Invariants for permutation-Hermite equivalence and critical dimension groups

David Handelman

(Communicated by Joachim Cuntz)

Abstract. Motivated by classification, up to order isomorphism, of dense subgroups of Euclidean space that are free of minimal rank, we obtain apparently new invariants for an equivalence relation (intermediate between Hermite and Smith) on integer matrices. These then participate in the classification of the dense subgroups. The same equivalence relation has appeared before, in the classification of lattice simplices. We discuss this equivalence relation (called *permutation-Hermite*), obtain fairly fine invariants for it, and have density results, and some formulas counting the numbers of equivalence classes for fixed determinant.

Introduction

Attempts at classification of particular families of dense subgroups of $\mathbf{R}^n$ as partially ordered (*simple dimension*) groups lead to two directed sets of invariants (in the form of finite sets of finite abelian groups, with maps between them) for an equivalence relation on integer matrices. These turn up occasionally in the study of lattice polytopes and commutative codes, among other places. The development in our case was classification of the dimension groups first, and then that of integer matrices; for expository reasons, we present the latter first.

Let B and B' be rectangular integer $m \times n$ matrices. Standardly, $\mathrm{GL}(n, \mathbf{Z})$ denotes the group of $n \times n$ integer matrices of determinant ± 1. We say B is *permutation-Hermite equivalent* (or *PHermite-equivalent,* or *PH-equivalent*) to B' if there exist $U \in \mathrm{GL}(m, \mathbf{Z})$ and a permutation matrix P of size n such that $UBP = B'$. Classification of matrices up to PH-equivalence is the same as classification of subgroups of (a fixed copy of) $\mathbf{Z}^{1 \times n}$ as partially ordered subgroups of $\mathbf{Z}^n$ (with the inherited ordering)—the row space of B, $r(B)$, is the subgroup, and the order automorphisms of $\mathbf{Z}^{1 \times n}$ are implemented by the permutation matrices (acting on the right). With this in mind, we can even

---

An earlier version is downloadable from arXiv, under the title *Invariants for critical dimension groups and permutation-Hermite equivalence*, arXiv:1309.7417v2 [math.AC].

define an equivalence relation on matrices $B \in \mathbf{Z}^{m \times n}$ and $B' \in \mathbf{Z}^{m' \times n}$, if we allow the additional operation of deleting a row of zeros any time it appears in the course of row reduction.

The Smith normal form (SNF) is an invariant for PH-equivalence, but a relatively crude one. For an important subclass of matrices (suggested by the dense subgroup problem), we construct two families of invariants that are surprisingly effective. These new invariants easily distinguish matrices with the same SNF in many cases. They also yield information about the matrices themselves, for example, whether the matrix is PH-equivalent to a matrix of the form $C := \left(\begin{smallmatrix} I_{n-1} & a \\ 0 & d \end{smallmatrix} \right)$—that is, an identity matrix of size $n - 1$, a column a, and $d = |\det B|$ (and also the content of a is relatively prime to d); such an $n \times n$ matrix is said to have 1-block size $n - 1$. When this happens, the cokernel is cyclic, but the converse fails. Matrices PH-equivalent to one of these forms are particularly amenable to complete classification. We also construct numerous examples with the expected unusual properties.

Let $G \subset \mathbf{R}^{1 \times n}$ be a finitely generated subgroup of $\mathbf{R}^{1 \times n}$ (or $\mathbf{R}^n$ for short, if there is no ambiguity). We can associate to G a lot of matrices as follows. Pick a $\mathbf{Z}$-basis, $F := \{f_1, \ldots, f_m\}$ for G, and let $B_F \in \mathbf{R}^{m \times n}$ be the matrix whose jth row is f_j. We define the *row space* of an $m \times n$ integer matrix to be the subgroup of $\mathbf{Z}^n$ generated by the rows of the matrix. Obviously, the row space of B_F, $r(B_F)$, is G, still viewed as a subgroup of $\mathbf{R}^n$. We can apply any element of $\mathrm{GL}(m, \mathbf{Z})$ on the left to B_F, and the row space is unchanged. So the inclusions $G \subset \mathbf{R}^n$ are classified (merely as a subgroup of $\mathbf{R}^n$) by the orbits of $\mathrm{GL}(m, \mathbf{Z})$ (acting from the left) on $\mathbf{R}^{m \times n}$.

This is strongly reminiscent of Hermite and Smith equivalence of (integer) matrices. If we let $G \subset \mathbf{Z}^n$ (this requires $m \leq n$), the classification of the subgroups of $\mathbf{Z}^n$ is just the orbit space of $\mathbf{Z}^{m \times n}$ under the action of $\mathrm{GL}(m, \mathbf{Z})$ (acting on the left), and gives rise to Hermite equivalence. If instead we want to classify the subgroups of $\mathbf{Z}^n$ up to isomorphism as subgroups of fixed $\mathbf{Z}^n$, we note that the automorphism group of $\mathbf{Z}^n$ is $\mathrm{GL}(n, \mathbf{Z})$ (acting on the right), so we are looking at the classification of matrices under the action of $\mathrm{GL}(m, \mathbf{Z}) \times \mathrm{GL}(n, \mathbf{Z})$; this gives rise to Smith equivalence, and the set of elementary divisors is a complete invariant.

PH-equivalence arises when we view the fixed $\mathbf{Z}^n$ as a partially ordered group, with the coordinatewise ordering, called *simplicial*. Subgroups inherit the partial ordering (but are themselves almost never simplicial), and we classify them up to order isomorphism. If the subgroup has full rank, such an order-isomorphism to another one (necessarily of the same rank) extends uniquely to an order isomorphism of $\mathbf{Z}^n$. These are given precisely by permutation matrices. We arrive at an equivalence relation that frequently turns up (e.g., [20, 21, 1, 22]), but has no name. So we give it one, at least restricted to square matrices.

The motivation for studying PH-equivalence comes from classification of dense subgroups, G, of $\mathbf{R}^n$ that are free of rank $n + 1$, viewed as partially ordered abelian groups, the ordering obtained by restricting the strict ordering

on $\mathbf{R}^n$ to G; that is, nonzero $g \in G$ is in the positive cone, G^+ if and only if each coordinate is a (strictly) positive real number. This defines (together with the embedding into $\mathbf{R}^n$, which we often suppress in notation) a *critical* (dimension) group. Equivalently, we can define a critical group to be a simple dimension group that is free of rank $n + 1$, and has exactly n pure traces (any affine representation, $G \to \mathrm{Aff}\, S(G, u)$, for some order unit u will yield the desired dense embedding in $\mathbf{R}^n \cong \mathrm{Aff}\, S(G, u)$; different order units yield isomorphisms among the images).

Let e_i denote the standard basis elements of $\mathbf{R}^n = \mathbf{R}^{1 \times n}$. A class of critical groups, known as *basic* critical groups, consists of those of the form, $G = \langle e_1, e_2, \ldots, e_n; \sum \alpha_i e_i \rangle$, where α_i are real numbers such that $\{1, \alpha_1, \ldots, \alpha_n\}$ is linearly independent over the rationals (this is equivalent to density of G in $\mathbf{R}^n$). Basic critical groups are a useful source of examples, as in [2]. They admit a characterization among critical groups in terms of their structure as simple dimension groups, via the pure traces.

For each subset of the pure trace space $\Omega \subset \partial_e S(G, u)$ such that $|\Omega| = n - 1$ (that is, Ω misses exactly one of the pure traces), define $\ker \Omega = \bigcap_{\tau \in \Omega} \ker \tau$. For any critical dimension group, the rank of $\ker \Omega$ will either be one or zero. We can thus write the kernel as $x_\Omega \mathbf{Z}$, where x_Ω is unique with respect to $\sigma(x_\Omega) \geq 0$, and σ is the pure trace not in Ω. Now form $E(G) \coloneqq \sum_\Omega x_\Omega \mathbf{Z} \subset G$. Then G is basic if and only if $G/E(G) \cong \mathbf{Z}$; when this occurs, all sets of pure traces are ugly (in the sense of [2]).

However, the converse to the latter statement is not correct—even if all sets of pure traces are ugly, the critical group need not be basic—leading to a larger family of critical groups. We say a critical group is *almost basic*, if it can be written in the form (that is, up to order isomorphism) $G = \langle f_1, f_2, \ldots, f_n; (\alpha_1, \ldots, \alpha_n) \rangle \subset \mathbf{R}^n$, where $f_i \in \mathbf{Z}^n$, the set $\{f_1, \ldots, f_n\}$ is real linearly independent, and $\{1, \alpha_1, \ldots, \alpha_n\}$ is linearly independent over the rationals; these are necessary and sufficient for G to be dense in $\mathbf{R}^n$. Then G is almost basic if and only if the torsion-free rank of $G/E(G)$ is one, and this is equivalent to all sets of pure traces being ugly.

Of course, $G/E(G)$ itself is an invariant of order isomorphism. In the case of almost basic critical groups, we can restrict to the span of the integer rows, and in doing so, not only do we obtain an invariant for integer matrices, but the invariant boils down to PH-equivalence. Moreover, for each subset $\Omega \subset \partial_e S(G, u)$ (this time, we allow arbitrary subsets, not just those of cosize one), we may form the quotient pre-ordered abelian group $G/\ker \Omega$ (in general, the quotient of a partially ordered abelian group by a subgroup that is not an order ideal—G is simple, so it has no proper order ideals—need not be partially ordered, and does not inherit many properties from the original).

When the set Ω is ugly (for example, if G is almost basic), $G_\Omega = G/\ker \Omega$ is itself a critical group with respect to the real vector space $\mathbf{R}^\Omega$. Thus we can also look at $G_\Omega/E(G_\Omega)$. This gives rise to an onto map from the torsion part of $G/E(G)$ to that of $G_\Omega/E(G_\Omega)$. If we now assume that G is almost basic, we see that the torsion lives entirely in the integer part of the row space. This

implies that it is a PH-invariant for the integer part (this requires an innocuous extra assumption on the integer part).

Almost basic critical groups admit a classification analogous to that for basic ones, but with an additional feature; after making a preliminary modification to A, the additional feature boils down to PH-equivalence.

Restricting to the relevant class of matrices B (for almost basic critical groups), we develop invariants (finer than elementary divisors/invariant factors). These are motivated by and apply back to almost basic critical groups, and correspond to subsets of the pure trace space. The invariants consist of a family of finite abelian groups, which are usually easy to calculate.

There are four appendices. The first deals with a general duality for some sets of rectangular matrices over arbitrary rings (related to the examples of Section 6). The second is joint work with my colleague Damien Roy, concerning a truncated form of the reciprocal of the Euler function, related to the density arguments in Section 7. The third shows that the obvious lower bound for the number of PH-equivalence classes of matrices with determinant d is asymptotically correct, with error bounds, at least when d is square-free. The fourth appendix has exact formulas for PH-equivalence classes, with special attention to those with 1-block size $n - 1$, when $n = 3$.

Statement of results

Section 1 contains the definitions of *terminal forms* (these apply to PH-equivalence classes); these are not quite normal forms, and are based on a result, [22, Thm. 4.1], on commutative codes. Discussed are the prototype PH-invariant(s), together with their elementary properties, dual elements (if B is an integer matrix, then there is a natural dual matrix B^{op}), and short exact sequences relating them. A particularly important class consists of those $(n \times n)$ matrices B that are PH-equivalent to a terminal form $\left(\begin{smallmatrix} I_{n-1} & a \\ 0 & d \end{smallmatrix} \right)$, where a is a column of size $n - 1$, and $d = |\det B|$; we say this type of terminal form has 1-block size $n - 1$.

The second section describes the (pseudo-) action of the permutation group S_n on matrices PH-equivalent to a terminal form whose 1-block size is $n - 1$. Proposition 2.1 precisely describes the orbits, and thus the PH-equivalence classes within this family.

Section 3 introduces two families of invariants, $\mathcal{J}(B)$ and $\mathcal{J}(B^{\mathrm{op}})$. These are lattices of finite abelian groups with homomorphisms among them, usually easy to compute. Theorem 3.8 shows that if $n \geq 3$ and every terminal form of the $n \times n$ matrix B has 1-block size $n - 1$, then $|\det B|$ is a power of a prime.

Section 4 discusses $(n \times n)$ matrices B which are PH-equivalent to a matrix with terminal form having 1-block size $n - 1$. Theorem 4.7 characterizes those whose dual also admits such a terminal form.

Section 5 deals with the (rare) phenomenon of matrices PH-conjugate to their duals; for matrices which are indecomposable in the appropriate sense

and have a terminal form with 1-block size $n - 1$, Theorem 5.3 is a characterization of this property, using the prime factorization of the determinant, and solvability of a quadratic modulo the determinant. A consequence is that when this occurs, the matrix is Hermite equivalent to its dual.

Section 6 discusses two conjectures concerning duality and the invariants $\mathcal{J}(B)$ and $\mathcal{J}(B^{\mathrm{op}})$; the stronger one is whether one can reconstruct $\mathcal{J}(B^{\mathrm{op}})$ just knowing $\mathcal{J}(B)$. This is true if B or B^{op} has a terminal form with 1-block size $n - 1$. We give a class of examples where the abelian groups appearing in $\mathcal{J}(B)$ are as homogeneous as possible, and show that we can recover one from the other via a Grassmann-like duality, discussed in more detail in Appendix A.

Section 7 gives a density result for size n matrices having a terminal form with 1-block size $n - 1$: it is at least .8 for $n \geq 6$ and converges up to $(\zeta(2)\zeta(3)/\zeta(6)) \cdot 1/(\zeta(2)\zeta(3)\zeta(4) \cdots) \sim .845$ as $n \to \infty$.

Sections 8–11 deal with critical groups, that is, dense subgroups of $\mathbf{R}^n$ that are free of rank $n + 1$, equipped (except in Section 8) with the strict ordering, making them into simple dimension groups. Section 8 contains a topological classification theorem, which for $n \geq 3$ corresponds to the classification of totally ordered subgroups of $\mathbf{R}$. *Basic* critical dimension groups [2] are characterized in Section 9, within the class of critical dimension groups, by means of the invariant which led to the development in Sections 1–6.

Almost basic critical dimension groups are introduced in Section 10. The classification of these reduces to PH-equivalence of integer matrices associated to them (Theorem 10.1). An invariant, introduced in previous section, is used to characterize almost basic critical groups among critical groups (Theorem 10.4).

Appendix A contains a general duality result for natural orbit spaces on classes of modules, a portion of which is used in Section 6 (Proposition A.6). Appendix B (joint with Damien Roy) is a short argument showing that the appropriate truncations of a form of the reciprocal of the Euler function yield a better than expected order of convergence. This is used in Section 8. Appendix C suggests an asymptotic formula for the number of PH-equivalence classes of fixed absolute determinant and size, and proves it when the determinant is square-free (Corollary C.5). Appendix D contains exact counting results on the numbers of PH-equivalence classes of size three matrices and fixed determinants, and also the numbers of PH-equivalence classes that contain a 1-block size two matrix.

Contents

1. PERMUTATION-HERMITE EQUIVALENCE

Let B and C be $n \times n$ integer matrices ($B, C \in \mathrm{M}_n\mathbf{Z}$). We consider a less well-known and two very well-known notions of equivalence between B and C.

The matrices B and C are *Hermite equivalent* if there exists U in $\mathrm{GL}(n, \mathbf{Z})$ such that $B = UC$ (this is more frequently defined on the right, rather than the left, but we will use this form here). In other words, B and C are obtainable from each other by $\mathbf{Z}$-elementary row operations (that is, row permutations, multiplication of a row by -1, and adding a row to another). Normal forms have been well-studied (for example, see the Wikipedia article[1]).

Matrices B and C are *Smith equivalent* if there exist U and V in $\mathrm{GL}(n, \mathbf{Z})$ such that $B = UCV$. Normal forms are even more well known, and correspond to invariant factors; they are used to classify finite abelian groups.

Matrices B and C are *permutation Hermite-equivalent* (or *PHermite-equivalent* or *PH-equivalent*) if there exist U in $\mathrm{GL}(n, \mathbf{Z})$ and a permutation matrix P such that $B = UCP$. In order words, B and C are obtainable from each other by finite sequences of $\mathbf{Z}$-elementary row operations (that is, permutations, multiplication of a row by -1, and adding a row to another), together with column permutations.

PH-equivalence classifies subgroups of a fixed copy of $\mathbf{Z}^n$ up to order-automorphism of the latter (when equipped with the simplicial, that is, coordinatewise, ordering); to see this, given the square matrix B, let $r(B)$ denote the abelian group span of its rows (known as its *row space*, despite there being no vector spaces involved) viewed as a subgroup of $\mathbf{Z}^n$. Left multiplication by elements of $\mathrm{GL}(n, \mathbf{Z})$ has no effect on the row space—only the generating set for $r(B)$ is changed—and column permutations implement the order-automorphisms of $\mathbf{Z}^{1 \times n}$ when the latter is given the usual coordinatewise partial ordering.

---

[1] http://en.wikipedia.org/wiki/Hermite_normal_form

It is helpful to permit the matrices B to be $m \times n$ with $m \geq n$; then elementary row operations are now implemented by elements of $\mathrm{GL}(m, \mathbf{Z})$. These do not change the row space, and it is convenient to add another operation: if at some point during a sequence of row and allowed column operations, a row becomes identically zero, then we delete it (and thus reduce the size). This obviously has no effect on the row space, and will be useful in the development of our invariants.

This section deals with an initial pair of invariants (one involving the dual of a matrix) and some of their properties.

Reduced forms for PH-equivalence have been obtained (see [22]; a special case is quoted as Theorem 1.1 below), but normal forms have not, as far as I can tell. (Informally, *reduced forms* for an equivalence relation constitute a useful collection of elements which contains representatives of each equivalence class; *normal forms* constitute a collection containing exactly one representative of each class.)

We say a sequence, vector, list, or set of integers, v, has *content c*, denoted $\mathrm{cont}(v) = c$, if c is the greatest common divisor of the nonzero entries of v (and if all the entries are zero, then $\mathrm{cont}(v) = 0$). We say v is *unimodular* (not to be confused with *unimodal*) if $\mathrm{cont}(v) = 1$.

We will restrict ourselves to the following class of matrices in $\mathrm{M}_n\mathbf{Z}$. Define $B \in \mathrm{M}_n\mathbf{Z}$ to be *weakly nonsingular* if the following two conditions apply:

(a) $\mathrm{rank}\, B = n$,
(b) every column of B is unimodular.

If C is any element of $\mathrm{M}_n\mathbf{Z}$ with full rank, then there is a factorization $C = BD$, where B is weakly nonsingular and D is diagonal with positive integer entries thereon.

Let $\mathcal{NS}_n$ (or simply $\mathcal{NS}$ when n is understood) denote the collection of weakly nonsingular $n \times n$ (integer) matrices. If $U \in \mathrm{GL}(n, \mathbf{Z})$ and w is any member of $\mathbf{Z}^{1 \times n}$, then $\mathrm{cont}(Uw) = \mathrm{cont}(w)$. Permutation of the columns of matrix simply permutes the contents of the columns. It follows that $\mathcal{NS}$ is preserved under PHermite-equivalence.

Given $B \in \mathcal{NS}$, there is a pseudo-algorithm that can be applied to reduce it to a more tractable form. First, apply the usual algorithm to obtain a Hermite normal form: since the content of the first column is one, there exists $U_1 \in \mathrm{GL}(n, \mathbf{Z})$ such that the first column of $U_1 B$ is $e_1 = (1, 0, \ldots, 0)^T$, the first standard basis element. Delete the first row and column, so that the second column has content possibly exceeding one (it cannot be zero, since the matrix has full rank), and continue in the obvious way, obtaining an upper triangular matrix whose first diagonal entry is 1, and for which the other diagonal entries are positive integers.

Permute the rows and columns so that all the diagonal ones are grouped together, in a block (it is easy to see how to do this), and now the matrix is in

the form

$$\begin{pmatrix} \mathrm{I}_s & Y \\ 0 & \mathcal{D} \end{pmatrix},$$

where $\mathcal{D}$ is an upper triangular matrix of size $n - s$, whose diagonal entries all exceed one. If, in $\mathcal{D}$, the content of any column is one, we may apply the same process to it via row operations, creating an additional standard basis vector via operations on the rows of size $n - s$. By permuting rows and columns, we may enlarge the identity block, and we continue this until there are no more columns of the resulting lower block matrix that are unimodular. (Recall however, that at every stage of this process, the size n matrix has all of its columns unimodular.) This yields the Hermite normal form; further processing may be required.

A PH-reduced form is obtained in the following result of [22], for convenience stated here only for full rank matrices.

Theorem 1.1 ([22, Thm. 4.1])**.** *Let $B \in M_n \mathbf{Z}$ be of full rank. Then there exists a PH-equivalent upper triangular matrix $C \in M_n \mathbf{Z}^+$ such that*

(a) $0 < C_{ii} \le C_{i+1,i+1}$ *for all* $1 \le i < n$,
(b) $0 \le C_{i,j} < C_{jj}$ *for all* $i < j$,
(c) $C_{ii} \le \gcd\{C_{sj} \mid i \le s \le j\}$ *for all* $i < j$.

We say C is *PH-terminal* (or just *terminal*) if it is in the form described in the theorem. *Terminal* suggests that there is nothing more that can be done to such matrices to simplify them. The size of the identity matrix that appears in the terminal form is called its 1-*block size*. If $B \in \mathcal{NS}_n$, then it has 1-block size at least one.

This is described in the cited reference as a normal form, but this is not with the usual meaning of the term—two distinct matrices C and C' each satisfying the conditions can be PHermite-equivalent. As a trivial example from $\mathcal{NS}$, set

$$C = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 6 \end{pmatrix}, \quad C' = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 6 \end{pmatrix}.$$

Then C and C' are conjugate via the transposition $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \oplus (1)$, hence are PHermite equivalent. This type of phenomenon can be avoided by refining the invariant. For example, we can make the top of the first column to the right of identity block be increasing; if there are ties, we can go to the next truncated column, and break the ties, etc. However, there is a less trivial difficulty with terminal matrices.

Applied to an $\mathcal{NS}$ matrix, the terminal form has an identity block of some size in the upper left corner. If two terminal forms are PH-equivalent, it is natural to ask whether the sizes of the identity blocks are the same. The answer is no, and we will see that this phenomenon occurs fairly frequently,

almost generically (Proposition 3.8). The equation,

$$
\begin{pmatrix} 2 & -1 & -1 \\ 3 & -1 & -2 \\ 6 & -3 & -4 \end{pmatrix} \begin{pmatrix} 1 & 1 & 2 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}
$$

is of the form $UC = C'P$, where C and C' belong to $\mathcal{NS}_3$, are in terminal form, C has just one 1 on the diagonal, C' has two; each has determinant 6 and $\det P = -1$, so $|\det U| = 1$, and thus $U \in \mathrm{GL}(3, \mathbf{Z})$. So C and C' are PH-equivalent but with different block sizes for 1.

Hermite normal forms of matrices in $\mathcal{NS}_n$, while themselves in $\mathcal{NS}_n$, need not be terminal: for p an integer exceeding 1, the matrix

$$
\begin{pmatrix} 1 & 1 & 1 \\ 0 & p & 1 \\ 0 & 0 & p \end{pmatrix}
$$

is in Hermite normal form, but is not a terminal form.

We define $\mathcal{NS}_{n,m}$ to be the class of matrices $B \in \mathcal{NS}_n$ which are PH-equivalent to a terminal form with 1-block size at least m. Obviously, $\mathcal{NS}_{n,n} = \mathrm{GL}(n, \mathbf{Z})$, and from the definition, $\mathcal{NS}_{n,1} = \mathcal{NS}_n$. The most important of these classes is $\mathcal{NS}_{n,n-1}$.

First, we give simple examples to distinguish the three equivalence relations. Barely any calculation is required. For each of $i = 0, 1, 2, 3, 4$, set

$$
B_i = \begin{pmatrix} 1 & i \\ 0 & 5 \end{pmatrix}.
$$

Then the following hold:

  (i) If $i \neq 0$, B_i is in $\mathcal{NS}_2$ and is in terminal form.
  (ii) Every 2×2 matrix with invariant factors $\{1, 5\}$ is Hermite-equivalent to one of the B_i.
  (iii) All five are mutually Hermite-*in*equivalent.
  (iv) B_2 and B_3 are PH-equivalent, but there are no other PH-equivalences among these matrices.
  (v) All five are mutually Smith equivalent, that is, their set of invariant factors is $\{1, 5\}$.

An obvious invariant for PH-equivalence of matrices $B \in \mathcal{NS}_n$ is simply the cokernel, $J(B) = \mathbf{Z}^{1 \times n}/\mathbf{Z}^{1 \times n}B$, the Smith invariant. We will often abbreviate this $\mathbf{Z}^n/\mathbf{Z}^n B$, or $\mathbf{Z}^n/r(B)$ (so that $r(B)$ denotes the subgroup generated by the rows of B). This is a coarse invariant.

A second invariant. We define: A *list* of objects is an unordered tuple (equivalently, a set with multiplicities recorded, sometimes known as a *multiset*). To distinguish between sets, ordered tuples, and lists, we use the notation $[\![x_i]\!]$ for lists. (There does not appear to be a standard notation for this.)

Let $B \in \mathcal{NS}$ (it need not be in terminal form); label its rows f_i. For each i, define x_i to be the unique row in $\mathbf{Z}^{1 \times n}$ with the following properties:

(a) $x_i = m(i)E_i$, where E_i is the ith standard basis element of $\mathbf{Z}^{1\times n}$ and $m(i)$ is a positive integer;
(b) $x_i \in \sum f_j \mathbf{Z}$;
(c) if $y \in \sum f_j \mathbf{Z}$ and $y = kE_i$ for some $k \in \mathbf{Z}$, then $m(i)$ divides $|k|$.

To see that each x_i exists, note that $r(B) = \sum f_j \mathbf{Z} \subseteq \mathbf{Z}^{1\times n}$ is just the row space of B, hence is of rank n, so it hits every nonzero cyclic subgroup of $\mathbf{Z}^{1\times n}$ in a nonzero element; then the usual well-ordering argument works.

Now form $X(B) = \sum x_i \mathbf{Z} = \oplus x_i \mathbf{Z}$. Then $I(B) := r(B)/X(B)$ is a finite abelian group (since the rank of $X(B)$ is obviously n). The claim is that this is an invariant for PHermite equivalence between matrices in $\mathcal{NS}$.

To see that it really is a PH-invariant (for matrices in $\mathcal{NS}$), suppose that C is another member of $\mathcal{NS}_n$, and $UCP = B$, where $U \in \mathrm{GL}(n, \mathbf{Z})$ and P is a permutation matrix. The row space of B is unaffected by the left action of $\mathrm{GL}(n, \mathbf{Z})$, and the *list* $[\![x_i]\!]$ is similarly unaffected by permutation of the columns.

This invariant would be useless if we could not compute with it, but it turns out to be rather easy to deal with.

Unless inconvenient, we write $\mathbf{Z}_k$ (for k a positive integer) in place of $\mathbf{Z}/k\mathbf{Z}$. This is not going to cause confusion with the other meaning of $\mathbf{Z}_k$, the k-adic completion, as we never use the latter.

The following will be subsumed by more easily obtained results after we have an equivalent form of the construction of $I(B)$.

