exists a matrix $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ such that $\operatorname{cok}(P_i(A_n)) \cong H_i$ for each i. In other words, determine the set*

$$\begin{aligned}\mathcal{C}(P_1, \dots, P_m) := \{(H_1, \dots, H_m) \in \mathcal{M} : & \text{ there exists } A_n \in \mathrm{M}_n(\mathbb{Z}_p) \text{ for some } n \\ & \text{ such that } \operatorname{cok}(P_i(A_n)) \cong H_i \text{ for each } 1 \leq i \leq m\}.\end{aligned}$$

Remark 1.7. (1) For $A \in \mathrm{M}_n(\mathbb{Z}_p)$ and $B \in \mathrm{M}_{n'}(\mathbb{Z}_p)$, we have

$$\operatorname{cok}\left(P_i\begin{pmatrix} A & O \\ O & B \end{pmatrix}\right) \cong \operatorname{cok}(P_i(A)) \times \operatorname{cok}(P_i(B))$$

so the set $\mathcal{C}(P_1, \dots, P_m)$ is closed under componentwise finite direct product.

(2) In the above problem, we allow the case that $\operatorname{cok}(P_i(A_n))$ have a free part (i.e. $\det(P_i(A_n)) = 0$), contrary to Theorem 1.4. The probability that $\det(P_i(A_n)) = 0$ for some i is always zero, but it does not mean that this event cannot happen.

In this paper, we analyze the case where $P_i(t) = t + px_i$ for some $x_1, \dots, x_m \in \mathbb{Z}_p$ whose reductions modulo p are distinct. Let $X_m := \{x_1, \dots, x_m\}$ be a finite ordered subset of $\mathbb{Z}_p$ of size m whose elements have distinct reductions modulo p and denote $\mathcal{C}_{X_m} := \mathcal{C}(t + px_1, \dots, t + px_m) \subset \mathcal{M}_{\mathbb{Z}_p}^m$. The main result of the paper is the following theorem, which determines the set $\mathcal{C}_{X_m}$ for $m \leq 4$. Note that in each case, the set $\mathcal{C}_{X_m}$ does not depend on the choice of X_m.

Theorem 1.8. *For $(H_1, \dots, H_m) \in \mathcal{M}_{\mathbb{Z}_p}^m$, write*

$$H_i \cong \mathbb{Z}_p^{d_{\infty,i}} \times \prod_{r=1}^{\infty} (\mathbb{Z}/p^r\mathbb{Z})^{d_{r,i}}$$

and

$$D_r := \sum_{i=1}^m d_{r,i}, \qquad s_i := \operatorname{rank}_{\mathbb{F}_p}(H_i/pH_i) = \sum_{r=1}^{\infty} d_{r,i} + d_{\infty,i} \quad \text{for each } i.$$

We have:

(1) $\mathcal{C}_{X_1} = \mathcal{M}_{\mathbb{Z}_p}$,

(2) $\mathcal{C}_{X_2} = \{(H_1, H_2) \in \mathcal{M}_{\mathbb{Z}_p}^2 : s_1 = s_2\}$,

(3) $\mathcal{C}_{X_3} = \{(H_1, H_2, H_3) \in \mathcal{M}_{\mathbb{Z}_p}^3 : s_1 = s_2 = s_3 \text{ and } 2d_{1,i} \leq D_1\ (1 \leq i \leq 3)\}$,

(4) $\mathcal{C}_{X_4} = \{(H_1, H_2, H_3, H_4) \in \mathcal{M}_{\mathbb{Z}_p}^4 : s_1 = s_2 = s_3 = s_4,\ 3d_{1,i} \leq D_1\ (1 \leq i \leq 4) \text{ and } d_{1,i} + 2(d_{1,j} + d_{2,j}) \leq D_1 + D_2\ (1 \leq i, j \leq 4)\}$.

If $(H_1, \dots, H_m) \in \mathcal{C}_{X_m}$, then there exists $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ such that $\operatorname{cok}(A_n + px_iI_n) \cong H_i$ for each i. In this case, we have $(\mathbb{Z}/p\mathbb{Z})^{s_i} \cong H_i/pH_i \cong \operatorname{cok}_{\mathbb{F}_p}(\overline{A_n})$ where $\overline{A_n} \in \mathrm{M}_n(\mathbb{F}_p)$ is the reduction modulo p of A_n, which implies that $s_1 = s_2 = \cdots = s_m$. When $m = 2$, this is the only condition we need for elements of $\mathcal{C}_{X_m}$. We need some additional relations between the numbers $d_{r,i}$ for larger m. It is natural to suggest the following conjecture from Theorem 1.8.

Conjecture 1.9. Let $d_{r,i}$, D_r and s_i be as in Theorem 1.8. For every integer $m \geq 1$, we have $(H_1, \dots, H_m) \in \mathcal{C}_{X_m}$ if and only if $s_1 = \cdots = s_m$ and

$$\sum_{k=1}^{r-1} \left(\sum_{l=1}^{k} d_{l,i_k} \right) + (m-r) \sum_{l=1}^{r} d_{l,i_r} \leq D_1 + \cdots + D_r$$

for every $1 \leq r \leq m-2$ and $1 \leq i_1, \dots, i_r \leq m$.

The paper is organized as follows. In Section 2.1, we provide basic notations and provide some basic properties of the sets $\mathcal{C}_{X_m,l,k}$ (see Problem 2.2) which are helpful to understand the set $\mathcal{C}_{X_m}$. We prove the main result of the paper (Theorem 1.8) for the case $m \leq 3$ in Section 2.2. The technical heart of the paper is a reduction procedure, which is explained in Section 3.1. Using this reduction procedure and explicit linear-algebraic computations on matrices over $\mathbb{Z}_p$, we prove the necessary condition of Theorem 1.8 for $m = 4$ in Section 3.2. After that, we prove the sufficient condition of Theorem 1.8 for $m = 4$ in Section 3.3 based on a zone theory.

The last section is devoted to the joint distribution of the cokernels $\operatorname{cok}(A_n + px_iI_n)$ $(1 \leq i \leq m)$. In Section 4.1, we prove that if each A_n is a Haar random matrix, then the joint distribution of the cokernels $\operatorname{cok}(A_n + px_iI_n)$ $(1 \leq i \leq m)$ converges as $n \to \infty$. In fact, we prove the following more general result. Note that our proof does not provide the limiting joint distribution.

Theorem 1.10 (Theorem 4.1). *Let $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ be a Haar random matrix for each $n \geq 1$, $y_1, \dots, y_m$ be distinct elements of $\mathbb{Z}_p$ and $H_1, \dots, H_m$ be finite abelian p-groups. Then the limit*

$$\lim_{n \to \infty} \mathbb{P}(\operatorname{cok}(A_n + y_iI_n) \cong H_i \textit{ for } 1 \leq i \leq m)$$

converges.

In Section 4.2, we compute the mixed moments of the cokernels $\operatorname{cok}(A_n + px_iI_n)$ $(1 \leq i \leq m)$, where each matrix $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ is given as in Theorem 1.5. Then it is natural to follow the proof of Theorem 1.5 given in [7], where the second author determined the unique joint distribution of $\operatorname{cok}(A_n)$ and $\operatorname{cok}(A_n + pI_n)$ from their mixed moments. However, it turns out that for $m \geq 3$, we cannot determine a unique joint distribution of $\operatorname{cok}(A_n + px_iI_n)$ $(1 \leq i \leq m)$ from their mixed moments using existing methods (see Example 4.6).

Let Y be a random m-tuple of finite abelian p-groups (or a random m-tuple of finitely generated $\mathbb{Z}_p$-modules in general). When Y is supported on a smaller set of m-tuples of finite abelian p-groups, it is more likely that the distribution of Y is uniquely determined by its mixed moments. Therefore the information on the support of Y would be helpful for determining its distribution. This is one of our motivations for concerning Problem 1.6 in this paper. In the future work, we hope to determine the joint distribution of $\operatorname{cok}(A_n + px_iI_n)$ $(1 \leq i \leq m)$ from their mixed moments, together with combinatorial relations between the cokernels provided in Theorem 1.8 and Conjecture 1.9.

2 Preliminaries

The following notations will be used throughout the paper.

- For a prime p, let $\mathcal{G}_p$ be the set of isomorphism classes of finite abelian p-groups and let $\mathcal{M}_{\mathbb{Z}_p}$ be the set of isomorphism classes of finitely generated $\mathbb{Z}_p$-modules.
- Set $\overline{\mathbb{Z}} := \mathbb{Z} \cup \{\infty\}$, $\mathbb{Z}_{\geq c} := \{x \in \mathbb{Z} : x \geq c\}$ and $\overline{\mathbb{Z}}_{\geq c} := \mathbb{Z}_{\geq c} \cup \{\infty\}$ for $c \in \mathbb{Z}$.
- Let m be a positive integer and let $X_m = \{x_1, \dots, x_m\}$ be a finite ordered subset of $\mathbb{Z}_p$ whose elements have distinct reductions modulo p.
- For $A \in \mathrm{M}_n(\mathbb{Z}_p)$, write
$$\operatorname{cok}(A) \cong \prod_{r \in \overline{\mathbb{Z}}_{\geq 1}} (\mathbb{Z}_p/p^r\mathbb{Z}_p)^{d_{r,A}}$$
(we use the convention that $p^\infty = 0$ and thus $\mathbb{Z}_p/p^\infty\mathbb{Z}_p = \mathbb{Z}_p$) and
$$d_{0,A} := n - \sum_{r \in \overline{\mathbb{Z}}_{\geq 1}} d_{r,A}.$$

In this case, the Smith normal form of A is given by

$$\operatorname{diag}(\overbrace{1,\dots,1}^{d_{0,A}},\overbrace{p,\dots,p}^{d_{1,A}},\dots,\overbrace{0,\dots,0}^{d_{\infty,A}}).$$

- For $A \in \mathrm{M}_n(\mathbb{Z}_p)$ and $k \in \mathbb{Z}_{\geq 1}$, $\operatorname{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(A)$ denotes the cokernel of A/p^kA as a $\mathbb{Z}_p/p^k\mathbb{Z}_p$-module. It is given as
$$\operatorname{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(A) \cong \prod_{r=1}^{k-1}(\mathbb{Z}_p/p^r\mathbb{Z}_p)^{d_{r,A}} \times (\mathbb{Z}_p/p^k\mathbb{Z}_p)^{\sum_{r\in\overline{\mathbb{Z}}_{\geq k}} d_{r,A}}.$$
Let $\overline{A} := A/pA \in \mathrm{M}_n(\mathbb{F}_p)$ be the reduction modulo p of A.
- For $A \in \mathrm{M}_{n\times n'}(\mathbb{Z}_p)$ and $k \geq 1$, denote $p^k \mid A$ if each entry of A is divisible by p^k and $p^k \nmid A$ otherwise.
- Denote
$$\mathcal{B}_m := \{(n; H_1,\dots,H_m) \in \mathbb{Z}_{\geq 0} \times \mathcal{M}_{\mathbb{Z}_p}^m : n \geq \operatorname{rank}_{\mathbb{F}_p}(H_i/pH_i) \text{ for every } 1 \leq i \leq m\}.$$
For an element $(n; H_1,\dots,H_m) \in \mathcal{B}_m$, write $H_i \cong \prod_{r\in\overline{\mathbb{Z}}_{\geq 1}}(\mathbb{Z}_p/p^r\mathbb{Z}_p)^{d_{r,i}}$ and $d_{0,i} := n - \sum_{r\in\overline{\mathbb{Z}}_{\geq 1}} d_{r,i}$ for each i. If a polynomial $P(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$ satisfies $\operatorname{cok}(P(x_i)) \cong H_i$ for each i, then we have $d_{r,P(x_i)} = d_{r,i}$ for every $r \in \overline{\mathbb{Z}}_{\geq 0}$ and $1 \leq i \leq m$.
- The *sum* of two elements in $\mathcal{B}_m$ is defined by the operation
$$(n; H_1,\dots,H_m) + (n'; H_1',\dots,H_m') := (n+n'; H_1 \times H_1', \dots, H_m \times H_m'). \tag{2.1}$$

2.1 The sets $\mathcal{C}_{X_m,l,k}$

For $A \in \mathrm{M}_n(\mathbb{Z}_p)$ with $n_1 = n - d_{0,A}$, the Smith normal form of A gives $U, V \in \mathrm{GL}_n(\mathbb{Z}_p)$ such that

$$UAV = \begin{pmatrix} pA' & O \\ O & I_{n-n_1} \end{pmatrix}$$

for some $A' \in \mathrm{M}_{n_1}(\mathbb{Z}_p)$. For $x \in \mathbb{Z}_p$ and $UV = \left(\begin{smallmatrix} B_1 & B_2 \\ B_3 & B_4 \end{smallmatrix}\right) \in \mathrm{GL}_{n_1+(n-n_1)}(\mathbb{Z}_p)$, we have

$$\begin{aligned}
\operatorname{cok}(A + pxI) &\cong \operatorname{cok}(UAV + pxUV) \\
&= \operatorname{cok}\left(\begin{pmatrix} pA' + pxB_1 & pxB_2 \\ pxB_3 & I_{n-n_1} + pxB_4 \end{pmatrix}\right) \\
&\cong \operatorname{cok}(p(A' + xB_1) - (pxB_2)(I_{n-n_1} + pxB_4)^{-1}(pxB_3)) \\
&= \operatorname{cok}\left(p(A' + xB_1 - \sum_{d=0}^{\infty} p^{d+1}x^{d+2}B_2(-B_4)^d B_3)\right).
\end{aligned}$$

For $A_0 = A'$, $A_1 = B_1$ and $A_r = -B_2(-B_4)^{r-2}B_3$ $(r \geq 2)$, we have

$$\operatorname{cok}(A + pxI) \cong \operatorname{cok}(pP^{(1)}_{A_0,A_1,\dots}(x)) := \operatorname{cok}\left(p(A_0 + \sum_{d=1}^{\infty} p^{d-1}x^d A_d)\right).$$

In this case, we have

$$d_{r,A+pxI} = d_{r-1,P^{(1)}_{A_0,A_1,\dots}(x)} \tag{2.2}$$

for every $r \in \overline{\mathbb{Z}}_{\geq 1}$. Thus if an inequality holds for the numbers $d_{r-1,P^{(1)}_{A_0,A_1,\dots}(x)}$ for any $A_0, A_1, \dots \in \mathrm{M}_{n_1}(\mathbb{Z}_p)$, then the same inequality holds for the numbers $d_{r,A+pxI}$. This observation motivates us to introduce the following variant of Problem 1.6.

Definition 2.1. A polynomial in $\mathrm{M}_n(\mathbb{Z}_p)[t]$ is called an *l-th integral of ascending polynomial*, or just an *l-th integral* if it is of the form

$$A_0 + tA_1 + \dots + t^l A_l + pt^{l+1}A_{l+1} + \dots + p^r t^{l+r} A_{l+r}$$

for some $r \in \mathbb{Z}_{\geq 0}$ and $A_0, \dots, A_{l+r} \in \mathrm{M}_n(\mathbb{Z}_p)$. For $l = \infty$, every polynomial in $\mathrm{M}_n(\mathbb{Z}_p)[t]$ is an ∞-th integral.

Problem 2.2. *For given X_m and $l, k \in \overline{\mathbb{Z}}_{\geq 0}$, determine the set*

$$\begin{aligned}\mathcal{C}_{X_m,l,k} := \{(n; H_1, \dots, H_m) \in \mathcal{B}_m :\ & \text{there exists an } l\text{-th integral } P(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t] \\ & \text{such that } \operatorname{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(P(x_i)) \cong H_i/p^k H_i \text{ for each } 1 \leq i \leq m\}.\end{aligned}$$

Now we provide basic properties of the sets $\mathcal{C}_{X_m,l,k}$. For $H \in \mathcal{M}_{\mathbb{Z}_p}$, denote $s(H) := \operatorname{rank}_{\mathbb{F}_p}(H/pH)$. Then we have $s(H_i) = \sum_{r \in \overline{\mathbb{Z}}_{\geq 1}} d_{r,i} = n - d_{0,i}$ for $(n; H_1, \dots, H_m) \in \mathcal{B}_m$.

Proposition 2.3. *The following statements hold:*

(1) *The set $\mathcal{C}_{X_m,l,k}$ is closed under the sum in $\mathcal{B}_m$. In particular, $\mathcal{C}_{X_m,l,k}$ is a monoid under the operation* (2.1) *with an identity* $(0; 1, \dots, 1)$.

(2) *For $l, l', k, k' \in \overline{\mathbb{Z}}_{\geq 0}$ and $x_0 \in \mathbb{Z}_p$, we have the followings:*
   - (a) $\mathcal{C}_{X_m,l,k} \subset \mathcal{C}_{X_m,l',k'}$ *for $l \leq l'$ and $k \geq k'$,*
   - (b) $\mathcal{C}_{X_m,l,\infty} = \mathcal{C}_{X_m,l,m-l-1}$ *for $l < m$,*
   - (c) $\mathcal{C}_{X_m,l,k} = \mathcal{C}_{X_m - x_0,l,k}$ *for $X_m - x_0 := \{x - x_0 : x \in X_m\}$.*

(3) *We have*

$$\begin{aligned}\mathcal{C}_{X_m} &= \{(H_1, \dots, H_m) \in \mathcal{M}_{\mathbb{Z}_p}^m : \text{there exists } n \in \mathbb{Z}_{\geq 1} \text{such that } (n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,0,\infty}\} \\ &= \{(H_1, \dots, H_m) \in \mathcal{M}_{\mathbb{Z}_p}^m : s(H_1) = \cdots = s(H_m) = s \text{ and } (s; pH_1, \dots, pH_m) \in \mathcal{C}_{X_m,1,\infty}\}.\end{aligned}$$

(4) *For every $l < m$, the map*

$$\varphi_{l,k} : \{(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,l,k+1} : d_{0,1} = \cdots = d_{0,m} = 0\} \to \mathcal{C}_{X_m,l+1,k}$$

given by

$$(n; H_1, \dots, H_m) \mapsto (n; pH_1, \dots, pH_m)$$

is well-defined and a bijection.