Lemma 1.2. *Let $n, d_i, z_i, d > 1$ $(i = 2, \ldots, n)$ be positive integers and let a_i $(i = 1, \ldots, n-1)$ be nonnegative integers with $a_i < d$ and $\gcd\{d_i, z_i\} = 1$. Suppose B and B' are the following $n \times n$ matrices:*

$$B = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & 0 & \ldots & 0 & a_2 \\ 0 & 0 & \ddots & & \vdots & \vdots \\ 0 & 0 & \ldots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & a_{n-1} \\ 0 & 0 & 0 & \ldots & 0 & d \end{pmatrix}, \quad B' = \begin{pmatrix} 1 & z_2 & z_3 & \ldots & z_{n-1} & z_n \\ 0 & d_2 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \ddots & & \vdots & \vdots \\ 0 & 0 & \ldots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & d_{n-1} & 0 \\ 0 & 0 & 0 & \ldots & 0 & d_n \end{pmatrix}.$$

Then both B and B' are $\mathcal{NS}$ matrices in terminal form. Moreover,

$$I(B) \cong \bigoplus_i \left(\mathbf{Z} \Big/ \left(\frac{d}{\gcd\{d, a_i\}} \right) \mathbf{Z} \right),$$

and $I(B')$ is cyclic of order

$$\mathrm{lcm}\{d_2, d_3, \ldots, d_n\}.$$

Proof. That the matrices have all their columns unimodular is an immediate consequence of the properties ascribed to the coefficients. Let f_j $(j = 1, \ldots, n)$ be the rows of B. Then for $i < n$, $E_i = f_i - (a_i/d)f_n$, so that

$$x_i = (d/\gcd\{d, a_i\})f_i - (a_i/\gcd\{d, a_i\})f_n.$$

In addition, $x_n = f_n$, so that a basis for $X(B)$ is $\{(d/\gcd\{d, a_i\})f_i\} \cup \{f_n\}$. As $\{f_1, \ldots, f_n\}$ is a basis for $r(B)$, we have that $I(B) \cong \bigoplus_i (\mathbf{Z}/(\frac{d}{\gcd\{a_i, d\}})\mathbf{Z})$.

Now let f_j be the j row of B', and let $l = \operatorname{lcm}\{d_i\}$. Then

$$E_1 = f_1 - \sum_{i \geq 2} \frac{z_i}{d_i} f_i, \quad lE_1 = lf_1 - \sum_{i \geq 2} z_i f_i \cdot \frac{l}{d_i}.$$

If $t > 1$ is a prime dividing l and all of the z_i, then it divides at least one of the d_j; but this would contradict $\gcd\{d, z_i\} = 1$ for all i. Hence lE_1 is a unimodular element of $\sum f_j \mathbf{Z}$, so that $x_1 = lE_1$. For $i > 2$, $x_i = f_i$. Hence a basis for $\sum_{i=1}^n x_i \mathbf{Z}$ is $\{lf_1, f_2, \ldots, f_n\}$, and thus $I(B')$ is cyclic of order l. □

Here are some very simple examples with $n = 2$. Define

$$B_{a,d} = \begin{pmatrix} 1 & a \\ 0 & d \end{pmatrix},$$

where $d > 1$; in order to be terminal, we need $\gcd\{a, d\} = 1$ and $1 \leq a < d$. By taking determinants, we see that $B_{a,d}$ PH-equivalent to $B_{a',d'}$ entails $d = d'$ (a peculiarity of the $n = 2$ case). So let a' be another integer in the interval $1 \leq a' < d$ relatively prime to d. Then $B_{a,d}$ is PH equivalent to $B_{a',d}$ if and only if either $a = a'$ or $aa' \equiv 1 \bmod d$ (that is, in $\mathbf{Z}/d\mathbf{Z}$, $[a] = [a]^{\pm 1}$). The second choice comes from letting P be the nontrivial permutation matrix, and working out the details. Here $I(B_{a,d}) \cong \mathbf{Z}/d\mathbf{Z}$, not very exciting.

Next, consider variations on the earlier example. Set

$$B = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 6 \end{pmatrix}, \quad C_1 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \quad C_2 = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

In order for B to be terminal, we require $\gcd\{b, c, 6\} = 1$ and $0 \leq b, c < 6$; we may assume $b \leq c$ (by conjugating with the obvious transposition). Every terminal form of an $\mathcal{NS}$ matrix with diagonal entries $1, 2, 3$ is PH-equivalent to one of C_1 or C_2; this is routine.

We will show that the only choices for B which are PH-equivalent to a terminal form whose 1-block has size unequal to two (which means it has size one) correspond to $(b, c) = (2, 3)$ and $(3, 4)$. The former comes from the earlier example, and it is PH-equivalent to C_2. A similar computation (which comes from an easy sequence of row reductions) shows that with $(b, c) = (3, 4)$ or $(4, 3)$, B is PH-equivalent to C_1.

There are no other terminal forms of size three with $2, 3$ along the diagonal than C_1 and C_2, since both numbers are prime.

We have, by the earlier result,

$$I(B) = (\mathbf{Z}/(6/\gcd\{6, b\})\mathbf{Z}) \oplus (\mathbf{Z}/(6/\gcd\{6, c\})\mathbf{Z}).$$

Hence if at least one of b or c is relatively prime to 6, then $I(B)$ is not cyclic and has $\mathbf{Z}/6\mathbf{Z}$ as a proper quotient.

Now $I(C_i) \cong \mathbf{Z}_6$, since $6 = \mathrm{lcm}\{2,3\}$. Hence if b or c is relatively prime to 6, B cannot be PH-equivalent to either C_i, and in particular, all terminal forms of B have the same 1-block size, two.

Finally, C_1 and C_2 are not PH-equivalent, since the corresponding B forms are not; this will come from a general result obtained later.

Lemma 1.3. *Let $B = \begin{pmatrix} I_r & X \\ 0 & \mathcal{D} \end{pmatrix}$ be in terminal form with $\mathcal{D}$ upper triangular, and whose diagonal entries satisfy $1 < d_{r+1} \le d_{r+2} \le d_n$. Set $l = \mathrm{lcm}\{d_i\}$.*

(a) *If $\mathcal{D}$ is diagonal, then $I(B)$ is a quotient of $(\mathbf{Z}_l)^r$.*

(b) *In general, $I(B)$ is a quotient of*

$$(\mathbf{Z}/l\mathbf{Z})^r \oplus \left(\bigoplus_{j=r+1}^{n-1} \mathbf{Z}/\mathrm{lcm}\{d_{j+1}, d_{j+2}, \ldots, d_n\}\mathbf{Z} \right).$$

Proof. For $1 \le i \le r$, $E_i = f_i - \sum_{j>1}(a_{ij}/d_j)f_j$ for some integers $\{a_{ij}\}$. Hence $lE_i \in \mathcal{C}(B)$, and thus $lE_i \in X(B)$. Hence $x_i = t_i E_i$ for some positive integer t_i dividing l.

(a) Here $x_i = f_i$ if $i > r$, and thus $X(B)$ is spanned by $\{x_i\}_{i \le r} \cup \{f_i\}_{i > r}$; from the form of $t_i E_i$, we have that $X(B)$ is spanned by $\{t_i f_i\}_{i \le r} \cup \{f_i\}_{i > r}$. Since $\{f_i\}$ is a basis for $r(B)$, it follows that $I(B) \cong \oplus_{i \le r}(\mathbf{Z}_{t_i})$. This is a quotient of $(\mathbf{Z}_l)^r$, since each t_i divides l.

(b) If $r < i < n$, we can write $E_i = f_i - \sum_{j>i}(a_{ij}/d_j)f_j$. Obviously, $x_n = f_n$. Set $l_i = \mathrm{lcm}\{d_{i+1}, d_{i+2}, \ldots, n\}$, so that $l_i E_i \in r(B)$ and thus is in $X(B)$. So again we can write $x_i = t_i E_i$ with t_i dividing l_i, and we obtain that $I(B)$ is a quotient of $(\mathbf{Z}_l)^r \oplus (\bigoplus_{i>r} \mathbf{Z}_{t_i})$, which is a quotient of the desired group. $\square$

The 1-block size (that is, the size of the identity matrix in the upper left corner) in terminal forms turns out to be significant, particularly if it is $n-1$—when this occurs, PH-equivalence classes can be determined exactly.

Corollary 1.4. *Suppose $B = \begin{pmatrix} I_a & X \\ 0 & \mathcal{D} \end{pmatrix}$ is in terminal form, and let $d = \det B$. If $I(B)$ has a quotient which is isomorphic to $(\mathbf{Z}_d)^s$, then all terminal forms PH-equivalent to B must have 1-block size at most $n - s$.*

Proof. Suppose $B' = \begin{pmatrix} I_r & X' \\ 0 & \mathcal{D}' \end{pmatrix}$ is a PH-equivalent terminal form with $r > n - s$. In particular, $\det B' = \det B = d$. All the factors that are quotients of $\mathbf{Z}/\mathrm{lcm}\{d'_j, \ldots, d'_n\}$ for $j > r$ have order at most $\prod d'_j/d'_{r+2} < d$. But then the preceding says that $I(B')$ has at most r copies of $\mathbf{Z}_d$ appearing as a factor, a contradiction. $\square$

Now we introduce the notion of opposite.

A dual formulation of the invariant. When we construct the x_i in order to determine $I(B)$, we also create a dual of the matrix B, call it B^{op}, also in $\mathcal{NS}_n$, and for which $I(B) = \mathbf{Z}^{1 \times n}/\mathbf{Z}^{1 \times n}B^{\mathrm{op}}$, that is, $I(B) \cong J(B^{\mathrm{op}})$. To see this, we have a unique representation for each i, $x_i = \sum_j c_{ij}f_j$ with $c_{ij} \in \mathbf{Z}$; since x_i is not a nontrivial multiple of any element of $\sum f_k \mathbf{Z}$, it follows that

the content of $\{c_{ij}\}_{j=1}^n$ is one for each i. Hence the matrix $C = (c_{ji})$ (the transpose of what is expected) belongs to $\mathcal{NS}_n$.

Next, we see that if B' is PH-equivalent to B, then C' (constructed out of the canonical x_i') is PH-equivalent to C. A row operation on B simply multiplies C^T on the right by an element of $\mathrm{GL}(n, \mathbf{Z})$, hence multiplies its transpose, C, on the left by an element of $\mathrm{GL}(n, \mathbf{Z})$. A column permutation applied to B multiplies the representation of the x_i by a row permutation of the matrix C^T, so induces a column permutation of C.

So we define $B^{\mathrm{op}} = C$. In general, when B is in terminal form, B^{op} will be far from terminal, requiring both row operations and column permutations to put it into terminal form. If we think in terms of the row space of B^{op}, then it is almost tautological that $I(B) = \mathbf{Z}^n/r(B^{\mathrm{op}})$. That being the case, $I(B)$ is determined from the Smith normal form of B^{op}. To some extent this explains some of the loss of information in going from the PH-equivalence class of B to $I(B)$. Unsurprisingly, $(B^{\mathrm{op}})^{\mathrm{op}} = B$. In general, $|\det B| \neq |\det B^{\mathrm{op}}|$; this occurs when $|\det B| \neq |I(B)|$, and we have seen an example for which $\det B = 8$, but $I(B) \cong \mathbf{Z}_8 \oplus \mathbf{Z}_2$. From the equations defining B^{op}, we have $(B^{\mathrm{op}})^T B = \Delta := \mathrm{diag}(m(i), \ldots, m(i))$, where the $m(i)$ are defined via the x_i, that is, $x_i = m(i)E_i$.

Because of potential confusion caused by the notation, we redefine $J(B) = I(B^{\mathrm{op}}) = \mathbf{Z}^{1 \times n}/\mathbf{Z}^{1 \times n}B$ (determined by the Smith normal form of B), and thus $J(B^{\mathrm{op}}) = I(B) = \mathbf{Z}^{1 \times n}/\mathbf{Z}^{1 \times n}B^{\mathrm{op}}$. We will soon obtain a simpler description for B^{op}.

Lemma 1.5. *Suppose that $B, B' \in \mathcal{NS}_n$ and Δ, Δ' are diagonal real matrices with strictly positive entries. If $B\Delta = B'\Delta'$, then $\Delta = \Delta'$ and $B = B'$.*

Proof. Since B is invertible in $\mathrm{M}_n\mathbf{Q}$, we have $B^{-1}B' = \Delta(\Delta')^{-1}$; thus the latter has only rational entries (all of which are nonnegative). We can therefore write $N\Delta(\Delta')^{-1} = \Delta''$ for some positive integer N and $\Delta'' = \mathrm{diag}(d_i)$ diagonal with only positive integer diagonal entries. From $NB^{-1}B' = \Delta''$, we have $B'N = B\Delta''$. Now the ith column of $B'N$ has content N, and the ith column of $B\Delta$ is just d_i times the ith column of B, hence has content d_i. Thus $d_i = N$ for all i, so $(B' - B)N = 0$ and thus $B' = B$. As B is invertible in $\mathrm{M}_n\mathbf{R}$, $\Delta = \Delta'$. $\qquad\square$

The following shows that B^{op} can be characterized via a more general equation.

Proposition 1.6. *Let $B \in \mathcal{NS}_n$. Then the following hold:*
(a) *$B^{\mathrm{op}} \in \mathcal{NS}_n$ and $(B^{\mathrm{op}})^T B = \mathrm{diag}(m(1), \ldots, m(n))$.*
(b) *If $C \in \mathcal{NS}_n$ and $C^T B$ is diagonal with only nonnegative entries, then $C = B^{\mathrm{op}}$.*
(c) *$(B^{\mathrm{op}})^{\mathrm{op}} = B$, and the lists $[\![m(i)]\!]$ are the same for B and B^{op}.*
(d) *If $B' \in \mathcal{NS}_n$ is PH-equivalent to B, then $(B')^{\mathrm{op}}$ is PH-equivalent to B^{op}.*

Proof. (a) is noted above.

(b) Write $(B^{\mathrm{op}})^T B = \Delta_0$. As $B \in \mathcal{NS}_n$, B^{-1} exists (in $\mathrm{M}_n\mathbf{Q}$), we can write $C = (\Delta B^{-1})^T = (B^{-1})^T \Delta$, and similarly, $B^{\mathrm{op}} = (B^{-1})^T \Delta_0$. Then

$$B^{\mathrm{op}}\Delta = (B^{-1})^T \Delta_0 \Delta = (B^{-1})^T \Delta \Delta_0 = C\Delta_0.$$

The result now follows from the preceding lemma.

(c) From $(B^{\mathrm{op}})^T B = \Delta_0$, on transposing, we obtain $B^T B^{\mathrm{op}} = \Delta_0$; as $B \in \mathcal{NS}_n$ implies $B^{\mathrm{op}} \in \mathcal{NS}_n$, we have $B = (B^{\mathrm{op}})^{\mathrm{op}}$ from (b). It then follows from $B^T B^{\mathrm{op}} = \Delta_0$ that the list $[\![m(i)]\!]$ (the list of diagonal entries of Δ_0) is the same, whether computed with respect to B or with respect to B^{op}.

(d) There exist $U \in \mathrm{GL}(n, \mathbf{Z})$ and a permutation matrix P such that $B = UB'P$; then $\Delta_0 = (B^{\mathrm{op}})^T B = (B^{\mathrm{op}})^T UB'P$. Pre-multiplying by P and post-multiplying by P^{-1}, we have $P\Delta_0 P^{-1} = P(B^{\mathrm{op}})^T UB'$. Now since $B', (P(B^{\mathrm{op}})^T U)^T \in \mathcal{NS}_n$ and $P\Delta_0 P^{-1}$ is diagonal, by the lemma, we have $(B')^{\mathrm{op}} = (P(B^{\mathrm{op}})^T U)^T = U^T B^{\mathrm{op}} P^{-1}$ (since $P^{-1} = P^T$), yielding that $(B')^{\mathrm{op}}$ is PH-equivalent to B^{op}. $\square$

This leads to a fast construction of B^{op} and Δ. Pick $B \in \mathcal{NS}_n$; form $B^{-1} \in \mathrm{M}_n\mathbf{Q}$. There exists a smallest positive integer $m(i)$ such that $m(i)$ times the ith row of B^{-1} consists of integers—and necessarily, the resulting row has content one. Set $\Delta = \mathrm{diag}(m(i))$; since the entries of ΔB^{-1} are all integers and the content of each row is one, it is immediate that $(\Delta B^{-1})^T \in \mathcal{NS}_n$. Then $B^{\mathrm{op}} = (\Delta B^{-1})^T$.

In [1], Atanasov et al. introduced two numbers associated to a matrix $B \in \mathcal{NS}_n$; the first was denoted I, which is $|\det B|$; the second was denoted I^*,[2] and is $|\det B^{\mathrm{op}}|$; they also use B^*, the dual matrix emanating from lattice polytopes, for what is called here B^{op}. Among other things, they constructed very useful tables of numbers of isomorphism classes, and explicit generators, which turned out to be particularly helpful for Appendix D.

Let B belong to $\mathcal{NS}_n$. Defining E_i, x_i, and $m(i)$ as we have above, there is an obvious short exact sequence,

$$0 \to \frac{r(B)}{\sum x_i \mathbf{Z}} \to \frac{\mathbf{Z}^{1 \times n}}{\sum x_i \mathbf{Z}} \to \frac{\mathbf{Z}^{1 \times n}}{r(B)} \to 0.$$

The left term is just $I(B)$ and the right is $I(B^{\mathrm{op}})$, which is determined by the invariant factors of B. For the middle term, we have that it is naturally isomorphic to $r(B)/(\sum x_i \mathbf{Z})B$ via B; the map sending $w \in \mathbf{Z}^n$ to wB induces a group homomorphism $\mathbf{Z}^{1 \times n}/\sum x_i \mathbf{Z} \to r(B)/(\sum x_i \mathbf{Z})B$, which is clearly onto; it is also one to one, since $wB = vB$ (with $v \in \sum x_i \mathbf{Z}$) entails $w = v$. In addition, $x_i B = m(i)f_i$, so that the middle group is just $\bigoplus \mathbf{Z}_{m(i)}$. So we can rewrite the short exact sequence as

$$0 \to J(B^{\mathrm{op}}) \to \bigoplus \mathbf{Z}_{m(i)} \to J(B) \to 0.$$

---

[2]Unfortunately, I came across this reference after I had established the notation for this paper, so that their I is $|I(B^{\mathrm{op}})| = |J(B)|$, and their I^* is $|I(B)| = |J(B^{\mathrm{op}})|$.

Since we may interchange B with B^{op} (from $(B^{\mathrm{op}})^T B = \Delta$, we obtain that $B^T B^{\mathrm{op}} = \Delta$), we also obtain a short exact sequence $0 \to J(B) \to \bigoplus \mathbf{Z}_{m(i)} \to J(B^{\mathrm{op}}) \to 0$. This can be re-interpreted more generally.

For a finite group G, the *exponent* of G, denoted $\operatorname{Exp} G$, is the smallest positive integer e such that the order of every element divides e.

Proposition 1.7. *Suppose $B \in \mathcal{NS}_n$. Then*
$$\operatorname{Exp} J(B) = \operatorname{Exp} J(B^{\mathrm{op}}) = \operatorname{Exp} \mathbf{Z}^n / \mathbf{Z}^n \Delta = \operatorname{lcm}\{m(i)\}.$$

Proof. From the short exact sequence $0 \to J(B) \to \bigoplus \mathbf{Z}_{m(i)} \to J(B^{\mathrm{op}}) \to 0$, obviously $\operatorname{Exp} J(B)$ and $\operatorname{Exp} J(B^{\mathrm{op}})$ divide the exponent of the middle term, which is $\operatorname{lcm}\{m(i)\}$. Set $d = \operatorname{Exp} J(B)$. This says that $\mathbf{Z}^n d \subseteq \mathbf{Z}^n B$. Applying B^{-1} (which exists in $\mathbf{Q}^{n \times n}$), we have $\mathbf{Z}^n d B^{-1} \subset \mathbf{Z}^n$, whence $C := d B^{-1}$ is an integral matrix satisfying $CB = d\mathrm{I}$. Since $(B^{\mathrm{op}})^T B = \Delta$, we deduce $(B^{\mathrm{op}})^T = d\Delta C$, so that $C^T = B^{\mathrm{op}} d \Delta^{-1}$ (as matrices with rational entries).

The ith column of C^T is thus $d/m(i)$ times the ith row of B^{op}. As each column of B^{op} has content one, this entails (as C^T has only integer entries) that $m(i)$ divide d. Hence $\operatorname{lcm}\{m(i)\}$ divides d; since d divides $\operatorname{lcm}\{m(i)\}$, we have $d = \operatorname{lcm}\{m(i)\}$.

Since $B^T B^{\mathrm{op}} = \Delta^T = \Delta$, we can interchange the roles of B and B^{op}, obtaining the final equality. $\square$

We let $d = \operatorname{Exp} J(B)$. Then we can regard each of $J(B)$, $J(B^{\mathrm{op}})$, and $\mathbf{Z}^{1 \times n} / \mathbf{Z}^{1 \times n} \Delta$ as $\mathbf{Z}_d$-modules. As $\mathbf{Z}_d$ is self-injective, each of them contains a nonzero free submodule as a direct summand; and $J(\Delta) := \bigoplus \mathbf{Z}_{m(i)}$ contains a free $\mathbf{Z}_d$-module on two generators as a direct summand.

Lemma 1.8. *Suppose that p is a prime and B in $\mathcal{NS}_n$ has terminal form*
$$\begin{pmatrix} I_{n-1} & X \\ 0 & p^m \end{pmatrix}$$
for some $m \geq 1$. If B' is a terminal matrix in $\mathcal{NS}$ that is PH-equivalent to B, then the 1-block of B' has size $n-1$.

Proof. From the terminal form, $J(B)$ is cyclic of order p^m. If B is PH-equivalent to B' in terminal form with block size less than $n-1$, then for each row of B', say the ith, that is not a standard basis element is of the form $(0^{i-1}, p^{m(i)}, b(i))$ (where $b(i)$ is a row of size $n-i$, possibly empty), and $m(i) \leq m(i+1)$, and we can take $i = n-1$. Then it follows from Theorem 1.1 that $p^{m(i)}$ divides each entry of $b(i)$. Then the ith row divided by $p^{m(i)}$, v_i, has order $p^{(i)}$ in $\mathbf{Z}^n / r(B')$. The order of the image of E_n (the bottom row divided by $p^{m(n)}$) is at least as large, $p^{m(n)}$.

As $J(B') \cong J(B)$ and is cyclic of order p^m, we must have that $v + r(B')$ belongs to the subgroup generated by $E_n + r(B)$, that is, there is an integer k such that $v - k E_n \in r(B')$. The initial nonzero term of $v - k E_n$ is 1, whereas the ith entry of every row is either 0 or divisible by p. Hence $v - k E_n \in r(B')$, a contradiction. $\square$

In particular, if $|\det B|$ is a power of a prime and $J(B^{\mathrm{op}})$ has exponent equalling $|\det B|$, then every terminal form PH-equivalent to B must have 1-block of size $n-1$.

The following is elementary.

Lemma 1.9. *Let $0 \to A \to B \to C \to 0$ be a short exact sequence of finite abelian groups. If any of the following hold:*

    (a) $\mathrm{Exp}\, B = \mathrm{Exp}\, A$ *and A is cyclic,*
    (b) $\mathrm{Exp}\, B = \mathrm{Exp}\, C$ *and C is cyclic,*
    (c) $\mathrm{Exp}\, B$ *is square-free,*

then the sequence splits.

Proof. Let $d = \mathrm{Exp}\, B$; as $\mathrm{Exp}\, A$ and $\mathrm{Exp}\, C$ divide d, the sequence is a short exact sequence of $\mathbf{Z}_d$-modules.

If $\mathrm{Exp}\, C = \mathrm{Exp}\, B$ and C is cyclic, then C is free as a $\mathbf{Z}_d$-module, so the sequence splits. If $\mathrm{Exp}\, A = \mathrm{Exp}\, B$ and A is cyclic, then A is free and singly generated; since $\mathbf{Z}_d$ is self-injective, A is injective as a $\mathbf{Z}_d$-module, so the sequence splits.

If $\mathrm{Exp}\, B := d$ is square-free, then C, being a $\mathbf{Z}_d$-module, is projective, hence the sequence splits. $\qquad\square$

A consequence of the method of proof is the following somewhat interesting result.

Lemma 1.10. *Suppose that H is a subgroup $\mathbf{Z}^n$ having rank n, with invariant factors $(f_1, f_2, \ldots, f_n)$. Let x be an element of $\mathbf{Z}^n$ such that $x + H$ has order f_n (the exponent of $\mathbf{Z}^n/H$) in $\mathbf{Z}^n/H$. Then $H + x \subset \mathbf{Z}^n$ has invariant factors $(1, f_1, \ldots, f_{n-1})$.*

Proof. The onto map $\mathbf{Z}^n/H \to \mathbf{Z}^n/(H + x\mathbf{Z})$ has kernel $(x\mathbf{Z} + H)/H$, which is free as a $\mathbf{Z}_{f_n}$ module, so is a direct summand. Therefore we can write $\mathbf{Z}^n/H = (x + H)\mathbf{Z} \oplus D$ for some $\mathbf{Z}_{f_n}$ module D. Since $D \cong \mathbf{Z}_{f_n}$ and the sequence invariant factors is unique, D must have invariant factors $1, f_2, \ldots, f_{n-1}$ (delete the last one, and insert a one at the beginning). Obviously $D \cong \mathbf{Z}^n/(H + x\mathbf{Z})$. $\qquad\square$

The following is presumably well known, but useful. If G is an abelian group, then $\mathrm{t}(G)$ denotes its torsion subgroup.

Lemma 1.11. *Let A be an $r \times n$ integer matrix. Then*

$$\mathrm{t}(\mathbf{Z}^n/\mathbf{Z}^r A) \cong \mathrm{t}(\mathbf{Z}^r/\mathbf{Z}^n A^T).$$

Proof. Let $s = \mathrm{rank}\, A$; then $s \le r, n$. The first step is to reduce to the case that $r = s = n$.

To that end, we observe that the row space of A, $\mathbf{Z}^r A$ is free of rank s; hence there exists $E \in \mathrm{GL}(r, \mathbf{Z})$ such that $EA\binom{A'}{0}$, where A' is $s \times n$. Since

A' has rank s, there exists $F \in \mathrm{GL}(n, \mathbf{Z})$ such that $A'F = \left(\begin{smallmatrix} A'' \\ 0 \end{smallmatrix} \right)$, where A'' is $s \times s$. In particular,

$$EAF = \begin{pmatrix} A'' & 0 \\ 0 & 0 \end{pmatrix}.$$

Hence

$$\mathbf{Z}^n/\mathbf{Z}^r A \cong \mathbf{Z}^n/\mathbf{Z}^r EAF \cong \mathbf{Z}^s/\mathbf{Z}^s A'' \oplus \mathbf{Z}^{n-s}.$$

From $F^T A^T E^T = (EAF)^T = \left(\begin{smallmatrix} (A'')^T & 0 \\ 0 & 0 \end{smallmatrix} \right)$, we similarly obtain $\mathbf{Z}^n/\mathbf{Z}^r A \cong \mathbf{Z}^s/\mathbf{Z}^s (A'')^T \oplus \mathbf{Z}^{r-s}$.

So it suffices to show that if $M \in \mathbf{Z}^{s \times s}$ is of rank s, then $\mathbf{Z}^s/\mathbf{Z}^s M \cong \mathbf{Z}^s/\mathbf{Z}^s M^T$. But this is straightforward. Let $(f_1, \ldots, f_s)$ be the sequence of invariant factors of M; then there exist $J, K \in \mathrm{GL}(s, \mathbf{Z})$ such that $JMK = \mathrm{diag}(f_1, \ldots, f_s) := \Delta$. Obviously $K^T M^T J^T = \Delta$, so M^T has the identical sequence of invariant factors. □

Lemma 1.12. *Let $A \in \mathbf{Z}^{r \times n}$, $B \in \mathbf{Z}^{n \times r}$. If A has rank r, then there is a short exact sequence,*

$$0 \to \mathbf{Z}^r/\mathbf{Z}^n B \to \mathbf{Z}^n/\mathbf{Z}^n BA \to \mathbf{Z}^n/\mathbf{Z}^r A \to 0,$$

the maps induced by $v \mapsto vA$ and $v \mapsto v$.

Proof. Since $\mathbf{Z}^n BA \subset \mathbf{Z}^r A$, the map from the middle to the right term, $v + \mathbf{Z}^n BA \mapsto v + \mathbf{Z}^r A$ is well-defined, and obviously onto. Its kernel is $\mathbf{Z}^r A/\mathbf{Z}^n BA$. The map $v + \mathbf{Z}^n B \mapsto vA + \mathbf{Z}^n BA$ is clearly well-defined, and maps onto the kernel; it suffices to show it is one to one. But $vA \in \mathbf{Z}^n BA$ entails $v = wBA$ for some $w \in \mathbf{Z}^n$, whence $(v - wB)A = 0$. However, A is $r \times n$ and of rank r, so right multiplication by A is one to one. Thus $v = wB$, and the map is one to one. □

Weirdly, even under the (strong) hypotheses that A, B are square of the same size and with nonzero determinant, it need not be true that $\mathbf{Z}^n/\mathbf{Z}^n AB \cong \mathbf{Z}^n/\mathbf{Z}^n BA$ (both of these are torsion).

Set $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 2 \end{smallmatrix} \right)$. Then $AA^T = \left(\begin{smallmatrix} 2 & 2 \\ 2 & 4 \end{smallmatrix} \right)$, so $\mathbf{Z}^2/\mathbf{Z}^2 AA^T \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2$. On the other hand, $A^T A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 5 \end{smallmatrix} \right)$, and thus $\mathbf{Z}^2/\mathbf{Z}^2 A^T A \cong \mathbf{Z}_4$. Label $B = A^T$.

In general, the sequence of torsion subgroups of a short exact sequence is not exact (take $0 \to \mathbf{Z} \to \mathbf{Z} \to \mathbf{Z}_2 \to 0$, where the middle map is multiplication by 2); however, in this case, it is. The following is presumably well known.

Corollary 1.13. *Suppose $A \in \mathbf{Z}^{r \times n}$, $B \in \mathbf{Z}^{n \times r}$, and BA has rank r. Then there is a short exact sequence,*

$$0 \to \mathbf{Z}^r/\mathbf{Z}^n B \to \mathrm{t}(\mathbf{Z}^n/\mathbf{Z}^r BA) \to \mathrm{t}(\mathbf{Z}^n/\mathbf{Z}^r A) \to 0.$$

Proof. Since B has rank (at least, hence exactly) r, $\mathbf{Z}^r/\mathbf{Z}^n B$ is finite, hence torsion. Suppose $v + \mathbf{Z}^r A$ is a torsion element of the third term in the short exact sequence in the previous lemma. Then there exists a positive integer N such that $Nv \in \mathbf{Z}^r A$. Since $\mathbf{Z}^r BA \subset \mathbf{Z}^r A$ and they have equal ranks, there exists an integer M such that $M\mathbf{Z}^r A \subset \mathbf{Z}^r BA$. Hence $MNv \in \mathbf{Z}^r BA$.

Therefore, all pre-images in the middle term, of $v + \mathbf{Z}^r A$, lie in the torsion subgroup of $\mathbf{Z}^n/\mathbf{Z}^r BA$. In particular, the right map is onto.

Since $\mathbf{Z}^r/\mathbf{Z}^n B$ is finite, it maps to the torsion subgroup of the middle term, and exactness of the original sequence now yields exactness of the sequence of torsion subgroups. $\qquad\square$

Now suppose that $B \in \mathcal{NS}_n$, and form B^{op}. From $(B^{\mathrm{op}})^T B = \Delta = \mathrm{diag}(m(1), \ldots, m(n))$, we deduce (setting $B = A$, etc.), a short exact sequence $0 \to \mathbf{Z}^n/\mathbf{Z}^n(B^{\mathrm{op}})^T \to \bigoplus \mathbf{Z}/m(i)\mathbf{Z} \to \mathbf{Z}^n/\mathbf{Z}^n B \to 0$. By Lemma 1.11, the first term is isomorphic to $\mathbf{Z}^n/\mathbf{Z}^n B^{\mathrm{op}}$. This yields a short exact sequence,

$$0 \to J(B^{\mathrm{op}}) \to \bigoplus \mathbf{Z}/m(i)\mathbf{Z} \to J(B) \to 0.$$

We also have $B^T B^{\mathrm{op}} = \Delta$ (by applying the transpose); this permits us to reverse the roles of B and B^{op}, and we obtain another short exact sequence,

$$0 \to J(B) \to \bigoplus \mathbf{Z}/m(i)\mathbf{Z} \to J(B^{\mathrm{op}}) \to 0.$$

By Lemmas 1.7 and 1.9, if either $J(B)$ or $J(B^{\mathrm{op}})$ is cyclic or, more generally, if either $J(B)$ or $J(B^{\mathrm{op}})$ is a free $\mathbf{Z}_d$-module, then the sequence splits; similarly, if the exponent, d, of $J(B)$ is square-free, the sequence splits. There are examples to show that neither of these need split. Unfortunately, because we are taking isomorphisms at various points, the extensions themselves need not be PH-invariants. However, whether the sequences split is a PH-invariant.

Example 1.14. The extension $0 \to J(B) \to \bigoplus \mathbf{Z}_{m(i)} \to J(B^{\mathrm{op}}) \to 0$ need not split; in fact, $J(B) \oplus J(B^{\mathrm{op}})$ need not be isomorphic to $\bigoplus \mathbf{Z}_{m(i)}$.

To construct an example, suppose that $n = 3$ and d is a power of a prime p. If we can find $B \in \mathcal{NS}_3$ such that $\det B = d$, and both $J(B)$ and $J(B^{\mathrm{op}})$ are not cyclic, then the extension cannot be split. We note that $J(B) \oplus J(B^{\mathrm{op}})$ cannot be generated by 3 elements, since it is a p-group and has at least four elementary divisors. But the list $[\![m_i]\!]$ consists of $n = 3$ elements, so that $\bigoplus \mathbf{Z}_{m(i)}$ has three generators; in particular, $\bigoplus \mathbf{Z}_{m(i)} \not\cong J(B) \oplus J(B^{\mathrm{op}})$.

So it suffices to find a matrix B with these properties. For any prime p, set

$$B = \begin{pmatrix} 1 & 1 & 1 \\ 0 & p & p^2 \\ 0 & 0 & p^3 \end{pmatrix}, \quad \text{so that } B^{\mathrm{op}} = \begin{pmatrix} p^3 & 0 & 0 \\ -p^2 & p & 0 \\ p-1 & -1 & 1 \end{pmatrix}.$$

Since the cokernel of $C := \left(\begin{smallmatrix} p & p^2 \\ 0 & p^3 \end{smallmatrix} \right)$ is $\mathbf{Z}_{p^3} \oplus \mathbf{Z}_p$, $J(B) \cong \mathbf{Z}_{p^3} \oplus \mathbf{Z}_p$ (in $\mathbf{Z}^2/\mathbf{Z}^2 C$, there is no element of order p^4, but there are elements of order p^3; alternatively, subtract p times the first column from the second, to create $\mathrm{diag}(p, p^3)$); similarly, the cokernel of $\left(\begin{smallmatrix} p & 0 \\ -p^2 & p^3 \end{smallmatrix} \right)$ is $\mathbf{Z}_{p^3} \oplus \mathbf{Z}_p$, so this is also $J(B^{\mathrm{op}})$. Hence $J(B) \oplus J(B^{\mathrm{op}})$ has elementary divisors $[\![p^3, p^3, p, p]\!]$, and is thus not 3-generated as an abelian group. In this case, $m(1) = m(3) = p^3$ and $m(2) = p^2$.

There is another invariant of PH-equivalence, concerning a particularly strong form of splitting. The imbeddings $J(B) \to \mathbf{Z}^{1 \times n}/\mathbf{Z}^{1 \times n}\Delta$ and $J(B^{\mathrm{op}}) \to \mathbf{Z}^{1 \times n}/\mathbf{Z}^{1 \times n}\Delta$ (we will sloppily abbreviate $\mathbf{Z}^{1 \times n}/\mathbf{Z}^{1 \times n}\Delta$ to $J(\Delta)$ from now

on) are given by first identifying $J(B) = \mathbf{Z}^{1 \times n}/\mathbf{Z}^{1 \times n}B$ with $\mathbf{Z}^{1 \times n}/\mathbf{Z}^{1 \times n}B^T$ (Lemmas 1.11 and 1.12), and then with the latter's image in $J(\Delta)$, given by $v + r(B^T) \mapsto vB^{\mathrm{op}} + \mathbf{Z}^{1 \times n}\Delta$, and then doing the same with $J(B^{\mathrm{op}})$.

This gives us two subgroups of $J(\Delta)$, specifically, $Y(B) := r(B^{\mathrm{op}})/r(\Delta) \cong J(B)$ and $Y(B^{\mathrm{op}}) := r(B)/r(\Delta) \cong J(B^{\mathrm{op}})$. Denote by $\pi_B \colon J(\Delta) \to J(B)$ and $\pi_{B^{\mathrm{op}}} \colon J(\Delta) \to J(B^{\mathrm{op}})$ the two quotient maps in the short exact sequences. Then we can ask whether the image of $J(B)$ in $J(\Delta)$ (that is, $Y(B)$) maps under π_B *onto* $J(B)$, that is, $\pi_B(Y(B)) = J(B)$. This of course entails that π_B splits, but is stronger than that (there are easy examples wherein π_B splits, but this property does not hold). We say that B *super-splits* when this occurs (it is a two-sided property, as we will see).

Lemma 1.15. *Let $B \in \mathcal{NS}_n$. The following are equivalent:*
- (a) B *is super-splitting,*
- (b) $r(B) + r(B^{\mathrm{op}}) = \mathbf{Z}^{1 \times n}$,
- (c) $r(B) \cap r(B^{\mathrm{op}}) = r(\Delta)$.

Remark. Since (b) and (c) are symmetric under the interchange of B with B^{op}, we deduce that B super-splits if and only if B^{op} does. It follows from (b) that super-splitting is a PH-invariant (which was not at all clear from the definition, since the latter uses identifications such as that of $J(B)$ with $\mathbf{Z}^{1 \times n}/\mathbf{Z}^{1 \times n}B^T$).

Proof. Obviously, $r(\Delta) \subseteq r(B) \cap r(B^{\mathrm{op}})$ follows directly from $(B^{\mathrm{op}})^T B = B^T B^{\mathrm{op}} = \Delta$, and the map π_B is $v + r(\Delta) \mapsto v + r(B)$.

(a) implies (b). The map π_B sends $Y(B^{\mathrm{op}}) = r(B)/r(\Delta)$ to zero, but is an isomorphism when restricted to $Y(B) = r(B^{\mathrm{op}})/r(\Delta)$. Hence $(r(B) + r(B^{\mathrm{op}}))/r(\Delta)$ has cardinality $|J(B)| \cdot |J(B^{\mathrm{op}})|$, and the latter is $\det \Delta = |\mathbf{Z}^{1 \times n}/\mathbf{Z}^{1 \times n}\Delta|$. If $r(B) + r(B^{\mathrm{op}})$ were strictly contained in $\mathbf{Z}^{1 \times n}$, then $J(\Delta)$ would be strictly larger than $|J(B)| \cdot |J(B^{\mathrm{op}})|$, a contradiction.

(b) implies (c). We have the map $J(B) \times J(B^{\mathrm{op}}) \to \mathbf{Z}^{1 \times n}/\mathbf{Z}^{1 \times n}\Delta$ (given by the identifications of $J(B)$ with $Y(B)$ and $J(B^{\mathrm{op}})$ with $Y(B^{\mathrm{op}})$), and this is onto by hypothesis (b). Since the cardinalities are the same, the map is an isomorphism. However,

$$(r(B^{\mathrm{op}}) + r(B))/(r(B) \cap r(B^{\mathrm{op}}))$$
$$\cong r(B^{\mathrm{op}})/(r(B) \cap r(B^{\mathrm{op}})) + r(B)/(r(B) \cap r(B^{\mathrm{op}}))$$
$$\cong J(B) \times J(B^{\mathrm{op}}),$$

so again by cardinality, $r(B) \cap r(B^{\mathrm{op}}) = r(\Delta)$.

(c) implies (a). Using the standard isomorphisms (as in (b) implies (c)), we have that $r(B^{\mathrm{op}}) + r(B)/r(\Delta)$ is the direct sum, and by cardinality, we obtain (b). Ontoness of π_B is then immediate. $\square$

We know that if $J(B)$ or $J(B^{\mathrm{op}})$ is cyclic or a free $\mathbf{Z}_d$-module ($d = \mathrm{Exp}\, J(B)$), then both sequences $J(B) \to J(\Delta) \to J(B^{\mathrm{op}})$ and $J(B^{\mathrm{op}}) \to J(\Delta) \to J(B)$ split. But not all of them super-split. For example, if $B \in \mathcal{NS}_{n,n-1}$ and

$B = \begin{pmatrix} I_{n-1} & a \\ 0 & d \end{pmatrix}$, where $a = (a_1, \ldots, a_{n-1})^T$ is unimodular modulo d, then B is super-split if and only if $1 + \sum a_i^2$ is relatively prime to d (this is obtained by looking at criterion (b) modulo d). Since we can easily solve $1 + \sum a_i^2 \equiv 0 \bmod d$ if $n, d \geq 3$ (with all a_i relatively prime to d), we have found many examples wherein the sequences split, but B is not super-split.

At one possible opposite extreme is the case that B is Hermite- (not just PHermite-) equivalent to B^{op}. This means that $B = EB^{\mathrm{op}}$ for some $E \in \mathrm{GL}(n, \mathbf{Z})$, or equivalently, that $r(B) = r(B^{\mathrm{op}})$. These are not super-split (unless $|\det B| = 1$). There are lots of such examples; for instance, if $B \in \mathcal{NS}_{n,n-1}$ and is weakly indecomposable, then it follows from Theorem 5.3 that if B is PH-equivalent to B^{op}, then B is Hermite-equivalent to B^{op}.

Dropping the assumption that $B \in \mathcal{NS}_{n,n-1}$, there are examples, even at size three, of $B \in \mathcal{NS}_n$ with B PH-equivalent to B^{op} but not being Hermite equivalent; the smallest d for which this occurs seems to be 5^3.

There are other situations that can occur, e.g., $r(B^{\mathrm{op}})$ is strictly contained in $r(B)$; examples with $\det B = p$ (a prime) are easy to obtain. Since $r(B)$ is then a maximal proper subgroup of $\mathbf{Z}^{1 \times n}$, there are only three possibilities: (i) B super-splits (this occurs when $r(B^{\mathrm{op}})$ not contained in $r(B)$), (ii) B^{op} is Hermite-equivalent to B^{op} (this arises when $r(B^{\mathrm{op}}) = r(B)$), or (iii) there exists noninvertible F such that $B^{\mathrm{op}} = FB$ (occurring when $r(B^{\mathrm{op}})$ is strictly contained in $r(B)$; then $|\det B^{\mathrm{op}}| = p^k$ for some $k > 1$). It is routine to construct examples illustrating each of these phenomena.

2. PH-equivalence for some terminal forms

We describe PH-equivalence between terminal forms of size n matrices, both of which have 1-block size $n - 1$. These are implemented via a partial action of the permutation group S_n.

Let $n, d > 1$ and consider all the terminal forms with 1-block size $n - 1$ and determinant d; that is, matrices of the form $B_a := \begin{pmatrix} I_{n-1} & a \\ 0 & d \end{pmatrix}$, where $a = (a_i)$ is in $\mathbf{Z}^{(n-1) \times 1}$ and satisfies $\gcd\{d, a_1, \ldots, a_{n-1}\} = 1$ and $0 \leq a_i < d$ for all i. Since we can add or subtract multiples of the bottom row to/from the others at any time in a sequence of PH-equivalences, we may regard the a_i as elements of $\mathbf{Z}_d$. If P is an $n \times n$ permutation matrix and $B \in \mathcal{NS}_n$ is in terminal form, then we say that P is *realizable over* B if there exists $U \in \mathrm{GL}(n, \mathbf{Z})$ such that UBP^{-1} is also in terminal form.

Proposition 2.1. *Let $d > 1$ be an integer. Let P be a permutation matrix of size n with corresponding permutation π, and let $a \in \mathbf{Z}^{(n-1) \times 1}$ be such that $\mathrm{cont}\{a, d\} = 1$. Then P is realizable over B_a with $B_{a'} = UB_aP^{-1}$ having 1-block of size $n-1$ if and only if either $\pi(n) = n$ or $a_{\pi(n)}$ is invertible modulo d. In the latter case, modulo d,*

$$a'_t \equiv \begin{cases} -a_{\pi(t)} a_{\pi(n)}^{-1} & \textit{if } t \neq \pi^{-1}(n), \\ a_{\pi(n)}^{-1} & \textit{if } t = \pi^{-1}(n). \end{cases}$$

Remark. It is important to emphasize that this result describes only PH-equivalence between terminal forms of NS_n-matrices, both of which have 1-block size $n-1$. It says only a limited amount about PH-equivalences between terminal forms only one of which has 1-block size $n-1$ (essentially, the statement that each permutation matrix P can contribute at most one new terminal form). In particular, if $\gcd\{a_i, d\} > 1$ for all i, then the only choices for P are those corresponding to S_{n-1}—in this context. Where we are allowed choices for terminal B' that have a smaller 1-block, we can obtain more realizable permutation matrices P.

Remark. For $n = 3$, this type of action of the symmetric group was discussed in [20]. When $n = 2$, B_a is PH-equivalent to $B_{a'}$ if and only if $aa' \equiv 1 \pmod{d}$; this can be shown directly, since only the transposition and identity matrices are involved.

Since the absolute value of the determinant (sometimes denoted *absolute determinant*) is a PH-invariant for matrices in $\mathcal{NS}$, we may fix the determinant, denoted $d > 0$; so the problem boils down to the column a. There is an obvious action of S_{n-1} on a, and this is implemented by left and right multiplication of B by the corresponding permutation matrix. Hence, at any time, we may assume that the entries of a are, for example, increasing. Alternatively, we can regard a merely as a list, thereby disregarding the action of S_{n-1}.

The equivalence relation on $(\mathbf{Z}_d)^{(n-1)\times 1}$ (that is, the columns a) induced by PH-equivalence between the corresponding B_a (with d fixed of course) is more complicated than that given merely by permutations.

First we describe a well-known action of S_n (not S_{n-1}) on A^{n-1}, where A is a finite abelian group; for convenience, A is written multiplicatively. The permutation representation of S_n on A^n admits the diagonal $\delta := \{(z, z, \ldots, z) \mid z \in A\}$ as a set of fixed points. Thus there is an action of S_n on the quotient group $A^n/\delta \cong A^{n-1}$. To see just what the resulting action is, pick $y = (a_i) \in A^{n-1}$ and lift it to an element of A^n by setting $y' = (y, 1)$ (since A is written multiplicatively, 1 means the identity element). Apply the permutation action of S_n to y'.

For $\pi \in S_n$, if π fixes the point n, then it comes from an element of S_{n-1}, so we just define $\pi(y)$ to be the first $n-1$ coordinates of y'. Otherwise, there exists $j < n$ such that $\pi(j) = n$, so that the last coordinate of $\pi(y')$ is a_j and a 1 appears in the $\pi(n)$-entry. Multiply the vector $\pi(y)$ by a_j^{-1}. Now the final entry is 1, so we can define $\pi(y)$ to be the first $n-1$-coordinates of $a_j^{-1}\pi(y')$. The multiplication operator is equivalent to performing the group action with the diagonal element $(a_j^{-1}, a_j^{-1}, \ldots, a_j^{-1})$ to $\pi(y')$, hence is compatible with the quotient action.

(Replacing n by $n+1$ and A by $\mathbf{Z}$—this time viewed additively—yields the Weyl group action of S_{n+1} on the dual of the maximal torus of $SU(n+1)$.)

Denote this action $\Pi_{A,n} : S_n \to \operatorname{Aut} A^{n-1}$. Now replace A by $\mathbf{Z}_d^*$, the group of (multiplicatively) invertible elements in $\mathbf{Z}_d$ (so $\phi(d) = |\mathbf{Z}_d^*|$). Suppose that $a \in (\mathbf{Z}_d)^{n-1}$ consists of elements relatively prime to d, that is, members of $\mathbf{Z}_d^*$.

Then we will see that the PH-equivalence class of B_a consists of a slightly twisted S_n-orbit of a under $\Pi_{\mathbf{Z}_d^*,n}$.

However, if some of the entries of a are zero divisors in the ring $\mathbf{Z}_d$, then the situation becomes a little more interesting. We may permute the entries so that the first k are invertible, and the rest are zero divisors. Then we can apply S_{k+1} to the column of the first k, obtaining (for each element of the group) an element a_j^{-1}—and instead of multiplying merely the top k entries by a_j^{-1}, we multiply all of a by it.

This of course preserves the entries that are zero divisors in the ring $\mathbf{Z}_d$, whose locations are unmoved. It also preserve the ideals the elements generate, e.g., there are the same number of zeros in the new element as in the original, the same number that are divisible by any prime p that divides d as in the original, etc.

The upshot is that there is no group structure (except when $n = 2$) on the set of equivalence classes, but instead the latter is a union of orbits of various groups.

For an integer $d > 1$, $\mathbf{Z}_d^*$ will denote the group of multiplicatively invertible elements in the *ring* $\mathbf{Z}_d$ (formerly, we just considered the latter as an additive group). If x is an integer relatively prime to d, then x^{-1} will denote a representative y such that $xy \equiv 1 \bmod d$.

Beginning of proof of Proposition 2.1. For $n > 2$, if each of the a_i is *not* relatively prime to d, then the equivalence class is simply the set of permutations of the entries, that is, via the action of S_{n-1}—in this case, there is an obvious normal form, with the entries of a arranged monotonically.

If a_i are all relatively prime to d, then the action is given by permutations and a twisted multiplication by each of the a_i^{-1} modulo d (it appears that these should generate a larger orbit—but this is not the case; for example, if all $a_i \equiv -1 \pmod{d}$, only elements of S_{n-1} can act non-trivially.) The orbit consists of $\{(-a_1 a_j^{-1}, \ldots, a_j^{-1}, \ldots, -a_{n-1} a_j^{-1})^T\}$ (j varying), together with the column (a_i) itself, and all their permutations.

To verify these claims, suppose $U B_a P = B_{a'}$. First, we note that if also $U_1 B_a P = B_{a''}$ (where B_a, $B_{a'}$, and $B_{a''}$ are all terminal) with the same P, then $B_{a'} = B_{a''}$. This follows from the equalities in $\mathrm{M}_n \mathbf{Q}$, $P = B_a^{-1} U^{-1} B_{a'} = B_a^{-1} U_1^{-1} B_{a''}$, whence $U^{-1} B_{a'} = U_1^{-1} B_{a''}$, so that $U_1 U^{-1} B_{a'} = B_{a''}$. Set $V = U_1 U^{-1} \in \mathrm{GL}(n, \mathbf{Z})$. From the form of the Bs (first $n-1$ columns are standard basis elements), $V = \left(\begin{smallmatrix} I_{n-1} & X \\ 0 & t \end{smallmatrix} \right)$; since the lower right entries of both Bs are d, $t = 1$, and we have $a' + dX = a''$; but this simply means that a and a' are coordinatewise congruent modulo d; since we have assumed the entries are in the interval $0 \leq a_i'', a_i' < d$, this forces $a' = a''$.

Thus for each permutation matrix P, there is a most one a' for which $U B_a P = B_{a'}$ for some $U \in \mathrm{GL}(n, \mathbf{Z})$ (and of course, there may be none).

Suppose that $B = \left(\begin{smallmatrix} I_{n-1} & a \\ 0 & d \end{smallmatrix} \right)$; its 1-block is size $n-1$. Let π be the permutation corresponding to the right action by P on columns (that is, if P takes the first column to the second, then $\pi(1) = 2$).

If $\pi(n) = n$, then $B' = PBP^{-1}$ is also in terminal form, since a has been replaced by Qa (a permutation of the entries of a), where $P = Q \oplus 1$. So in this case, all of S_{n-1} is realizable. Moreover, if P' is realizable over B and $P = Q \oplus 1$, then $P'P$ is also realizable, so that the realizable permutation matrices form a coset space over S_{n-1}. However, this is fairly complicated.

For $a \in \mathbf{Z}^{(n-1)\times 1}$ such that $\mathrm{cont}\{a, d\} = 1$, recall that $B_a = \left(\begin{smallmatrix} I_{n-1} & a \\ 0 & d \end{smallmatrix} \right)$. Proposition 2.1 determines precisely the permutation matrices P such that there exist $a' \in \mathbf{Z}^{(n-1)\times 1}$ such that B'_a satisfies $UB_a = B_{a'}P$ for some $U \in \mathrm{GL}(n, \mathbf{Z})$. This is not the full realizability problem, since P may be realizable over B, but the outcome, B', although in terminal form, need not have its 1-block of size $n-1$. (We have already seen such an example.)

Now suppose that $UB_a = B_{a'}P$ for some $U \in \mathrm{GL}(n, \mathbf{Z})$, and $\pi(n) \neq n$. Then the ith column of UB_a is Ue_i, except when $i = n$, in which case, it is $U\left(\begin{smallmatrix} a \\ d \end{smallmatrix} \right)$. On the other hand, the ith column of $B_{a'}P$ is the π^{-1}th column of $B_{a'}$, which is $e_{\pi^{-1}}$, unless $\pi(i) = n$, in which case it is $\left(\begin{smallmatrix} a' \\ d \end{smallmatrix} \right)$.

In particular,

$$Ue_i = \begin{cases} e_{\pi^{-1}(i)} & \text{if } i \notin \{n, \pi(n)\}, \\ \begin{pmatrix} a' \\ d \end{pmatrix} & \text{if } i = \pi(n), \end{cases}$$

$$U\begin{pmatrix} a \\ d \end{pmatrix} = e_{\pi(n)}.$$

We have that $n - 2$ of the columns of U are standard basis vectors and the $\pi(n)$th column is $\left(\begin{smallmatrix} a' \\ d \end{smallmatrix} \right)$; let $(h_j)^T$ be the nth column of U. The basic vectors represented in the columns exclude e_n and $e_{\pi(n)}$; hence in the $\pi(n)$ and nth rows of U, there are at most two nonzero entries, $a'_{\pi(n)}$ and $h_{\pi(n)}$, and d and h_n, respectively.

Now we can apply this to the third equation, and obtain (after sorting through the subscripts and cases)

$$a_{\pi(t)} + a'_t a_{\pi(n)} + h_t d = 0 \quad \text{if } t \neq n, \pi^{-1}(n),$$
$$a'_{\pi^{-1}(n)} a_{\pi(n)} + h_{\pi(n)} d = 1.$$

The second equation says that $a_{\pi(n)}$ is invertible modulo d, and $a'_{\pi^{-1}(n)} \equiv a_{\pi(n)} \bmod d$. Now that we know that $a_{\pi(n)}$ is invertible modulo d, the first equation yields the rest of what we want.

As to the converse, if $\pi(n) = n$, that is, $\pi \in S_{n-1}$, then π simply permutes the entries of the column a, and so the corresponding P is realizable.

If $\pi(n) \neq n$ and $a_{\pi(n)}$ (which is now defined) is invertible modulo d, define a' (modulo d) according to the formula in the statement of Proposition 2.1, and the corresponding matrix $B_{a'}$. Define $U := B_{a'}PB_a^{-1}$. Since B has determinant equalling that of P, to show $U \in \mathrm{GL}(n, \mathbf{Z})$, it suffices to show that the entries of U are integers. This is a straightforward computation.

We have $B_a^{-1} = \begin{pmatrix} I & -a/d \\ 0 & 1/d \end{pmatrix}$. It is easy to check that the first $n-1$ columns of U have only integer entries, and the last column of $B_{a'} P B_a^{-1}$ is the product

$$\begin{pmatrix} 1 & & & & & & a'_1 \\ & 1 & & & & & a'_2 \\ & & \ddots & & & & \vdots \\ & & & 1 & & & a'_{\pi^{-1}(n)} \\ & & & & \ddots & & \vdots \\ & & & & & \ddots & \vdots \\ & & & & & & d \end{pmatrix} \begin{pmatrix} -a_{\pi^{-1}(1)}/d \\ -a_{\pi^{-1}(2)}/d \\ \vdots \\ 1/d \\ \vdots \\ \vdots \\ -a_{\pi^{-1}(n)}/d \end{pmatrix}.$$

The $\pi^{-1}(n)$ entry of the column on the right is $1/d$; otherwise, the ith entry of the column is $-a_{\pi^{-1}(i)}/d$.