Proof. (1) For every $(n; H_1, \dots, H_m), (n'; H_1', \dots, H_m') \in \mathcal{C}_{X_m,l,k}$, there are l-th integrals $P(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$ and $P'(t) \in \mathrm{M}_{n'}(\mathbb{Z}_p)[t]$ such that $\operatorname{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(P(x_i)) \cong H_i$ and $\operatorname{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(P'(x_i)) \cong H_i'$ for each i. Then the *concatenation* of $P(t)$ and $P'(t)$ given by

$$Q(t) := \begin{pmatrix} P(t) & O \\ O & P'(t) \end{pmatrix} \in \mathrm{M}_{n+n'}(\mathbb{Z}_p)[t]$$

is also an l-th integral and $\operatorname{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(Q(x_i)) \cong H_i \times H_i'$ for each i. Thus we have

$$(n + n'; H_1 \times H_1', \dots, H_m \times H_m') \in \mathcal{C}_{X_m,l,k}.$$

(2a) It follows from the facts that an l-th integral is also an l'-th integral and

$$\operatorname{cok}_{\mathbb{Z}_p/p^{k'}\mathbb{Z}_p}(A) \cong \operatorname{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(A)/p^{k'} \operatorname{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(A).$$

(2b) The inclusion $\subset$ holds by (a). Now suppose that $(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,l,m-l-1}$. Then there exists an l-th integral $P(t) \in \mathrm{M}_n(\mathbb{Z}_p)$ such that $\operatorname{cok}_{\mathbb{Z}_p/p^{m-l-1}\mathbb{Z}_p}(P(x_i)) \cong H_i/p^{m-l-1}H_i$ for each i. The Smith normal form of $P(x_i)$ gives $U_i, V_i \in \mathrm{GL}_n(\mathbb{Z}_p)$ such that

$$P(x_i) = U_i \operatorname{diag}(\overbrace{1, \dots, 1}^{d_{0,P(x_i)}}, \dots, \overbrace{p^{m-l-1}, \dots, p^{m-l-1}}^{d_{m-l-1,P(x_i)}}, \overbrace{p^{m-l}, \dots, p^{m-l}}^{d_{m-l,P(x_i)}}, \dots, \overbrace{0, \dots, 0}^{d_{\infty,P(x_i)}}) V_i.$$

Define $L_{m,i}(t) := \prod_{1 \leq j \leq m, j \neq i} \frac{t - x_j}{x_i - x_j} \in \mathbb{Z}_p[t]$, $D_{m-l-1,i} := \sum_{r \in \overline{\mathbb{Z}}_{\geq m-l-1}} d_{r,P(x_i)}$ and

$$Q(t) := P(t) + \sum_{i=1}^{m} L_{m,i}(t) U_i \operatorname{diag}(\overbrace{0, \dots, 0}^{n - D_{m-l-1,i}}, p^{a_{i,1}} - b_{i,1}, \dots, p^{a_{i,D_{m-l-1,i}}} - b_{i,D_{m-l-1,i}}) V_i,$$

where

$$(b_{i,1}, \dots, b_{i,D_{m-l-1,i}}) := (\overbrace{p^{m-l-1}, \dots, p^{m-l-1}}^{d_{m-l-1,P(x_i)}}, \dots, \overbrace{0, \dots, 0}^{d_{\infty,P(x_i)}})$$

and $a_{i,j} \in \overline{\mathbb{Z}}_{\geq m-l-1}$ for $1 \leq i \leq m$ and $1 \leq j \leq D_{m-l-1,i}$. Then $Q(t)$ is also an l-th integral as $p^{m-l-1} \mid p^{a_{i,j}} - b_{i,j}$ for each i, j and $L_{m,i}(t)$ is of degree $m-1$, while

$$\begin{aligned} Q(x_i) &= P(x_i) + U_i \operatorname{diag}(\overbrace{0, \dots, 0}^{n-D_{m-l-1,i}}, p^{a_{i,1}} - b_{i,1}, \dots, p^{a_{i,D_{m-l-1,i}}} - b_{i,D_{m-l-1,i}})V_i \\ &= U_i \operatorname{diag}(\overbrace{1, \dots, 1}^{d_{0,P(x_i)}}, \dots, \overbrace{p^{m-l-2}, \dots, p^{m-l-2}}^{d_{m-l-2,P(x_i)}}, p^{a_{i,1}}, \dots, p^{a_{i,D_{m-l-1,i}}})V_i \end{aligned}$$

for each i. Now we can choose $a_{i,j} \in \overline{\mathbb{Z}}_{\geq m-l-1}$ $(1 \leq i \leq m,\ 1 \leq j \leq D_{m-l-1,i})$ such that $\operatorname{cok}(Q(x_i)) \cong H_i$ for each i, which implies that $(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,l,\infty}$.

(2c) It holds that $P(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$ is an l-th polynomial if and only if $P_1(t) := P(t + x_0) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$ is an l-th polynomial and $\operatorname{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(P(x_i)) \cong \operatorname{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(P_1(x_i - x_0))$ so we have $\mathcal{C}_{X_m,l,k} = \mathcal{C}_{X_m - x_0,l,k}$.

(3) Consider the sets

$$\begin{aligned} S_1 &:= \{(H_1, \dots, H_m) \in \mathcal{M}_{\mathbb{Z}_p}^m : \text{there exists } n \in \mathbb{Z}_{\geq 1} \text{ such that } (n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,0,\infty}\}, \\ S_2 &:= \{(H_1, \dots, H_m) \in \mathcal{M}_{\mathbb{Z}_p}^m : s(H_1) = \cdots = s(H_m) = s \text{ and } (s; pH_1, \dots, pH_m) \in \mathcal{C}_{X_m,1,\infty}\}. \end{aligned}$$

We have:

- ($\mathcal{C}_{X_m} = S_1$) The inclusion $\subset$ follows from the definition. Suppose that $(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,0,\infty}$ so that there exists a zeroth integral $P(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$ such that $\operatorname{cok}(P(x_i)) \cong H_i$ for each i. Let

  $$Q(t) := P(t) + p^{d+m}t^d(t - x_1) \cdots (t - x_m)I_n = A_0 + ptA_1 + \cdots + p^{d+m-1}t^{d+m-1}A_{d+m-1} + p^{d+m}t^{d+m}I_n$$

  for $d = \deg(P)$ and $A_0, \dots, A_{d+m-1} \in \mathrm{M}_n(\mathbb{Z}_p)$. The rational canonical form of $Q(t)$, i.e.

  $$A := \begin{pmatrix} & & & A_0 \\ -I_n & & & A_1 \\ & \ddots & & \vdots \\ & & -I_n & A_{d+m-1} \end{pmatrix} \in \mathrm{M}_{(d+m)n}(\mathbb{Z}_p)$$

  satisfies $\operatorname{cok}(A + px_iI) \cong \operatorname{cok}(Q(x_i)) \cong \operatorname{cok}(P(x_i)) \cong H_i$ for each i so we have $(H_1, \dots, H_m) \in \mathcal{C}_{X_m}$.
- ($\mathcal{C}_{X_m} \subset S_2$) Suppose that $(H_1, \dots, H_m) \in \mathcal{C}_{X_m}$ so that there exists $A \in \mathrm{M}_n(\mathbb{Z}_p)$ for some $n \geq 1$ such that $\operatorname{cok}(A + px_iI) \cong H_i$ for each i. Then

  $$s(H_i) = \operatorname{rank}_{\mathbb{F}_p}(H_i/pH_i) = \operatorname{rank}_{\mathbb{F}_p}(\operatorname{cok}(\overline{A}))$$

  so we have $s(H_1) = \cdots = s(H_m) = s$. By equation (2.2), there exists a first integral $P(t) \in \mathrm{M}_s(\mathbb{Z}_p)[t]$ such that $\operatorname{cok}(P(x_i)) \cong pH_i$ for each i, which implies that $(s; pH_1, \dots, pH_m) \in \mathcal{C}_{X_m,1,\infty}$.
- ($S_2 \subset S_1$) Suppose that $(H_1, \dots, H_m) \in S_2$ so that $s(H_1) = \cdots = s(H_m) = s$ and $(s; pH_1, \dots, pH_m) \in \mathcal{C}_{X_m,1,\infty}$. Let $P(t) \in \mathrm{M}_s(\mathbb{Z}_p)[t]$ be a first integral such that $\operatorname{cok}(P(x_i)) \cong pH_i$ for each i. Since $pP(t)$ is a zeroth integral and $\operatorname{cok}(pP(x_i)) \cong H_i$ for each i, we have $(s; H_1, \dots, H_m) \in \mathcal{C}_{X_m,0,\infty}$.

(4) Assume that $(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,l,k+1}$ with $d_{0,1} = \cdots = d_{0,m} = 0$. Then there exists an l-th integral $P(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$ such that $\operatorname{cok}_{\mathbb{Z}_p/p^{k+1}\mathbb{Z}_p}(P(x_i)) \cong H_i/p^{k+1}H_i$ and $d_{0,P(x_i)} = 0$ (so $p \mid P(x_i)$) for each i. This implies that

$$P(t) = (t - x_1) \cdots (t - x_m)Q(t) + pP_1(t)$$

for some $Q(t), P_1(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$ such that $\deg((t - x_1) \cdots (t - x_m)Q(t)) \leq l$ and $P_1(t)$ is an $(l+1)$-th integral. Since we have $P(x_i) = pP_1(x_i)$ for each i, we have $d_{r,P_1(t)} = d_{r+1,P(t)}$ for every $r \in \overline{\mathbb{Z}}_{\geq 1}$ so

$$\operatorname{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(P_1(x_i)) = pH_i/p^{k+1}H_i$$

for each i. Thus the map $\varphi_{l,k}$ is well-defined.

Now assume that $(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,l+1,k}$. Then there exists an $(l+1)$-th integral $P(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$ such that $\operatorname{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(P(x_i)) \cong H_i/p^kH_i$ for each i. Since $pP(t)$ is an l-th integral which satisfies $d_{0,pP(t)} = 0$ and $d_{r,P(t)} = d_{r+1,pP(t)}$ for every $r \in \overline{\mathbb{Z}}_{\geq 0}$, the map

$$\psi_{l,k} : \mathcal{C}_{X_m,l+1,k} \to \{(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,l,k+1} : d_{0,1} = \cdots = d_{0,m} = 0\}$$

given by $(n; H_1, \dots, H_m) \mapsto (n; \operatorname{cok}(pP(x_1)), \dots, \operatorname{cok}(pP(x_m)))$ is the inverse of $\varphi_{l,k}$. □

As an example, we determine the elements of the set $\mathcal{C}_{X_m,l,\infty}$ which are of the form $(1;H_1,\dots,H_m)$. This result will be frequently used in the proof of Theorem 1.8. We note that if $(n;H_1,\dots,H_m)\in\mathcal{C}_{X_m,l,k}$, then $(n;H_{\sigma(1)},\dots,H_{\sigma(m)})\in\mathcal{C}_{X_m,l,k}$ for any permutation $\sigma\in S_m$.

Example 2.4. For an element $(1;H_1,\dots,H_m)\in\mathcal{C}_{X_m,l,\infty}$, there exists an l-th integral $P(t)\in\mathbb{Z}_p[t]$ such that $\mathbb{Z}_p/P(x_i)\mathbb{Z}_p\cong H_i$ for each i. If $P(t)=0$, then $H_1=\cdots=H_m=\mathbb{Z}_p$. If $P(t)$ is not identically zero, then there uniquely exists $r\in\mathbb{Z}_{\ge 0}$ such that $P(t)=p^rQ(t)$ for some $(l+r)$-th integral $Q(t)\in\mathbb{Z}_p[t]$ whose reduction modulo p is not identically zero in $\mathbb{F}_p[t]$. Since $Q(t)\equiv 0 \pmod p$ has at most $l+r$ roots modulo p, the number of $1\le i\le m$ such that $H_i=\mathbb{Z}_p/p^r\mathbb{Z}_p$ is at least $m-(l+r)$. Conversely, for every integer $0\le r\le m-l$ and $b_1,\dots,b_{r'}\in\overline{\mathbb{Z}}_{\ge r+1}$ with $r'\le l+r$, an l-th integral

$$P(t)=p^r\prod_{i=1}^{r'}(t-x_i)+\sum_{i=1}^{r'}p^{b_i}L_{r',i}(t)\in\mathbb{Z}_p[t]$$

satisfies $\mathbb{Z}_p/P(x_i)\mathbb{Z}_p\cong\mathbb{Z}_p/p^{b_i}\mathbb{Z}_p$ for $1\le i\le r'$ and $\mathbb{Z}_p/P(x_i)\mathbb{Z}_p\cong\mathbb{Z}_p/p^r\mathbb{Z}_p$ for $i>l+r$. (The polynomials $L_{m,i}(t)$ are defined as in the proof of Proposition 2.3 (b).)

Now we deduce that $(1;H_1,\dots,H_m)\in\mathcal{C}_{X_m,l,\infty}$ if and only if $(H_1,\dots,H_m)$ is a permutation of

$$(\mathbb{Z}_p/p^{b_1}\mathbb{Z}_p,\dots,\mathbb{Z}_p/p^{b_{r+l}}\mathbb{Z}_p,\overbrace{\mathbb{Z}_p/p^r\mathbb{Z}_p,\dots,\mathbb{Z}_p/p^r\mathbb{Z}_p}^{m-r-l})$$

for some $0\le r\le m-l$ and $b_1,\dots,b_{r+l}\in\overline{\mathbb{Z}}_{\ge r}$. In particular, we have

$$(\mathbb{Z}_p/p^{b_1}\mathbb{Z}_p,\dots,\mathbb{Z}_p/p^{b_r}\mathbb{Z}_p,\overbrace{\mathbb{Z}_p/p^r\mathbb{Z}_p,\dots,\mathbb{Z}_p/p^r\mathbb{Z}_p}^{m-r})\in\mathcal{C}_{X_m}$$

for every $0\le r\le m$ and $b_1,\dots,b_r\in\overline{\mathbb{Z}}_{\ge r}$ by Proposition 2.3 (3).

2.2 Proof of Theorem 1.8: The case $m\le 3$

The case $m=1$ is trivial. When $m=2$, we have $\mathcal{C}_{X_2}\subset\{(H_1,H_2)\in\mathcal{M}^2_{\mathbb{Z}_p}: s_1=s_2\}$ (see the paragraph after Theorem 1.8). Conversely, every element $(H_1,H_2)\in\mathcal{M}^2_{\mathbb{Z}_p}$ such that $s_1=s_2=s$ is of the form

$$\left(\prod_{j=1}^{s}\mathbb{Z}_p/p^{a_j}\mathbb{Z}_p,\prod_{j=1}^{s}\mathbb{Z}_p/p^{b_j}\mathbb{Z}_p\right)\quad(a_j,b_j\in\overline{\mathbb{Z}}_{\ge 1}).$$

Since the set $\mathcal{C}_{X_2}$ is closed under finite direct product, to prove Theorem 1.8 for $m=2$ it is enough to show that $(\mathbb{Z}_p/p^a\mathbb{Z}_p,\mathbb{Z}_p/p^b\mathbb{Z}_p)\in\mathcal{C}_{X_2}$ for every $a,b\in\overline{\mathbb{Z}}_{\ge 1}$. We already proved this in Example 2.4.

Now we consider the case $m=3$. First we prove that every element $(H_1,H_2,H_3)\in\mathcal{C}_{X_3}$ satisfies the condition $2d_{1,i}\le D_1$. By equation (2.2), it is enough to show that the numbers $d_{0,P^{(1)}_{A_0,A_1,\dots}(x_i)}$ $(1\le i\le 3)$ satisfy the triangle inequality for every $A_0,A_1,\dots\in\mathrm{M}_{n_1}(\mathbb{Z}_p)$. The congruence $P^{(1)}_{A_0,A_1,\dots}(x_i)\equiv A_0+x_iA_1 \pmod p$ implies that

$$d_{0,P^{(1)}_{A_0,A_1,\dots}(x_i)}=d_{0,A_0+x_iA_1}=\dim_{\mathbb{F}_p}N(\overline{A_0+x_iA_1}),$$

where $N(\overline{A_0+x_iA_1})$ denotes the null space of $\overline{A_0+x_iA_1}\in\mathrm{M}_n(\mathbb{F}_p)$. By the relation

$$(x_2-x_3)(A_0+x_1A_1)+(x_3-x_1)(A_0+x_2A_1)+(x_1-x_2)(A_0+x_3A_1)=O,$$

the numbers $\dim_{\mathbb{F}_p}N(\overline{A_0+x_iA_1})$ $(1\le i\le 3)$ satisfy the triangle inequality. We conclude that

$$\mathcal{C}_{X_3}\subset\{(H_1,H_2,H_3)\in\mathcal{M}^3_{\mathbb{Z}_p}: s_1=s_2=s_3\text{ and }2d_{1,i}\le D_1\ (1\le i\le 3)\}.$$

It remains to show that every $(H_1,H_2,H_3)\in\mathcal{M}^3_{\mathbb{Z}_p}$ satisfying the conditions $s_1=s_2=s_3=s$ and $2d_{1,i}\le D_1$ $(1\le i\le 3)$ is an element of $\mathcal{C}_{X_3}$. For each i, let $c_i:=d_{1,i}$ and

$$H_i\cong(\mathbb{Z}_p/p\mathbb{Z}_p)^{c_i}\times\prod_{j=c_i+1}^{s}\mathbb{Z}_p/p^{b_{i,j}}\mathbb{Z}_p$$

for some $b_{i,c_i+1},\dots,b_{i,s} \in \overline{\mathbb{Z}}_{\geq 2}$. We may assume that $c_1 = \max_{1\leq i\leq 3} c_i$. Then $c_2+c_3-c_1 \geq 0$ and

$$\begin{aligned}(H_1,H_2,H_3) \cong (\mathbb{Z}_p/p\mathbb{Z}_p, \mathbb{Z}_p/p\mathbb{Z}_p, \mathbb{Z}_p/p\mathbb{Z}_p)^{c_2+c_3-c_1} \prod_{j=1}^{c_1-c_3} (\mathbb{Z}_p/p\mathbb{Z}_p, \mathbb{Z}_p/p\mathbb{Z}_p, \mathbb{Z}_p/p^{b_{3,j+c_3}}\mathbb{Z}_p)& \\ \times \prod_{j=1}^{c_1-c_2} (\mathbb{Z}_p/p\mathbb{Z}_p, \mathbb{Z}_p/p^{b_{2,j+c_2}}\mathbb{Z}_p, \mathbb{Z}_p/p\mathbb{Z}_p) \prod_{j=c_1+1}^{s} (\mathbb{Z}_p/p^{b_{1,j}}\mathbb{Z}_p, \mathbb{Z}_p/p^{b_{2,j}}\mathbb{Z}_p, \mathbb{Z}_p/p^{b_{3,j}}\mathbb{Z}_p).&\end{aligned} \tag{2.3}$$

Each term on the right-hand side of equation (2.3) is contained in $\mathcal{C}_{X_3}$ by Example 2.4 and the set $\mathcal{C}_{X_3}$ is closed under finite direct product, we conclude that $(H_1,H_2,H_3) \in \mathcal{C}_{X_3}$. This finishes the proof of Theorem 1.8 for $m \leq 3$.

3 Proof of Theorem 1.8 for $m = 4$

In this section, we prove Theorem 1.8 for $m = 4$. First we prove a necessary condition for an element of $\mathcal{C}_{X_4}$ using a reduction procedure. The purpose of a reduction procedure is to reduce the size of a matrix n without information loss of $(H_1,\dots,H_m)$ and to extract inequalities using Proposition 2.3. After that, we prove that the same condition is also a sufficient condition for an element of $\mathcal{C}_{X_4}$ using zone theory. Throughout this section, we assume that $x_1 = 0$. (We may assume this by Proposition 2.3 (c)).

3.1 A reduction procedure

We begin by clarifying the relation between zeroth and first integrals. Recall that if $(n; H_1,\dots,H_m) \in \mathcal{C}_{X_m,0,k}$ for $k \in \overline{\mathbb{Z}}_{\geq 1}$, then $d_{0,1} = \cdots = d_{0,m}$ where $d_{0,i} = n - \sum_{r\in\overline{\mathbb{Z}}_{\geq 1}} d_{r,i}$ for each i.

Proposition 3.1. *If* $(n; H_1,\dots,H_m) \in \mathcal{C}_{X_m,0,k}$ *and* $d_{0,1} = \cdots = d_{0,m} > 0$*, then* $(n-1; H_1,\dots,H_m) \in \mathcal{C}_{X_m,0,k}$*.*

Proof. Since $\mathcal{C}_{X_m,0,\infty} = \mathcal{C}_{X_m,0,m-1}$, we may assume that k is finite. Let $P(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$ be a zeroth integral which satisfies $\mathrm{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(P(x_i)) \cong H_i/p^kH_i$ for each i. The constant term of $P(t)$ satisfies $\mathrm{rank}_{\mathbb{F}_p}(P(0)) = d_{0,1} > 0$. Using the Smith normal form of $P(0)$, we may assume that

$$P(t) = \begin{pmatrix} A_0 & O \\ O & 1 \end{pmatrix} + ptA_1 + \cdots + p^rt^rA_r =: \begin{pmatrix} P_1(t) & ptf(t) \\ ptg(t) & 1+pth(t) \end{pmatrix} \in \mathrm{M}_{(n-1)+1}(\mathbb{Z}_p)[t]$$

for some $r \in \mathbb{Z}_{\geq 0}$ and zeroth integrals $f(t), g(t), h(t), P_1(t)$. Then we have

$$\begin{aligned}\mathrm{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(P(t)) &= \mathrm{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}\left(\begin{pmatrix} P_1(t) & ptf(t) \\ ptg(t) & 1+pth(t) \end{pmatrix}\right) \\ &\cong \mathrm{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}\left(\begin{pmatrix} P_1(t) - p^2t^2(1+pth(t))^{-1}f(t)g(t) & O \\ O & 1+pth(t) \end{pmatrix}\right) \\ &\cong \mathrm{cok}_{\mathbb{Z}_p/p^k\mathbb{Z}_p}(Q(t)),\end{aligned}$$

where $Q(t) := P_1(t) - p^2t^2(\sum_{j=0}^{k-1}(-1)^jp^jt^jh(t)^j)f(t)g(t) \in \mathrm{M}_{n-1}(\mathbb{Z}_p)[t]$ is a zeroth integral as the set of zeroth integrals is closed under sum and product. This implies that $(n-1; H_1,\dots,H_m) \in \mathcal{C}_{X_m,0,k}$. □

Recall that the set $\mathcal{C}_{X_m,l,k}$ has a monoid structure by Proposition 2.3 (1). For $S \subset \mathcal{C}_{X_m,l,k}$, let $\langle S\rangle$ be the submonoid of $\mathcal{C}_{X_m,l,k}$ generated by the elements of S.

Corollary 3.2. *For every* $k \in \overline{\mathbb{Z}}_{\geq 0}$*, we have* $\mathcal{C}_{X_m,0,k+1} = \langle\{(1;1,\dots,1)\} \cup \varphi_{0,k}^{-1}(\mathcal{C}_{X_m,1,k})\rangle$*.*

Proof. The inclusion $\supset$ is clear since a zeroth integral $P(t) = 1$ gives $(1;1,\dots,1) \in \mathcal{C}_{X_m,0,k+1}$. Conversely, every element $(n; H_1,\dots,H_m) \in \mathcal{C}_{X_m,0,k+1}$ satisfies $n \geq s = s(H_1) = \cdots = s(H_m)$ so

$$(n; H_1,\dots,H_m) = (n-s)(1;1,\dots,1) + (s; H_1,\dots,H_m) \in \langle\{(1;1,\dots,1)\} \cup \varphi_{0,k}^{-1}(\mathcal{C}_{X_m,1,k})\rangle$$

by Proposition 3.1 and Proposition 2.3 (4). □

By Proposition 2.3 (b) and Proposition 2.3 (3), the set $\mathcal{C}_{X_m}$ is determined by the set $\mathcal{C}_{X_m,0,m-1}$, which is determined by the set $\mathcal{C}_{X_m,1,m-2}$ by Corollary 3.2. Since we have $\mathcal{C}_{X_m,1,m-2} \subset \mathcal{C}_{X_m,1,1}$ for every $m \geq 3$, an inequality which holds for elements of $\mathcal{C}_{X_m,1,1}$ also holds for elements of $\mathcal{C}_{X_m,1,m-2}$.

Lemma 3.3. *If* $(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,1,1}$, *then*

$$\sum_{i=1}^{m} d_{0,i} - (m-1)\alpha_0 \geq 0$$

for some non-negative integer $\alpha_0 \geq \max_{1 \leq i \leq m} d_{0,i}$.

Proof. It suffices to show that $\sum_{i=1}^{m} d_{0,i} \geq (m-1)\max_{1 \leq i \leq m} d_{0,i}$. We phrased the result in this way to make it consistent with Theorem 3.7.

We use induction on n. The case $n = 1$ follows from Example 2.4. Now assume that $n > 1$ and the theorem holds for every $n' < n$. Suppose that there exists $(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,1,1}$ such that

$$\sum_{i=1}^{m} d_{0,i} < (m-1) \max_{1 \leq i \leq m} d_{0,i}.$$

Let $P(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$ be a first integral such that $\mathrm{cok}_{\mathbb{Z}_p/p\mathbb{Z}_p}(P(x_i)) \cong H_i/pH_i$ for each i. Applying the Smith normal form of the constant term of $P(t)$, we may assume that

$$P(t) = \begin{pmatrix} pA & O \\ O & I_{d_{0,1}} \end{pmatrix} + tB + pQ(t)$$

for some $A \in \mathrm{M}_{n-d_{0,1}}(\mathbb{Z}_p)$, $B \in \mathrm{M}_n(\mathbb{Z}_p)$ and $Q(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$. Moreover,

$$P_1(t) := \begin{pmatrix} O & O \\ O & I_{d_{0,1}} \end{pmatrix} + tB$$

satisfies $d_{0,P(x_i)} = d_{0,P_1(x_i)}$ for each i so we may assume that

$$P(t) = \begin{pmatrix} O & O \\ O & I_{d_{0,1}} \end{pmatrix} + t\begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix}.$$

Case 1: $p \nmid B_1$. The Smith normal form of B_1 gives $U, V \in \mathrm{GL}_{n-d_{0,1}}(\mathbb{Z}_p)$ such that $UB_1V = \begin{pmatrix} 1 & O \\ O & B_1' \end{pmatrix}$ for some $B_1' \in \mathrm{M}_{n-d_{0,1}-1}(\mathbb{Z}_p)$. For every non-zero $x \in X_m$, we have

$$\begin{aligned} \mathrm{cok}_{\mathbb{Z}_p/p\mathbb{Z}_p}(P(x)) &\cong \mathrm{cok}_{\mathbb{Z}_p/p\mathbb{Z}_p}\left(\begin{pmatrix} U & O \\ O & I_{d_{0,1}} \end{pmatrix} P(x) \begin{pmatrix} V & O \\ O & I_{d_{0,1}} \end{pmatrix}\right) \\ &= \mathrm{cok}_{\mathbb{Z}_p/p\mathbb{Z}_p}\left(\begin{pmatrix} \begin{matrix} x & O \\ O & xB_1' \end{matrix} & xUB_2 \\ xB_3V & I_{d_{0,1}} + xB_4 \end{pmatrix}\right) \\ &\cong \mathrm{cok}_{\mathbb{Z}_p/p\mathbb{Z}_p}\left(\begin{pmatrix} x & O \\ O & Q(x) \end{pmatrix}\right) \end{aligned}$$

for a first integral

$$Q(t) := \begin{pmatrix} O & O \\ O & I_{d_{0,1}} \end{pmatrix} + t\begin{pmatrix} B_1' & B_2' \\ B_3' & B_4' \end{pmatrix} \in \mathrm{M}_{n-1}(\mathbb{Z}_p)[t].$$

Then we have $d_{0,Q(x_1)} = d_{0,1}$, $d_{0,Q(x_i)} = d_{0,i} - 1$ for $2 \leq i \leq m$ and $(n-1; \mathrm{cok}(Q(x_1)), \dots, \mathrm{cok}(Q(x_m)))$ contradicts the induction hypothesis since

$$\begin{aligned} \sum_{i=1}^{m} d_{0,Q(x_i)} - (m-1) \max_{1 \leq i \leq m} d_{0,Q(x_i)} &= \sum_{i=1}^{m} d_{0,i} - (m-1)(\max_{1 \leq i \leq m} d_{0,Q(x_i)} + 1) \\ &\leq \sum_{i=1}^{m} d_{0,i} - (m-1) \max_{1 \leq i \leq m} d_{0,i} < 0. \end{aligned}$$

Case 2: $p \mid B_1$ and $[p \nmid B_2$ or $p \nmid B_3]$. We may assume that $p \nmid B_2$. Choose invertible matrices U and V such that $UB_2V = \left(\begin{smallmatrix} 1 & O \\ O & B_2' \end{smallmatrix}\right)$. For every non-zero $x \in X_m$, we have

$$\begin{aligned} \operatorname{cok}_{\mathbb{Z}_p/p\mathbb{Z}_p}(P(x)) &\cong \operatorname{cok}_{\mathbb{Z}_p/p\mathbb{Z}_p}\left(\begin{pmatrix} U & O \\ O & V^{-1} \end{pmatrix} P(x) \begin{pmatrix} I_{d_{1,1}} & O \\ O & V \end{pmatrix}\right) \\ &= \operatorname{cok}_{\mathbb{Z}_p/p\mathbb{Z}_p}\left(\begin{pmatrix} O & \begin{matrix} x & O \\ O & xB_2' \end{matrix} \\ xV^{-1}B_3 & I_{d_{0,1}} + xV^{-1}B_4V \end{pmatrix}\right) \\ &\cong \operatorname{cok}_{\mathbb{Z}_p/p\mathbb{Z}_p}\left(\begin{pmatrix} x & O \\ O & Q(x) \end{pmatrix}\right) \end{aligned}$$

for a first integral

$$Q(t) := \begin{pmatrix} O & O \\ O & I_{d_{0,1}-1} \end{pmatrix} + t \begin{pmatrix} O & B_2' \\ B_3' & B_4' \end{pmatrix} \in \mathrm{M}_{n-1}(\mathbb{Z}_p)[t].$$

Then $d_{0,Q(x_i)} = d_{0,i} - 1$ for $1 \leq i \leq m$ and $(n-1; \operatorname{cok}(Q(x_1)), \dots, \operatorname{cok}(Q(x_m)))$ contradicts the induction hypothesis since

$$\sum_{i=1}^{m} d_{0,Q(x_i)} - (m-1) \max_{1 \leq i \leq m} d_{0,Q(x_i)} = \sum_{i=1}^{m} d_{0,i} - (m-1) \max_{1 \leq i \leq m} d_{0,i} - 1 < 0.$$

In the remaining cases, we have $p \mid B_1, B_2, B_3$ so that $d_{0,1} = \max_{1 \leq i \leq m} d_{0,i}$. By the same reason, we obtain that $d_{0,1} = \cdots = d_{0,m}$. Then we have $\sum_{i=1}^{m} d_{0,i} - (m-1)\max_{1 \leq i \leq m} d_{0,i} = d_{0,1} \geq 0$, a contradiction. □

We need some work to find the conditions for elements of $\mathfrak{C}_{X_m,1,2}$.

Lemma 3.4. *Assume that $J \in \mathrm{M}_n(\mathbb{Z}_p)$ has a single non-zero row or column. For every $r \in \mathbb{Z}_{\geq 1}$, $x \in \mathbb{Z}_p$ and $A \in \mathrm{M}_n(\mathbb{Z}_p)$, there exists $x_0 \in \mathbb{Z}_p$ and $d \in \mathbb{Z}_{\geq 0}$ such that*

$$d_{i,A} = d_{i,A+p^rxJ} \quad \text{for } i < r \qquad \text{and} \qquad d_{r,A+p^rxJ} = \begin{cases} d-1 \text{ or } d, & x \equiv x_0 \pmod{p}, \\ d, & x \not\equiv x_0 \pmod{p}. \end{cases}$$

The matrix J is called singular of order r at x_0 over A if $d_{r,A+p^rx_0J} = d - 1$.

Proof. We may assume $J = \begin{pmatrix} J_1 & O_{n\times(n-1)} \end{pmatrix}$. The isomorphism $\operatorname{cok}_{\mathbb{Z}_p/p^r\mathbb{Z}_p}(A) \cong \operatorname{cok}_{\mathbb{Z}_p/p^r\mathbb{Z}_p}(A + p^rxJ)$ implies that $d_{i,A} = d_{i,A+p^rxJ}$ for each $i < r$. Let A_j be the j-th column of A for each j and $A_{s_1}, \dots, A_{s_D}$ $(2 \leq s_j \leq m)$ any maximal subset of $\{A_2, \dots, A_m\}$ whose elements are linearly independent modulo p^{r+1}, i.e. $\sum_{j=1}^{D} c_jA_{s_j} \equiv 0 \pmod{p^{r+1}}$ implies that $c_1, \dots, c_D \equiv 0 \pmod{p}$. (For example, $(1,1), (1, p+1) \in \mathbb{Z}_p^2$ are not linearly independent modulo p but are linearly independent modulo p^2.) Define

$$\begin{aligned} S := \{v \in \mathbb{Z}_p^n : {} & \text{there exist } c_0, \dots, c_D \in \mathbb{Z}_p \text{ such that } p \nmid c_j \text{ for some } 0 \leq j \leq D \\ & \text{and } c_0v + c_1A_{s_1} + \cdots + c_DA_{s_D} \equiv 0 \pmod{p^{r+1}}\}. \end{aligned}$$

Since the number $\sum_{i=0}^{r} d_{i,A}$ is the maximum number of linearly independent columns of A modulo p^{r+1}, we have

$$D_x := \sum_{i=0}^{r} d_{i,A+p^rxJ} = \begin{cases} D & \text{if } A_1 + p^rxJ_1 \in S, \\ D+1 & \text{otherwise.} \end{cases}$$

If we have $D_x = D + 1$ for every $x \in \mathbb{Z}_p$, then the lemma holds for $d = d_{r,A} + 1$ and any $x_0 \in \mathbb{Z}_p$. Now assume that $D_{x_0} = D$ for some $x_0 \in \mathbb{Z}_p$. Then there exist $c_0, \dots, c_D \in \mathbb{Z}_p$ such that $p \nmid c_j$ for some j and

$$c_0(A_1 + p^rx_0J_1) + c_1A_{s_1} + \cdots + c_DA_{s_D} \equiv 0 \pmod{p^{r+1}}.$$

If $p \mid c_0$, then $c_0(A_1 + p^rx_0J_1) \equiv c_0(A_1 + p^rxJ_1) \pmod{p^{r+1}}$ for every $x \in \mathbb{Z}_p$ so we have $D_x = D$ for every $x \in \mathbb{Z}_p$. If $p \nmid c_0$, then $A_1 + p^rx_0J_1$ is a $\mathbb{Z}_p$-linear combination of $A_{s_1}, \dots, A_{s_D}$ modulo p^{r+1}. If there exists $x_1 \not\equiv x_0 \pmod{p}$ such that $A_1 + p^rx_1J_1$ is a $\mathbb{Z}_p$-linear combination of $A_{s_1}, \dots, A_{s_D}$ modulo p^{r+1}, then

$$\frac{(A_1 + p^rx_0J_1) - (A_1 + p^rx_1J_1)}{x_0 - x_1} = p^rJ_1$$

is also a $\mathbb{Z}_p$-linear combination of $A_{s_1}, \dots, A_{s_D}$ modulo p^{r+1} so we have $D_x = D$ for every $x \in \mathbb{Z}_p$. If there is no such x_1, then $D_x = D + 1$ if and only if $x \not\equiv x_0 \pmod{p}$. □

The following lemma is the most technical part of this paper.