So that if $j \neq \pi(n)$, the jth entry of the product is $-(a'_j a_{\pi^{-1}(n)} + a_{\pi^{-1}(j)})/d$, which from the definition of a'_j is an integer. If $j = \pi(n)$, the corresponding entry is $(1 - a'_{\pi^{-1}(n)} a_{\pi^{-1}(n)})/d$, which is an integer. This concludes the proof of Proposition 2.1. $\qquad\square$

In particular, the number of i such that $\gcd\{a_i, d\} = 1$ is an invariant of this equivalence relation, as is for each prime p dividing d and each m, the number of a_i such that p^m divides a_i since up to permutation, we are multiplying the entries by an invertible modulo d, except in one place, where an invertible is replaced by another invertible. Both of these are also obtainable from $I(B_a)$ as in Lemma 1.2 above. Generically, the number of elements in the equivalence class of B_a is

$$(n-1)! \cdot |\{i \mid \gcd\{d, a_i\} = 1\}|,$$

but it could be less. Observe that if $a_i = a_j \in \mathbf{Z}_d^*$, on taking a permutation π such that $\pi(n) = i$, the corresponding a' is, up to permutation (that is, the S_{n-1}-action), obtained by multiplying all the entries by $-a_i^{-1}$ and replacing one of the -1 terms that result by a_i^{-1}; the same set, up to the S_{n-1} action, will arise from a permutation sending $n \mapsto j$. In this case, different permutations, even modulo S_{n-1} are realizable, but yield the same matrices.

Example 2.2. For $n = 2$, the only possible action is $a \mapsto a^{-1}$ (modulo d). In particular,

$$\begin{pmatrix} 1 & a \\ 0 & d \end{pmatrix} \text{ is PH-equivalent to } \begin{pmatrix} 1 & a' \\ 0 & d' \end{pmatrix}$$

if and only if $d = d'$ and either of $a' \equiv a^{\pm 1} \bmod d$.

The partial S_3-action allows us to conclude that

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 6 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 3 \\ 0 & 0 & 6 \end{pmatrix}$$

are not PH-equivalent. As they are respectively equivalent to

$$\begin{pmatrix} 1 & 1 & 2 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix},$$

the latter two are not PH-equivalent to each other either. All four matrices have $J(B) \cong \mathbf{Z}_6$.

If two matrices $B = \begin{pmatrix} I_{n-1} & a \\ 0 & d \end{pmatrix}, B' = \begin{pmatrix} I_{n-1} & a' \\ 0 & d' \end{pmatrix} \in \mathcal{NS}_{n,n-1}$ are in terminal form, then there is a relatively efficient procedure for deciding whether they are PH-equivalent. The absolute values of the determinants must be the same, d, and each has a list $[\![a]\!]$, $[\![a']\!]$ (consisting of the integers in the last column, above the d). There are only n cosets of S_n/S_{n-1}, and we just have to test those for which the corresponding element of $[\![a]\!]$ is relatively prime to d (testing for relative primeness of a_i and d requires at most $O(\ln a_i)$ steps, usually far fewer), and for each one of those, do the operation described in Proposition 2.1, and check whether the new list is that of a'. To make it more efficient, we may rearrange the lists as they appear so they are descending, etc. This amounts to sorting lists of nonnegative integers with a fixed upper bound, $d-1$, on the entries. An easy algorithm (good if $d \ll n$) is to decide for each $i = 0, 1, \ldots, n-1$, which of the numbers in $\{0, 1, 2, \ldots, d-1\}$ a_i is, and keep d running counts. The final counts determine the ordering.

If merely one of them has 1-block size $n-1$, then we first test whether B' does as well, by deleting the ith column and testing whether the resulting row space is all of the standard copy of $\mathbf{Z}^{n-1}$—one way is to take the n determinants of the submatrices of size $n-1$, and see if their greatest common divisor is one (it would be enough to show their greatest common divisor is relatively prime to the determinant of B'). If B' is already in terminal (or merely upper triangular) form, this will likely be very fast.

3. A FAMILY OF INVARIANTS

We will use *lattice* in the sense of partially ordered sets with least upper and greatest lower bounds.

In this section, we introduce and investigate a family of invariants for $\mathcal{NS}$, $\mathcal{J}(B)$, constituting a lattice of abelian groups with factor maps between them.

Recall, from Section 1, the definition of a list of elements (roughly, a set with multiplicities), denoted $[\![x_i]\!]$.

Fix n, and for $1 \le i \le n$, let $p_i : \mathbf{Z}^{1 \times n} \to \mathbf{Z}$ be the coordinate maps, and let $S = \{1, 2, \ldots, n\}$. Let $\Omega \subset 2^S$. For $B \in \mathcal{NS}_n$, define $B_\Omega \in \mathcal{NS}_{|\Omega|}$ (up to PH-equivalence) as follows. Delete from B the columns whose index is not in Ω (thus, if $1 \notin \Omega$, delete the first column of B) to create an $n \times |\Omega|$ matrix, each of whose columns has content one. The rank of the resulting matrix is exactly $|\Omega|$, since the set of columns of B was linearly independent over the rationals at the outset. By applying elementary (integer) row operations to B with columns deleted, we can obtain a matrix of the form $\begin{pmatrix} C \\ 0 \end{pmatrix}$, where C is $|\Omega| \times |\Omega|$. Since

elementary row operations preserve the content of columns, $C \in \mathcal{NS}_{|\Omega|}$. All choices for such C are Hermite- (and therefore PHermite-) equivalent (within $\mathcal{NS}_{|\Omega|}$). We choose one, and call it B_Ω.

An alternative approach (leading to the same thing) is to consider the PH-equivalence class of B as a means of studying the row space of B, $r(B) \subset \mathbf{Z}^n$, up to the restriction of the action of the permutation matrices acting on the right (that is, as column permutations). We delete the columns not corresponding to elements of Ω and take the row space of the resulting matrix, and use that to define $r(B_\Omega)$, without defining $B_\Omega(!)$.

If $\Omega = S$, then $B_\Omega = B$. If Ω consists of a singleton, then the resulting column, being unimodular, row-reduces to the first (or any) standard basis element of $\mathbf{Z}^{n \times 1}$, and thus $B_\Omega = (1)$, the size one identity matrix.

Define, for each $i = 1, 2, \ldots, n$, the subset $\Omega(i) = S \setminus \{i\}$.

If $\Omega' \subset \Omega$, let $P_{\Omega',\Omega} \colon \mathbf{Z}^{1 \times \Omega} \to \mathbf{Z}^{1 \times \Omega'}$ and $P_\Omega \colon \mathbf{Z}^{1 \times n} \to \mathbf{Z}^{1 \times \Omega}$ be the obvious projection maps (sometimes we will rewrite the last as $\mathbf{Z}^\Omega$). Then $P_\Omega(r(B)) = r(B_\Omega)$ (and similarly for $P_{\Omega',\Omega}$), thus inducing well-defined, onto group homomorphisms $p_\Omega \colon J(B) \to J(B_\Omega)$ and $p_{\Omega',\Omega} \colon J(B_\Omega) \to J(B_{\Omega'})$. It is routine to verify that the maps are transitive (that is, if $\Omega'' \subset \Omega' \subset \Omega$, then $p_{\Omega'',\Omega'} \circ p_{\Omega',\Omega} = p_{\Omega'',\Omega}$). In case there is ambiguity about which B they are referring to, we will occasionally use p_Ω^B.

The lattice of maps and quotient groups $p_{\Omega',\Omega} \colon J(B_\Omega) \to J(B_{\Omega'})$ will be denoted $\mathcal{J}(B)$. We say $\mathcal{J}(B) \cong \mathcal{J}(B')$ if there is an isomorphism $\phi \colon J(B) \to J(B')$ and a permutation π on S such that for all $\Omega \subset S$, $\phi(\ker p_\Omega^B) = \ker p_{\pi\Omega}^{B'}$. This yields isomorphisms induced by ϕ, $J(B_\Omega) \to J(B'_{\pi\Omega})$. In some cases, the permutation is uniquely determined by the list $[\![J(B_{\Omega(i)})]\!]$—this occurs when $J(B_{\Omega(i)})$ are mutually nonisomorphic for $i = 1, 2, \ldots, n$.

This results in a fairly strong invariant, as we will see later, but it is also somewhat more difficult to calculate (except in special cases), compared to the list $[\![J(B)_\Omega]\!]_{|\Omega|=n-1}$.

Lemma 3.1. *The lattice of finite abelian groups and homomomorphisms, $\mathcal{J}(B)$, is a PH-invariant for matrices B in $\mathcal{NS}_n$. If $k \leq n$, then the list $[\![J(B_\Omega)]\!]_{|\Omega|=k}$ is also a PH-invariant.*

Proof. Suppose that B and B' belong to $\mathcal{NS}_n$ and there is a PH-equivalence between them. Then we claim this implies that there exists a permutation of $S = \{1, 2, \ldots, n\}$, together with a compatible family of group isomorphisms $J(B_\Omega) \to J(B'_{\pi\Omega})$. This is trivial: if we apply an element of $\mathrm{GL}(n, \mathbf{Z})$, the row space is unchanged, and we obtain the identity maps. If we permute columns, π is the corresponding permutation, etc. We thus see that not only is $\mathcal{J}(B)$ a PH-equivalence, but so is the list of maps $J(B) \to J(B_\Omega)$, where we restrict the Ωs to have the same cardinality. $\square$

When we put $k = n - 1$, we obtain the list of n groups $[\![J(B_{\Omega(i)})]\!]$. This contains a lot of information (although generally less than that of $\mathcal{J}(B)$).

Originally, the $J(B_\Omega)$ groups were developed in order to find a finer invariant than $J(B^{\mathrm{op}})$: even together with $|\det B^{\mathrm{op}}|$ (another PH-invariant), $J(B)$ does not determine the family $\{J((B^{\mathrm{op}})_\Omega)\}$, or $\{J((B^{\mathrm{op}})_{\Omega(i)})\}$. More interestingly, those Ω for which $J(B_\Omega) = \{0\}$ play a particularly important role. For example, we will see there exists Ω of cardinality r such that $J(B_\Omega) = \{0\}$ if and only if B is PH-equivalent to a terminal form whose 1-block size is at least r. This is practically tautological, but provides a useful test for examples.

We also have a second family of PH-invariants, specifically, $\mathcal{J}(B^{\mathrm{op}})$. In general $(B_\Omega)^{\mathrm{op}}$ is not PH-equivalent to $(B^{\mathrm{op}})_\Omega$, nor need they yield isomorphic invariants. So we have to be careful with respect to the notation, that is, construct the opposite, B^{op}, first, then the cut-down matrices, $(B^{\mathrm{op}})_\Omega$. However, I could not decide whether $(J((B^{\mathrm{op}})_\Omega))_{\Omega \in 2^S}$ is determined by $(J(B_\Omega))_{\Omega \in 2^S}$, that is, whether for $B, B' \in \mathcal{NS}_n$ such that $(J(B_\Omega)) \cong (J(B'_\Omega))$ (as a family-meaning, does $\mathcal{J}(B) \cong \mathcal{J}(B')$ imply that $\mathcal{J}(B^{\mathrm{op}}) \cong \mathcal{J}(B'^{\mathrm{op}})$?). This, called the *duality conjecture*, is still open, and will be discussed in more detail in Section 6.

Recall that $r(B)$ frequently is used to denote $\mathbf{Z}^{1 \times n} B$, re-inforcing the idea that it is the subgroup of $\mathbf{Z}^{1 \times n}$ generated by the rows of B. The jth standard basis element of $\mathbf{Z}^{1 \times n}$ is denoted E_j.

Lemma 3.2. *Suppose that $B \in \mathcal{NS}_n$. Then $\ker p_\Omega$ is spanned by*

$$\{E_j + r(B)\}_{i \notin \Omega}.$$

Proof. Obviously, $P_\Omega(E_j)$ is zero if $j \notin E$, so that $E_j + r(B) \in \ker p_\Omega$ for all $j \notin \Omega$.

Suppose for $v \in \mathbf{Z}^n$ that $P_\Omega(v) \in r(B_\Omega)$. Then there exist $a_i \in \mathbf{Z}$ and corresponding rows r_i of B such that $P_\Omega(v) - \sum a_i P_\Omega(r_i) = 0$. Thus the only nonzero entries of $w := v - \sum a_i r_i$ can only appear in position j, where $j \notin \Omega$. We can thus write $w = \sum_{\Omega^c} b_j E_j$, and so $v \in r(B) + \sum_{\Omega^c} E_j \mathbf{Z}$. $\square$

Corollary 3.3. *If $\Omega' \subset \Omega$, then $\ker p_{\Omega', \Omega}$ is spanned by*

$$\left\{ E_j + r(B) + \sum_{i \in \Omega} E_i \mathbf{Z} \right\}_{j \in \Omega \setminus \Omega'}.$$

Proof. One inclusion is obvious; for the other, suppose that $p_{\Omega', \Omega}(v + \ker p_\Omega) = 0$. Then $p_{\Omega'}(v + r(B)) = 0$. Hence by the preceding, there exist integers a_i and b_j $(j \notin \Omega')$ such that $a - \sum a_i r_i = \sum_{j \in \Omega'^c} b_j E_j$. If $j \notin \Omega$, then $E_j + r(B) \in \ker p_\Omega$; thus the right side decomposes as $\sum_{j \in \Omega \setminus \Omega'} b_j E_j$ plus an element of $\ker p_\Omega$. $\square$

As a consequence, if $\Omega' \subset \Omega$ and $J(B_{\Omega'})$ is generated (as an abelian group, or as a $\mathbf{Z}_d$-module) by k elements, then $J(B_\Omega)$ has a generating set of cardinality at most $k + |\Omega| - |\Omega'|$.

As usual, S_n will denote the full permutation group on $S = \{1, 2, \ldots, n\}$; sometimes this will be identified with $\mathcal{P}_n$, the group of $n \times n$ permutation matrices.

Proposition 3.4. *Let B, B' belong to $\mathcal{NS}_n$. Necessary and sufficient for $\mathcal{J}(B) \cong \mathcal{J}(B')$ is the following:*

- *There exist $\pi \in S_n$ and an isomorphism $\phi\colon J(B) \to J(B')$ such that for all i, $\phi(\ker p^B_{\Omega(i)}) = \ker p^{B'}_{\Omega(\pi i)}$.*

Proof. Necessity is obvious, so let us prove sufficiency. Let d be exponent of $J(B)$ (which by the isomorphism, is also the exponent of $J(B')$). If P is the permutation matrix representing π^{-1}, then we can replace B' by $B'P$, and thus assume that π is the identity.

By the preceding characterization of $\ker p_\Omega$, for any i, we obtain

$$\phi(\langle E_i + r(B)\rangle) = \phi(\ker p^B_{\Omega(i)}) = \ker p^{B'}_{\Omega(i)} = \langle E_i + r(B')\rangle.$$

Hence, for any proper subset Ω, $\phi(\langle E_i + r(B)\rangle_{i \notin \Omega}) = \langle E_i + r(B')\rangle_{i \notin \Omega}$. By the preceding proposition, $\phi(\ker p^B_\Omega) = \ker p^{B'}_\Omega$. Then we define the map $\phi_\Omega\colon J(B_\Omega) \to J(B'_\Omega)$ in the obvious way

$$v + r(B) + \sum_{i \notin \Omega} E_i \mathbf{Z} \mapsto \phi\Big(v + r(B') + \sum_{i \notin \Omega} E_i \mathbf{Z}\Big);$$

this is well-defined by the preceding sentence, and is an isomorphism. Thus the following diagram commutes:

$$
\begin{array}{ccc}
J(B) & \xrightarrow{\phi} & J(B') \\
\downarrow{\scriptstyle p^B_\Omega} & & \downarrow{\scriptstyle p^{B'}_\Omega} \\
J(B_\Omega) & \xrightarrow{\phi_\Omega} & J(B'_\Omega).
\end{array}
$$

If $\Omega' \subset \Omega$, then from $P_{\Omega',\Omega} \circ P_\Omega = P_{\Omega'}$, the corresponding diagram with B_Ω replaced by $B_{\Omega'}$ and B replaced by B_Ω also commutes. Hence ϕ induces an isomorphism of lattices of quotient groups, $\mathcal{J}(B) \cong \mathcal{J}(B')$. $\square$

Corollary 3.5. *Suppose $B, B' \in \mathcal{NS}_n$ and $J(B)$ is cyclic. Sufficient for $\mathcal{J}(B) \cong \mathcal{J}(B')$ is that $J(B) \cong J(B')$ and there exist $\pi \in S_n$ such that for all Ω, $|J(B_\Omega)| = |J(B'_{\pi\Omega})|$.*

Proof. Any quotient of $J(B)$ (and therefore of $J(B')$ is cyclic and therefore their cardinality determines uniquely their isomorphism class (so that $J(B_\Omega) \cong J(B'_{\pi\Omega})$)) and the kernel (as cyclic groups have at most one subgroup of given cardinality). Now the preceding proposition applies. $\square$

Particularly useful are the $J(B_{\Omega(i)})$ (recall that $\Omega(i) = S \setminus \{i\}$, the subset of $\{1, 2, \ldots, n\}$ missing only i). Recall that $\mathcal{NS}_{n,m}$ consists of the elements $B \in \mathcal{NS}_n$ which have a terminal form with 1-block of size at least m.

A matrix $B \in \mathcal{NS}_n$ is *decomposable* if it is PH-equivalent to a direct sum of matrices in $\mathcal{NS}$, and *indecomposable* otherwise. It is *weakly indecomposable* if it is not PH-equivalent to a matrix of the form $1 \oplus C$, where $C \in \mathrm{M}_{n-1}\mathbf{Z}$ (if such a C exists, necessarily it would belong to $\mathcal{NS}_{n-1}$).

Lemma 3.6. *Suppose that $B \in \mathcal{NS}_n$.*

(a) *$B \in \mathcal{NS}_{n,m}$ if and only if there exists $\Omega \subset 2^S$ with $|\Omega| = m$ and $J(B_\Omega) = 0$.*

(b) *$B \in \mathcal{NS}_{n,n-1}$ if and only if there exists i such that $J(B_{\Omega(i)}) = 0$.*

(c) *B is weakly indecomposable if and only if for all $i = 1, 2, \ldots, n$, the kernel of $p_{\Omega(i)} \colon J(B) \to J(B_{\Omega(i)})$ is not zero.*

Proof. (a) If such an Ω exists, the set of Ω-truncated rows of B contain a **Z**-basis for $\mathbf{Z}^\Omega$; by rearranging the rows of B, we can assume that the top $|\Omega|$ rows of B, $(B_{(i)})_{i=1}^{|\Omega|}$, satisfy $(P_\Omega(B_{(i)}))$ is a basis for $\mathbf{Z}^\Omega$. By permuting the columns, we can also assume that $\Omega = \{1, 2, \ldots, |\Omega|\}$. Then the upper left $|\Omega| \times |\Omega|$ corner of the current B belongs to $\mathrm{GL}(|\Omega|, \mathbf{Z})$ (since the rows form a **Z**-basis for $\mathbf{Z}^\Omega$). Hence there exists $E \in \mathrm{GL}(n, \mathbf{Z})$ of the form $E = F \oplus I_{\Omega^c}$, with $F \in \mathrm{GL}(|\Omega|, \mathbf{Z})$ such that $EB = \left(\begin{smallmatrix} I_{|\Omega|} & X \\ Y & Z \end{smallmatrix}\right)$. The obvious row operations allow us to reduce to the case that $Y = 0$. Now we can apply the procedure of [22] to put Z itself in terminal form. There is nothing to prevent additional 1s from appearing along the main diagonal, so when we proceed to fix X (by applying row operations corresponding to the rows of the new Z) so that the $n \times n$ matrix is in terminal form, the identity block size may have become larger. The resulting matrix is a terminal form with 1-block size at least $|\Omega|$.

If B has a terminal form $C = \left(\begin{smallmatrix} I_{|\Omega|} & X \\ 0 & Z \end{smallmatrix}\right)$, then with $\Omega = \{1, 2, \ldots, |\Omega|\}$, we see that C_Ω consists of the first Ω standard basis elements as columns, hence $J(C_\Omega) = 0$. Since B is PH-equivalent to C, there exists Ω' (obtained from a permutation in S_n, hence of equal cardinality) such that $J(B_{\Omega'}) = 0$.

(b) Apply (a) to subsets consisting of $n - 1$ elements.

(c) If B is PH-equivalent to $1 \oplus C$, then $\ker p_{\Omega(1)}^C$ is spanned by the image of the standard basis element E_1; but this already belongs to $r(C)$, so the kernel is zero. Conversely, suppose $\ker p_{\Omega(i)}^B = 0$. Then $E_i \in r(B)$ (by 3.2 above); applying the obvious row operations to eliminate all the other nonzero entries in the ith column, and then rearranging the columns (moving the ith column to the first), we see that the resulting matrix is a direct sum. $\square$

Example 3.7. Matrices $B \in \mathcal{NS}_3$ ($\mathcal{NS}_4$) such that $J(B)$ is cyclic, but neither B nor B^{op} has a size two (respectively, three) 1-block terminal form.

(i) Let

$$B = \begin{pmatrix} 1 & 1 & 8 \\ 0 & 2 & 6 \\ 0 & 0 & 15 \end{pmatrix}, \quad \text{so } B^{-1} = \begin{pmatrix} 1 & -\frac{1}{2} & -\frac{1}{3} \\ 0 & -\frac{1}{2} & -\frac{1}{5} \\ 0 & 0 & \frac{1}{15} \end{pmatrix}.$$

As $\det B = 30$ is square-free, $\mathbf{Z}^3/\mathbf{Z}^3 B$ is cyclic. It is easy to check that the list of $J(B_{\Omega(i)})$ is $[\![\mathbf{Z}_5, \mathbf{Z}_3, \mathbf{Z}_2]\!]$; by Lemma 3.6 (b), B has no size two 1-block terminal forms.

From the inverse, we see that the $[\![m(i)]\!] = [\![6, 10, 15]\!]$ ($m(i)$ is the smallest positive integer multiplication by which makes the corresponding row integral),

and thus
$$B^{\mathrm{op}} = \begin{pmatrix} 6 & 0 & 0 \\ -3 & 5 & 0 \\ -2 & -2 & 1 \end{pmatrix}.$$

Thus $\det B^{\mathrm{op}} = 30$, so again $\mathbf{Z}^3/\mathbf{Z}^3 B^{\mathrm{op}} = \mathbf{Z}_{30}$. It is straightforward to verify that $[\![J((B^{\mathrm{op}})_{\Omega(i)})]\!]$ is $[\![\mathbf{Z}_5, \mathbf{Z}_3, \mathbf{Z}_2]\!]$ (again); since none of them are zero, B^{op} has no size two 1-block terminal forms.

(ii) A different type of example arises from decomposable matrices. Recall that $B \in \mathcal{NS}_n$ is *decomposable* if there exists a matrix $B' = A \oplus C \in \mathcal{NS}_n$ that is PH-equivalent to B (from the fact that $B' \in \mathcal{NS}_n$, it follows easily that both A and C belong to their corresponding $\mathcal{NS}_j$).

Set $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 3 \end{smallmatrix}\right)$ and $C = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 5 \end{smallmatrix}\right)$, and define $B = A \oplus C$. Each of A and C belong to $\mathcal{NS}_2$, so $B \in \mathcal{NS}_4$. Moreover, $B^{\mathrm{op}} = A^{\mathrm{op}} \oplus C^{\mathrm{op}}$, so $\det B = \det B^{\mathrm{op}} = 15$. The latter being square-free, both $J(B)$ and $J(B^{\mathrm{op}})$ are cyclic.

However, for any i, $J(B_{\Omega(i)})$ has a direct summand which is one of A or B (this is true for any direct sum); in this case, both A and B are not invertible, so $J(A)$ and $J(B)$ are both nonzero. Thus $J(B_{\Omega(i)})$ is not zero for any i, so $B \notin \mathcal{NS}_{4,3}$, and similarly, $B^{\mathrm{op}} \notin \mathcal{NS}_{4,3}$ by Lemma 3.6 (b).

Now we want to address the near-ubiquity of matrices some, but not all, of whose terminal forms have 1-block size $n-1$. A useful PH-equivalence tool (found in [1]) is that C and C' are PH-equivalent via the permutation matrix P or its inverse if and only if $C'PC^{-1}$ has only integer entries (to see this, observe that the determinant is up to sign $\det C'C^{-1}$, which has determinant ± 1, since C and C are PH-equivalent and thus have the same determinant up to sign). We use this frequently, without further comment.

The following is complementary to Lemma 1.8.

Theorem 3.8. *Let d be a positive integer and $n > 2$. Suppose that B belongs to $\mathcal{NS}_n \setminus \mathrm{GL}(n, \mathbf{Z})$, and set $d = |\det B|$. If every terminal form of B has 1-block size $n-1$, then d is a power of a prime.*

Proof. Let B denote the $n \times n$ integer matrix $\left(\begin{smallmatrix} I_{n-1} & a \\ 0 & d \end{smallmatrix}\right)$, with $d > 1$, where $a = (a_1, \ldots, a_{n-1})^T \in \mathbf{Z}^{(n-1) \times 1}$, and assume B is in terminal form. Thus $\mathrm{cont}\{a, d\} = 1$ and $0 \le a_i < d$.

Now let $n - 1 > r > 1$ be an integer, and $d_{r+1}, \ldots, d_n$ be integers exceeding 1 such that $d = \prod d_j$. Form the matrix $C = \left(\begin{smallmatrix} I_r & X \\ 0 & \mathrm{diag}(d_{r+1}, \ldots, d_n) \end{smallmatrix}\right)$; also assume that $C \in \mathcal{NS}$, so that the content of any column is one. Here $X \in \mathbf{Z}^{r \times (n-r)}$.

Let P be a permutation matrix. We want to establish conditions (in terms of all the variables) so that $UB = CP$ for some $U \in \mathrm{GL}(n, \mathbf{Z})$. Since $\det B \ne 0$, B^{-1} exists as an element of $\mathrm{M}_n\mathbf{Q}$, and so existence of such a U implies $CPB^{-1} \in \mathrm{M}_n\mathbf{Z}$; but this is also sufficient as $|\det CPB^{-1}| = 1$. As B^{-1} is particularly easy to calculate, the conditions are not difficult to obtain, and the argument is similar to that of Proposition 2.1.

Let π denote the permutation corresponding to the action of P on the right; that is, if right multiplication sends the ith column to the jth column, then

$\pi(i) = j$. We have (with zeros deleted)

$$U_0 := CPB^{-1}$$

$$= \frac{1}{d} \begin{pmatrix} I_r & & X & & \\ & d_{r+1} & & & \\ & & d_{r+2} & & \\ & & & \ddots & \\ & & & & d_n \end{pmatrix} P \begin{pmatrix} d & & & & -a_1 \\ & d & & & -a_2 \\ & & \ddots & & \vdots \\ & & & d & -a_{n-1} \\ & & & & 1 \end{pmatrix}.$$

Let $S_0 \subset \{1, 2, \ldots, n\}$ be the image of $\{1, 2, \ldots, r\}$ under π, and T its complement. First, we must have $n \in S_0$. If not, say $n = \pi(k)$ (with $k > r$), then the kth row of CP is just $(0\ 0\ 0 \cdots 0\ d_k)$. Thus the (k, n) entry of the product is d_k/d, which is not an integer. Thus $n \in S_0$.

We calculate the (k, n) entry of the product, where $k > r$; set $t = \pi(k)$. By the preceding, $t \neq n$. The kth row of CP is $d_k E_t$ (where E_i are the standard basis elements of $\mathbf{Z}^{1 \times n}$). Thus the (k, n) entry is $-d_k a_t/d$. We deduce the following:

    (1) for all $t \in T$, $d/d_{\pi^{-1}(t)}$ divides a_t.