Lemma 3.5. *Let $P(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$ be a first integral. Then either one of the following holds:*

(1) *There exists a first integral $Q(t) \in \mathrm{M}_{n-1}(\mathbb{Z}_p)[t]$ satisfies, for at most one $1 \le r \le m$,*

(a) *either*

$$\begin{cases} d_{0,Q(x_i)} = d_{0,P(x_i)} - 1 \textit{ for every } 1 \le i \le m, \\ d_{1,Q(x_i)} \in \{d_{1,P(x_i)}, d_{1,P(x_i)} + 1\} \textit{ for } i = r \textit{ and } d_{1,Q(x_i)} = d_{1,P(x_i)} \textit{ otherwise,} \end{cases}$$

(b) *or*

$$\begin{cases} d_{0,Q(x_i)} = d_{0,P(x_i)} \textit{ for } i = r \textit{ and } d_{0,Q(x_i)} = d_{0,P(x_i)} - 1 \textit{ otherwise,} \\ d_{1,Q(x_i)} \in \{d_{1,P(x_i)} - 1, d_{1,P(x_i)} - 2\} \textit{ for } i = r \textit{ and } d_{1,Q(x_i)} = d_{1,P(x_i)} \textit{ otherwise,} \end{cases}$$

(c) *or*

$$\begin{cases} d_{0,Q(x_i)} = d_{0,P(x_i)} \textit{ for } i = r \textit{ and } d_{0,Q(x_i)} = d_{0,P(x_i)} - 1 \textit{ otherwise,} \\ d_{1,Q(x_i)} = d_{1,P(x_i)} \textit{ for every } 1 \le i \le m. \end{cases}$$

(2) *The number $d_{0,P(x_i)}$ is constant for every $1 \le i \le m$ and there exists a first integral $Q(t) \in \mathrm{M}_{n-d_{0,P(x_i)}}(\mathbb{Z}_p)[t]$ satisfying $d_{0,Q(x_i)} = 0$ and $d_{1,Q(x_i)} = d_{1,P(x_i)}$ for each i.*

Proof. As in the proof of Lemma 3.3, we may assume that

$$P(t) := \begin{pmatrix} O & O & O \\ O & pI_{d_{1,1}} & O \\ O & O & I_{d_{0,1}} \end{pmatrix} + t \begin{pmatrix} B_{11} & B_{12} & B_{13} \\ B_{21} & B_{22} & B_{23} \\ B_{31} & B_{32} & B_{33} \end{pmatrix} + pt^2 C \in \mathrm{M}_{(n-d_{0,1}-d_{1,1})+d_{1,1}+d_{0,1}}(\mathbb{Z}_p).$$

Denote $d'_{2,1} := \sum_{r \in \overline{\mathbb{Z}}_{\ge 2}} d_{r,1} = n - (d_{0,1} + d_{1,1})$ for simplicity.

Case 1: $p \nmid B_{11}$. The Smith normal form of B_{11} gives $U, V \in \mathrm{GL}_{d'_{2,1}}(\mathbb{Z}_p)$ such that $UB_{11}V = \left(\begin{smallmatrix} 1 & O \\ O & B^{rd}_{11} \end{smallmatrix}\right)$ for some $B^{rd}_{11} \in \mathrm{M}_{d'_{2,1}-1}(\mathbb{Z}_p)$. Then for every non-zero $x \in X_m$, we have

$$\begin{aligned} \mathrm{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(P(x)) &\cong \mathrm{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} U & O \\ O & I_{d_{0,1}+d_{1,1}} \end{pmatrix} P(x) \begin{pmatrix} V & O \\ O & I_{d_{0,1}+d_{1,1}} \end{pmatrix}\right) \\ &= \mathrm{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} \begin{matrix} x & O \\ O & xB^{rd}_{11} \end{matrix} & xUB_{12} & xUB_{13} \\ xB_{21}V & pI_{d_{1,1}} + xB_{22} & xB_{23} \\ xB_{31}V & xB_{32} & I_{d_{0,1}} + xB_{33} \end{pmatrix} + px^2 C_1\right) \\ &= \mathrm{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} x & O & xB^u_{12} & xB^u_{13} \\ O & xB^{rd}_{11} & xB^d_{12} & xB^d_{13} \\ xB^l_{21} & xB^r_{21} & pI_{d_{1,1}} + xB_{22} & xB_{23} \\ xB^l_{31} & xB^r_{31} & xB_{32} & I_{d_{0,1}} + xB_{33} \end{pmatrix} + px^2 C_1\right) \\ &\cong \mathrm{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} x & O & O & O \\ O & xB^{rd}_{11} & xB^d_{12} & xB^d_{13} \\ O & xB^r_{21} & pI_{d_{1,1}} + xB'_{22} & xB'_{23} \\ O & xB^r_{31} & xB'_{32} & I_{d_{0,1}} + xB'_{33} \end{pmatrix} + px^2 \begin{pmatrix} c & C_{ru} \\ C_{ld} & C_{rd} \end{pmatrix}\right) \\ &\cong \mathrm{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(Q(x)) \end{aligned}$$

for

$$Q(t) := \begin{pmatrix} O & O & O \\ O & pI_{d_{1,1}} & O \\ O & O & I_{d_{0,1}} \end{pmatrix} + t \begin{pmatrix} B^{rd}_{11} & B^d_{12} & B^d_{13} \\ B^r_{21} & B'_{22} & B'_{23} \\ B^r_{31} & B'_{32} & B'_{33} \end{pmatrix} + pt^2 C_{rd} \in \mathrm{M}_{n-1}(\mathbb{Z}_p)[t].$$

Here the last isomorphism is due to the relation

$$\begin{aligned} \mathrm{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} x + pcx^2 & pf_1(x) \\ pf_2(x) & Q(x) \end{pmatrix}\right) &\cong \mathrm{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} x + pcx^2 & O \\ O & Q(x) - pf_2(x)(x + pcx^2)^{-1} pf_1(x) \end{pmatrix}\right) \\ &\cong \mathrm{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(Q(x)) \end{aligned}$$

for every $x \not\equiv 0 \pmod{p}$. Since $Q(t)$ is a first integral with $d_{0,Q(x_1)} = d_{0,P(x_1)}$, $d_{0,Q(x_i)} = d_{0,P(x_i)} - 1$ for every $2 \le i \le m$ and $d_{1,Q(x_i)} = d_{1,P(x_i)}$ for every $1 \le i \le m$, it satisfies condition (c) for $r = 1$.

Case 2: $p \mid B_{11}$ and $[p \nmid B_{12}$ or $p \nmid B_{21}]$. We may assume that $p \nmid B_{12}$. Choose invertible matrices U and V such that $UB_{12}V = \left(\begin{smallmatrix} 1 & O \\ O & B_{12}^{rd} \end{smallmatrix}\right)$ and write $B_{11} = pB'_{11}$. Then for every non-zero $x \in X_m$, we have

$$\begin{aligned}
\operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(P(x)) &\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} U & O & O \\ O & V^{-1} & O \\ O & O & I_{d_{0,1}} \end{pmatrix} P(x) \begin{pmatrix} I_{d'_{2,1}} & O & O \\ O & V & O \\ O & O & I_{d_{0,1}} \end{pmatrix}\right) \\
&= \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} pxUB'_{11} & \begin{matrix} x & O \\ O & xB_{12}^{rd} \end{matrix} & xUB_{13} \\ xV^{-1}B_{21} & pI_{d_{1,1}} + xV^{-1}B_{22}V & xV^{-1}B_{23} \\ xB_{31} & xB_{32}V & I_{d_{0,1}} + xB_{33} \end{pmatrix} + px^2C_1\right) \\
&= \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} pxB_{11}^u & x & O & xB_{13}^u \\ pxB_{11}^d & O & xB_{12}^{rd} & xB_{13}^d \\ xB_{21}^u & p + xB_{22}^{lu} & xB_{22}^{ru} & xB_{23}^u \\ xB_{21}^d & xB_{22}^{ld} & pI_{d_{1,1}-1} + xB_{22}^{rd} & xB_{23}^d \\ xB_{31} & xB_{32}^l & xB_{32}^r & I_{d_{0,1}} + xB_{33} \end{pmatrix} + px^2C_1\right) \\
&\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} O & x & O & O \\ pxB_{11}^d & O & xB_{12}^{rd} & xB_{13}^d \\ xB_{21}^{u'} & p & xB_{22}^{ru} & -pB_{13}^u + xB_{23}^{u'} \\ xB_{21}^{d'} & O & pI_{d_{1,1}-1} + xB_{22}^{rd} & xB_{23}^{d'} \\ xB'_{31} & O & xB_{32}^r & I_{d_{0,1}} + xB'_{33} \end{pmatrix} + px^2C_2\right) \\
&\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} O & x + pcx^2 & O \\ xB_l + px^2C_l & O & \begin{pmatrix} O & O \\ O & -pB_{13}^u \\ pI_{d_{1,1}-1} & O \\ O & I_{d_{0,1}} \end{pmatrix} + xB_r + px^2C_r \end{pmatrix}\right).
\end{aligned}$$

Then

$$Q(t) := \begin{pmatrix} O & O & O \\ O & O & -pB_{13}^u \\ O & pI_{d_{1,1}-1} & O \\ O & O & I_{d_{0,1}} \end{pmatrix} + t\begin{pmatrix} B_l & B_r \end{pmatrix} + pt^2\begin{pmatrix} C_l & C_r \end{pmatrix} \in \mathrm{M}_{n-1}(\mathbb{Z}_p)[t]$$

satisfies condition (b) for $r = 1$.

Case 3: $[p \mid B_{11}, B_{12}, B_{21}]$ and $[p \nmid B_{13}$ or $p \nmid B_{31}]$. We may assume that $p \nmid B_{13}$. Choose invertible matrices U and V such that $UB_{13}V = \left(\begin{smallmatrix} 1 & O \\ O & B_{13}^{rd} \end{smallmatrix}\right)$ and write $B_{ij} = pB'_{ij}$ for $(i,j) \in \{(1,1),(1,2)\}$. Then for every non-zero $x \in X_m$, we have

$$\begin{aligned}
\operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(P(x)) &\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} U & O & O \\ O & I_{d_{1,1}} & O \\ O & O & V^{-1} \end{pmatrix} P(x) \begin{pmatrix} I_{d'_{2,1}} & O & O \\ O & I_{d_{1,1}} & O \\ O & O & V \end{pmatrix}\right) \\
&= \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} pxUB'_{11} & pxUB'_{12} & \begin{matrix} x & O \\ O & xB_{13}^{rd} \end{matrix} \\ xB_{21} & pI_{d_{1,1}} + xB_{22} & xB_{23}V \\ xV^{-1}B_{31} & xV^{-1}B_{32} & I_{d_{0,1}} + xV^{-1}B_{33}V \end{pmatrix} + px^2C_1\right) \\
&= \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} pxB_{11}^u & pxB_{12}^u & x & O \\ pxB_{11}^d & pxB_{12}^d & O & xB_{13}^{rd} \\ xB_{21} & pI_{d_{1,1}} + xB_{22} & xB_{23}^l & xB_{23}^r \\ xB_{31}^u & xB_{32}^u & 1 + xB_{33}^{lu} & xB_{33}^{ru} \\ xB_{31}^d & xB_{32}^d & xB_{33}^{ld} & I_{d_{0,1}-1} + xB_{33}^{rd} \end{pmatrix} + px^2C_1\right)
\end{aligned}$$

$$\begin{aligned}
&\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} O & O & x & O \\ pxB^{d}_{11} & pxB^{d}_{12} & O & xB^{rd}_{13} \\ xB'_{21} & pI_{d_{1,1}} + xB'_{22} & O & xB^{r}_{23} \\ -pB^{u}_{11} + xB^{u'}_{31} & -pB^{u}_{12} + xB^{u'}_{32} & 1 & xB^{ru}_{33} \\ xB^{d'}_{31} & xB^{d'}_{32} & O & I_{d_{0,1}-1} + xB^{rd}_{33} \end{pmatrix} + px^2C_2\right) \\
&\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} O & x + pcx^2 & O \\ \begin{pmatrix} O & O \\ O & pI_{d_{1,1}} \\ -pB^{u}_{11} & -pB^{u}_{12} \\ O & O \end{pmatrix} + xB_l + px^2C_l & O & \begin{pmatrix} O \\ O \\ O \\ I_{d_{0,1}-1} \end{pmatrix} + xB_r + px^2C_r \end{pmatrix}\right).
\end{aligned}$$

Then

$$Q(t) := \begin{pmatrix} O & O & O \\ O & pI_{d_{1,1}} & O \\ -pB^{u}_{11} & -pB^{u}_{12} & O \\ O & O & I_{d_{0,1}-1} \end{pmatrix} + t\begin{pmatrix} B_l & B_r \end{pmatrix} + pt^2\begin{pmatrix} C_l & C_r \end{pmatrix} \in \mathrm{M}_{n-1}(\mathbb{Z}_p)[t]$$

satisfies condition (a) for any r.

Case 4: $[p \mid B_{11}, B_{12}, B_{21}, B_{13}, B_{31}]$ and $p \nmid B_{22}$. Choose invertible matrices U and V such that $UB_{22}V = \left(\begin{smallmatrix} 1 & O \\ O & B^{rd}_{22} \end{smallmatrix}\right)$ and write $B_{ij} = pB'_{ij}$ for $(i,j) \in \{(1,1),(1,2),(2,1)\}$. Let $UV = \left(\begin{smallmatrix} d & D_1 \\ D_2 & D_3 \end{smallmatrix}\right) \in \mathrm{GL}_{d_{1,1}}(\mathbb{Z}_p)$. Then for every non-zero $x \in X_m$, we have

$$\begin{aligned}
\operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(P(x)) &\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} I_{d'_{2,1}} & O & O \\ O & U & O \\ O & O & I_{d_{0,1}} \end{pmatrix} P(x) \begin{pmatrix} I_{d'_{2,1}} & O & O \\ O & V & O \\ O & O & I_{d_{0,1}} \end{pmatrix}\right) \\
&= \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} pxB'_{11} & pxB'_{12}V & xB_{13} \\ pxUB'_{21} & \begin{matrix} x + pd & pD_1 \\ pD_2 & pD_3 + xB^{rd}_{22} \end{matrix} & xUB_{23} \\ xB_{31} & xB_{32}V & I_{d_{0,1}} + xB_{33} \end{pmatrix} + px^2C_1\right) \\
&= \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} pxB'_{11} & pxB^{l}_{12} & pxB^{r}_{12} & xB_{13} \\ pxB^{u}_{21} & x + pd & pD_1 & xB^{u}_{23} \\ pxB^{d}_{21} & pD_2 & pD_3 + xB^{rd}_{22} & xB^{d}_{23} \\ xB_{31} & xB^{l}_{32} & xB^{r}_{32} & I_{d_{0,1}} + xB_{33} \end{pmatrix} + px^2C_1\right) \\
&\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} pxB'_{11} & O & pxB^{r}_{12} & xB'_{13} \\ O & x + pd & pD_1 & -pdB^{u}_{23} \\ pxB^{d}_{21} & pD_2 & pD_3 + xB^{rd}_{22} & -pD_2B^{u}_{23} + xB^{d}_{23} \\ xB'_{31} & -pdB^{l}_{32} & -pB^{l}_{32}D_1 + xB^{r}_{32} & I_{d_{0,1}} - pdB^{l}_{32}B^{u}_{23} + xB'_{33} \end{pmatrix} + px^2C_2\right) \\
&\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} xB'_{11} + px^2C_{lu} & O & xB_{ru} + px^2C_{ru} \\ O & x + p(d + cx^2) & O \\ xB_{ld} + px^2C_{ld} & O & \left(\begin{smallmatrix} pD_3 & pA_{ru} \\ pA_{ld} & I_{d_{0,1}} + pA_{rd} \end{smallmatrix}\right) + xB_{rd} + px^2C_{rd} \end{pmatrix}\right).
\end{aligned}$$

Then

$$Q(t) := \begin{pmatrix} O & O & O \\ O & pD_3 & pA_{ru} \\ O & pA_{ld} & I_{d_{0,1}} + pA_{rd} \end{pmatrix} + t\begin{pmatrix} B'_{11} & B_{ru} \\ B_{ld} & B_{rd} \end{pmatrix} + pt^2\begin{pmatrix} C_{lu} & C_{ru} \\ C_{ld} & C_{rd} \end{pmatrix} \in \mathrm{M}_{n-1}(\mathbb{Z}_p)[t]$$

satisfies condition (b) for $r = 1$ if $\operatorname{rank}_{\mathbb{F}_p}(\overline{D_3}) \in \{d_{1,1} - 1, d_{1,1} - 2\}$. This is true by the inequality

$$\operatorname{rank}_{\mathbb{F}_p}(\overline{D_3}) \geq \operatorname{rank}_{\mathbb{F}_p}\begin{pmatrix} \overline{D_2} & \overline{D_3} \end{pmatrix} - 1 \geq \operatorname{rank}_{\mathbb{F}_p}(\overline{UV}) - 2 = d_{1,1} - 2.$$