Now we calculate the (l, n) entries of the product for $l \leq r$; the crucial case is $m = \pi^{-1}(n)$. The mth row of CP has 1 as its final entry, zeros in the entries corresponding to S_0, and various xs (entries of X, too complicated to establish a notation for) in the entries corresponding to T. Then the (m, n) entry of dU_0 is $-\sum_{t \in T} x_{m, \pi^{-1}(t)} a_t + 1$, so this expression is divisible by d. This yields

    (2) $\gcd\{\{a_t\}_{t \in T} \cup \{d\}\} = 1$.

It also yields a corresponding condition on the mth row of X.

If $l \neq m$, lth row of CP has a one in the $\pi(l) \neq n$ position and various xs located in coordinates corresponding to T (which does not include n). This yields that $-a_{\pi(l)} + \sum x_{l,t} a_t$ is divisible by d. So we obtain the additional (semi-) condition

    $(2^1/_2)$ every a_s (for $s \in S_0 \setminus \{n\}$) is an additive combination of $\{a_t\}_{t \in T}$ modulo d.

Suppose a is given, and we want to decide whether C and P exist so that with CPB^{-1} is an integer matrix. Then conditions (1), (2) are necessary, and $(2^1/_2)$ is a consequence of (2). Moreover, conditions (1) and (2) imply that the d_i must be mutually coprime (that is, $\gcd\{d_i, d_j\} = 1$ if $i \neq j$).

To see this, from (1), we may write $a_t = h_t(d/d_{\pi^{-1}(t)})$, which we can rewrite as a product of all the d_i with $d_{\pi^{-1}(t)}$ replaced by h_t. If p is a prime dividing both d_i and d_j (with $i \neq j$), then it obviously divides all the a_t, contradicting (2). We also see that each h_t is relatively prime to $d_{\pi^{-1}(t)}$ (for the same reason). The fact that B is reduced entails $h_t < d_{\pi^{-1}(t)}$ as well, although this does not seem useful.

Hence the d_i are mutually coprime. In particular, if d has exactly f distinct prime divisors, then $n - r \leq f$ (no prime can divide two of the d_i); when d is a power of single prime, this gives an alternative but much more tedious proof of

Lemma 1.8, that the 1-block size is constant on terminal forms PH-equivalent to B. This means that if we write $d = \prod p^{m(p)}$ in its prime decomposition, the only factorizations permitted here are those such that for all i, and all p dividing d, we must have either p does not divide d_i or $p^{m(p)}$ does, and in the latter case, p cannot divide the other d_j.

Now suppose that d and a, the partition $S_0 \dot{\bigcup} T$, etc. satisfy the necessary conditions (1) and (2) (and their consequences) with corresponding factorization and indexing $d = \prod_{i>r} d_i$. Then we can pick X ($r = |S|$ is already determined) and P so as to construct the corresponding C; this yields a terminal form for which the 1-block size is $r < n - 1$. $\square$

When $n = 2$, all terminal forms of noninvertible matrices in $\mathcal{NS}_2$ have size $n - 1 = 1$.

We also have the following sufficient conditions to have a terminal form with 1-block of size $n - 1$. With no work whatsoever, if $B \in \mathcal{NS}_n$ and $|\det B| = p$, a prime, then all terminal forms of B have 1-block size $n - 1$. On the other hand, if $\det B$ is a product of two distinct primes, then at least one of the terminal forms has 1-block size strictly less than $n - 1$, as follows from Proposition 3.8, and an explicit example with $n = 3$ is given just after the statement of Theorem 1.1.

Proposition 3.9. *Let $n \geq 3$. Suppose that $B \in \mathcal{NS}_n$, and let p, q be distinct primes.*

   (i) *If B is PH-indecomposable and $|\det B| = pq$, then $B \in \mathcal{NS}_{n,n-1}$.*

   (ii) *If B is PH-indecomposable, $|\det B| = p^r$, where $r \geq 1$, and $J(B)$ is cyclic, then $B \in \mathcal{NS}_{n,n-1}$.*

   (iii) *If $n = 3$, $J(B)$ is cyclic, and $|\det B| = p^a q^b$ for some $a, b \in \mathbf{N}$, then $B \in \mathcal{NS}_{3,2}$.*

Remark. These results do not contradict Theorem 3.8—here the conclusions are that at least one terminal form has 1-block size $n - 1$.

Proof. Suppose $n \geq 4$ and $|\det B| = pq$ (the case that $n = 3$ will follow from (c)). We may assume that B is in terminal form; if the form does not already have 1-block size $n - 1$, then its terminal form is $\begin{pmatrix} I_{n-1} & X \\ 0 & \text{diag}(p,q) \end{pmatrix}$ (up to possible transposition of the primes). Label the two columns of X, Y and Z. Each column consists of zeros and numbers between 1 and $p - 1$ (respectively, between 1 and $q - 1$). Set $S = \{j \mid Y_j \neq 0\}$ and $T = \{l \mid Z_l \neq 0\}$. If $S \cap T$ is empty, then up to a permutation of the indices, the terminal form is a direct sum of matrices, contradicting PH-indecomposability. Hence we may select $k \in S \cap T$. Then $J(B_{\Omega(j)})$ is a quotient of $\mathbf{Z}^2 / \langle (p,0), (0,q), (X_k, Y_k) \rangle$, and the relative primeness (Y_k to q, X_k to p) yields that this is zero. Hence $J(B_{\Omega(j)}) = 0$, so $B \in \mathcal{NS}_{n,n-1}$.

(ii) Write $B = \begin{pmatrix} I_{n-k} & X \\ 0 & \mathcal{D} \end{pmatrix}$ in terminal form, with $\mathcal{D}$ being $k \times k$ upper triangular and having nontrivial powers of p along its diagonal, the powers appearing in increasing order of size. Suppose $k > 1$ (if $k = 1$, then B already has 1-block size $n - 1$). The lower right 2×2 block is of the form $\begin{pmatrix} p^a & x \\ 0 & p^b \end{pmatrix}$, where $a \leq b$, and if $x \neq 0$, then $p^a \leq \gcd(p^b, x)$. In the latter case, p^a divides x.

Now the image of $E_n + r(B)$ (as an element of $J(B)$) is easily seen (from the upper triangular form) to be of order exactly p^b, and thus $z := p^{b-1}E_n + r(B)$ has order p. Similarly, $E_{n-1} + (x/p^a)E_n + r(B)$ has order exactly p^a in $J(B)$, and thus $y := p^{a-1}E_{n-1} + (x/p)E_n$ has order p as well.

Since $J(B)$ is cyclic, there is at most one subgroup of each order, and thus there exists v relatively prime to p such that $y - vz \in r(B)$. But this is impossible, as easily follows from the form of $\mathcal{D}$.

If instead, $x = 0$, then we set $y = E_{n-1}$, and deduce the same conclusion. Hence $k = 1$.

(iii) Suppose $n = 3$ and $\det B = p^r q^s$. Put B in terminal form; if it does not have a 1-block of size two, then

$$B = \begin{pmatrix} 1 & a & b \\ 0 & c & d \\ 0 & 0 & f \end{pmatrix},$$

where $(a, p) = 1$, $\text{cont}(b, d, f) = 1$, $cf = p^r q^s$, and $c \leq (d, f)$. We will show that $B_{\Omega(1)} = (0)$; this implies that $B \in \mathcal{NS}_{3,2}$. Sufficient is that $\text{cont}(ad - bc, cf, af) = 1$. Without loss of generality, we may relabel the primes so that $q | f$.

If $d = 0$, then $J(B) \cong \mathbf{Z}_c \oplus \mathbf{Z}_f$; the latter being cyclic entails that $(c, f) = 1$, which forces $c = p^r$, $d = q^s$. Then $(ad - bc, f) = (bp^r, q^s)$; since $p \neq q$, and $(b, q) = 1$, we have $(ad - bc, f) = 1$. Also, we have $\text{cont}(ad - bc, c, a) = \text{cont}(bp^r, p^r, a) = 1$, so $\text{cont}(ad - bc, cf, af) = 1$.

If $d \neq 0$, then $(d, f) \geq c > 1$. We may interchange p and q if necessary, and thus assume that $q | (d, f)$. If $q | c$ as well, then it is routine to see that $J(B)$ cannot be cyclic (since q would divide all the entries of $\begin{pmatrix} a & d \\ 0 & f \end{pmatrix}$). Hence $c = p^t$ for some $1 \leq t \leq r$. Since the content of the third column is one, we must have $(b, q) = 1$. Then $(ad - bc, q) = (bc, q) = 1$. It remains to show that if $p | f$, then $(ad - bc, p) = 1$.

If p does not divide d, then $(ad - bc, p) = (ad, p) = 1$.

Hence we may assume that $p | d$. Then p cannot divide f, as then it would divide all the entries of $\begin{pmatrix} a & d \\ 0 & f \end{pmatrix}$, which contradicts cyclicity of $J(B)$. Thus f can only be a power of q, so $c = p^r$ and $f = q^s$. Hence p does not divide f, and we are done. □

Example 3.7 (i) shows that (i) can fail if $|\det B|$ is a product of three distinct primes. If we try to generalize Theorem 3.8 (i) by insisting that $|\det B| = p^2 q$, B is PH-indecomposable and $J(B)$ cyclic, the result fails already at $n = 4$.

Example (Example 3.7 part two). PH-indecomposable $B \in \mathcal{NS}_4$ with cyclic $J(B)$ and $\det B = p^2 q$, but $B \notin \mathcal{NS}_{4,3}$.

Require $q < p$, and set

$$B = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & p \\ 0 & 0 & q & p \\ 0 & 0 & 0 & p^2 \end{pmatrix}.$$

Then $B \in \mathcal{NS}_4$ and is in terminal form. Since $\gcd(p,q) = 1$, there exists $U \in \mathrm{GL}(2, \mathbf{Z})$ such that $(q \ p)U = (1 \ 0)$, and since absolute values of the determinants are preserved, $\begin{pmatrix} q & p \\ 0 & p^2 \end{pmatrix} U = \begin{pmatrix} 1 & 0 \\ x & \pm p^2 q \end{pmatrix}$. It follows that $J(B)$ is cyclic of order $p^2 q$.

It is also routine to calculate $[\![B_{\Omega(i)}]\!] = [\![\mathbf{Z}_q, \mathbf{Z}_p, \mathbf{Z}_p, \mathbf{Z}_q]\!]$. Since none of them are zero, $B \notin \mathcal{NS}_{4,3}$ (Lemma 3.6 (b)). If B were equivalent to $A \oplus C$ and both A and C have determinants bigger than 1, then two of the four in the list would have to have direct summands isomorphic to $J(A)$ and the other two would have direct summands isomorphic to $J(B)$. This would force $J(A) \cong \mathbf{Z}_p$ and $J(B) \cong \mathbf{Z}_q$ (or vice versa), entailing $|\det B| = pq$, a contradiction. The only remaining possibility is that B is PH-equivalent to a matrix of the form $1 \oplus C$, where $C \in \mathcal{NS}_3$—but this is excluded by the fact that none of the kernels of $p_{\Omega(i)}$ are trivial (Lemma 3.6 (c)).   □

Now we can obtain some results about relations between $J(B)$ and $J(B^{\mathrm{op}})$. Let $\pi_B \colon J(\Delta) \to J(B)$ and $\pi_{B^{\mathrm{op}}} \colon J(\Delta) \to J(B^{\mathrm{op}})$ be the respective onto maps in the two short exact sequences; these are given by $v + r(\Delta) \mapsto v + r(B)$ and $v + r(\Delta) \mapsto J(B^{\mathrm{op}})$, respectively. Then $E_i + r(\Delta) \mapsto E_i + r(B)$ and to $E_i + r(B^{\mathrm{op}})$ (via $\pi_{B^{\mathrm{op}}}$). It follows from Lemma 3.1 that $\pi_B(\ker p_{\Omega(i)}^B) = \ker p_{\Omega(i)}^B$, and the same applies with B^{op} replacing B.

Lemma 3.10. *Let $B \in \mathcal{NS}_n$. For each i, $\ker p_{\Omega(i)}^B$ and $\ker p_{\Omega(i)}^{B^{\mathrm{op}}}$ are cyclic of order $m(i)$, the isomorphism $\ker p_{\Omega(i)}^\Delta \to \ker p_{\Omega(i)}^B$ being induced by the restriction of π_B; furthermore, $\ker p_{\Omega(i)}^B$, $\ker p_{\Omega(i)}^{B^{\mathrm{op}}}$, and $\mathbf{Z}_{m\mathbf{Z}} \cong \ker p_{\Omega(i)}^\Delta$ are isomorphic to each other.*

Proof. The results preceding *furthermore* are proved in the previous paragraph. Since π_B restricts to an onto map from $\ker p_\Omega^\Delta$ to $\ker p_{\Omega(i)}^B$, it suffices to show the map is one to one. If for some positive integer t, $tE_i + r(\Delta)$ maps to zero (under π_B), then $tE_i \in r(B)$, i.e., $tE_i = wB$ for some $w \in \mathbf{Z}^{1 \times n}$. From the original definition of $m(i)$, we must have $m(i)$ divides t. Hence the restriction of π_B is an isomorphism. The same applies with B^{op} replacing B.   □

Corollary 3.11. *Let $B \in \mathcal{NS}_n$. Then*

(a) $m(i) = |J(B)|/|J(B_{\Omega(i)})| = |J(B^{\mathrm{op}})|/|J((B^{\mathrm{op}})_{\Omega(i)})|$,

(b) $|\det B^{\mathrm{op}}| = \dfrac{|\det B|^{n-1}}{\prod_{i=1}^n |J(B_{\Omega(i)})|}$,

(c) $|J((B^{\mathrm{op}})_{\Omega(i)})| = \dfrac{|\det B|^{n-1}}{m(i) \cdot \prod_{i=1}^n |J(B_{\Omega(i)})|}$.

Proof. Part (a) is an immediate consequence of Lemma 3.10. For (b), we have $\prod_i (|J(B)|/|J(B_{\Omega(i)})|) = \prod m(i)$; the latter is $\det \Delta = |J(B)| \cdot |J(B^{\mathrm{op}})|$, and now we can solve for $|J(B^{\mathrm{op}})| = |\det B|$. Part (c) is a consequence of (a) and (b).   □

Corollary 3.11 (a) entails that $\Delta = \mathrm{diag}(|J(B)|/|J(B_{\Omega(i)})|)$, so is determined by $J(B)$ and the list $[\![J(B_{\Omega(i)})]\!]$—a fragment of $\mathcal{J}(B)$. However, it is difficult to see how to obtain the embedding (up to equivalence) $J(B) \to J(\Delta)$ from $\mathcal{J}(B)$.

Parts (b) and (c) imply that $|J(B^{\mathrm{op}})|$ and the $|J((B^{\mathrm{op}})_{\Omega(i)})|$ are determined by $|J(B)|$ and the $|J(B_{\Omega(i)})|$; see the discussion in Section 6 concerning the duality conjecture.

We note that there is more information available than the numbers $m(i) = |J(B)|/|J(B_{\Omega(i)})|$. Identify, as usual, $J(B)$ with $r(B^{\mathrm{op}})/r(\Delta)$. We define $\Delta_{\Omega(i)}$ to be the *square* matrix with ith row and column deleted, and of course, $J(\Delta_{\Omega(i)})$ is $\bigoplus_{j \neq i} \mathbf{Z}_{m(j)}$.

Corollary 3.12. *For each $i = 1, 2, \ldots, n$, there are short exact sequences $0 \to J(B) \to J(\Delta_{\Omega(i)}) \to J((B^{\mathrm{op}})_{\Omega(i)}) \to 0$ and $0 \to J(B^{\mathrm{op}}) \to J(\Delta_{\Omega(i)}) \to J(B_{\Omega(i)}) \to 0$.*

Proof. Let $\pi\colon J(\Delta) \to J(B^{\mathrm{op}})$ be the quotient map in the original short exact sequence. We have seen that π maps $\ker p^{\Delta}_{\Omega(i)}$ isomorphically onto $\ker p^{B^{\mathrm{op}}}_{\Omega(i)}$. This allows us to define $\overline{\pi}\colon J(\Delta_{\Omega(i)}) \to J((B^{\mathrm{op}})_{\Omega(i)})$, via π; explicitly, we have $v + r(\Delta) + E_i\mathbf{Z} \mapsto v + r(B^{\mathrm{op}}) + E_i\mathbf{Z}$.

Now consider $r(B^{\mathrm{op}})/r(\Delta)$, the kernel of π. We claim that $r(B^{\mathrm{op}}) \cap E_i\mathbf{Z} \subseteq r(\Delta)$. Pick $wB^{\mathrm{op}} = tE_i + v\Delta$; writing $\Delta = B^T B^{\mathrm{op}}$, we have $(w - vB^T)B^{\mathrm{op}} = tE_i\mathbf{Z}$. From the original definition of $m(i)$, we must have $m(i)$ divides t. Since $m(i)E_i \in r(\Delta)$, we have that $r(B)/r(\Delta)$ misses $\ker p^{\Delta}_{\Omega(i)}$. Thus the composed map $r(B^{\mathrm{op}})/r(\Delta) \to J(\Delta) \to J(\Delta_{\Omega(i)})$ is one to one, and clearly contained in the kernel of $\overline{\pi}$. Since $|r(B)/r(\Delta)| = |J(B^{\mathrm{op}})|$ and $|J(B^{\mathrm{op}})| \cdot |J(B)| = |\det \Delta|/m(i) = \det \Delta_{\Omega(i)}$, the sequence

$$0 \to r(B)/r(\Delta) \to J(\Delta_{\Omega(i)}) \to J(B^{\mathrm{op}})_{\Omega(i)} \to 0$$

must be exact.

The other sequence comes from interchanging B with B^{op}. $\qquad\square$

Let $\Omega \subset 2^S$ and $j \in \Omega$. There are natural onto homomorphisms $J(\Delta_{\Omega \setminus \{j\}}) \to J((B^{\mathrm{op}})_{\Omega})$ and $J(\Delta_{\Omega \setminus \{j\}}) \to J(B_{\Omega})$; but it is not clear how to relate their kernels to obvious invariants of B and B^{op}, respectively. It is also not clear (but likely true) that there are exact sequences $J(B_{\Omega(i)}) \to J(\Delta_{\Omega(i)}) \to J(B^{\mathrm{op}})$ or $J(B_{\Omega(i)}) \to J(\Delta_{\Omega(i,j)}) \to J(B^{\mathrm{op}})_{\Omega(j)}$ for all $i \neq j$.

4. Terminal forms with 1-blocks of size $n-1$

In this section, we deal with $B \in \mathcal{NS}_n$ having a terminal form with 1-block size $n-1$, that is, $B \in \mathcal{NS}_{n,n-1}$. Computations are relatively tractable, and lead to conjectures, for general B in $\mathcal{NS}_n$, that can be proved in our restricted case. We will see in subsequent sections that the density of $\mathcal{NS}_{n,n-1}$ in $\mathcal{NS}_n$ approaches approximately .845 as $n \to \infty$ (already at $n = 6$, the density exceeds .8), so that this special cases covers a large proportion of matrices.

Perhaps the most important reason for studying this special class is that it is easier to formulate and verify conjectures than in the general case. Proposition 1.7, and Corollaries 3.3 and 3.11 were obtained first for matrices in $\mathcal{NS}_{n,n-1}$, suggesting their validity in general. (Not all results extend in this fashion.)

Let $B = \left(\begin{smallmatrix} I_{n-1} & a \\ 0 & d \end{smallmatrix}\right)$, where $a = (a_1, a_2, \ldots, a_{n-1})^T \in \mathbf{Z}^{n-1}$, d is a positive integer exceeding one, $\mathrm{cont}(d, a) = 1$, and the entries of a are ordered so that $\gcd(d, a_i)$ are monotone decreasing. We call this a *standard form* for $C \in \mathcal{NS}_{n,n-1}$ if C is PH-equivalent to B in this form. There can be several standard forms for the same matrix.

Standard forms are terminal and every $C \in \mathcal{NS}_{n,n-1}$ is PH-equivalent to one in standard form. To arrange the latter, from the definition, there is a matrix of the form $B' = \left(\begin{smallmatrix} I_{n-1} & a' \\ 0 & d \end{smallmatrix}\right)$ PH-equivalent to C, which is almost in standard form, the only obstruction being that the entries of a' need not be ordered. However, we can conjugate B' by any permutation matrix of the form $Q = P \oplus (1)$ (where P is a permutation matrix of size $n-1$). Then $Q^{-1}B'Q$ is still in terminal form, but the a' entries have been permuted (according to the permutation induced by Q).

Proposition 4.1. *Suppose that $B = \left(\begin{smallmatrix} I_{n-1} & a \\ 0 & d \end{smallmatrix}\right) \in \mathcal{NS}_{n,n-1}$ is in standard form. Then*

$$
B^{\mathrm{op}} = \begin{pmatrix} & & \mathcal{D} & & 0_{n-1} \\ \frac{-a_1}{(d,a_1)} & \frac{-a_2}{(d,a_2)} & \cdots & \frac{-a_{n-1}}{(d,a_{n-1})} & 1 \end{pmatrix},
$$

and this is PH-equivalent to

$$
\begin{pmatrix} 1 & \frac{-a_1}{(d,a_1)} & \cdots & \frac{-a_{n-1}}{(d,a_{n-1})} \\ 0_{n-1} & & \mathcal{D} & \end{pmatrix},
$$

where $\mathcal{D} = \mathrm{diag}(d/(d, a_i)) \in M_{n-1}\mathbf{Z}$. The last matrix is in terminal form, and $m(i) = d/(d, a_i)$.

Proof. As $B^{-1} = \left(\begin{smallmatrix} I_{n-1} & -a/d \\ 0 & 1/d \end{smallmatrix}\right)$, we see that $m(i) = d/(d, a_i)$, and $B^{\mathrm{op}} = (\Delta B^{-1})^T$. Conjugating with the obvious cyclic permutation puts it into the indicated form. It is in terminal form, since $(d/(d, a_i))$ is increasing. $\square$

An immediate corollary follows, using the computations in Lemma 1.2.

Corollary 4.2. *Let $B = \left(\begin{smallmatrix} I_{n-1} & a \\ 0 & d \end{smallmatrix}\right)$ be in terminal form with $a = (a_1, \ldots, a_{n-1})^T$. Then*

  (i) *$J(B) \cong \mathbf{Z}_d$ and $J(B^{\mathrm{op}}) \cong \bigoplus_{i=1}^{n-1} \mathbf{Z}_{d/(a_i, d)}$,*
  (ii) *if $n \in \Omega$, then $J(B_\Omega) \cong \mathbf{Z}_{\gcd(d, \mathrm{cont}(a_i; i \in \Omega))}$, and if $n \notin \Omega$, $J(B_\Omega) = (0)$,*
  (iii) *if $n \in \Omega$, then $J((B^{\mathrm{op}})_\Omega) \cong \bigoplus_{i \in \Omega \setminus \{n\}} \mathbf{Z}_{d/(a_i, d)}$, and if $n \notin \Omega$, then $J(B^{\mathrm{op}})_\Omega$ is isomorphic to any quotient of $\bigoplus_{i \in \Omega \setminus \{n\}} \mathbf{Z}_{d/(a_i, d)}$ by a cyclic subgroup of order $\mathrm{lcm}\{d/(a_i, d) \mid i \in \Omega\}$.*

Proof. (i) Since $|\det B| = d$ and $J(B)$ is cyclic, $J(B) \cong \mathbf{Z}_d$. From Proposition 4.1, it follows that for each i, with $1 \leq i \leq n-1$, the element $E_i := (0 \cdots 0\ 1\ 0 \cdots 0)$ has order $d/(a_i, d)$ modulo $r(B^{\mathrm{op}})$, and the set of them is linearly independent.

(ii) After deleting the columns corresponding to the indices not in Ω, we reduce $r(B_\Omega)$ to the row space of $B' = \left(\begin{smallmatrix} I_k & a' \\ 0 & d \end{smallmatrix}\right)$, where $a' = (a_i)_{i \in \Omega}$ and $|\Omega| = k$. Now part (i) applies if $n \in \Omega$, whereas $J(B_\Omega)$ is trivially zero if $n \notin \Omega$.

Part (iii) is a routine computation. $\qquad\square$

Corollary 4.3. *Suppose $C \in \mathcal{NS}_{n,n-1}$ is PH-equivalent to B in standard form with determinant d. Then*

(i) *$J(B_\Omega) = 0$ if $n \notin \Omega$, and $J(B_\Omega) \cong \mathbf{Z}_{\text{cont}(\{a_i\}_{i \in \Omega} \cup \{d\})}$ otherwise,*

(ii) *$J(B^{\text{op}}) \cong \bigoplus \mathbf{Z}_{d/(d,a_i)}$; moreover, $J((B^{\text{op}})_\Omega) \cong \bigoplus_{i \in \Omega} \mathbf{Z}_{d/(d,a_i)}$ if $1 \in \Omega$, and $J((B^{\text{op}})_{\Omega(1)}) \cong J(B^{\text{op}})/A$, where A is cyclic of order d.*

Proof. All the computations easily follow from Corollary 4.2, together with $\text{Exp}\, J(B^{\text{op}}) = \text{Exp}\, J(B) = d$ (Proposition 1.7). $\qquad\square$

As a consequence of this and Corollary 3.5, for all $B \in \mathcal{NS}_{n,n-1}$, the lattice $\mathcal{J}(B)$ determines $\mathcal{J}(B^{\text{op}})$. Whether this is true for all $B \in \mathcal{NS}_n$ is unknown (this is the duality conjecture of Section 6).

A special case arises when all $J(B_{\Omega(i)})$ are zero. This implies $J(B_\Omega)$ is zero for all proper subsets Ω of S, and occurs if and only if $(a_i, d) = 1$ for all i. Other special cases will be addressed in section 5.

Corollary 4.4. *Suppose that $B \in \mathcal{NS}_n$ and $|\det B| = d$. Then $J(B_{\Omega(i)}) = 0$ for all i if and only if $B \in \mathcal{NS}_{n,n-1}$ and in one (or all) of its standard forms, all a_i are relatively prime to d. When this occurs, $J((B^{\text{op}})_\Omega) \cong \mathbf{Z}_d^{|\Omega|-1}$.*

Proof. Since one of $J(B_{\Omega(i)})$ is zero, $B \in \mathcal{NS}_{n,n-1}$, and so we can assume B is in standard form. Then (i) of the preceding, with $\Omega = \Omega(i)$, yields $(a_i, d) = 1$ for all i. The converse is trivial. The rest follows from Corollary 4.3 (ii). $\qquad\square$

Recall from Section 1 what it means for $B \in \mathcal{NS}_n$ to super-split.

Lemma 4.5. *Suppose $B = \left(\begin{smallmatrix} I_{n-1} & a \\ 0 & d \end{smallmatrix}\right) \in \mathcal{NS}_{n,n-1}$, where $a = (a_i)^T \in \mathbf{Z}^{1 \times (n-1)}$.*

(i) *Sufficient for B to super-split is that $1 + \sum a_i^2/(d, a_i)$ be relatively prime to d.*

(ii) *If all a_i are relatively prime to d, then the condition in (i) is also necessary for B to super-split.*

Remark. It is possible that the relative primeness conditions $(d, a_i) = 1$ of part (ii) are redundant.

Proof. Necessary and sufficient for $\mathbf{Z}^{1 \times n} B + \mathbf{Z}^{1 \times n} B^{\text{op}} = \mathbf{Z}^{1 \times n}$ is that the same hold modulo d, since $r(\Delta) \subseteq r(B) \cap r(B^{\text{op}})$. Necessary and sufficient for this to occur is that the set of all $n \times n$ determinants obtained from the $2n$ rows of $\left(\begin{smallmatrix} B \\ B^{\text{op}} \end{smallmatrix}\right)$ has content relatively prime to d. If we take the first $n-1$ rows of B and the bottom row of B^{op}, from Proposition 4.1, we obtain the matrix

$$C = \begin{pmatrix} & I_{n-1} & & a \\ -\frac{a_1}{(d,a_1)} & \cdots & -\frac{a_{n-1}}{(d,a_{n-1})} & 1 \end{pmatrix}.$$

The determinant of this is $1 + \sum a_i^2/(d, a_i)$. This yields (i).