Case 5: $[p \mid B_{11}, B_{12}, B_{21}, B_{13}, B_{31}, B_{22}]$ and $[p \nmid B_{23}$ or $p \nmid B_{32}]$. We may assume that $p \nmid B_{23}$. Choose invertible matrices U and V such that $UB_{23}V = \left(\begin{smallmatrix} 1 & O \\ O & B^{rd}_{23} \end{smallmatrix}\right)$ and write

$$B_{ij} = pB'_{ij} \quad \text{for each } i + j \leq 4.$$

Then for every non-zero $x \in X_m$, we have

$$
\begin{aligned}
&\operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(P(x)) \\
&\quad\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} I_{d'_{2,1}} & O & O \\ O & U & O \\ O & O & V^{-1} \end{pmatrix} P(x) \begin{pmatrix} I_{d'_{2,1}} & O & O \\ O & U^{-1} & O \\ O & O & V \end{pmatrix}\right) \\
&\quad= \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} pxB'_{11} & pxB'_{12}U^{-1} & pxB'_{13}V \\ pxUB'_{21} & pI_{d_{1,1}} + pxUB'_{22}U^{-1} & \begin{matrix} x & O \\ O & xB^{rd}_{23} \end{matrix} \\ pxV^{-1}B'_{31} & xV^{-1}B_{32}U^{-1} & I_{d_{0,1}} + xV^{-1}B_{33}V \end{pmatrix} + px^2C_1\right) \\
&\quad= \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} pxB'_{11} & pxB^l_{12} & pxB^r_{12} & pxB^l_{13} & pxB^r_{13} \\ pxB^u_{21} & p + pxb^{lu}_{22} & pxB^{ru}_{22} & x & O \\ pxB^d_{21} & pxB^{ld}_{22} & pI_{d_{1,1}-1} + pxB^{rd}_{22} & O & xB^{rd}_{23} \\ pxB^u_{31} & xb^{lu}_{32} & xB^{ru}_{32} & 1 + xb^{lu}_{33} & xB^{ru}_{33} \\ pxB^d_{31} & xB^{ld}_{32} & xB^{rd}_{32} & xB^{ld}_{33} & I_{d_{0,1}-1} + xB^{rd}_{33} \end{pmatrix} + px^2C_1\right) \\
&\quad\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} pxB'_{11} & pxB^l_{12} & pxB^r_{12} & O & pxB^r_{13} \\ O & p & O & x & O \\ pxB^d_{21} & pxB^{ld}_{22} & pI_{d_{1,1}-1} + pxB^{rd}_{22} & O & xB^{rd}_{23} \\ pA_1 + pxB^{u'}_{31} & pa_2 + xb^{lu'}_{32} & pA_3 + xB^{ru'}_{32} & 1 & xB^{ru}_{33} \\ pxB^{d'}_{31} & pA_4 + xB^{ld'}_{32} & xB^{rd'}_{32} & O & I_{d_{0,1}-1} + xB^{rd}_{33} \end{pmatrix} + px^2C_2\right) \\
&\quad\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}\left(\begin{pmatrix} * & * & * & O & * \\ O & O & O & x + pcx^2 & O \\ * & * & pI_{d_{1,1}-1} + * & O & * \\ pA_1 + * & p(x + pcx^2)^{-1} + pa_2 + * & pA_3 + * & O & * \\ * & pA_4 + * & * & O & I_{d_{0,1}-1} + * \end{pmatrix}\right) \\
&\quad\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(px^{-1}J + P_1(x)),
\end{aligned}
$$

where each $*$ is of the form $xB + px^2C$,

$$J := \begin{pmatrix} O & O & O & O \\ O & O & O & O \\ O & -1 & O & O \\ O & O & O & O \end{pmatrix} \in \mathrm{M}_{n-1}(\mathbb{Z}_p) \quad (J_{n-d_{0,1},d'_{2,1}+1} = -1)$$

and

$$P_1(t) := \begin{pmatrix} O & O & O & O \\ O & O & pI_{d_{1,1}-1} & O \\ pA_1 & pa_2 & pA_3 & O \\ O & pA_4 & O & I_{d_{0,1}-1} \end{pmatrix} + tB' + pt^2C' \in \mathrm{M}_{n-1}(\mathbb{Z}_p)[t].$$

Now we have $d_{0,P_1(x_i)} = d_{0,i} - 1$ and $|d_{1,P_1(x_i)} - d_{1,i}| \leq 1$ by Lemma 3.4. Precisely,

$$d_{1,P_1(x_1)} = \begin{cases} d_{1,1} - 1 & \text{if } p \mid A_1 \text{ and } p \mid a_2, \\ d_{1,1} & \text{otherwise,} \end{cases}$$

and for every $2 \leq i \leq m$,

$$d_{1,P_1(x_i)} = \begin{cases} d_{1,i} + 1 & \text{if } J \text{ is singular of order 1 at } x_i^{-1} \text{ over } P_1(x_i), \\ d_{1,i} - 1 & \text{if } J \text{ is singular of order 1 at 0 over } P_1(x_i), \\ d_{1,i} & \text{otherwise.} \end{cases}$$

Let $P_1(t) = \begin{pmatrix} q_1(t) & \cdots & q_{n-1}(t) \end{pmatrix}$ and $q_i(t) = \mathbf{a}_i + t\mathbf{b}_i + pt^2\mathbf{c}_i$ for some $\mathbf{a}_i, \mathbf{b}_i, \mathbf{c}_i \in \mathbb{Z}_p^{n-1}$.

Case 5.1: J is singular of order 1 at x_r^{-1} over $P_1(x_r)$ for some $2 \le r \le m$. Let e_i be the i-th unit vector in $\mathbb{Z}_p^{n-1}$, so that the non-zero column of J is $-e_{n-d_{0,1}}$. The proof of Lemma 3.4 tells us that the $(d'_{2,1}+1)$-th column of $P_1(x_r)$ is a $\mathbb{Z}_p$-linear combination of other columns of $P_1(x_r)$, i.e.

$$q_{d'_{2,1}+1}(x_r) - px_r^{-1}e_{n-d_{0,1}} \equiv \sum_{i \neq d'_{2,1}+1} c_i q_i(x_r) \pmod{p^2}$$

for some $c_i \in \mathbb{Z}_p$ $(i \neq d'_{2,1})$. Then

$$(pt^{-1}J + P_1(t)) \begin{pmatrix} I_{d'_{2,1}} & \begin{matrix} -c_1 \\ \vdots \\ -c_{d'_{2,1}} \end{matrix} & O \\ O & 1 & O \\ O & \begin{matrix} -c_{d'_{2,1}+2} \\ \vdots \\ -c_{n-1} \end{matrix} & I_{d_{0,1}+d_{1,1}-2} \end{pmatrix} = \begin{pmatrix} q_1(t) & \cdots & q_{d'_{2,1}}(t) & g(t) & q_{d'_{2,1}+2}(t) & \cdots & q_{n-1}(t) \end{pmatrix}$$

and $g(x_r) \equiv 0 \pmod{p^2}$ so we have $g(t) \equiv (t - x_r)f(t) \pmod{p^2}$ for

$$f(t) := pt^{-1}x_r^{-1}e_{n-d_{0,1}} + \mathbf{a}' + pt\mathbf{b}' \quad (\mathbf{a}', \mathbf{b}' \in \mathbb{Z}_p^{n-1}).$$

Now

$$P_2(t) := \begin{pmatrix} q_1(t) & \cdots & q_{d'_{2,1}}(t) & tf(t) & q_{d'_{2,1}+2}(t) & \cdots & q_{n-1}(t) \end{pmatrix} \in \mathrm{M}_{n-1}(\mathbb{Z}_p)[t]$$

satisfies condition (a) or (c) for the same r.

- For $i \notin \{1, r\}$, we have

  $$\operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(P(x_i)) \cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(px_i^{-1}J + P_1(x_i)) \cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(P_2(x_i))$$

  so $d_{0,P_2(x_i)} = d_{0,i} - 1$ and $d_{1,P_2(x_i)} = d_{1,i}$.
- For $i = 1$, we have

  $$P_2(0) = \begin{pmatrix} O & O & O & O \\ O & O & pI_{d_{1,1}-1} & O \\ pA_1 & px_r^{-1} & pA_3 & O \\ O & O & O & I_{d_{0,1}-1} \end{pmatrix}$$

  so $d_{0,P_2(x_1)} = d_{0,1} - 1$ and $d_{1,P_2(x_1)} = d_{1,1}$.
- For $i = r$, we have

  $$\begin{aligned} \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(P(x_r)) &\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(px_r^{-1}J + P_1(x_r)) \\ &\cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p} \begin{pmatrix} q_1(t) & \cdots & q_{d'_{2,1}}(t) & q_{d'_{2,1}+2}(t) & \cdots & q_{n-1}(t) \end{pmatrix} \end{aligned}$$

  so $(d_{0,P_2(x_r)}, d_{1,P_2(x_r)}) \in \{(d_{0,r}, d_{1,r}), (d_{0,r} - 1, d_{1,r}), (d_{0,r} - 1, d_{1,r} + 1)\}$.

Case 5.2: J is not singular of order 1 at x_r^{-1} over $P_1(x_r)$ for all $2 \le r \le m$. Let

$$P_b(t) := p(a_2 + 1 + bt)J + P_1(t) \in \mathrm{M}_{n-1}(\mathbb{Z}_p)[t]$$

for $b \in \{0, 1, \dots, p-1\}$. Then we have

$$\operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(px_r^{-1}J + P_1(x_r)) \cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(P_b(x_r))$$

unless J is singular of order 1 at $a_2 + 1 + bx_r$ over $P_1(x_r)$. Since $p > m - 1$, one can choose $b_0 \in \{0, 1, \dots, p-1\}$ such that J is not singular of order 1 at $a_2 + 1 + b_0x_r$ over $P_1(x_r)$ for every $2 \le r \le m$. Now $P_{b_0}(t)$ is a first integral and satisfies condition (a) for $r = 1$.

- For $i \neq 1$, we have

  $$\operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(P(x_i)) \cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(px_i^{-1}J + P_1(x_i)) \cong \operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(P_{b_0}(x_i))$$

  so $d_{0,P_{b_0}(x_i)} = d_{0,i} - 1$ and $d_{1,P_{b_0}(x_i)} = d_{1,i}$.

- For $i = 1$,

$$P_{b_0}(0) = \begin{pmatrix} O & O & O & O \\ O & O & pI_{d_{1,1}-1} & O \\ pA_1 & -p & pA_3 & O \\ O & pA_4 & O & I_{d_{0,1}-1} \end{pmatrix}$$

so $d_{0,P_{b_0}(x_1)} = d_{0,1} - 1$ and $d_{1,P_{b_0}(x_1)} = d_{1,1}$.

In the remaining cases, we have $B_{ij} \equiv 0 \pmod{p}$ except for $(i,j) = (3,3)$ so that $d_{0,1} = \max_{1 \le i \le m} d_{0,i}$. By the same reason, we have $d_{0,1} = \cdots = d_{0,m}$. Then the matrix $I_{d_{0,1}} + x_i B_{33} + px_i^2 C_{33}$ is invertible for each i and thus

$$Q(t) := \begin{pmatrix} O & O \\ O & pI_{d_{1,1}} \end{pmatrix} + t \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} + pt^2 \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix}$$

satisfies condition (2). □

3.2 Necessary condition for an element of $\mathcal{C}_{X_4}$

For a given $(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,1,\infty}$, there exists a first integral $P(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$ such that $\operatorname{cok}(P(x_i)) \cong H_i$ for each i. We will use Lemma 3.5 repeatedly until we obtain $(n'; H_1', \dots, H_m') \in \mathcal{C}_{X_m,1,\infty}$ which satisfies $\operatorname{rank}_{\mathbb{F}_p}(H_i'/pH_i') = n'$ for each i. For the case $m = 4$, the elements of $(n'; H_1', \dots, H_4') \in \mathcal{C}_{X_4,1,2}$ which satisfies $\operatorname{rank}_{\mathbb{F}_p}(H_i'/pH_i') = n'$ for each i bijectively corresponds to the elements of $\mathcal{C}_{X_4,2,1}$ by Proposition 2.3 (4). The following lemma, which provides an information about the set $\mathcal{C}_{X_4,2,1}$, is a generalization of Lemma 3.3.

Lemma 3.6. *If $(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,l,1}$ and $l \le m$, then*

$$\sum_{i=1}^{m} d_{0,i} - (m-l)\alpha_0 \ge 0$$

for some non-negative integer $\alpha_0 \ge \max_{1 \le i \le m} d_{0,i}$.

Proof. We use induction on n. The case $n = 1$ follows from Example 2.4. Now assume that $n > 1$ and the lemma holds for every $n' < n$. Suppose that there exists $(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,l,1}$ such that

$$\sum_{i=1}^{m} d_{0,i} < (m-l) \max_{1 \le i \le m} d_{0,i}.$$

As in the proof of Lemma 3.3, we may assume that $d_{0,1} = \max_{1 \le i \le m} d_{0,i}$ and there exists an l-th integral

$$P(t) = \begin{pmatrix} O & O \\ O & I_{d_{0,1}} \end{pmatrix} + tA_1 + \cdots + t^l A_l \in \mathrm{M}_n(\mathbb{Z}_p)[t]$$

such that $\operatorname{cok}_{\mathbb{Z}_p/p\mathbb{Z}_p}(P(x_i)) \cong H_i/pH_i$ for each i.

Assume that $d_{0,1} < n$ and let $Q(t) \in \mathrm{M}_{n-1}(\mathbb{Z}_p)[t]$ be the l-th integral which is obtained by eliminating first column and row from $P(t)$. Then we have $d_{0,Q(x_1)} = d_{0,1}$ and $d_{0,Q(x_i)} \le d_{0,i} \le d_{0,1}$ for $2 \le i \le m$. The induction hypothesis implies that

$$\sum_{i=1}^{m} d_{0,i} - (m-l) \max_{1 \le i \le m} d_{0,i} \ge \sum_{i=1}^{m} d_{0,Q(x_i)} - (m-l) \max_{1 \le i \le m} d_{0,Q(x_i)} \ge 0,$$

which is a contradiction. Thus we have $d_{0,1} = n$. Now consider the first integral

$$P_1(t) := \begin{pmatrix} tI & & & & A_0 \\ -I & tI & & & A_1 \\ & \ddots & \ddots & & \vdots \\ & & -I & tI & A_{l-2} \\ & & & -I & A_{l-1} + tA_l \end{pmatrix} \in \mathrm{M}_{ln}(\mathbb{Z}_p)[t],$$

where $A_0 = P(0) = \left(\begin{smallmatrix} O & O \\ O & I_{d_{0,1}} \end{smallmatrix}\right)$. It satisfies $\operatorname{cok}(P_1(t)) \cong \operatorname{cok}(P(t))$ so that $d_{0,P_1(x_i)} = d_{0,i} + (l-1)n$ for every $1 \le i \le m$ and $\max_{1 \le i \le m} d_{0,P_1(x_i)} = ln$. Then we have

$$\sum_{i=1}^{m} d_{0,i} - (m-l)n = \sum_{i=1}^{m} d_{0,P_1(x_i)} - (m-1)ln \ge 0$$

by Lemma 3.3, which is a contradiction. This finishes the proof. □

Now we prove a necessary condition for an element of $\mathcal{C}_{X_m,1,2}$ using Lemma 3.5 and 3.6.

Theorem 3.7. *If $(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,1,2}$, then*

$$\sum_{i=1}^{m} d_{0,i} - (m-1)\alpha_0 \ge 0$$

and

$$\left(\sum_{i=1}^{m} d_{0,i} - (m-1)\alpha_0\right) + \left(\sum_{i=1}^{m} \min(d_{1,i}, \alpha_1) - (m-2)\alpha_1\right) \ge 0$$

for some non-negative integers α_0 and α_1 such that $\alpha_0 \ge \max_{1 \le i \le m} d_{0,i}$ and $2\alpha_0 + \alpha_1 \ge \max_{1 \le i \le m}(2d_{0,i} + d_{1,i})$.

Proof. We use induction on n. The case $n = 1$ follows from Example 2.4. Now assume that $n > 1$ and the theorem holds for every $n' < n$. Let $P(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$ be a first integral such that $\operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(P(x_i)) \cong H_i/p^2H_i$ for each i. If $d_{0,i} = 0$ for each i, then we have $(n; pH_1, \dots, pH_m) \in \mathcal{C}_{X_m,2,1}$ by Proposition 2.3 (4) and $d_{0,pH_i} = d_{1,i}$. By Lemma 3.6, there exists $\beta_0 \ge \max_{1 \le i \le m} d_{0,pH_i}$ such that $\sum_{i=1}^{m} d_{0,pH_i} - (m-2)\beta_0 \ge 0$. Now $(\alpha_0, \alpha_1) = (0, \beta_0)$ satisfies the desired properties. Otherwise, choose a first integral $Q(t) \in \mathrm{M}_{n'}(\mathbb{Z}_p)$ with $n' < n$ satisfying one of the conditions in Lemma 3.5. By the induction hypothesis, we have

$$\sum_{i=1}^{m} d_{0,Q(x_i)} - (m-1)\alpha_0' \ge 0$$

and

$$\left(\sum_{i=1}^{m} d_{0,Q(x_i)} - (m-1)\alpha_0'\right) + \left(\sum_{i=1}^{m} \min(d_{1,Q(x_i)}, \alpha_1') - (m-2)\alpha_1'\right) \ge 0$$

for some $\alpha_0', \alpha_1' \in \mathbb{Z}_{\ge 0}$ such that $\alpha_0' \ge \max_{1 \le i \le m} d_{0,Q(x_i)}$ and $2\alpha_0' + \alpha_1' \ge \max_{1 \le i \le m}(2d_{0,Q(x_i)} + d_{1,Q(x_i)})$. Now we divide the cases according to the condition of $Q(t)$.