When $(a_i, d) = 1$ for all i, modulo d, the only nonzero row of B^{op} is the bottom one, and it is simply $(-a^T, 1)$. Modulo d, the bottom row of B is zero—so the only combination of rows to give a nonzero determinant (modulo d) consists of the top $n-1$ rows of B with the bottom row of B^{op}, which is the matrix C. Super-splitting thus implies $(\det C, d) = 1$, proving (ii). $\qquad\square$

It is of interest to give criteria for both B and B^{op} to belong to $\mathcal{NS}_{n,n-1}$. These will be used when we determine when $\mathcal{J}(B) \cong \mathcal{J}(B^{\mathrm{op}})$ and the stronger property that B be PH-equivalent to B^{op}.

Corollary 4.6. *Let $B \in \mathcal{NS}_n$. The following are equivalent:*

(a) *$J(B)$ and $J(B^{\mathrm{op}})$ are cyclic,*
(b) *$\bigoplus \mathbf{Z}_{m(i)} \cong \mathbf{Z}_d^2$ for some $d > 1$.*

Proof. (a) implies (b). Set $d = \mathrm{Exp}\, J(B) = \mathrm{Exp}\, J(B^{\mathrm{op}})$; the groups being cyclic, they are cyclic of order d. By Corollary 1.13, the sequence $J(B) \to \bigoplus \mathbf{Z}_{m(i)} \to J(B^{\mathrm{op}})$ splits.

(b) implies (a). Since $\mathrm{Exp} \bigoplus \mathbf{Z}_{m(i)} = d$, we have $\mathrm{Exp}\, J(B) = \mathrm{Exp}\, J(B^{\mathrm{op}}) = d$. From $|\bigoplus \mathbf{Z}_{m(i)}| = |J(B)| \cdot |J(B^{\mathrm{op}})|$, as the exponent of a group is at most the order, we deduce $|J(B)| = |J(B^{\mathrm{op}})| = d$, since the exponents equal the order, the groups are cyclic. $\qquad\square$

The following is an obvious consequence of the preceding.

Corollary 4.7. *Suppose that $B \in \mathcal{NS}_{n,n-1}$ has determinant of absolute value d. Then the following are equivalent:*

(i) *$B^{\mathrm{op}} \in \mathcal{NS}_{n,n-1}$,*
(ii) *$J(B^{\mathrm{op}})$ is cyclic,*
(iii) *$|\det B^{\mathrm{op}}| = |\det B|$,*
(iv) *$\bigoplus \mathbf{Z}_{m(i)} \cong \mathbf{Z}_d^2$,*
(v) *in standard form, $\gcd(d/(d, a_i), d/(d, a_j)) = 1$ for all $i \neq j$.*

Remark. Any (and every) standard form will do in part (v).

5. Dual-conjugacy and dual-compatibility

In this section, we determine necessary and sufficient conditions on indecomposable $B \in \mathcal{NS}_{n,n-1}$ so that $\mathcal{J}(B) \cong \mathcal{J}(B^{\mathrm{op}})$ (as lattices of groups), or the stronger condition, that B is PH-equivalent to B^{op}. The latter requires a number-theoretic condition on the entries in a standard form.

An obvious way to obtain an example (decomposable) is to take $B = C \oplus C^{\mathrm{op}}$ (since, as is evident from Proposition 1.6 or otherwise, $(A \oplus A')^{\mathrm{op}} = A^{\mathrm{op}} \oplus (A')^{\mathrm{op}}$). To avoid such trivial examples, we recall notions of indecomposability, this time applied to subgroups of $\mathbf{Z}^{1 \times n}$, not just to matrices.

Let $H \subset \mathbf{Z}^n$ be a subgroup of H of full rank, and for which there exists no $m > 1$ such that $H \subset m\mathbf{Z}^n$ (this corresponds to the content one condition of all the columns in the corresponding matrix). As usual, let $S = \{1, 2, \ldots, n\}$. We say that $H \subset \mathbf{Z}^n$ is *decomposable* if there exists a proper subset $T \subset S$

such that $H = H_1 \oplus H_2$, where $H_1 \times \{0\} \subset \mathbf{Z}^T \times \{0\}$, $H_2 \subset \{0\} \times \mathbf{Z}^{S \setminus T}$, and neither H_1 nor H_2 is contained in any $m\mathbf{Z}^n$ for $m > 1$. As defined, this is clearly a PH-invariant property. If $H \subset \mathbf{Z}^n$ is not decomposable, then it is *indecomposable*.

If we translate this back to square matrices (with $H = r(B)$), then $B \in \mathcal{NS}_n$ is (PH)-indecomposable if and only if the corresponding subgroup is indecomposable. The same applies to weak indecomposability.

So we look for PH-indecomposable $B \in \mathcal{NS}_n$ such that either $\mathcal{J}(B) \cong \mathcal{J}(B^{\mathrm{op}})$ (B is *dual-compatible*) or B is PH-equivalent to B^{op} (B is *dual-conjugate*). With indecomposability and 1-block size $n - 1$, the first property is fairly drastic; the second property is even more restrictive.

We make a comment about the ordered n-tuple (not merely the list, with which we have been dealing up to now) $(J(B_{\Omega(i)})_{i=1}^n)$. Suppose $B, C \in \mathcal{NS}_n$, and B is PH-equivalent to C. Thus there exists a permutation matrix P and $U \in \mathrm{GL}(n, \mathbf{Z})$ such that $B = UCP$. Let π be the permutation induced by P, extended in the obvious way to subsets of S. We must have, for all Ω, $J(B_\Omega) = J((CP)_\Omega) = \mathbf{Z}^{\pi^{-1}\Omega}/\mathbf{Z}^{\pi^{-1}\Omega} C_{\pi^{-1}\Omega}$. If we specialize to $\Omega(i) := S \setminus \{i\}$, we have $J(B_{\Omega(i)}) \cong J(C_{\Omega(\pi^{-1}i)})$.

In particular, if $J(B_{\Omega(i)})$ are distinct (meaning mutually nonisomorphic), then π is uniquely determined, and thus P is uniquely determined—so we know exactly which P to use (this can also be extended to the permutation action on $\mathcal{J}(B)$, but we never use this), and thus if B is PH-equivalent to C, then the P is uniquely determined (by the $n - 1$-tuples of the abelian groups $(J(B_{\Omega(i)}))$ and $(J(C_{\Omega(i)}))$). Thus to show PH-equivalence, it is necessary and sufficient that CPB^{-1} have only integer entries.

In the special case that P must be the identity (that is, $J(B_{\Omega(i)}) \cong J(C_{\Omega(i)})$ for all i and the $J(B_{\Omega(i)})$ are pairwise nonisomorphic), then the test is merely that CB^{-1} have only integer entries.

Lemma 5.1. *Suppose $B, C \in \mathcal{NS}_n$ and the following conditions hold:*

    (a) *For all $i = 1, 2, \ldots, n$, $J(B_{\Omega(i)}) \cong J(C_{\Omega(i)})$.*
    (b) *The $J(B_{\Omega(i)})$ are pairwise nonisomorphic.*

Then B is PH-equivalent to C if and only if $CB^{-1} \in M_n\mathbf{Z}$ if and only if B is Hermite equivalent to C.

Remark. It can happen that (a) holds, but the conclusion does not. There are examples with $J(B_{\Omega(i)}) \cong \mathbf{Z}_{13}$ for all i, as is the case for $J(B^{\mathrm{op}})_{\Omega(i)}$), and B is PH-equivalent to B^{op}. However, in these examples, $B^{\mathrm{op}}B^{-1}$ is not an integer matrix, so B cannot be Hermite equivalent to B^{op}.

Proof. Suppose $B = ECP$, where $E \in \mathrm{GL}(n, \mathbf{Z})$ and P is a permutation matrix. Then the permutation corresponding to P, call it π, induces isomorphisms $J(B_{\Omega(i)}) \cong J(C_{\Omega(\pi^{-1}i)})$ directly from the equation. The two conditions (a) and (b) together force π to be the identity permutation, hence $P = \mathrm{I}$, and thus $B = EC$.

If B is PH-equivalent to C, then $|\det B| = |\det C|$, and thus $\det CB^{-1} = \pm 1$. Thus $CB^{-1} \in \mathrm{M}_n\mathbf{Z}$ entails that $CB^{-1} \in \mathrm{GL}(n, \mathbf{Z})$. □

Proposition 5.2. *Let B be a weakly indecomposable element of $\mathcal{NS}_{n,n-1}$, and let $|\det B| := d = \prod_{p \in U} p^{m(p)}$ be the prime factorization of the absolute determinant of B. Then B is dual-compatible (that is, $\mathcal{J}(B) \cong \mathcal{J}(B^{\mathrm{op}})$) if and only if the following holds:*

- *There exists a partition $U = \dot\bigcup_{i=1}^{n-1} T_i$, with $|T_i| \geq 1$ such that on defining $d(i) = \prod_{T_i} p^{m(p)}$, we have $J(B_{\Omega(i)}) \cong \mathbf{Z}_{d/d(i)}$, up to a permutation on the indices.*

Remark. In other words, B is PH-equivalent to

$$B' = \begin{pmatrix} I_{n-1} & a \\ 0 & d \end{pmatrix},$$

where $a = (a_1, \ldots, a_{n-1})^T$ satisfies $d(i) = d/(a_i, d)$; to see this, observe that $J(B'_{\Omega(i)}) = \mathbf{Z}_{(d,a_i)}$ for $i \leq n-1$. Of course, $J(B'_{\Omega(n)}) = (0)$.

Proof. We may assume that B is already in terminal form, and of the form $B = \begin{pmatrix} I_{n-1} & a \\ 0 & d \end{pmatrix}$, where $a = (a_1, \ldots, a_{n-1})^T$ and $\mathrm{cont}(a_1, \ldots, a_{n-1}; d) = 1$. We have already seen (Proposition 4.1) that $J(B_{\Omega(i)}) \cong \mathbf{Z}_{(d,a_i)}$ for $1 \leq i \leq n-1$, and $J(B_{\Omega(n)}) = (0)$.

By Proposition 4.1, we have that $\det B^{\mathrm{op}} = \prod d/(a_i, d)$ and $J((B^{\mathrm{op}})_{\Omega(i)}) = \bigoplus_{j \neq i} \mathbf{Z}_{d/(a_j, d)}$ for $1 \leq i \leq n-1$, and moreover, by Corollary 4.2, $J((B^{\mathrm{op}})_{\Omega(i)}) \cong \bigoplus \mathbf{Z}_{d/(a_j, d)}/\mathbf{Z}_{\mathrm{lcm}\{d/(a_i, d)\}}$. As $\mathcal{J}(B) \cong \mathcal{J}(B^{\mathrm{op}})$, we must have $d = \prod d/(a_i, d)$; since $J(B)$ is cyclic, so must $J(B^{\mathrm{op}})$ be; this forces $d/(a_j, d)$ to be pairwise relatively prime.

Let U be the set of prime divisors of d; the fact that $d/(a_j, d)$ are pairwise relatively prime and d is their product forces each $d(i) := d/(a_i, d)$ to be expressible as a product $d(i) = \prod_{T_i} p^{m(p)}$ for some partition $U = \dot\bigcup T_i$ of U. If any of the T_i were empty, we would obtain the corresponding $d_i = 1$, so that $(a_i, d) = d$; that $0 \leq a_i < d$ forces $a_i = 0$. But then B would be, up to a permutation, decomposable as $1 \oplus C$ for some $C \in \mathcal{NS}_{n-1}$, contradicting weak indecomposability. Hence $|T_i| \geq 1$. The rest of the necessity is straightforward.

Conversely, suppose that B satisfies the conditions. We may assume it is in terminal form, and the a_i satisfy $d = (a_i, d)d(i)$. Then it is easy to verify that $J(B_\Omega)$ and $J((B^{\mathrm{op}})_\Omega)$ are isomorphic, and the isomorphisms are compatible with the projections, $p_{\Omega, \Omega'}$. □

Theorem 5.3. *Let B be a weakly indecomposable dual-conjugate matrix in $\mathcal{NS}_{n,n-1}$ with $n \geq 3$. Then there exists a partition $U = \dot\bigcup_{i=1}^{n-1} T_i$, with $|T_i| \geq 1$, such that on defining $d(i) = \prod_{T_i} p^{m(p)}$ such that B is PH-conjugate to a matrix of the form*

$$B' = \begin{pmatrix} I_{n-1} & a \\ 0 & d \end{pmatrix},$$

where $a = (a_1, \ldots, a_{n-1})^T$ satisfies $d(i) = d/(a_i, d)$, and on writing $v_i = a_i/(a_i, d)$ (where $(v_i, d(i)) = 1$), we have

$$\sum v_i^2 \prod_{p \in T_i^c} p^{m(p)} \equiv -1 \mod d.$$

Conversely, any such B' is dual-conjugate, and B is Hermite-equivalent to B^{op}.

Remark. The congruence condition can be rewritten in simpler form, suitable for computing with. It imposes a strong condition on the possible determinants d for which such matrices exist.

Proof. By Proposition 5.2, we can assume B is already in the form described therein; with v_i defined as $a_i/(a_i, d)$, we have $a_i = v_i \prod_{T_i^c} p^{m(p)}$. We see that $J(B_{\Omega(i)}) = \mathbf{Z}_{(a_i,d)}$ for $1 \le i \le n-1$, and $J(B_{\Omega(n)}) = 0$. The set $\{\mathbf{Z}_{(a_i,d)}\} \cup \{(0)\}$ consists of n distinct elements (none of the a_i can be relatively prime to T, since the partition is nontrivial).

Now consider B^{op}; this is given in Proposition 4.1, and we have (if $i \neq n$) $J((B^{\mathrm{op}})_{\Omega(i)})$ is $\bigoplus_{j \neq i} \mathbf{Z}_{d_j}$; as the d_j are pairwise relatively prime, $J((B^{\mathrm{op}})_{\Omega(i)}) \cong \mathbf{Z}_{d/\prod_{j \neq i} d(j)} \cong \mathbf{Z}_{(a_i,d)} \neq (0)$. Now assume that B is dual-conjugate. Then $B^{\mathrm{op}} \in \mathcal{NS}_{n,n-1}$, so at least one of the collection $J(B^{\mathrm{op}})_{\Omega(j)})$ must equal zero; hence the corresponding j must equal n. In particular, we have $J(B_{\Omega(i)}) \cong J((B^{\mathrm{op}})_{\Omega(i)})$ for *all* $i = 1, 2, \ldots, n$.

As B is PH-equivalent to B^{op}, we may apply Lemma 5.1, and thus the only choice for permutation matrix P such that $B = EB^{\mathrm{op}}P$, with $E \in \mathrm{GL}(n, \mathbf{Z})$, is $P = \mathrm{I}$; in particular, B is Hermite-equivalent to B^{op}. Hence $B^{\mathrm{op}}B^{-1}$ is an integer matrix. But $B^{-1} = \left(\begin{smallmatrix} I_{n-1} & -a/d \\ 0 & 1/d \end{smallmatrix} \right)$, and the computation of $B^{\mathrm{op}}B^{-1}$ is particularly easy: the constraint that all the entries be integers is exactly the congruence condition, resulting from the (n, n) entry of the product.

The converse is obtained by reversing this argument; we can assume that $B = B'$. If the congruence condition holds, then $U := B^{\mathrm{op}}B^{-1}$ is an integer matrix; by Proposition 5.2, $|\det B| = |\det B^{\mathrm{op}}|$, and thus $|\det U| = 1$, and so B is Hermite-equivalent to B^{op}; this implies that B is dual-conjugate. $\square$

In the case of $n = 2$ (in the proof, we used $n \ge 3$ in order to obtain that none of the a_i could be zero—equivalently, divisible by d—so that the $J(B_{\Omega(i)})$ are distinct), the condition on $B = \left(\begin{smallmatrix} 1 & a \\ 0 & d \end{smallmatrix} \right)$ (this time, a is just an integer) is that $a^2 \equiv -1 \mod d$. Such an a will exist if and only if all odd primes dividing d are congruent to one modulo 4, and 4 does not divide d. For larger n, the situation is much more complicated.

For example, to obtain $B \in \mathcal{NS}_{n,n-1}$ that is weakly indecomposable, dual-conjugate and of determinant d, the partition condition requires that d have at least $n - 1$ distinct prime divisors (so that a nontrivial partition of U is possible). If d is a square (and has at least $n - 1$ distinct prime divisors), the pair (d, n) can be realized if and only if d is odd, and every prime divisor is congruent to one modulo four. But if $d/2$ is a square, the condition is more complicated: there should exist an odd prime p dividing d such that (the

Legendre symbol) $(\frac{-2}{p}) = 1$, and all primes q dividing d with $(\frac{-2}{q}) \neq 1$ must be congruent to 1 modulo 4. And if d is 2^k times a square for some $k \geq 2$, the pair cannot be realized at all.

The congruence relation in Theorem 5.3 can be rewritten in simpler form. Write $d = 2^{m(2)} \prod p^{m(p)}$. The Chinese remainder theorem implies solvability of the equation is equivalent to $v_i^2 \prod_{p \in T_i^c} p^{m(p)} \equiv -1 \bmod q^{m(q)}$ for every prime q in T_i, for all i; that is, the negative product is a square modulo $q^{m(q)}$. For odd q, we can replace $q^{m(q)}$ by q, and if $q = 2$, by 8 if $m(2) \geq 3$, and we can delete the condition if $m(q) = 2$. So the conditions for the existence of solutions to the equation boil down (after deleting the even powers of primes) to

$$\left(\frac{-1}{q}\right) \prod_{p \in T_i^c;\ \text{odd}\ m(p)} \left(\frac{p}{q}\right) = 1 \qquad\qquad \text{for all odd } q \in T_i, \text{ for all } i,$$

$$-\prod_{p \in T_i^c;\ \text{odd}\ m(p)} p \text{ is a square modulo } 2^{m(2)} \quad \text{if } 2 \in T_i.$$

If $m(2) = 0$ or 1, the last condition is vacuous; if $m(2) \geq 3$, the term $2^{m(2)}$ can be replaced by 8.

This imposes drastic conditions on the possible determinants of indecomposable dual-conjugate matrices. For example, if d is an odd square, then all the prime divisors of d must satisfy $(\frac{-1}{p}) = 1$, that is, $p \equiv 1 \pmod 4$, and if d is an even square, then there are no partitions possible, that is, there does not exist $B \in \mathcal{NS}_{n,n-1}$ such that $\det B = \pm d$ and B is PH-equivalent to B^{op}. In general, some partitions will work and others will not.

Things change if we ask for indecomposable dual-conjugate matrices in $\mathcal{NS}_n$ (note the switch from $\mathcal{NS}_{n,n-1}$ to $\mathcal{NS}_n$, and from weakly indecomposable to indecomposable; the latter is needed, because for any B in $\mathcal{NS}_n$, $B \oplus B^{\mathrm{op}}$ is trivially a dual-conjugate member of $\mathcal{NS}_{2n}$). For example, we can realize $(p^3, 3)$ for any odd prime p (not all of these are Hermite-equivalent to their opposite, unlike the situation in Theorem 5.3), while $(8, 3)$ is not realizable—but $(8, 4)$ is. Since in these examples U consists of a single prime, the situation is obviously quite different when we drop the requirement on the 1-block size.

6. Duality?

Now we refer to definitions and results in Appendix A. We discuss what we have called the duality conjecture (briefly, whether $\mathcal{J}(B) \cong \mathcal{J}(B')$ implies $\mathcal{J}(B^{\mathrm{op}}) \cong \mathcal{J}((B')^{\mathrm{op}})$), and prove it for a class of matrices for which $J(B_\Omega)$ depends only on $|\Omega|$.

Let $n > k$, let d be an integer, and let X be an $(n-k) \times k$ matrix with integer entries between 0 and $d-1$ inclusive; assume that the content of each column of X is relatively prime to d. Form the matrices (as X varies),

$$B(X) = \begin{pmatrix} I_{n-k} & X \\ 0 & dI_k \end{pmatrix}.$$

Each of these is in terminal form. Obviously, we have $J(B(X)) \cong \mathbf{Z}_d^k$, and $\operatorname{Exp} J(B(X)) = d$. So we can regard $J(B(X))_\Omega$ as $\mathbf{Z}_d$-modules. It is easy to calculate $J(B(X_{\Omega(i)}))$. If every row of X has content relatively prime to d (a reasonable assumption), then $J(B(X))_{\Omega(i)} \cong \mathbf{Z}_d^{k-1}$ for every i. If we further assume for all $j \leq k$ that every $j \times j$ submatrix of X has nonzero determinant which is relatively prime to d (in particular, all entries of X are units modulo d), then $J(B(X)_\Omega) \cong \mathbf{Z}_d^{|\Omega|-1}$. This is equivalent to the matrix $\binom{X}{I_k}$ belonging to $F_{\binom{n}{k}}(n, k)$, if we regard the entries of X as belonging to $\mathbf{Z}_d$ (see the comment between Propositions A.5 and A.6 in Appendix A).

In these cases, the lists $[\![J(B(X))_\Omega]\!]_{|\Omega|=j}$ are largely useless for distinguishing $\mathcal{J}(B(X))$ from $\mathcal{J}(B(X'))$. We can say when $\mathcal{J}(B(X)) \cong \mathcal{J}(B(X'))$, however, by appealing to the orbit spaces under the actions of $W(n) \times \operatorname{GL}(k, \mathbf{Z}_d)$, as discussed in Appendix A.

We make a minimal assumption on the X: they have no zero rows (modulo d). This is equivalent to $B(X)$ being weakly indecomposable, and entails that $\ker p_{\Omega(i)}$ is nonzero (Lemma 3.6). Set $M(X) := \binom{-X}{I_k}$, regarded as an element of $\mathbf{Z}_d^{n \times k}$. Let $W(n)$ denote (as in Appendix A) the group of $n \times n$ weighted permutation matrices (nonzero entries are invertible elements of $\mathbf{Z}_d$). Then $W(n) \times \operatorname{GL}(k, \mathbf{Z}_d)$ acts on $\mathbf{Z}_d^{n \times k}$ ($W(n)$ from the left, $\operatorname{GL}(k, \mathbf{Z}_d)$ from the right). Define

$$\mathcal{X} = \left\{ X \in \mathbf{Z}^{(n-k) \times k} \;\middle|\; \begin{array}{l} 0 \leq X_{ij} \leq d-1, \\ \text{all columns of } X \text{ have content prime to } d, \\ \text{all rows are nonzero modulo } d \end{array} \right\}$$

Proposition 6.1. *Suppose that $X, X' \in \mathcal{X}$. Then $\mathcal{J}(B(X)) \cong \mathcal{J}(B(X'))$ if and only if $M(X)$ is in the same orbit as $M(X')$ under the action of $W(n) \times \operatorname{GL}(k, \mathbf{Z}_d)$.*

Proof. For each of X and X', define an explicit isomorphism $J(B(X)) \to \mathbf{Z}_d^k = \mathbf{Z}_d \times \mathbf{Z}_d \times \cdots \times \mathbf{Z}_d$ (with k copies of $\mathbf{Z}_d$), sending (for $j = 1, \ldots, k$) $E_{n-k+j} + r(B(X))$ to $e_j := (0, \ldots, 0, 1, 0, \ldots, 0)$, the 1 appearing in the jth position (and similarly with X'). Since the kernel of $J(B(X)) \to J(B(X)_{\Omega(i)})$ is generated by $E_i + r(B(X))$ (here $i \in \{1, 2, \ldots, n\}$), and this has order d (as $X, X' \in \mathcal{X}$), we can identify the kernels with the following subgroups of $\mathbf{Z}_d^k$: for $i \leq n-k$, $\langle -r_i(X) \rangle$ (the subgroup generated by the ith row of X, viewed as an element of $\mathbf{Z}_d^k$), since $E_i + (0^{n-k}, r_i(X)) \in r(B(X))$; and for $i > n - k$, $\langle e_{i-(n-k)} \rangle$.

Putting the generators into an $n \times (n-k)$ column with entries in $\mathbf{Z}_p$, we obtain the matrix $M(X) = \binom{-X}{I_k}$.

Now $\operatorname{Aut} J(B(X)) = \operatorname{GL}(k, \mathbf{Z}_d)$, and we have the natural action of $W(n) \times \operatorname{GL}(k, \mathbf{Z}_d)$ on $\mathbf{Z}_d^{n \times k}$ (corresponding to $F(n, k)$ in Appendix A). If two points, $M(X)$ and $M(X')$, are in the same orbit, then there exists an automorphism $\psi \colon J(B(X)) \to J(B(X'))$ such that the subgroups match, that is, there exists a permutation π such that $\psi(\langle E_i + r(B(X)) \rangle) = \langle E_{\pi i} + r(B(X)) \rangle$. This is exactly

the condition, $\psi(\ker p_{\Omega(i)}^{B(X)}) = \ker p_{\Omega(\pi i)}^{B(X')}$, discussed in Proposition 3.4. Hence $M(X)$ being in the same orbit as $M(X')$ implies that $\mathcal{J}(B(X)) \cong \mathcal{J}(B(X'))$.

Conversely, if $\mathcal{J}(B(X)) \cong \mathcal{J}(B(X'))$, then there exists an isomorphism $\phi\colon J(B(X)) \to J(B(X'))$ sending the factor groups, $J(B(X)_\Omega)$, to their counterparts $J(B(X')_{\pi\Omega})$ by means of the kernels, that is, $\phi(\ker p_\Omega) = \ker p_{\pi\Omega}^{B(X')}$. Identifying $J(B(X))$ and $J(B(X'))$ with $\mathbf{Z}_d^k$ as in the first paragraph of this argument, ϕ acts as an element of $\mathrm{GL}(k, \mathbf{Z}_d)$, and the weighted permutation matrix comes from π and the units of $\mathbf{Z}_d$ required to send one generator of the same subgroup to another one. $\qquad\square$

For example, suppose $d = p$, a prime, $n = 5$, and $k = 2$. Form $F_{10}(5, 2)$ over $\mathbf{Z}_p$. The condition that $M(X)$ belongs to this is simply that every entry of X is relatively prime to p and all pairs of rows of X are linearly independent modulo p (that is, every entry of X, and every one of the three 2×2 determinants arising from pairs of rows of X is a unit of $\mathbf{Z}_p$). From Appendix A, when $p = 5$ or 7, there is only a single orbit (that is, $W(5) \times \mathrm{GL}(2, \mathbf{Z}_p)$ acts transitively on $F_{10}(5, 2)$), whereas when $p > 7$, the action is not transitive. In the former case, $M(X), M(X') \in F_{10}(5, 2)$ implies $\mathcal{J}(B(X)) \cong \mathcal{J}(B(X'))$; but in the latter ($p > 7$), we can choose $M(X), M(X')$ in different orbits, and then $\mathcal{J}(B(X)) \ncong \mathcal{J}(B(X'))$.

From the earlier comments, $M(X) \in F_{10}(5, 2)$ implies $J(B(X)_\Omega) \cong \mathbf{Z}_p^{|\Omega|-3}$ for all Ω, i.e., $J(B(X)_\Omega)$ depends only on $|\Omega|$. If we put $p = 11$, the presence of more than one orbit yields an example of two matrices B and B' with the property that $J(B)_\Omega \cong J(B')_\Omega$ for all Ω, but $\mathcal{J}(B) \ncong \mathcal{J}(B')$.

Duality. We state the duality conjecture.

Duality Conjecture. Suppose $B, B' \in \mathcal{NS}_n$ and $\mathcal{J}(B) \cong \mathcal{J}(B')$. Then $\mathcal{J}(B^{\mathrm{op}}) \cong \mathcal{J}((B')^{\mathrm{op}})$.

This is known if $J(B)$ is cyclic, or if either of B or B^{op} belongs to $\mathcal{NS}_{n,n-1}$ (Corollary 3.5). The conjecture is also true when both $B = B(X)$ and $B' = B(X')$ above, as we will show. We will put the conjecture in the form of a possible generalization of the dualities established in Appendix A. There is also a stronger form.

Constructive Duality Question. Determine $\mathcal{J}(B^{\mathrm{op}})$ from $\mathcal{J}(B)$.

A small step in this direction appears in Corollary 3.11: Δ, $\det B^{\mathrm{op}}$, and $\{|J((B^{\mathrm{op}})_{\Omega(i)})|\}$ are determined from $\det B$ and $\{|J(B_{\Omega(i)})|\}$.

Lemma 6.2. *Suppose that $B = B(X)$ and $B' = B(X')$, where $X, X' \in \mathcal{X}$. Then $\mathcal{J}(B(X)) \cong \mathcal{J}(B(X'))$ implies that $\mathcal{J}(B(X)^{\mathrm{op}}) \cong \mathcal{J}(B(X')^{\mathrm{op}})$.*

Remark. So the duality conjecture holds for this class of matrices.

Proof. We have $B^{-1} = \left(\begin{smallmatrix} \mathrm{I}_{n-k} & -X/d \\ 0 & \mathrm{I}_k/d \end{smallmatrix}\right)$. As all rows of X have content relatively prime to d, it follows that $\Delta = d\mathrm{I}$, and thus $B^{\mathrm{op}} = \left(\begin{smallmatrix} d\mathrm{I}_{n-k} & 0 \\ -X^T & \mathrm{I}_k \end{smallmatrix}\right)$. It is not in terminal form, but this does not matter. We wish to verify the duality conjecture for a subclass of these matrices.

First, $J(B^{\mathrm{op}}) \cong \mathbf{Z}_d^{n-k}$; this follows from the short exact sequence $0 \to J(B) \to \mathbf{Z}_d^n \to J(B^{\mathrm{op}}) \to 0$; here the middle term is $\mathbf{Z}^n/d\mathbf{Z}^n$, since $\Delta = d\mathrm{I}_n$. Its automorphism group is thus $\mathrm{GL}(n-k, \mathbf{Z}_d)$. Identifying the kernels of $p_{\Omega(i)}^{B^{\mathrm{op}}}$ with the rows of X^T, we form the analogue of $M(X)$, that is, $N(X) = \left(\begin{smallmatrix} \mathrm{I}_{n-k} \\ X^T \end{smallmatrix} \right)$.

Then $M(X)^T N(X) = 0$, and it easily follows (see Appendix A) that the map ϕ defined therein sends $[M(X)] \to [N(X)]$. We do the same thing for $M(X')$ and $N(X')$, and then we have the following sequence of implications (the middle one from Theorem A.6):

$$\mathcal{J}(B) \cong \mathcal{J}(B') \implies M(X), M(X') \text{ are in the same orbit}$$
$$\implies N(X), N(X') \text{ are in the same orbit}$$
$$\implies \mathcal{J}(B^{\mathrm{op}}) \cong \mathcal{J}((B')^{\mathrm{op}}). \qquad \square$$

In general, the duality conjecture can be rephrased so that it vaguely resembles the results in Appendix A. Let $B \in \mathcal{NS}_n$ and define $d = \mathrm{Exp}\, J(B) = \mathrm{Exp}\, J(B')$ (Proposition 1.7); we view $J(B)$ and $J(B^{\mathrm{op}})$ as $\mathbf{Z}_d$-modules. Let $E = \mathrm{End}\, J(B)$ and $E^o = \mathrm{End}\, J(B^{\mathrm{op}})$. Then $\mathrm{Aut}\, J(B)$ is just the group of units of E, and $\mathrm{Aut}\, J(B^{\mathrm{op}})$ is the group of units of E^o.

The centres of E and E^o are both $\mathbf{Z}_d$ (this is true for the endomorphism ring of any finite abelian group with exponent d). Pick a representative for a generator of each of $\ker p_{\Omega(i)}^B$, and form them into a column of size n, that is, an element of $J(B)^n$. Let $\mathcal{P}_n$ be the group of permutations of n-element sets, define $\mathcal{D}_n$ to be the diagonal matrices with entries from $\mathbf{Z}_d^\times$, and define $W(n)$ to be $\mathcal{P}_n \mathcal{D}_n$. Then we view $J(B)^n$ as a set with the obvious $W(n) \times \mathrm{Aut}\, J(B)$ action. We do the same with B^{op}. Then the duality conjecture boils down to a bijection between these orbit spaces.

In the $B(X)$ examples, the corresponding rings E and E^o are just $\mathrm{M}_k \mathbf{Z}_d$ and $\mathrm{M}_{n-k} \mathbf{Z}_d$, and in particular, they are Morita equivalent; moreover, $J(B)$ and $J(B^{\mathrm{op}})$ are free $\mathbf{Z}_d$-modules. In general, E and E^o are not Morita equivalent and neither $J(B)$ nor $J(B^{\mathrm{op}})$ need be free $\mathbf{Z}_d$-modules.

In addition, the condition on the elements of the column, that they generate a cyclic subgroup corresponding to a $\ker p_{\Omega(i)}$ is somewhat restrictive. For example, if $n = 3$ and $J(B) \cong \mathbf{Z}_{p^2} \oplus \mathbf{Z}_p$ (lots of such examples exist), then $J(B_{\Omega(i)})$ must be cyclic (by Lemma 3.2 and Corollary 3.3). Hence we must rule out $p\mathbf{Z}_{p^2} \oplus 0$ as a subgroup appearing as $\ker p_{\Omega(i)}$, hence $(p, 0)$ cannot appear as an entry in the column.

Perhaps the key feature of the $B(X)$ matrices is that both $J(B(X))$ and $J(B(X)^{\mathrm{op}})$ are free $\mathbf{Z}_d$-modules, and thus E is Morita equivalent to E'. In addition, their ranks add up to exactly the right number, in order that the duality of Appendix A can be applied; this is a consequence of $\Delta = d\mathrm{I}$.

A bilinear function. The identification of $J(B)$ and $J(B^{\mathrm{op}})$ with subgroups of $J(\Delta) := \mathbf{Z}^{1 \times n}/r(\Delta)$ leads to a bilinear function, potentially useful for the duality conjecture.

Let $B \in \mathcal{NS}_n$, form B^{op}, and as usual, let $d = \mathrm{Exp}\, J(B) = \mathrm{lcm}\{m(i)\}$, and $\Delta = \mathrm{diag}(m(i))$. Then $d\Delta^{-1}$ is an integer matrix, and we define the bilinear

function $\mathbf{Z}^{1\times n} \times \mathbf{Z}^{1\times n} \to \mathbf{Z}$ by $\langle\!\langle v, w \rangle\!\rangle = vd\Delta^{-1}w^T$. This clearly induces a faithful bilinear function

$$\frac{\mathbf{Z}^{1\times n}}{\mathbf{Z}^{1\times n}\Delta} \times \frac{\mathbf{Z}^{1\times n}}{\mathbf{Z}^{1\times n}\Delta} \to \mathbf{Z}_d, \quad (\overline{v}, \overline{w}) \mapsto \langle\!\langle \overline{v}, \overline{w} \rangle\!\rangle_d \coloneqq vd\Delta^{-1}w^T \pmod{d}$$

(overlines indicate equivalence classes modulo $r(\Delta)$).

Recall from the discussion at the end of Section 1, the two subgroups of $J(\Delta)$, given by $Y(B) \coloneqq r(B^{\mathrm{op}})/r(\Delta) \cong J(B)$ and $Y(B^{\mathrm{op}}) \coloneqq r(B)/r(\Delta) \cong J(B^{\mathrm{op}})$. These are the images of $J(B)$ and $J(B^{\mathrm{op}})$ in the two short exact sequences discussed therein.

Now we note that $Y(B)$ and $Y(B^{\mathrm{op}})$ are dual with respect to the bilinear form (even if they are equal, as could well be the case, e.g., if B is Hermite-equivalent to B^{op}, examples appear in Theorem 5.3). Specifically, if $\langle\!\langle \overline{xB}, \overline{y} \rangle\!\rangle_d = 0$ for all x, then $\overline{y} \in Y(B^{\mathrm{op}}) = r(B)/r(\Delta)$. To see this, we have $xBd\Delta^{-1}y^T \in d\mathbf{Z}$ for all x; then $B\Delta^{-1}y^T$ has only integer coefficients. Replacing Δ^{-1} by $B^{-1}((B^{\mathrm{op}})^T)^{-1}$, we see that $((B^{\mathrm{op}})^T)^{-1}y^T$ has only integer coefficients; applying the transpose, it follows that $y(B^{\mathrm{op}})^{-1}$ has integer coefficients, and thus $y \in r(B^{\mathrm{op}})$. The reverse inclusion is trivial. So the dual of $Y(B^{\mathrm{op}})$ is $Y(B)$ with respect to this bilinear function on $J(\Delta)$, and vice versa.

In particular, we can realize elements of $J(\Delta)$ as $\mathbf{Z}_d$-module homomorphisms $J(\Delta) \to \mathbf{Z}_d$, with those that kill $Y(B^{\mathrm{op}})$ coming from elements in $Y(B)$ (and again, vice versa).

The duality conjecture can be translated to this setting. Pick a set of n elements of $J(B)$ (or better, $Y(B)$), each generating the cyclic subgroup which is the kernel of $p_{\Omega(i)}^B$, and form them into a column, M, that is, an element of $Y(B)^{n\times 1}$. Then $\operatorname{Aut} J(B)$ acts the right, and on the left, $\mathcal{P}_n\mathcal{D}_n$, where $\mathcal{D}_n$ consists of diagonal matrices with entries in $\mathbf{Z}_d^\times$. We do the same with $J(B^{\mathrm{op}})$. Each entry of M can be viewed as a module homomorphism $J(\Delta) \to \mathbf{Z}_d$, so we can view M, essentially the transpose, as a $\mathbf{Z}_d$-module homomorphism $\tilde{M} \colon J(\Delta)^n \to \mathbf{Z}_d^n$. Then the kernel should correspond to the analogous matrix made out of B^{op}, rather than B, as in the arguments in Appendix A. But it is not clear how to proceed.

The identifications of $J(B)$ with $r(B^{\mathrm{op}})/r(\Delta)$ and the corresponding one interchanging B with B^{op} are particularly well-behaved with respect to applying p_Ω. We can create Δ_Ω, obtained by deleting all the rows and columns indexed by an integer not in Ω, and it is easy to check that $((B^{\mathrm{op}})_\Omega)^T B_\Omega = \Delta_\Omega$ (if $c_i(\cdot)$ denotes the ith column, then $(B^{\mathrm{op}})^T B = \Delta$ means $c_i(B^{\mathrm{op}})^T c_j(B) = m(i)\delta_{ij}$, and the columns of B_Ω and B are identical unless they are completely eliminated). The results in 3.10–3.12 suggest that more can be done along these lines.

7. Densities for PH-equivalence to 1-block size $n-1$

Here we give estimates for the likelihood that a matrix $B \in \mathcal{NS}_n$ has a terminal form with 1-block of size at least $n-1$. The definition of natural density of a subset S of $\mathbf{Z}^n$ is given in [17, Def. 2]. If for all $z \in \mathbf{Z}^n$, the

following limit exists and is independent of $z = (z_i) \in \mathbf{Z}^n$, then $\mathbf{D}(S)$ is known as the *natural density* of S:

$$\mathbf{D}(S) = \lim_{0 < B \to \infty} \frac{\left| S \cap \left(\prod_{i=1}^k [z_i - B, z_i + B) \right) \right|}{(2B)^k}.$$

Fortunately, we do not have to make much use of this definition, since we can simply adapt the methods of [17] and [18] to our setting.

Theorem 7.1. *The natural density of matrices in $\mathcal{NS}_{n,n-1}$ increases upwards (as $n \to \infty$) to*

$$\frac{\zeta(2)\zeta(3)}{\zeta(6)} \cdot \frac{1}{\zeta(2) \cdot \zeta(3) \cdot \zeta(4) \cdots} \sim .845.$$

Remark. We actually give an explicit formula, valid for each n; however, it is difficult to compute with. The first factor is the Landau totient, and the second factor the likelihood that $B \in \mathrm{M}_n \mathbf{Z}$ has an Hermite normal form with at least $n - 1$ ones [18]. The methods derive from that reference, with a few added twists.

Remark. In fact, it also follows from the method of proof that if $T(n)$ is the natural density of $\mathcal{NS}_{n,n-1}$, and if $\epsilon(n)$ is the difference between the limit and $T(n)$, then $\sum \epsilon(n) < \infty$. So convergence is somewhat faster than expected.

First, we obtain an upper bound. Suppose that $B \in \mathrm{M}_n \mathbf{Z}$. Then $B \in \mathcal{NS}_n$ if and only if modulo every prime, each column is not zero. That by itself, together with the usual notion of natural density (see [18] for very clear explanations), says that the likelihood that B is in $\mathcal{NS}_n$ is $1/\zeta(n)^n = 1 - n2^{-n} - \boldsymbol{O}(n3^{-n})$, which goes to one quickly.

Now suppose that $B \in \mathrm{M}_n \mathbf{Z}$ is PH-equivalent to a terminal form having 1-block size at least $n-1$. Then for every prime p, the matrix $B + p\mathrm{M}_n \mathbf{Z} \in \mathrm{M}_n \mathbf{Z}_p$ has rank at least $n - 1$. The converse fails—examples are ubiquitous. Let $\mathcal{TF}_n$ denote the collection of matrices in $\mathrm{M}_n \mathbf{Z}$ PH-equivalent to a matrix with at least $n - 1$ ones in its terminal form (for large n, $\mathcal{TF}_n \cap \mathcal{NS}_n = \mathrm{GL}(n, \mathbf{Z}) \cup \mathcal{NS}_{n,n-1}$ is practically the same as $\mathcal{TF}_n$, so we do not require members of the latter collection to be in $\mathcal{NS}_n$). This does give an upper bound for the natural density (assuming it exists) of $\mathcal{TF}_n$.

In fact, we can do a bit better. For fixed n and for every prime p, let $\pi_p \colon \mathrm{M}_n \mathbf{Z} \to \mathrm{M}_n \mathbf{Z}_p$ be the usual modulo p onto homomorphism. We define a property for $n \times n$ matrices in terms of its reduction modulo every prime. We say that a matrix $B \in \mathrm{M}_n \mathbf{Z}$ is of *deficiency* at most s if for every prime p, the image $\pi_p(B)$ has rank at least $n - s$. For fixed n, the collection of these has a natural density, and if $n \geq (s + 1)^2$, it is

$$\frac{1}{\psi_{(s+1)^2+2} \cdot \zeta((s+1)^2) \cdot \zeta((s+1)^2 + 1) \cdot \cdots \cdot \zeta(n)},$$

where $\psi_{(s+1)^2+2}$ is defined as $\prod_p f(1/p)$, where f is a function (given explicitly below) with the property that $f(z) = 1 - z^{-(s+1)^2+2} + \boldsymbol{O}(z^{-(s+1)^2+3})$ (except

for small primes, the product is more or less $\zeta((s+1)^2+2))$. At $s=1$ (so for $n \geq 4$), the outcome is at least .845, at $s=2$, it is bigger than .99, at $s=3$, it is at least .9999, and each addition of one to s results in the difference from one approximately squaring.

The case of $s=1$ gives the upper bound.

However, when we look at the original problem, density of $\mathcal{TF}_n$, the situation is more complicated, and the best we can do is to use the inclusion-exclusion principle to obtain a formula, which is difficult to evaluate, except for small or large n.

Throughout this section, we refer to *natural density* of families of integer matrices, although most of the effort is spent on counting matrices modulo primes, and multiplying the results over all the primes. The problem is then to relate the relatively easily obtained infinite product expressions to the notion of natural density, as discussed in [18, 17].

The methods of [op cit] can be used to justify the expression natural density, and we will outline what has to be done, at various points.

Upper bound. Fix integers s, n with $n > (s+1)^2+1$ and let p be a prime. The normalized number of matrices in $M_n \mathbf{Z}_p$ of rank at least $n-s$ (that is, divided by the cardinality of $M_n \mathbf{Z}_p$, which is p^{n^2}) is given by Landsberg's theorem [16] (quoted in Appendix B) as $(\prod_{i=1}^{n}(1-z^i))(1 + \sum_{1 \leq j \leq s} c_j(z))|_{z=1/p}$, where

$$c_j(z) = \frac{z^{j^2}(1-z^n)(1-z^{n-1})\cdots(1-z^{n-j+1})}{(1-z)^2(1-z^2)^2\cdots(1-z^j)^2},$$

although for some computations we could take the simplified (and slightly less accurate)

$$c_j \sim \frac{z^{j^2}}{(1-z)^2(1-z^2)^2\cdots(1-z^j)^2}.$$

By Proposition B.2, the Maclaurin series of

$$a_s = \left(\prod_{i=1}^{(s+1)^2-1}(1-z^i) \right)\left(1 + \sum_{1 \leq j \leq s} c_j(z) \right)$$

(or c_j replaced by its simpler form) expands as $1 - z^{(s+1)^2+2}+$ higher order terms. Then the normalized number of matrices of rank at least $n-s$ in $M_n \mathbf{Z}_p$ is

$$n_{s,p} := a_s \cdot \prod_{i=(s+1)^2}^{n}(1-z^i)\Bigg|_{z=1/p}.$$

Form the infinite product $\psi_{n,s} = \prod_p a_s(1/p)$ (this converges—very fast— since $(s+1)^2+2 \geq 2$). Then $\prod_p n_p$ is $\psi_{n,s}/(\zeta((s+1)^2) \cdot \zeta((s+1)^2+1)\cdots\zeta(n))$. For very large n, $\psi_{n,s}$ is extremely close to 1 (just as $\zeta(n)$ is). So as $n \to \infty$, the limiting value is

$$(1) \qquad\qquad \frac{1}{\prod_{j \geq (s+1)^2} \zeta(j)}.$$

The case of interest occurs when $s = 1$, and an easy computation reveals that $a_1 = 1 - z^6$ (exactly!). Hence

$$
(2) \qquad \prod_p n_{1,p} = \frac{1}{\zeta(6) \cdot \prod_{j=4}^n \zeta(j)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \cdot \frac{1}{\prod_{j=2}^n \zeta(j)}.
$$

The left factor is Landau's totient constant (On-line Encyclopedia of Integer Sequences [oeis] A082695); about $1.94\ldots$; the right factor, for large n, is about $.436$, see [18] (with fast convergence in n), so the product is about $.845$ or so. As n increases, the value decreases.

When $s = 2$, the limiting value in (1) is in excess of $.99$, and when $s = 3$, the limiting value exceeds $.9999$ (with the distance from 1 approximately squaring with each addition of 1 to s).

To check that the expressions $\prod_p n_p$, (1), and (2) really do represent natural densities (that is, the number of $B \in \mathrm{M}_n\mathbf{Z}$ with all entries in $[-N, N)$ such that for every prime p, the rank of $\pi_p(B) \in \mathrm{M}_n\mathbf{Z}$ is at least $n-s$, divided by $(2N)^{n^2}$, tends as $N \to \infty$ to the corresponding expression), we note that the method of [18] works almost verbatim. Specifically, the Chinese remainder theorem argument in the proof of [18, Lem. 3] applies here, as does the argument of [18, Lem. 4]. This is made easier by the fact that we are defining the property of matrices in terms of properties modulo every prime. In contrast, when we deal with $\mathcal{TF}_n \cap \mathcal{NS}_n$, there does not appear to be a simple characterization of the set by properties modulo p.

In particular, if $n \geq 6$, the density of matrices $M \in \mathrm{M}_n\mathbf{Z}$ with the property that for every prime p, the rank of $\pi_p(M)$ is at least $n - 1$ is given by the expression in (2), and is at least the limiting value as $n \to \infty$. This gives an upper bound for the (upper) density of matrices such that $M \in \mathcal{TF}_n \cap \mathcal{NS}_n$.

Counting $\mathcal{TF}_n \cap \mathcal{NS}_n$. First, we count the number of matrices $b \in \mathrm{M}_n\mathbf{Z}_p$ whose leftmost $n - 1$ columns form a linearly independent set, and the last column is not zero. (If this happens modulo p for every prime p, then the original matrix belongs to $\mathcal{NS}_n \cap \mathcal{TF}_n$.) This is almost the same as a special case of [19, Cor. 7].

There are $N_p = (p^n - 1)(p^n - p) \cdots (p - 1)$ full rank matrices. If the last column is dependent on the preceding $n - 1$ columns and they form a linearly independent set, then we can write it $c_n = \sum_{i<n} a_i c_i$; since we have required that the last column be not zero, we must also have $(a_i) \neq (0, 0, \ldots, 0)$, and every such choice will do. The number of $(n - 1) \times n$ matrices of full rank is just $N_p/(p^n - p^{n-1})$. Thus the total number of matrices whose set of leftmost $n - 1$ columns is not zero and whose nth column is not zero is

$$
N_p \cdot \left(1 + \frac{p^{n-1} - 1}{p^n - p^{n-1}} \right)
$$

$$
= p^{n^2}(1 - 1/p)(1 - 1/p^2) \cdots (1 - 1/p^n)\left(1 + \frac{1 - 1/p^{n-1}}{p(1 - 1/p)} \right)
$$

$$= p^{n^2}(1 - 1/p)(1 - 1/p^2) \cdots (1 - 1/p^n)\frac{1 - 1/p^n}{1 - 1/p}$$
$$= p^{n^2}(1 - 1/p^2) \cdots (1 - 1/p^{n-1})(1 - p^n)^2.$$

This yields that the natural density (see below) of $B \in \mathcal{NS}_n$ such that removing the last column yields a matrix with full row space (equivalently, the Hermite normal form of B is $\left(\begin{smallmatrix} I_{n-1} & a \\ 0 & d \end{smallmatrix}\right)$) is

(3) $$\frac{1}{\zeta(2) \cdot \zeta(3) \cdots \zeta(n-1) \cdot \zeta(n)^2}.$$

This differs from the natural density of matrices with Hermite normal form with at least $n - 1$ ones [17, Cor. 7] only by the extra factor of $1/\zeta(n)$, which appeared because we insisted that the last column be nonzero (in order to ensure that it came from a matrix in $\mathcal{NS}_n$).

As in all of these computations, the $1 - 1/p$ factor that appears in N_p/p^{n^2} has conveniently been wiped out, thereby removing the singularity that would have arisen from $\zeta(1)$. If Φ is a subset of $\{1, 2, \ldots, n\}$, let D_Φ be the set of matrices in $\mathcal{NS}_n$ such that for *every* $j \in \Phi$, the gcd of the $(n-1) \times (n-1)$ determinants of the matrix with the jth column deleted is one. Clearly, if $|\Phi| = |\Phi'|$ and D_Φ has a natural density, then so does $D_{\Phi'}$ and their natural densities are equal.

That this number is the natural density for this problem is practically immediate from the special case of [17, Cor. 7] with $d_1 = d_2 = \cdots = d_{n-1} = 1$ in the notation there—the only (slight) difference is that we have insisted here that the final column be unimodular, so nonzero modulo every prime. This resulted in the extra factor of $\zeta(n)$.

We have just shown that if $|\Phi| = 1$, then D_Φ has a natural density, given by the number in (3). Now $\bigcup D_\Phi$, where Φ ranges over all one-element sets, is precisely the set of $B \in \mathcal{NS}_n$ such that B is PH-equivalent to a terminal form with at least $n - 1$ ones.

Inclusion-exclusion can now be used. We will obtain a density for every D_Φ. At various points, it will be convenient to use a variable z which will be evaluated at $z = 1/p$ for p prime.

Say $|\Phi| = s > 1$; then we may assume that $\Phi = \{n, n - 1, \ldots, n - s + 1\}$, that is, corresponding to the final s columns. Again, if we restrict to invertible matrices, there are N_p; otherwise, the first $n - 1$ columns constitute a linearly independent set, and we can write $c_n = \sum_{i < n} a_i c_i$. Only this time, we also require that if $i \in \Phi$, then $a_i \neq 0$ (this occurs if and only if the ith column can be expressed as a linear combination of all the other columns; it also guarantees all the columns are nonzero). Hence the number of choices for the (a_i) is $p^{n-|\Phi|}(p-1)^{|\Phi|-1} = p^{n-s}(p-1)^{s-1}$. Hence the normalized number of such matrices is

$$\frac{N_p}{p^{n^2}}\left(1 + \frac{p^{n-s}(p-1)^{s-1}}{p^n - p^{n-1}}\right) = (1 - 1/p) \ldots (1 - 1/p^n)\left(1 + \frac{(1 - 1/p)^{s-2}}{p}\right)$$
$$= (1 - z)(1 - z^2) \ldots (1 - z^n)\left(1 + z(1 - z)^{s-2}\right),$$

where we set $z = 1/p$. Denote by f_s the polynomial (now in the variable z) $(1 - z)(1 + z(1 - z)^{s-2})$; this is $(1 - z)(1 + z - (s - 2)z^2 + \cdots)$, so $f_s = 1 - (s-1)z^2 + \boldsymbol{O}(z^3)$. This permits us to define the function (which turns out to be entire)

$$F(s) := \prod_p f_s(1/p) = \prod_p \left(1 - \frac{p^{s-1} - (p-1)^{s-1}}{p^s}\right).$$

Provided the (now, complex) s is such that for every prime p, we have $p^{s-1} - (p-1)^{s-1} \neq p^s$ (this simplifies), it is easy to check that F is analytic on a neighborhood of s, and a routine verification assures us that at any of the trivial zeros, t, $\lim_{s \to t} F_s/(s - t)$ exists and is not zero, hence F is also analytic on neighborhoods of the zeros; so F is entire. Its zeros are precisely the set

$$\left\{s \in \mathbf{C} \mid \text{there exists a prime } p \text{ such that } p^s = p^{s-1} - (p-1)^{s-2}\right\};$$

this can be rewritten as

$$\left\{1 + \frac{(2k+1)\pi i + \ln(p-1)}{\ln \frac{p}{p-1}}\right\}_{p \in \mathrm{Spec}\, \mathbf{Z}, k \in \mathbf{Z}}$$

The values of F at various integers are interesting, and will play a role in what follows. We have

$$F(0) = \prod_p \left(1 + \frac{1}{p(p-1)}\right)$$

(the Landau totient constant $\zeta(2)\zeta(3)/\zeta(6) \sim 1.94$),

$$F(1) = 1, \quad F(2) = \prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)}$$

and

$$F(3) = \prod_p \left(1 - \frac{2p-1}{p^3}\right)$$

(the *carefree* constant $\sim .426$, see [19]). The values at other integers (both positive and negative) have likely appeared before, but I could not locate them in the huge literature on constants. The density of D_Φ (when $|\Phi| = s > 1$) is thus

$$\frac{F(s)}{\zeta(2)\cdots\zeta(n)}.$$

Once again, we may use the methods of [17, Section 4] to justify the natural density. With this, we also see that the inclusion-exclusion principle applies (first to subsets of $\mathcal{TF}_n \cap \mathcal{NS}_n$ inside $[-N, N)^{n^2}$ and their translations, then letting $N \to \infty$).

For $s = 2$, the density of D_Φ is $1/(\zeta(2)^2\zeta(3)\cdots\zeta(n))$. The inclusion-exclusion principle reveals that the density of matrices in $\mathcal{NS}_n$ PH-equivalent

to a terminal form with 1-block size at least $n-1$ is

$$(4) \qquad \frac{\frac{n}{\zeta(n)} - \frac{\binom{n}{2}}{\zeta(2)} + \sum_{j=3}^{n} (-1)^{j-1}\binom{n}{j}F(j)}{\zeta(2)\zeta(3)\dots\zeta(n)}.$$

The leading term does not involve $F(1)$, as we would have expected; however, for large n, $1/\zeta(n)$ is practically $1 = F(1)$; and we have substituted $F(2) = 1/\zeta(2)$.