Case 1: $Q(t)$ satisfies condition (1) of Lemma 3.5. Let $(\alpha_0, \alpha_1) = (\alpha_0' + 1, \alpha_1')$. Then we have

$$\begin{aligned} \alpha_0 &\ge \max_{1 \le i \le m} d_{0,Q(x_i)} + 1 = \max_{1 \le i \le m} d_{0,i}, \\ 2\alpha_0 + \alpha_1 &\ge \max_{1 \le i \le m}(2(d_{0,Q(x_i)} + 1) + d_{1,Q(x_i)}) \ge \max_{1 \le i \le m}(2d_{0,i} + d_{1,i}), \\ \sum_{i=1}^{m} d_{0,i} - (m-1)\alpha_0 &\ge \sum_{i=1}^{m} d_{0,Q(x_i)} - (m-1)\alpha_0' \ge 0. \end{aligned}$$

If $Q(t)$ satisfies condition (a), then we have

$$\begin{aligned} 0 &\le \left(\sum_{i=1}^{m} d_{0,Q(x_i)} - (m-1)\alpha_0' + 1\right) + \left(\sum_{i=1}^{m} \min(d_{1,Q(x_i)}, \alpha_1') - (m-2)\alpha_1' - 1\right) \\ &\le \left(\sum_{i=1}^{m} d_{0,i} - (m-1)\alpha_0\right) + \left(\sum_{i=1}^{m} \min(d_{1,i}, \alpha_1) - (m-2)\alpha_1\right). \end{aligned}$$

If $Q(t)$ satisfies condition (b) or (c), then we have

$$\begin{aligned} 0 &\le \left(\sum_{i=1}^{m} d_{0,Q(x_i)} - (m-1)\alpha_0'\right) + \left(\sum_{i=1}^{m} \min(d_{1,Q(x_i)}, \alpha_1') - (m-2)\alpha_1'\right) \\ &\le \left(\sum_{i=1}^{m} d_{0,i} - (m-1)\alpha_0\right) + \left(\sum_{i=1}^{m} \min(d_{1,i}, \alpha_1) - (m-2)\alpha_1\right). \end{aligned}$$

Case 2: $Q(t)$ satisfies condition (2) of Lemma 3.5. In this case, $\alpha_0' = 0$ and $\sum_{i=1}^m \min(d_{1,i}, \alpha_1') - (m-2)\alpha_1' \geq 0$ for some $\alpha_1' \geq \max_{1 \leq i \leq m} d_{1,i}$. Let $d_0 = d_{0,i}$ for each i and $(\alpha_0, \alpha_1) = (d_0, \alpha_1')$. Then we have

$$\begin{aligned}
\alpha_0 &\geq \max_{1 \leq i \leq m} d_{0,i}, \\
2\alpha_0 + \alpha_1 &\geq 2 \max_{1 \leq i \leq m} d_{0,i} + \max_{1 \leq i \leq m} d_{1,i} \geq \max_{1 \leq i \leq m}(2d_{0,i} + d_{1,i}), \\
\sum_{i=1}^m d_{0,i} - (m-1)\alpha_0 &= md_0 - (m-1)d_0 \geq 0, \\
d_0 &\leq \Big(\sum_{i=1}^m d_{0,i} - (m-1)\alpha_0\Big) + \Big(\sum_{i=1}^m \min(d_{1,i}, \alpha_1) - (m-2)\alpha_1\Big). \qquad \square
\end{aligned}$$

As a corollary of Theorem 3.7, we prove one direction of Theorem 1.8 for the case $m = 4$.

Corollary 3.8. *The inclusion*

$$\begin{aligned}
\mathcal{C}_{X_4} \subset \{(H_1, H_2, H_3, H_4) \in \mathcal{M}_{\mathbb{Z}_p}^4 : s_1 = s_2 = s_3 = s_4,\ 3d_{1,i} \leq D_1\ (1 \leq i \leq 4) \text{ and} \\
d_{1,i} + 2(d_{1,j} + d_{2,j}) \leq D_1 + D_2\ (1 \leq i, j \leq 4)\}
\end{aligned}$$

holds where $s_i = \operatorname{rank}_{\mathbb{F}_p}(H_i/pH_i)$ *(*$1 \leq i \leq 4$*) and* $D_r = \sum_{i=1}^4 d_{r,i}$ *for* $r = 1, 2$.

Proof. Suppose that $(H_1, H_2, H_3, H_4) \in \mathcal{C}_{X_4}$. By Proposition 2.3, we have

$$s_1 = s_2 = s_3 = s_4 \text{ and } (n; pH_1, pH_2, pH_3, pH_4) \in \mathcal{C}_{X_4,1,\infty} = \mathcal{C}_{X_4,1,2}$$

for some $n \in \mathbb{Z}_{\geq 1}$. Let $P(t) \in \mathrm{M}_n(\mathbb{Z}_p)[t]$ be a first integral which satisfies $\operatorname{cok}_{\mathbb{Z}_p/p^2\mathbb{Z}_p}(P(x_i)) \cong pH_i/p^3H_i$ so that $d_{0,P(x_i)} = d_{1,i}$ and $d_{1,P(x_i)} = d_{2,i}$ for each i. By Theorem 3.7, there exist $\alpha_0, \alpha_1 \in \mathbb{Z}_{\geq 0}$ such that

$$D_1 - 3\alpha_0 \geq 0 \text{ and } (D_1 - 3\alpha_0) + \Big(\sum_{i=1}^4 \min(d_{2,i}, \alpha_1) - 2\alpha_1\Big) \geq 0$$

with $\alpha_0 \geq \max_{1 \leq i \leq 4} d_{1,i}$ and $2\alpha_0 + \alpha_1 \geq \max_{1 \leq i \leq 4}(2d_{1,i} + d_{2,i})$.

- For every $1 \leq i \leq 4$, we have $3d_{1,i} \leq 3\alpha_0 \leq D_1$.
- For every $1 \leq i, j \leq 4$, we have

$$\begin{aligned}
D_1 + D_2 - d_{2,j} &\geq (D_1 - 3\alpha_0) + \Big(\sum_{i_0=1}^4 \min(d_{2,i_0}, \alpha_1) - 2\alpha_1\Big) + (3\alpha_0 + \alpha_1) \\
&\geq \alpha_0 + (2\alpha_0 + \alpha_1) \geq d_{1,i} + (2d_{1,j} + d_{2,j})
\end{aligned}$$

so we conclude that $d_{1,i} + 2(d_{1,j} + d_{2,j}) \leq D_1 + D_2$. □

3.3 Zone theory

In this subsection, we prove the sufficient condition of Theorem 1.8 for $m = 4$. We will find a generating set of $\mathcal{C}_{X_4}$ and will prove that each element in a generating set satisfies the desired condition. To do this, we introduce a way to visualize an element of $\mathcal{B}_m$.

Definition 3.9. For given $k \in \mathbb{Z}_{\geq 0}$, a *k-presentation* of $(n; H_1, \ldots, H_m) \in \mathcal{B}_m$ (denoted by $\mathrm{Prs}_k(n; H_1, \ldots, H_m)$) is an $m \times n$ matrix with entries in $\{0, 1, \ldots, k-1, k^+\}$ whose i-th row contains $d_{r,i}$ numbers of r $(0 \leq r \leq k-1)$ and $\sum_{r \in \overline{\mathbb{Z}}_{\geq k}} d_{r,i}$ numbers of k^+. (It is unique up to ordering of the numbers in each row.) Each entry in a presentation of a block is called a *type*.

Remark 3.10. For given $l \in \overline{\mathbb{Z}}_{\geq 0}$ and $k \in \mathbb{Z}_{\geq 0}$, assume that $\mathrm{Prs}_k(n; H_1, \ldots, H_m) = \mathrm{Prs}_k(n; H_1', \ldots, H_m')$. Then we have $H_i/p^kH_i \cong H_i'/p^kH_i'$ for each i so $(n; H_1, \ldots, H_m) \in \mathcal{C}_{X_m,l,k}$ if and only if $(n; H_1', \ldots, H_m') \in \mathcal{C}_{X_m,l,k}$. Hence it is enough to consider a k-presentation of $(n; H_1, \ldots, H_m)$ to determine whether it is an element of $\mathcal{C}_{X_m,l,k}$ or not.

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \\ 1 & 0 & 0 & 1 & 1 & 1 & 3^+ & 3^+ & 0 \\ 0 & 0 & 3^+ & 3^+ & 0 & 0 & 0 & 3^+ & 3^+ \end{bmatrix}$$

Figure 1: A 3-presentation of $(9; (\mathbb{Z}_p/p\mathbb{Z}_p)^3 \times (\mathbb{Z}_p/p^2\mathbb{Z}_p)^4, (\mathbb{Z}_p/p\mathbb{Z}_p)^4 \times (\mathbb{Z}_p/p^3\mathbb{Z}_p)^2, \mathbb{Z}_p^4) \in \mathcal{B}_4$.

A k-presentation of a sum of two elements in $\mathcal{B}_m$ is given by the concatenation of a k-presentation of each element. By Proposition 2.3 (1), the set of k-presentations of elements in $\mathcal{C}_{X_m,l,k}$ is closed under concatenation.

Example 3.11. The equation $(3; (\mathbb{Z}_p/p\mathbb{Z}_p)^2, 1) + (2; 1, \mathbb{Z}_p/p\mathbb{Z}_p) = (5; (\mathbb{Z}_p/p\mathbb{Z}_p)^2, \mathbb{Z}_p/p\mathbb{Z}_p)$ is presented as

$$\begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Consider an action of a permutation group S_m on $\mathcal{B}_m$ by $\sigma \cdot (n; H_1, \dots, H_m) := (n; H_{\sigma(1)}, \dots, H_{\sigma(m)})$. Then $\mathrm{Prs}_k(\sigma \cdot (n; H_1, \dots, H_m))$ is obtained by permuting the rows of $\mathrm{Prs}_k(n; H_1, \dots, H_m)$ according to σ. For a subset $\mathcal{A} \subset \mathcal{B}_m$, denote $S_m \cdot \mathcal{A} := \{\sigma \cdot (n; H_1, \dots, H_m) : \sigma \in S_m, (n; H_1, \dots, H_m) \in \mathcal{A}\} \subset \mathcal{B}_m$.

Now we are ready to find a generating set of $\mathcal{C}_{X_m,1,1}$. Note that, by the proof of Lemma 3.3, for any element $(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,1,1}$, either one of the following holds:

(1) There exists a 1-presentation $\mathcal{P}$ of an element of $\mathcal{C}_{X_m,1,1}$ such that one of the following holds:
 (a) $\mathcal{P} + \sigma \cdot \begin{pmatrix} 1^+ & 0 & \cdots & 0 \end{pmatrix}^T = \mathrm{Prs}_1(n; H_1, \dots, H_m)$ for some $\sigma \in S_m$.
 (b) $\mathcal{P} + \begin{pmatrix} 0 & \cdots & 0 \end{pmatrix}^T = \mathrm{Prs}_1(n; H_1, \dots, H_m)$,

(2) There is no type 0 on $\mathrm{Prs}_1(n; H_1, \dots, H_m)$.

We can repeat the above procedure until we find a 1-presentation $\mathcal{P}_H$ of an element of $\mathcal{C}_{X_m,1,1}$ which has no type 0 and there exist $r_1, \dots, r_t \in \overline{\mathbb{Z}}_{\geq 0}$ and $\sigma_1, \dots, \sigma_t \in S_m$ such that

$$\mathcal{P}_H + \sum_{i=1}^{t} \sigma_i \cdot (1; \mathbb{Z}_p/p^{r_i}\mathbb{Z}_p, 1, \dots, 1) = \mathrm{Prs}_1(n; H_1, \dots, H_m).$$

Since $\mathcal{P}_H$ has no type 0, it is also a 1-presentation of an element of $\varphi_{1,0}^{-1}(\mathcal{C}_{X_m,2,0}) = \varphi_{1,0}^{-1}(\mathcal{B}_m)$ by Proposition 2.3 (4). Conversely, by Example 2.4, $\sigma \cdot (1; \mathbb{Z}_p/p^r\mathbb{Z}_p, 1, \dots, 1) \in \mathcal{C}_{X_m,1,1}$ for every $r \in \overline{\mathbb{Z}}_{\geq 0}$ and $\sigma \in S_m$. Hence we proved that $\mathcal{C}_{X_m,1,1} = \langle \mathcal{A}_{0,1} \cup \mathcal{A}_{1,m} \rangle$, where

$$\mathcal{A}_{r,d} := S_m \cdot \{(1; \mathbb{Z}_p/p^{r_1}\mathbb{Z}_p, \dots, \mathbb{Z}_p/p^{r_d}\mathbb{Z}_p, \mathbb{Z}_p/p^r\mathbb{Z}_p, \dots, \mathbb{Z}_p/p^r\mathbb{Z}_p) \in \mathcal{B}_m : r_1, \dots, r_d \in \overline{\mathbb{Z}}_{\geq r}\}$$

for $r \in \overline{\mathbb{Z}}_{\geq 0}$ and $0 \leq d \leq m$. We can generalize this to the set $\mathcal{C}_{X_m,l,1}$ for every $1 \leq l \leq m$.

Theorem 3.12. *For every* $1 \leq l \leq m$, $\mathcal{C}_{X_m,l,1} = \langle \mathcal{A}_{0,l} \cup \mathcal{A}_{1,m} \rangle$ *and* $(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,l,1}$ *if and only if*

$$\sum_{i=1}^{m} d_{0,i} - (m - l)a_0 \geq 0 \tag{3.1}$$

for some (non-negative) integer $a_0 \geq \max_{1 \leq i \leq m} d_{0,i}$.

Proof. Consider the sets $S_1 := \langle \mathcal{A}_{0,l} \cup \mathcal{A}_{1,m} \rangle$ and

$$S_2 := \Big\{(n; H_1, \dots, H_m) \in \mathcal{B}_m : \text{inequality (3.1) holds for some integer } a_0 \geq \max_{1 \leq i \leq m} d_{0,i}\Big\}.$$

By Example 2.4, we have $\mathcal{A}_{0,l}, \mathcal{A}_{1,m} \subset \mathcal{C}_{X_m,l,1}$ so $S_1 \subset \mathcal{C}_{X_m,l,1}$. Lemma 3.6 implies $\mathcal{C}_{X_m,l,1} \subset S_2$. Now it is enough to show that $S_2 \subset S_1$. For any element $(n; H_1, \dots, H_m) \in S_2$, there exists a non-negative integer $a_0 \geq \max_{1 \leq i \leq m} d_{0,i}$ which satisfies inequality (3.1). If $d_{0,i} = 0$ for each i, then each H_i is of the form $\prod_{k=1}^{n} \mathbb{Z}_p/p^{r_k}\mathbb{Z}_p$ $(r_1, \dots, r_n \in \overline{\mathbb{Z}}_{\geq 1})$ so $(n; H_1, \dots, H_m) \in \langle \mathcal{A}_{1,m} \rangle$. Now assume that $d_{0,i} \geq 1$ for some i, so that $a_0 \geq 1$. Also we may assume that $a_0 = \max_{1 \leq i \leq m} d_{0,i} \leq n$.

For an integer a, let $[a]_{a_0}$ be an integer such that $a \equiv [a]_{a_0} \pmod{a_0}$ and $1 \leq [a]_{a_0} \leq a_0$. Choose a 1-presentation $\mathrm{Prs}_1(n; H_1, \dots, H_m)$ whose r-th row has type 0 at columns $[a_r]_{a_0}$ for $\sum_{i=1}^{r-1} d_{0,i} + 1 \leq a_r \leq \sum_{i=1}^{r} d_{0,i}$ for every $1 \leq r \leq m$. (See Figure 2.) By the inequality (3.1), each of the first a_0 columns has at least $m - l$ type 0's so it

$$\left[\underbrace{\begin{matrix}0&0&0&1^+\\0&0&1^+&0\\1^+&1^+&0&0\\0&0&0&0\end{matrix}}_{\text{Zero}}\quad\underbrace{\begin{matrix}1^+&1^+&1^+&1^+\\1^+&1^+&1^+&1^+\\1^+&1^+&1^+&1^+\\1^+&1^+&1^+&1^+\end{matrix}}_{\text{One+}}\right]$$

Figure 2: A choice of a 1-presentation of $(8; (\mathbb{Z}_p/p\mathbb{Z}_p)^5, (\mathbb{Z}_p/p\mathbb{Z}_p)^2 \times (\mathbb{Z}_p/p^2\mathbb{Z}_p)^3, (\mathbb{Z}_p/p\mathbb{Z}_p)^2 \times (\mathbb{Z}_p/p^3\mathbb{Z}_p)^4, \mathbb{Z}_p^4) \in \mathcal{B}_4$.

is a 1-presentation of an element of $\mathcal{A}_{0,l}$. The remaining columns have no type 0 so they are 1-presentations of elements of $\mathcal{A}_{1,m}$. Thus $\mathrm{Prs}_1(n; H_1, \dots, H_m) = \mathrm{Prs}_1(n; H'_1, \dots, H'_m)$ for some $(n; H'_1, \dots, H'_m) \in S_1$ such that $H_i/pH_i \cong H'_i/pH'_i$ for each i. By the definition of the sets $\mathcal{A}_{0,l}$ and $\mathcal{A}_{1,m}$, if we replace a term $\mathbb{Z}_p/p^r\mathbb{Z}_p$ ($r \in \overline{\mathbb{Z}}_{\geq 1}$) in H'_i with $\mathbb{Z}_p/p^{r'}\mathbb{Z}_p$ for any $r' \in \overline{\mathbb{Z}}_{\geq 1}$, then it is still an element of S_1. By iterating this process, we conclude that $(n; H_1, \dots, H_m) \in S_1$. □

Similarly, one can find a generating set of $\mathcal{C}_{X_m,1,2}$ as follows.

Lemma 3.13. *We have* $\mathcal{D}_m = \mathcal{D}_{m,1} \cup \mathcal{D}_{m,2} \subset \mathcal{C}_{X_m,1,2}$ *for*

$$\mathcal{D}_{m,1} := S_m \cdot \{(d+1; \mathbb{Z}_p/p^{r_1}\mathbb{Z}_p, \dots, \mathbb{Z}_p/p^{r_{d+2}}\mathbb{Z}_p, \mathbb{Z}_p/p\mathbb{Z}_p, \dots, \mathbb{Z}_p/p\mathbb{Z}_p) \in \mathcal{B}_m : 0 \leq d \leq m-2 \text{ and } r_1, \dots, r_{d+2} \in \overline{\mathbb{Z}}_{\geq 2}\}$$

and

$$\mathcal{D}_{m,2} := S_m \cdot \{(d+1; (\mathbb{Z}_p/p\mathbb{Z}_p)^2, \dots, (\mathbb{Z}_p/p\mathbb{Z}_p)^2, \mathbb{Z}_p/p^{r_1}\mathbb{Z}_p, \dots, \mathbb{Z}_p/p^{r_{m-d}}\mathbb{Z}_p) \in \mathcal{B}_m : 0 \leq d \leq m \text{ and } r_1, \dots, r_{m-d} \in \overline{\mathbb{Z}}_{\geq 2}\}.$$

Proof. For $0 \leq d \leq m-2$ and $f_1(t) = \sum_{k=0}^{d+2} a_k t^k := \prod_{j=1}^{d+2}(t - x_j)$, the first integral

$$P_1(t) := \begin{pmatrix} 1 & & & & pa_{d+1}t + pa_{d+2}t^2 \\ -t & 1 & & & pa_r t \\ & \ddots & \ddots & & \vdots \\ & & -t & 1 & pa_2 t \\ & & & -t & pa_0 + pa_1 t \end{pmatrix} \in \mathrm{M}_{d+1}(\mathbb{Z}_p)[t]$$

satisfies $\mathrm{cok}(P_1(t)) \cong \mathrm{cok}(pf_1(t))$ so we have $\mathcal{D}_{m,1} \subset \mathcal{C}_{X_m,1,2}$. For $0 \leq d \leq m$, the first integral

$$P_2(t) := \begin{pmatrix} t - x_1 & & & p \\ & \ddots & & \vdots \\ & & t - x_d & p \\ p & \cdots & p & \end{pmatrix} \in \mathrm{M}_{d+1}(\mathbb{Z}_p)[t]$$

satisfies $\mathrm{cok}(P_2(x_i)) \cong (\mathbb{Z}_p/p\mathbb{Z}_p)^2$ for $1 \leq i \leq d$ and $\mathrm{cok}(P_2(x_i)) \cong \mathbb{Z}_p/p^{r_i}\mathbb{Z}_p$ ($r_i \in \overline{\mathbb{Z}}_{\geq 2}$) for $d+1 \leq i \leq m$ so we have $\mathcal{D}_{m,2} \subset \mathcal{C}_{X_m,1,2}$. □

Theorem 3.14. *We have* $\mathcal{C}_{X_m,1,2} = \langle \mathcal{A}_{0,1} \cup \mathcal{A}_{1,2} \cup \mathcal{A}_{2,m} \cup \mathcal{D}_m \rangle$. *Moreover,* $(n; H_1, \dots, H_m) \in \mathcal{C}_{X_m,1,2}$ *if and only if*

$$\sum_{i=1}^{m} d_{0,i} - (m-1)\alpha_0 \geq 0, \tag{3.2}$$

$$\left(\sum_{i=1}^{m} d_{0,i} - (m-1)\alpha_0\right) + \left(\sum_{i=1}^{m} \min(d_{1,i}, \alpha_1) - (m-2)\alpha_1\right) \geq 0 \tag{3.3}$$

for some non-negative integers α_0 *and* α_1 *such that* $\alpha_0 \geq \max_{1 \leq i \leq m} d_{0,i}$ *and* $2\alpha_0 + \alpha_1 \geq \max_{1 \leq i \leq m}(2d_{0,i} + d_{1,i})$.

Proof. Consider the sets $S_1 := \langle \mathcal{A}_{0,1} \cup \mathcal{A}_{1,2} \cup \mathcal{A}_{2,m} \cup \mathcal{D}_m \rangle$ and

$$S_2 := \Big\{(n; H_1, \dots, H_m) \in \mathcal{B}_m : \text{inequalities (3.2) and (3.3) hold for some } \alpha_0, \alpha_1 \in \mathbb{Z}_{\geq 0} \text{ such that } \alpha_0 \geq \max_{1 \leq i \leq m} d_{0,i} \text{ and } 2\alpha_0 + \alpha_1 \geq \max_{1 \leq i \leq m}(2d_{0,i} + d_{1,i})\Big\}.$$

$$\left[\underbrace{\begin{matrix}0&0&0&0\\0&0&*&*\\0&*&0&0\\0&0&0&0\end{matrix}}_{\text{Zero}}\;\underbrace{\begin{matrix}*&*\\1&1\\1&*\\*&*\end{matrix}}_{\text{One}}\right] \to \left[\underbrace{\begin{matrix}0&0&0&0\\0&0&1&1\\0&*&0&0\\0&0&0&0\end{matrix}}_{\text{Zero}}\;\underbrace{\begin{matrix}*&*\\1&1\\1&*\\*&*\end{matrix}}_{\text{One}}\right]$$

$$\to \left[\underbrace{\begin{matrix}0&0&0&0\\0&0&1&1\\0&2^+&0&0\\0&0&0&0\end{matrix}}_{\text{Zero}}\;\underbrace{\begin{matrix}2^+&2^+\\1&1\\1&2^+\\2^+&2^+\end{matrix}}_{\text{One}}\;\underbrace{\begin{matrix}2^+&2^+\\1&1\\2^+&2^+\\2^+&2^+\end{matrix}}_{\text{Two+}}\right] = \begin{bmatrix}0&2^+\\0&1\\0&2^+\\0&2^+\end{bmatrix} + 2\begin{bmatrix}0&2^+\\1&1\\0&2^+\\0&2^+\end{bmatrix} + \begin{bmatrix}0\\0\\2^+\\0\end{bmatrix} + \begin{bmatrix}2^+\\1\\1\\2^+\end{bmatrix}$$

Figure 3: A process for $(8; (\mathbb{Z}_p/p^2\mathbb{Z}_p)^2 \times (\mathbb{Z}_p/p^3\mathbb{Z}_p)^2, (\mathbb{Z}_p/p\mathbb{Z}_p)^6, \mathbb{Z}_p/p\mathbb{Z}_p \times \mathbb{Z}_p/p^3\mathbb{Z}_p \times (\mathbb{Z}_p/p^5\mathbb{Z}_p)^3, \mathbb{Z}_p^4) \in \mathcal{B}_4$ $(a_0 = 4, a_1 = 2)$.

By Example 2.4 and Lemma 3.13, we have

$$\mathcal{A}_{0,1}, \mathcal{A}_{1,2}, \mathcal{A}_{2,m}, \quad \mathcal{D}_m \subset \mathcal{C}_{X_m,1,2}$$

so $S_1 \subset \mathcal{C}_{X_m,1,2}$. (Recall that $\mathcal{C}_{X_m,1,\infty} \subset \mathcal{C}_{X_m,1,2}$ by Proposition 2.3 (a).) Theorem 3.7 implies $\mathcal{C}_{X_m,1,2} \subset S_2$. It is enough to show that $S_2 \subset S_1$. For any element $(n; H_1, \dots, H_m) \in S_2$, there exist $a_0, a_1 \in \mathbb{Z}_{\geq 0}$ such that $a_0 \geq \max_{1 \leq i \leq m} d_{0,i}$, $2a_0 + a_1 \geq \max_{1 \leq i \leq m}(2d_{0,i} + d_{1,i})$ and inequalities (3.2) and (3.3) hold.

Allocate a_0 columns to *Zero Zone* and a_1 columns to *One Zone*. Arrange type 0's on Zero Zone and type 1's on One Zone as in the proof of Theorem 3.12. Then all type 0's are placed because $a_0 \geq d_{0,i}$ for each i, while type 1's may not. Fill the remaining type 1's to Zero Zone. If there are still remaining type 1's, then allocate new columns for remaining type 1's to *Two+ Zone* and then fill type 2^+'s on empty entries. Finally, allocate new columns to *Two+ Zone* for remaining type 2^+'s if necessary. Then we have the followings:

(a) Each column on Zero Zone contains at least $m - 1$ type 0's.

(b) There are exactly $\sum_{i=1}^m d_{0,i} - (m-1)a_0$ numbers of $\begin{pmatrix}0 & \cdots & 0\end{pmatrix}^T$ columns.

(c) By replacing at most $\sum_{i=1}^m d_{0,i} - (m-1)a_0$ entries, we can make each column on One Zone contains at least $m - 2$ type 1's.

(d) Type 1 appears more or equal on Zero Zone than on Two+ Zone for each row.

Properties (a) and (b) are easy to prove, and (c) follows from inequality (3.3). For each i, the inequality $2a_0 + a_1 \geq 2d_{0,i} + d_{1,i}$ is equivalent to $a_0 - d_{0,i} \geq (d_{1,i} - a_1) - (a_0 - d_{0,i})$, which implies (d).

If there are some empty entries, then swap them to the rightmost non-empty entry on each row and delete all empty columns. Then we obtain a 2-presentation of $(n; H_1, \dots, H_m)$, which still satisfies properties (a), (b), (c), and (d). Figure 3 illustrates the process to place the types.

For each column on One Zone which has $m - 2 - d$ type 1 for $d > 0$, concatenate $d\begin{pmatrix}0 & \cdots & 0\end{pmatrix}^T$; this is possible due to (b) and (c). For each column on Two+ Zone which has type 1 on rows $i_1, \dots, i_d$, concatenate $e_{i_1}, \dots, e_{i_d}$ (e_i is a column on Zero Zone whose i-th row is 1); this is possible due to (d). These are elements of $\mathcal{D}_m$ and the other columns are elements of $\mathcal{A}_{0,1} \cup \mathcal{A}_{1,2} \cup \mathcal{A}_{2,m}$, so we have $(n; H_1, \dots, H_m) \in S_1$. □

Now we can complete the proof of Theorem 1.8 for $m = 4$.

Proof of Theorem 1.8 for $m = 4$. Suppose that $(H_1, H_2, H_3, H_4) \in \mathcal{M}_{\mathbb{Z}_p}^4$ satisfies the conditions

$$s := s_1 = \cdots = s_4, \qquad 3d_{1,i} \leq D_1 \quad \text{and} \quad d_{1,i} + 2(d_{1,j} + d_{2,j}) \leq D_1 + D_2 \quad \text{for every } 1 \leq i,j \leq 4.$$

We claim that $(s; H_1, H_2, H_3, H_4) \in \mathcal{C}_{X_4,0,3}$ so that $(H_1, H_2, H_3, H_4) \in \mathcal{C}_{X_4}$. By Proposition 2.3 (4), it suffices to prove that $(s; pH_1, pH_2, pH_3, pH_4) \in \mathcal{C}_{X_4,1,2}$. Set $a_0 = \max_{1 \leq i \leq 4} d_{1,i}$ and $a_1 = \max_{1 \leq i \leq 4}(2d_{1,i} + d_{2,i}) - 2\max_{1 \leq i \leq 4} d_{1,i}$. Then $D_1 - 3a_0 = D_1 - 3\max_{1 \leq i \leq 4} d_{1,i} \geq 0$ by the assumption. To apply Theorem 3.14, we need to prove

$$(D_1 - 3a_0) + \left(\sum_{i=1}^{4} \min(d_{2,i}, a_1) - 2a_1 \right) \geq 0.$$

The case $F(a_1) := \sum_{i=1}^4 \min(d_{2,i}, a_1) - 2a_1 \geq 0$ is clear, so we may assume that $F(a_1) < 0$ and $d_{2,i} \geq a_1$ for at most one i. For i_0 such that $2d_{1,i_0} + d_{2,i_0} = \max_{1 \leq i \leq 4}(2d_{1,i} + d_{2,i})$, we have $a_1 = 2d_{1,i_0} + d_{2,i_0} - 2\max_{1 \leq i \leq 4} d_{1,i} \leq d_{2,i_0}$ so

$d_{2,i_0} = \max_{1 \le i \le 4} d_{2,i}$. Now we have $F(\alpha_1) = D_2 - d_{2,i_0} - \alpha_1$ so

$$(D_1 - 3\alpha_0) + F(\alpha_1) = (D_1 - 3\alpha_0) + (D_2 - \alpha_1 - d_{2,i_0}) = D_1 + D_2 - \max_{1 \le i \le 4} d_{1,i} - 2d_{1,i_0} - 2d_{2,i_0} \ge 0$$

by the assumption. We conclude that $(s; pH_1, pH_2, pH_3, pH_4) \in \mathcal{C}_{X_4,1,2}$ by Theorem 3.14. □

4 Joint distribution of multiple cokernels

4.1 Convergence of the joint distribution

In this subsection, we study the limit

$$\lim_{n \to \infty} \mathbb{P}(\operatorname{cok}(A_n + y_i I_n) \cong H_i \text{ for } 1 \le i \le m),$$

where $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ is a Haar random matrix for each $n \ge 1$, $y_1, \dots, y_m \in \mathbb{Z}_p$ are distinct and $H_1, \dots, H_m \in \mathcal{G}_p$. Although we do not know the value of the above limit, we can prove the convergence of the limit. The proof is based on the probabilistic argument in [5, Section 2.2].

Theorem 4.1. *Let $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ be a Haar random matrix for each $n \ge 1$, let $y_1, \dots, y_m$ be distinct elements of $\mathbb{Z}_p$ and $H_1, \dots, H_m \in \mathcal{G}_p$. Then the limit*

$$\lim_{n \to \infty} \mathbb{P}(\operatorname{cok}(A_n + y_i I_n) \cong H_i \textit{ for } 1 \le i \le m)$$

converges.

The following lemma will be frequently used in the proof of Theorem 4.1.

Lemma 4.2 ([5, Lemma 2.3]). *For any integers $n \ge r > 0$ and a Haar random $C \in \mathrm{M}_{n \times r}(\mathbb{Z}_p)$, we have*

$$\mathbb{P}\left(\textit{there exists } Y \in \mathrm{GL}_n(\mathbb{Z}_p) \textit{ such that } YC = \begin{pmatrix} I_r \\ O \end{pmatrix}\right) = c_{n,r} := \prod_{j=0}^{r-1}\left(1 - \frac{1}{p^{n-j}}\right).$$

Proof of Theorem 4.1. For any $n \in \mathbb{Z}_{\ge 1}$ and $k \in \mathbb{Z}_{\ge 0}$, denote

$$P_{n,k} := \mathbb{P}(\operatorname{cok}(M_{A,[B_1,\dots,B_k]}(y_i)) \cong H_i \text{ for } 1 \le i \le m),$$

where $A \in \mathrm{M}_n(\mathbb{Z}_p)$, $B_1, \dots, B_k \in \mathrm{M}_{n \times 1}(\mathbb{Z}_p)$ are random and independent matrices and

$$M_{A,[B_1,\dots,B_k]}(y) := A + y\begin{pmatrix} 0 & \\ & I_{n-1} \end{pmatrix} + \sum_{j=1}^{k} y^j \begin{pmatrix} B_j & O_{n \times (n-1)} \end{pmatrix} + y^{k+1}\begin{pmatrix} 1 & \\ & O_{n-1} \end{pmatrix} \in \mathrm{M}_n(\mathbb{Z}_p).$$

To prove the convergence of the limit

$$\lim_{n \to \infty} P_{n,0} = \lim_{n \to \infty} \mathbb{P}(\operatorname{cok}(A_n + y_i I_n) \cong H_i \text{ for } 1 \le i \le m),$$

we will show that $P_{n,k}$ and $P_{n-1,k+1}$ are very close. For $n > 1$, $A = \left(\begin{smallmatrix} A_1 & A_2 \\ A_3 & A_4 \end{smallmatrix}\right) \in \mathrm{M}_{1+(n-1)}(\mathbb{Z}_p)$, $B_1, \dots, B_k \in \mathrm{M}_{n \times 1}(\mathbb{Z}_p)$ and

$$U = \begin{pmatrix} 1 & O \\ O & U_1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{Z}_p) \ \ (U_1 \in \mathrm{GL}_{n-1}(\mathbb{Z}_p)),$$

we have

$$UM_{A,[B_1,\dots,B_k]}(y)U^{-1} = M_{A',[B_1',\dots,B_k']}(y)$$

for

$$A' = \begin{pmatrix} A_1 & A_2U_1^{-1} \\ U_1A_3 & U_1A_4U_1^{-1} \end{pmatrix}, \ B_j' = UB_j$$

by a direct computation. For a random A_2, the probability that there exists $U_1 \in \mathrm{GL}_{n-1}(\mathbb{Z}_p)$ such that

$$A_2 U_1^{-1} = \begin{pmatrix} -1 & O_{(n-2)\times 1} \end{pmatrix}$$

is $c_{n-2,1}$ by Lemma 4.2. Moreover, for any given A_2 and U_1, the matrices U_1A_3, $U_1A_4U_1^{-1}$ and UB_j $(1 \le j \le k)$ are random and independent if and only if A_3, A_4 and B_j $(1 \le j \le k)$ are random and independent. These imply that

$$|P_{n,k} - \widetilde{P}_{n,k}| \le 1 - c_{n-2,1} \tag{4.1}$$

for

$$\widetilde{\mathrm{M}}_n(\mathbb{Z}_p) := \{\begin{pmatrix} A_1 & -1 & O \\ A_2 & A_3 & A_4 \\ A_5 & A_6 & A_7 \end{pmatrix} \in \mathrm{M}_{1+1+(n-2)}(\mathbb{Z}_p)\} \subset \mathrm{M}_n(\mathbb{Z}_p)$$

and

$$\widetilde{P}_{n,k} := \mathbb{P}(\mathrm{cok}(M_{A,[B_1,\dots,B_k]}(y_i)) \cong H_i \text{ for } 1 \le i \le m),$$

where $A \in \widetilde{\mathrm{M}}_n(\mathbb{Z}_p)$, $B_1, \dots, B_k \in \mathrm{M}_{n\times 1}(\mathbb{Z}_p)$ are random and independent. Let

$$A = \begin{pmatrix} A_1 & -1 & O \\ A_2 & A_3 & A_4 \\ A_5 & A_6 & A_7 \end{pmatrix} \in \widetilde{\mathrm{M}}_n(\mathbb{Z}_p), \qquad B_j = \begin{pmatrix} c_j \\ d_j \\ e_j \end{pmatrix} \in \mathrm{M}_{(1+1+(n-2))\times 1}(\mathbb{Z}_p) \quad (1 \le j \le k).$$

By elementary operations, we have

$$\begin{aligned} M_{A,[B_1,\dots,B_k]}(y) &= \left(\begin{array}{c|c|c} A_1 + \sum_{j=1}^{k} y^j c_j + y^{k+1} & -1 & O \\ \hline A_2 + \sum_{j=1}^{k} y^j d_j & A_3 + y & A_4 \\ \hline A_5 + \sum_{j=1}^{k} y^j e_j & A_6 & A_7 + yI_{n-2} \end{array}\right) \\ &\Rightarrow \left(\begin{array}{c|c|c} 0 & -1 & O \\ \hline (A_2 + \sum_{j=1}^{k} y^j d_j) + (A_3 + y)(A_1 + \sum_{j=1}^{k} y^j c_j + y^{k+1}) & A_3 + y & A_4 \\ \hline (A_5 + \sum_{j=1}^{k} y^j e_j) + A_6(A_1 + \sum_{j=1}^{k} y^j c_j + y^{k+1}) & A_6 & A_7 + yI_{n-2} \end{array}\right) \\ &\Rightarrow \left(\begin{array}{c|c} A_2 + A_3A_1 & A_4 \\ \hline A_5 + A_6A_1 & A_7 \end{array}\right) + y\begin{pmatrix} 0 & \\ & I_{n-2} \end{pmatrix} + \sum_{j=1}^{k} y^j \left(\begin{array}{c|c} d_j + A_3c_j + c_{j-1} & O \\ \hline e_j + A_6c_j & O \end{array}\right) \\ &\qquad + y^{k+1}\left(\begin{array}{c|c} A_3 + c_k & O \\ \hline A_6 & O \end{array}\right) + y^{k+2}\begin{pmatrix} 1 & \\ & O_{n-2} \end{pmatrix} \quad (c_0 := A_1) \\ &=: M_{A',[B'_1,\dots,B'_{k+1}]}(y). \end{aligned}$$

Since the elementary operations do not change the cokernel, we have

$$\mathrm{cok}(M_{A,[B_1,\dots,B_k]}(y_i)) \cong \mathrm{cok}(M_{A',[B'_1,\dots,B'_{k+1}]}(y_i))$$

for each i. The matrices $B'_1, \dots, B'_k$ are given by

$$B'_j = \begin{pmatrix} d_j \\ e_j \end{pmatrix} + N_j \quad (1 \le j \le k),$$

where $N_1, \dots, N_k \in \mathrm{M}_{(n-1)\times 1}(\mathbb{Z}_p)$ depending only on A_1, A_3, A_6 and c_j $(1 \le j \le k)$. Similarly,

$$A' = \begin{pmatrix} A_2 & A_4 \\ A_5 & A_7 \end{pmatrix} + N$$

for some $N \in \mathrm{M}_{n-1}(\mathbb{Z}_p)$ depending only on A_1, A_3 and A_6 and

$$B'_{k+1} = \begin{pmatrix} A_3 + c_k & O \\ A_6 & O \end{pmatrix}.$$

Therefore $A', B'_1, \dots, B'_{k+1}$ are random and independent if d_j, e_j $(1 \le j \le k)$, A_l $(2 \le l \le 7)$ are random and independent, or $A, B_1, \dots, B_k$ are random and independent. This implies that

$$\widetilde{P}_{n,k} = P_{n-1,k+1}. \tag{4.2}$$

Choose $M > 0$ such that $p^M H_i = 0$ for every i. By equations (4.1) and (4.2), we have

$$|P_{n,0} - P_{n-d,d}| \le \sum_{i=1}^{d} |P_{n-i+1,i-1} - P_{n-i,i}| \le \sum_{i=1}^{d} (1 - c_{n-i-1,1}) < \frac{2}{p^{n-d-1}} \tag{4.3}$$

for $d \ge M$ and $n > d$. For every $n > M + 1$, we have $P_{n-M,M} = P_{n-M,M+1}$ and

$$|P_{n,0} - P_{n+1,0}| \le |P_{n,0} - P_{n-M,M}| + |P_{n+1,0} - P_{n-M,M+1}| < \frac{4}{p^{n-M-1}}$$

by equation (4.3). This finishes the proof. □

4.2 Mixed moments

Now we compute the mixed moments of the cokernels $\operatorname{cok}(A_n + px_iI_n)$ $(1 \le i \le m)$ where each random matrix $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ $(n \ge 1)$ is given as in Theorem 1.5. Nguyen and Van Peski [8] and the second author [7] independently defined mixed moments of multiple random groups and extended the universality results of Wood [13, Theorem 1.3] to the joint distribution of various multiple cokernels. The *mixed moments* of (not necessarily independent) random finite groups $Y_1, \dots, Y_r$ are defined to be the expected values

$$\mathbb{E}\biggl(\prod_{k=1}^{r} \# \operatorname{Sur}(Y_k, G_k)\biggr)$$

for finite groups $G_1, \dots, G_r$.

For a partition $\lambda = (\lambda_1 \ge \cdots \ge \lambda_r)$, let λ' be the conjugate of λ, let $G_\lambda := \prod_{i=1}^{r} \mathbb{Z}/p^{\lambda_i}\mathbb{Z}$ be the finite abelian p-group of type λ and denote

$$m(G_\lambda) := p^{\sum_i \frac{(\lambda'_i)^2}{2}}.$$

The following theorem is a special case of [7, Theorem 1.3] (taking $P = \{p\}$), which extends [14, Theorem 2.5] to the multiple random groups. We note that Nguyen and Van Peski [8, Theorem 9.1] independently obtained a similar result.

Theorem 4.3 ([7, Theorem 1.3]). *Let $Y = (Y^{(1)}, \dots, Y^{(r)})$ and $Y_n = (Y_n^{(1)}, \dots, Y_n^{(r)})$ $(n \ge 1)$ be random r-tuples of elements in $\mathcal{G}_p$. Suppose that for every $G^{(1)}, \dots, G^{(r)} \in \mathcal{G}_p$, we have*

$$\lim_{n\to\infty} \mathbb{E}\biggl(\prod_{k=1}^{r} \# \operatorname{Sur}(Y_n^{(k)}, G^{(k)})\biggr) = \mathbb{E}\biggl(\prod_{k=1}^{r} \# \operatorname{Sur}(Y^{(k)}, G^{(k)})\biggr) = O\biggl(\prod_{k=1}^{r} m(G^{(k)})\biggr).$$

Then for every $H^{(1)}, \dots, H^{(r)} \in \mathcal{G}_p$, we have

$$\lim_{n\to\infty} \mathbb{P}(Y_n^{(k)} \cong H^{(k)} \text{ for } 1 \le k \le r) = \mathbb{P}(Y^{(k)} \cong H^{(k)} \text{ for } 1 \le k \le r).$$

Example 4.4 ([14, Section 2.2]). Let Y_{odd} and Y_{even} be random elements of $\mathcal{G}_p$ given as in [14, (2.7)]. (We consider them as random finite abelian p-groups which are always elementary abelian p-groups.) Let $Y_1^{(1)}, \dots, Y_1^{(r)}$ (resp. $Y_2^{(1)}, \dots, Y_2^{(r)}$) be i.i.d. random variables in $\mathcal{G}_p$ following the distribution of Y_{odd} (resp. Y_{even}). Then we have

$$\mathbb{E}\biggl(\prod_{k=1}^{r} \# \operatorname{Sur}(Y_1^{(k)}, (\mathbb{Z}/p\mathbb{Z})^t)\biggr) = \mathbb{E}\biggl(\prod_{k=1}^{r} \# \operatorname{Sur}(Y_2^{(k)}, (\mathbb{Z}/p\mathbb{Z})^t)\biggr) = p^{\frac{r(t^2+t)}{2}}$$

by [14, Theorem 2.8]. This example shows that Theorem 4.3 can fail even if the mixed moments are slightly larger than the upper bound, which is given by $O(\prod_{k=1}^{r} m((\mathbb{Z}/p\mathbb{Z})^t)) = O(p^{\frac{rt^2}{2}})$ here.

Let $P_1, \dots, P_m \in \mathbb{Z}_p[t]$ be monic polynomials whose reductions modulo p are irreducible and let $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ be a random matrix for each $n \geq 1$. Assume that one can determine the (limiting) joint distribution of the cokernels $\operatorname{cok}(P_i(A_n))$ $(1 \leq i \leq m)$ when each A_n is equidistributed. Then the next goal would be to prove universality of the joint distribution of the cokernels for general ε_n-balanced matrices A_n. The only known way to prove such universality is to compute the mixed moments of the cokernels. Recall that $X_m = \{x_1, \dots, x_m\}$ is a finite ordered subset of $\mathbb{Z}_p$ whose elements have distinct reductions modulo p.

Theorem 4.5. *Let $(\varepsilon_n)_{n\geq 1}$ be a sequence of real numbers such that for every $\Delta > 0$, we have $\varepsilon_n \geq \frac{\Delta \log n}{n}$ for sufficiently large n. Let $A_n \in \mathrm{M}_n(\mathbb{Z}_p)$ be an ε_n-balanced random matrix for each $n \geq 1$, let $G_1, \dots, G_m \in \mathcal{G}_p$ and let $p_k : \prod_{i=1}^m G_i \to G_k$ $(1 \leq k \leq m)$ be the natural projections. Then we have*

$$\lim_{n\to\infty} \mathbb{E}\left(\prod_{i=1}^m \# \operatorname{Sur}(\operatorname{cok}(A_n + p x_i I_n), G_i) \right) = |S_{G_1,\dots,G_m}(X_m)|, \tag{4.4}$$

where $T_x \in \operatorname{End}(\prod_{i=1}^m G_i)$ $((g_1, \dots, g_m) \mapsto (x_1 g_1, \dots, x_m g_m))$ and

$$S_{G_1,\dots,G_m}(X_m) := \left\{ G \leq \prod_{i=1}^m G_i : p_i(G) = G_i \text{ for each } i \text{ and } pT_x(G) \leq G \right\}.$$

Proof. Choose $k \in \mathbb{Z}_{\geq 1}$ such that $p^k G_i = 0$ for all i. Let $R = \mathbb{Z}/p^k\mathbb{Z}$, $A_n' \in \mathrm{M}_n(R)$ be the reduction of A_n modulo p^k (which is also ε_n-balanced) and $v_j = A_n' e_j \in R^n$ where $\{e_1, \dots, e_n\}$ is the standard basis of R^n. Then we have

$$\begin{aligned} \mathbb{E}\left(\prod_{i=1}^m \# \operatorname{Sur}(\operatorname{cok}(A_n + p x_i I_n), G_i) \right) &= \sum_{\substack{F_i \in \operatorname{Sur}(R^n, G_i) \\ 1 \leq i \leq m}} \mathbb{P}(F_i(v_j + p x_i e_j) = 0 \text{ for all } 1 \leq j \leq n) \\ &= \sum_{\substack{F_i \in \operatorname{Sur}(R^n, G_i) \\ 1 \leq i \leq m}} \mathbb{P}(F v_j = -pT_x(F e_j) \text{ for all } 1 \leq j \leq n) \\ &= \sum_{\substack{F_i \in \operatorname{Sur}(R^n, G_i) \\ 1 \leq i \leq m}} \mathbb{P}(F A_n' = -pT_x F). \end{aligned} \tag{4.5}$$

If the probability $\mathbb{P}(FA_n' = -pT_x F)$ is non-zero, then $G = \operatorname{im}(F)$ is an element of $S_{G_1,\dots,G_m}(X_m)$. Following the proof of [10, Theorem 4.12], one can prove that there are constants $c, K > 0$ (depend only on G and X_m) such that

$$\left| \sum_{F \in \operatorname{Sur}_R(R^n, G)} \mathbb{P}(F A_n' = -pT_x F) - 1 \right| \leq K n^{-c} \tag{4.6}$$

for every $n \geq 1$ and $G \in S_{G_1,\dots,G_m}(X_m)$. (To do this, we need to generalize [10, Lemma 4.11] to an upper bound of $\mathbb{P}(FX = A)$ for every $A \in \operatorname{im}(F)$. For any X_0 such that $FX_0 = A$, we have $\mathbb{P}(FX = A) = \mathbb{P}(F(X - X_0) = 0)$ and $X - X_0$ is also an ε_n-balanced matrix so this immediately follows from the case $A = 0$.)

Now equations (4.5) and (4.6) imply that

$$\begin{aligned} \lim_{n\to\infty} \mathbb{E}\left(\prod_{i=1}^m \# \operatorname{Sur}(\operatorname{cok}(A_n + p x_i I_n), G_i) \right) &= \lim_{n\to\infty} \sum_{\substack{F_i \in \operatorname{Sur}(R^n, G_i) \\ 1 \leq i \leq m}} \mathbb{P}(F A_n' = -pT_x F) \\ &= \lim_{n\to\infty} \sum_{G \in S_{G_1,\dots,G_m}(X_m)} \sum_{F \in \operatorname{Sur}(R^n, G)} \mathbb{P}(F A_n' = -pT_x F) \\ &= |S_{G_1,\dots,G_m}(X_m)|. \end{aligned}$$

□

Example 4.6. Let $p \geq m \geq 3$, let $G_1 = \cdots = G_m = (\mathbb{Z}/p\mathbb{Z})^t$ and let $\{e_1, \dots, e_t\}$ be the standard basis of $(\mathbb{Z}/p\mathbb{Z})^t$. Then we have

$$\begin{aligned} |S_{G_1,\dots,G_m}(X_m)| &:= \# \left\{ G \leq \prod_{i=1}^m G_i : p_i(G) = G_i \text{ for each } i \right\} \\ &\geq \#\{G = \langle (e_j, u_{2,j}, \dots, u_{m,j}) : 1 \leq j \leq t \rangle : \langle u_{i,1}, \dots, u_{i,t} \rangle = (\mathbb{Z}/p\mathbb{Z})^t \text{ for every } 2 \leq i \leq m\} \\ &= \left(\prod_{k=0}^{t-1} (p^t - p^k) \right)^{m-1} \\ &> c_\infty(p) p^{(m-1)t^2}. \end{aligned}$$

To apply Theorem 4.3, the mixed moments of the cokernels for $G_1, \dots, G_m$ should be

$$O\biggl(\prod_{i=1}^{m} m(G_i)\biggr) = O((p^{\frac{t^2}{2}})^m) = O(p^{\frac{mt^2}{2}}).$$

However, the above inequality implies that for every constant $C > 0$, we have

$$|S_{G_1,\dots,G_m}(X_m)| > c_\infty(p)p^{(m-1)t^2} > Cp^{\frac{mt^2}{2}}$$

for sufficiently large t. Therefore we cannot apply Theorem 4.3 in this case. In fact, Example 4.4 tells us that there are two different m-tuples of random elements in $\mathcal{G}_p$ whose mixed moments for $G_1 = \cdots = G_m = (\mathbb{Z}/p\mathbb{Z})^t$ are $p^{\frac{m(t^2+t)}{2}}$, which is smaller than $c_\infty(p)p^{(m-1)t^2}$ for every $t \geq 4$ by the inequality $c_\infty(p) > \frac{1}{4}$.

By the above example, we cannot determine the joint distribution of the cokernels $\operatorname{cok}(A_n + px_iI_n)$ $(1 \leq i \leq m)$ for $m \geq 3$ using existing methods. As we mentioned in the introduction, we believe that one needs to combine combinatorial relations between the cokernels (Theorem 1.8 and Conjecture 1.9) and the mixed moments of the cokernels (Theorem 4.5) to solve this problem.

Acknowledgment: The authors thank Gilyoung Cheong and Seongsu Jeon for their helpful comments.

Funding: Jiwan Jung was partially supported by Samsung Science and Technology Foundation (SSTF-BA2001-04). Jungin Lee was supported by the new faculty research fund of Ajou University (S-2023-G0001-00236).

References

[1] G. Cheong and Y. Huang, Cohen–Lenstra distributions via random matrices over complete discrete valuation rings with finite residue fields, *Illinois J. Math.* **65** (2021), no. 2, 385–415.
[2] G. Cheong and N. Kaplan, Generalizations of results of Friedman and Washington on cokernels of random p-adic matrices, *J. Algebra* **604** (2022), 636–663.
[3] G. Cheong and M. Yu, The distribution of the cokernel of a polynomial evaluated at a random integral matrix, preprint (2023), https://arxiv.org/abs/2303.09125.
[4] E. Friedman and L. C. Washington, On the distribution of divisor class groups of curves over a finite field, in: *Théorie des nombres* (Quebec 1987), De Gruyter, Berlin (1989), 227–239.
[5] J. Lee, Joint distribution of the cokernels of random p-adic matrices, *Forum Math.* **35** (2023), no. 4, 1005–1020.
[6] J. Lee, Universality of the cokernels of random p-adic Hermitian matrices, *Trans. Amer. Math. Soc.* **376** (2023), no. 12, 8699–8732.
[7] J. Lee, Mixed moments and the joint distribution of random groups, *J. Algebra* **641** (2024), 49–84.
[8] H. H. Nguyen and R. Van Peski, Universality for cokernels of random matrix products, *Adv. Math.* **438** (2024), Article ID 109451.
[9] H. H. Nguyen and M. M. Wood, Local and global universality of random matrix cokernels, preprint (2022), https://arxiv.org/abs/2210.08526.
[10] H. H. Nguyen and M. M. Wood, Random integral matrices: Universality of surjectivity and the cokernel, *Invent. Math.* **228** (2022), no. 1, 1–76.
[11] R. Van Peski, Hall–Littlewood polynomials, boundaries, and p-adic random matrices, *Int. Math. Res. Not. IMRN* **2023** (2023), no. 13, 11217–11275.
[12] M. M. Wood, The distribution of sandpile groups of random graphs, *J. Amer. Math. Soc.* **30** (2017), no. 4, 915–958.
[13] M. M. Wood, Random integral matrices and the Cohen–Lenstra heuristics, *Amer. J. Math.* **141** (2019), no. 2, 383–398.
[14] M. M. Wood, Probability theory for random groups arising in number theory, in: *Proceedings of the International Congress of Mathematicians 2022*, Proc. Int. Cong. Math. 6, European Mathematical Society, Zürich (2022), 4476–4508.
[15] E. Yan, Universality for cokernels of Dedekind domain valued random matrices, preprint (2023), https://arxiv.org/abs/2301.09196.