Now we have to estimate the expression (4). The denominator converges extremely rapidly, and has been calculated as around .44 for large (and not so large) n, see [17]. Also, $\{F(j)\}_{j\in\mathbf{N}}$ forms a decreasing, log convex sequence, as easily follows by taking the logarithmic derivative of F. The logarithmic derivative, F'/F, is analytic except at the zeros of F, and is given by

$$\sum_p \frac{\ln(1-1/p)}{(\frac{p}{p-1})^{s-1}(p-1)+1}.$$

This converges uniformly on compact subsets of $|\mathrm{Im}\, s| < \pi/\ln 2$.

With single-digit accuracy, I managed to approximate (with pencil and paper) the values of the expression in (4) for $n = 3, 4, 5, 6$; they are respectively, .55, .6, .7, .8. The last is surprisingly close to the upper bound computed from (2) above, which is $(\zeta(2)\zeta(3)/\zeta(6)) \cdot 1/\zeta(2)\zeta(3)\cdots \sim .845$. This suggests that the numerator of (4) tends to $\zeta(2)\zeta(3)/\zeta(6)$; in other words, that the upper bound be approximately achieved. We will prove this after putting it in a more recognizable form.

Let us rewrite the numerator, substituting innocuously (when n is large) $F(1) = 1$ for $1/\zeta(n)$ and $F(2) = 1/\zeta(2)$; then, subtracting the expression from $F(0) = \zeta(2)\zeta(3)/\zeta(6)$, we obtain

$$D(n) := F(0) - nF(1) + \binom{n}{2}F(2) - \cdots + (-1)^n F(n) = \sum_{i=0}^{n}(-1)^n\binom{n}{i}F(i).$$

We will show

$$\lim_{n\to\infty} D(n) = 0.$$

This is equivalent to the numerator in (4) converging (in n) to $F(0) = \zeta(2)\cdot\zeta(3)/\zeta(6)$, which will complete the proof of Theorem 7.1.

A function $f\colon \mathbf{R} \to \mathbf{R}$ is *completely monotone* if $(-1)^n f^{(n)}(r) \geq 0$ for all $n \in \mathbf{Z}^+$ and $r \in \mathbf{R}$ (here $f^{(n)}$ is the nth derivative); it is *logarithmically completely monotone* if $f(r) > 0$ for all r and $-\ln f$ is completely monotone. It is known that logarithmically completely monotone functions are completely monotone.

Proposition 7.2. *The restriction of F to $\mathbf{R}$ is logarithmically completely monotone. In particular, F is completely monotone.*

Proof. With $\ln F$ given above, we see that $\ln F|\mathbf{R}$ is strictly positive, and its logarithmic derivative, F'/F, converges on compact subsets of the strip

$|\operatorname{Im} z| < \pi/\ln 2$, and is a sum of terms each of which the negative of a completely monotone function. $\square$

Let Δ denote the usual difference operator, acting on functions on $\mathbf{Z}$ or $\mathbf{R}$, that is, $\Delta f(k) = f(k+1) - f(k)$. This use of Δ is confined to this section, so will not conflict with the use of Δ as a diagonal matrix affiliated to the PH-equivalence class of a matrix, in the other sections. If $f\colon \mathbf{Z} \to \mathbf{R}$ satisfies $(-1)^n \Delta^n f(k) \geq 0$ for all $n \in \mathbf{Z}^+$ and $k \in \mathbf{Z}$, then we say that f is *completely monotone*.

Suppose that $f\colon \mathbf{R} \to \mathbf{R}$ is completely monotone; then it is routine to see that $f|\mathbf{Z}$ (or f restricted to any other discrete subgroup) is completely monotone (in the sense of functions on $\mathbf{Z}$). By the higher order mean value theorem, given $r \in \mathbf{R}$ and $n \in \mathbf{Z}^+$, there exists $\xi \in [r, r+n]$ such that $\Delta^n f(r) = f^{(n)}(\xi)$; setting $r = k \in \mathbf{Z}$, the sign of $\Delta^n f(k)$ is the same as the sign of $f^{(n)}(\xi)$ at some real number, and we are done.

Completion of proof of Theorem 7.1. It is straightforward to see that $D(n) = (-1)^n \Delta^n F(0)$; so it is enough to show that $(-1)^n \Delta^n F(0) \to 0$, which turns out to be relatively simple. Set $d_n(k) = (-1)^n \Delta^n F(k)$.

From the definition of Δ, we have, for $n \geq 1$,

$$
\begin{aligned}
d_{n-1}(k-1) &= d_n(k-1) + d_{n-1}(k) \\
&= d_{n+1}(k-1) + d_n(k) + d_{n-1}(k) \quad \text{(iterating)} \\
&= d_{n+N+1}(k-1) + \sum_{j=-1}^{N} d_{n+j}(k) \quad \text{for all } N.
\end{aligned}
$$

Since F is completely monotone, $d_n(k) \geq 0$ for all $k \in \mathbf{Z}$ and $n \in \mathbf{Z}^+$. Hence for all integers k, $d_N(k) \to 0$ as $N \to \infty$. In particular, this applies to $k = 0$. $\square$

It also follows that $\lim_{N \to \infty} j = 0^N (-1)^j \Delta^j F(k) = F(k-1)$ for all integers k (that is, $I + \sum_{j=1}^{N} (-1)^j \Delta^j = (I + \Delta)^{-1}$ when applied to F).

Question 7.3. If we consider 1-block size at least $n - 2$ instead, the upper bound is then in excess of .99; so if the upper bound is achieved (as $n \to \infty$), then for sufficiently large n, over 99% of random integer matrices will have a terminal form with 1-block size at least $n - 2$. This suggests that it might be worthwhile obtaining the analog of Proposition 2.1 for $n - 2$, describing the equivalence classes containing a terminal form of this type).

Question 7.4. It would be reasonable to determine the likelihood that at least *one* of B and B^{op} be PH-equivalent to a terminal form with 1-block size $n - 1$. The simplest possible form of inclusion-exclusion would yield a likelihood of $2a - b$, where a is the likelihood that B have a terminal form with 1-block size $n - 1$ (about .845 as just calculated above), and b is the likelihood that both B and B^{op} have such a terminal form. Computing b appears to be difficult ($b \neq a^2$; the properties are not independent). Towards

this, the characterizations for $J(B)$ and $J(B^{\mathrm{op}})$ to both belong to $\mathcal{NS}_{n,n-1}$ (Corollary 4.6) might be useful.

8. Topological isomorphism for topologically critical groups

In this section, we state some well-known and not-so-well-known results about topologically critical groups; see also [10]. Suppose $G \to V$ and $H \to W$ are group homomorphisms from abelian groups to ordered real Banach spaces. We say $f \colon G \to H$ is *continuous* if there exists continuous and linear $F \colon V \to W$ whose restriction to G is f (typically, the images of G and H will be dense in their respective Banach spaces; in this case, continuity is equivalent to the usual notion with respect to the relative topologies on G and H).

A subgroup G of $\mathbf{R}^n$ is *topologically critical of rank $n+1$* if it is free of rank $n+1$ and dense. In this section (only), when we regard $g \in G$ as an element of $\mathbf{R}^n$, we denote it $\widehat{g}$. Associated to a topologically critical group is an isomorphism class of rank $n+1$ subgroups of $\mathbf{R}$, $\mathrm{TO}(G)$, defined as follows. Select any ordered $\mathbf{Z}$-basis for G, $(g_i)_{i=1}^{n+1}$. Since $\{g_i\}_{i=1}^n$ generates a discrete subgroup, it is a real basis for $\mathbf{R}^n$; hence we can write $\widehat{g}_{n+1} = \sum_{i=1}^n \alpha_i \widehat{g}_i$ for $\alpha_i \in \mathbf{R}$. It is easy to check that $\{1, \alpha_1, \ldots, \alpha_n\}$ is linearly independent over the rationals, and so we may form the subgroup of $\mathbf{R}$, $\mathbf{Z} + \sum \alpha_i \mathbf{Z}$, of rank $n+1$. Every topologically critical subgroup of $\mathbf{R}^n$ is topologically isomorphic to the group generated by $\{e_i; \sum e_j \alpha_j\}$ (where e_i are the standard basis elements of $\mathbf{R}^n$) by this construction (for example, see [10]).

Then we define $\mathrm{TO}(G)$ to denote the isomorphism class of the inclusion $\mathbf{Z} + \sum \alpha_i \mathbf{Z} \subset \mathbf{R}$, that is, with respect to continuous maps. Alternatively, we may view $\mathrm{TO}(G)$ as an isomorphism class of totally ordered groups (the ordering inherited from $\mathbf{R}$), and use order-preserving group isomorphisms between any subgroup of $\mathbf{R}$ of the form $\mathbf{Z} + \sum \alpha_i \mathbf{Z}$; the resulting equivalence classes are the same, since in this case, any nonzero continuous group homomorphism is either order-preserving or its negative is.

Topologically critical groups have an interesting property: every subgroup is either dense (those of full rank) or discrete (those of lesser rank).

Lemma 8.1. *Suppose G and H are topologically critical groups such that $\mathrm{TO}(G) \cong \mathrm{TO}(H)$. Then H and G are continuously isomorphic.*

Proof. Suppose $\{\alpha_i\}_{i=0}^n$ and $\{\beta_i\}_{i=1}^{n+1}$ are subsets of $\mathbf{R}$ that are linearly independent over the rationals, and $\alpha_{n+1} = 1 = -\beta_{n+1}$, and moreover, $\sum \alpha_i \mathbf{Z} = \sum \beta_i \mathbf{Z}$ (as subgroups of $\mathbf{R}$). Let $G = \langle e_i; e_{n+1} \coloneqq \sum_{i=1}^n \alpha_i e_i \rangle$ be the (dense) subgroup of $\mathbf{R}^n$, where $\{e_i\}_{i=1}^n$ is the standard basis for $\mathbf{R}^n$. Then there exist $\{h_i\}_{i=1}^n$ such that $G = \sum h_i \mathbf{Z}$ and $h_{n+1} = \sum_{i=1}^n \beta_i h_i$.

For each $i = 1, 2, \ldots, n$, there exist integers $a_{i,t}$ ($t = 0, 1, \ldots, n$) such that $\alpha_i = \sum_{t=1}^{n+1} \beta_i a_{it}$. Complete (a_{it}) to an $(n+1) \times (n+1)$ matrix A by defining $a_{n+1,t} = \delta_{n+1,t}$ (so the bottom row is $(0, 0, \ldots, 0, 1)$).

Set $g_i = e_i$ (to avoid confusion between the standard bases) for $i = 1, 2, \ldots,$ $n + 1$. Define for each $j = 1, 2, \ldots, n + 1$,

$$h_j = \sum_i a_{i,j} g_i$$

(so here we are using A^T). Obviously, $h_j \in G$. We first show that $h_{n+1} = \sum_{t=1}^{n+1} \beta_t h_t$. On one hand,

$$h_{n+1} = \sum_{i=1}^{n+1} a_{i,n+1} g_i = \sum_{i=1}^{n} (a_{i,n+1} + a_{n+1,n+1} \alpha_i) g_i;$$

on the other hand,

$$\sum_{t=1}^{n} \beta_t h_t = \sum_{t=1}^{n} \beta_t \sum_{i=1}^{n+1} a_{i,t} g_i$$

$$= \sum_{t=1}^{n} \beta_t \left(\sum_{i=1}^{n} a_{i,t} g_i + \alpha_i \beta_t a_{n+1,t} \right)$$

$$= \sum_{i=1}^{n} g_i \cdot \left(\sum_{t=1}^{n} a_{i,t} \beta_t + 0 \right)$$

$$= \sum_{i=1}^{n} g_i \cdot (\alpha_i - \beta_{n+1} a_{i,n+1}).$$

Since $\beta_{n+1} = -1$, we are done.

As $\sum \alpha_i \mathbf{Z} = \sum \beta_i \mathbf{Z}$, we can find the inverse map (both are free abelian groups of rank $n + 1$ to A); this takes the h_j to g_j, and it follows immediately that $\sum h_j \mathbf{Z} = \sum g_j \mathbf{Z}$, and the rank condition guarantees that the sums are direct.   □

9. Basic critical dimension groups

This section deals with a class of dimension groups (known as *critical*) and an invariant for them that determines if they can be realized in particularly nice forms, known as *basic* and *almost basic*. In the next section, it will be shown that PH-equivalence is part of a complete invariant deciding whether two almost basic critical dimension groups are (order) isomorphic.

A *dimension group* is a direct limit of simplicial (partially ordered abelian) groups; see [6], the standard reference for partially ordered abelian groups, for far more information than can be given here. By [8, 4], a partially ordered abelian group G is a dimension group if and only if it is *unperforated* (for $n \in \mathbf{N}$ and $g \in G$, $ng \geq 0$ entails $g \geq 0$) and satisfies *Riesz interpolation* (for $a_i, b_j \in G$, with $i, j \in \{1, 2\}$, with $a_i \leq b_j$ for all i, j, there exists $c \in G$ such that $a_i \leq c \leq b_j$ for all i, j). All partially ordered groups will be abelian.

An *order unit* of a partially ordered group G is an element $u \in G^+$ such that for all $g \in G$, there exists $n \in \mathbf{N}$ such that $-nu \leq g \leq nu$. A partially ordered abelian group is *simple* if every nonzero element of G^+ is an order unit.

A *trace* (or *state*) of G is a nonzero positive real-valued group homomorphism; it is *normalized* at the order unit u if its value thereat is 1. The collection of normalized traces, denoted $S(G, u)$ and equipped with the point-open (weak) topology, is a compact convex subset of a Banach space. The *value group* of a trace τ is simply $\tau(G)$, its set of values.

The real vector space consisting of convex-linear continuous (*affine*) real-valued functions $f : S(G, u) \to \mathbf{R}$ is denoted Aff $S(G, u)$. It is a Banach space with respect to the supremum norm. There is a natural order preserving group homomorphism, the *affine representation* (with respect to u), $\widehat{\ } : (G, u) \to$ Aff $S(G, u)$ given by $g \mapsto \widehat{g}$, where $\widehat{g}(\tau) = \tau(g)$ for $\tau \in S(G, u)$. This imposes a pseudo-norm topology on G, which is a norm if the affine representation is one to one.

When G is a dimension group, $S(G, u)$ is a Choquet simplex. When G is also simple, there is a complete characterization available: the affine representation $G \to$ Aff $S(G, u)$ (with respect to any, or equivalently all, choices of order unit u) has dense range, and $G^+ \setminus \{0\}$ consists of $\{g \in G \mid \widehat{g} \text{ is strictly positive}\}$. The converse is also true.

A trace is *pure* (or *extremal*) if it is not a proper convex-linear combination of other traces. The *extremal boundary* (of $S(G, u)$), denoted $\partial_e S(G, u)$, consists of the pure normalized traces. When $S(G, u)$ is finite-dimensional, it is a simplex in the usual sense (as a compact convex subset of Euclidean space), and in that case, Aff $S(G, u)$ can be identified with $\mathbf{R}^n$ for some integer n, the standard basis elements identified with the pure traces (possibly with normalization). The *strict ordering* on $\mathbf{R}^n$ or Aff $S(G, u)$ is the partial ordering whose positive cone consists of the strictly positive functions.

A consequence is that if G is a simple dimension group with finitely many, say n, pure traces and the kernel of the affine representation is zero, then G is order isomorphic to a dense subgroup of $\mathbf{R}^n$ equipped with the strict ordering. The pure traces are just (up to renormalization) the coordinate maps. For more on dimension groups, see the book [6].

We say a simple dimension group G is *critical* if it is free of rank $n+1$ and has n pure traces. By the preceding, this means it can be identified with a dense subgroup of $\mathbf{R}^n$, and since the partial ordering determines the topology (here the affine representation is automatically one to one), it is also topologically critical (Section 8).

We are interested in classification of critical groups. It turns out that there is a class of them whose classification incorporates PH-equivalence.

A critical group is called *basic* if it is order isomorphic to a dense subgroup of $\mathbf{R}^n$ (equipped with the strict ordering) with generators $\{e_1, \ldots, e_n; \sum \alpha_i e_i\}$, where e_i are the standard basis elements, and α_i are real numbers. For a subgroup so generated, density is equivalent to the set $\{1, \alpha_1, \ldots, \alpha_n\}$ being linearly independent over the rationals. We will give a characterization that avoids such a specific realization, referring only to internal properties.

Critical, and especially basic critical groups, are a useful source of examples. For example, in [2], we translated Akin's notion of *good measure* on a Cantor set to dimension groups, and we were able use these to illustrate various properties of good and non-good traces. Following [2], we say that a trace τ on a dimension group G is *good* if for all $b \in G^+$ and $a \in G$ such that $0 < \tau(a) < \tau(b)$, there exists $a' \in G^+$ such that $a' \leq b$ and $\tau(a') = \tau(a)$. For simple dimension groups, this is equivalent to a much simpler criterion (in context), that the image of $\ker \tau$ in the affine representation of G be norm-dense in $\tau^\vdash := \{h \in \operatorname{Aff} S(G, u) \mid h(\tau) = 0\}$.

This led to the definition of ugly for a trace on a dimension group; τ is *ugly* (see [2]) if $\ker \tau$ has discrete image in $\operatorname{Aff} S(G, u)$ and the trace $\tau \otimes 1_{\mathbf{Q}}$ on $G \otimes \mathbf{Q}$ is good.

For sets of traces, there are corresponding definitions, which become rather complicated—but if $S(G, u)$ is finite-dimensional, and $\Omega \subset \partial_e S(G, u)$, the relevant ones for this article reduce to the following:

(i) Ω is *good* if whenever $b \in G^+$ and $a \in G$ satisfy $0 < \tau(a) < \tau(b)$ for all $\tau \in \Omega$, then there exists $a' \in G^+$ such that $a - a' \in \ker \Omega := \bigcap_{\tau \in \Omega} \ker \tau$ and $a' \leq b$.

(ii) Ω is *ugly* if the image of $\ker \Omega$ is discrete in $\operatorname{Aff} S(G, u)$ and the extension of Ω to a set of traces on $G \otimes \mathbf{Q}$ is good.

These are not equivalent to the definitions for general dimension groups; the restriction to $\Omega \subset \partial_e S(G, u)$ allows considerable simplification. Among other things, these correspond to faces in $S(G, u)$. For critical groups and any nonempty family of traces, $\ker \Omega$, being a subgroup of rank at most $n - 1$, is automatically discrete. So the definition of ugly simplifies further.

Necessarily, when G is a basic critical group, for all pure traces τ, we have $\operatorname{rank} \tau(G) = 2$, and this forces all the pure traces to be ugly. Conversely, the pure trace τ is ugly if $\operatorname{rank} \tau(G) = 2$. Given in Example 10.5 are critical groups of all ranks larger than two, all of whose pure traces are ugly, and even with the additional property that $\{\tau_i(G)\}$ are mutually order isomorphic as real subgroups, that are not basic (or even a modest extension, to be defined later, almost basic).

Basic critical groups admit rather strong properties. The first is that every proper subset of the pure trace space is ugly. For a simple dimension group (G, u) with one to one affine representation and finite-dimensional $S(G, u)$, and $\Omega \subset \partial_e S(G, u)$, the definition of ugliness of Ω simplifies to Ω satisfying (a) $\ker \Omega := \bigcap_{\tau \in \Omega} \ker \tau$ is discrete, and (b) $\ker \Omega \otimes \mathbf{Q}$ is dense in $\Omega^\perp = \{h \in \operatorname{Aff} S(G, u) \mid h | \Omega \equiv 0\}$ (Ω can be replaced by the face it spans in $S(G, u)$).

Lemma 9.1. *Let (G, u) be a critical group of rank $n + 1$, and let Ω be a proper set of pure traces. Then Ω is ugly if and only if $\operatorname{rank} \ker \Omega = n - |\Omega|$.*

Proof. Every subgroup of rank n or less is discrete, hence any $\mathbf{Z}$-linearly independent subset of size at most n is real linearly independent. If $\Omega \subseteq \partial_e S(G, u)$, then $\Omega^\perp$ has (real) dimension exactly $n - |\Omega|$ (the set of pure traces is a dual basis for $\operatorname{Aff} S(G, u)$). The result follows immediately. $\square$

Although the definition involves a choice of order unit, the criterion does not. In other words, it does not matter at which order unit u we choose to normalize the traces.

It is trivial that if G is basic, then the criterion is satisfied for every proper subset Ω of $\partial_e S(G, u)$. However, there exist non-basic but critical groups which also have the property that for every proper $\Omega \subset \partial_e S(G, u)$, Ω is ugly. In this case, there is a finite obstruction to being basic.

In the examples in 10.5, r is a real number that satisfies no nonconstant rational polynomial of degree n or less, and we form the groups $G(n, r) \subset \mathbf{R}^n$. These are critical dimension groups with the interesting property that for all pure traces τ, the value groups $\tau(G)$ are equal to each other. Equality of the value groups is not an invariant (since by changing the order unit, we change the value groups), except in the case that we are looking at invariants for (G, u), that is, where u is specified. However, what is an invariant is that all $\tau(G)$ be order-isomorphic as subgroups of the reals as τ varies over the pure traces.

We analyze potential isomorphisms of critical groups of rank $n + 1$ as follows. Begin with any ordered $\mathbf{Z}$-basis, $\{v_1, v_2, \ldots, v_n, v_{n+1}\}$, which we regard as elements of $\mathbf{R}^{1 \times n}$, that is, rows of real numbers. We construct an $(n+1) \times n$ real matrix A by letting its ith row be v_i.

Applying any element of $\mathrm{GL}(n + 1, \mathbf{Z})$ to A (from the left) just changes the $\mathbf{Z}$-basis, hence leaves the group they generate the same.

Let $P(n, \mathbf{R})^+$ denote the group of weighted permutation matrices of size n with only positive weights—that is, the set of products $P\Delta$ where P is a permutation matrix, and Δ is a diagonal matrix with only strictly positive real entries along the diagonal. The group of order-automorphisms of $\mathbf{R}^{1 \times n}$ with respect to either the strict or the usual ordering is just $P(n, \mathbf{R})^+$, and since any order isomorphism between critical groups (necessarily of the same rank) extends uniquely to an order automorphism of $\mathbf{R}^{1 \times n}$ (after identifying the two sets of pure traces), we have that the order isomorphisms between critical groups are determined by right actions of $P(n, \mathbf{R})^+$.

So we can act on A from the left by $\mathrm{GL}(n + 1, \mathbf{Z})$ and from the right by $P(n, \mathbf{R})^+$. In particular, we can permute rows, we can permute columns, perform elementary row operations (over the integers), and multiply columns by positive real scalars. If after a sequence of such actions, we arrive at a matrix A' where the top $n \times n$ part is just the identity, then the critical dimension group is basic.

We illustrate this with a simple example. This is the case of $n = 2$ of $G(n, r)$ in Example 10.5. Here r is a real number that is not quadratic or rational. Let $G = \langle (r, 0), (1, r), (1, 1) \rangle \subset \mathbf{R}^2$. We have the following series of transformations,

$$\begin{pmatrix} 1 & 1 \\ 1 & r \\ r & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 \\ 0 & r - 1 \\ r & 0 \end{pmatrix} \mapsto \begin{pmatrix} r & 0 \\ 0 & r - 1 \\ 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ \frac{1}{r} & \frac{1}{r-1} \end{pmatrix}.$$

Thus G is basic (since $\{1, 1/r, 1/(r-1)\}$ is linearly independent over $\mathbf{Q}$ if and only if $\{1, r, r^2\}$ is). It also satisfies the property that $\tau(G)$ are mutually isomorphic as τ varies over the pure trace space.

Suppose A is partitioned as $\binom{B}{\alpha}$, where B is $n \times n$ (so $\alpha = (\alpha_1, \ldots, \alpha_n)$ is just the bottom row), and now assume that B is a rank n matrix (necessary for it to yield a critical group anyway) with only integer entries. Some of the time (but not always), we restrict the actions of $\mathrm{GL}(n+1, \mathbf{Z})$ to be those of $\mathrm{GL}(n, \mathbf{Z}) \times \{1\}$, that is, performing only elementary row operations not affecting the bottom row α. Necessary and sufficient for the row space of A to be a critical dimension group is that the set $\{1, \alpha_1, \ldots, \alpha_n\}$ be linearly independent over the rationals.

Since multiplying on the right by weighted positive diagonal matrices preserves order isomorphism, we may assume that each column of B is unimodular (of course, the corresponding entry of α is multiplied by a rational at the same time). Hence we may assume that $B \in \mathcal{NS}_n$.

Every $U \in \mathrm{GL}(n, \mathbf{Z})$ and permutation matrix P yield an order isomorphism of the dimension group (by extending U to $C = U \oplus (1)$), so we may assume that B is in terminal form.

In particular, if the terminal form is simply the identity (of size n), then G is basic. More generally, let G' be the subgroup of $\mathbf{R}^n$ generated by the rows of the current matrix, renamed $A = \binom{B}{\alpha}$; as we have observed, this is order isomorphic to G. The pure traces are still the coordinate functions, τ_i. It is easy to check that $\tau_i(G') = \mathbf{Z} + \alpha_i \mathbf{Z}$, and the latter being of rank two implies that all pure traces are ugly. But more is true. If we manipulate further using $\mathrm{GL}(n, \mathbf{Q})$ (that is rational elementary row operations), we can reduce B to the identity matrix. This means that $G' \otimes \mathbf{Q}$ is order isomorphic to $G_0 \otimes \mathbf{Q}$ for some basic critical group G_0. It follows immediately that every proper subset of the pure trace space of G' is ugly.

An invariant for critical dimension groups. Now we design an invariant that tests for the property of being basic (and later, for being almost basic). For any critical dimension group with pure trace space $\partial_e S(G, u) = \{\tau_i\}$, set $J_i = \ker \Omega(i)$. It is easy to see that either $J_i = (0)$ or rank $J_i = 1$. In the latter case, pick a generator x_i for J_i (we only have two choices, $\pm x_i$). Form $E \equiv E(G) := \sum x_i \mathbf{Z}$ where, the i varies over those such that J_i is not zero. The x_i are the same as those in the original construction of the invariant for the integer part of G.

Lemma 9.2. *Let G and G' be critical dimension groups of rank $n + 1$.*

(i) *Any order isomorphism $G \rightarrow G'$ induces a group isomorphism $G/E(G) \rightarrow G'/E'(G)$.*

(ii) *If G is spanned by the rows of $A = \binom{B}{\alpha}$, where $B \in \mathcal{NS}_n$ and $\alpha \in \mathbf{R}^n$, then $\mathrm{t}(G/E(G)) \cong J(B^{\mathrm{op}})$ as groups.*

Proof. (i) Since any order isomorphism induces a permutation on the pure traces (possibly with a renormalization), $J_i = \ker \tau_i$ is sent to $J'_{\pi i}$ for some

permutation π. If J_i is nonzero, it is cyclic and its only two one-element generators are $\pm x_i$. Hence the image of x_i is one of $\pm x'_{\pi i}$, and it follows that the restriction of the isomorphism to $E(G)$ is an isomorphism onto $E(G')$. This induces an isomorphism $G/E(G) \to G'/E'(G)$.

(ii) It suffices to show that $r(B)/X(B)$ (a subgroup of $G/E(G)$) is exactly the torsion part of $G/E(G)$. Since $E(G)$ has rank n (when G is of the indicated form), $G/E(G)$ is torsion. Thus we have inclusion.

Now suppose that $g + E(G)$ is a torsion element in $G/E(G)$. There thus exists $n > 0$ such that $ng \in E(G)$, in particular, we can write ng as an integer combination of elements of x_i, so that $ng \in \sum f_j \mathbf{Z}$ (as the $x_i \in \sum f_j \mathbf{Z}$). On the other hand, since $\{f_j\} \cup \{\alpha\}$ is a $\mathbf{Z}$-basis for G, we may write g uniquely as $\sum t_j f_j + m\alpha$, so that $ng = \sum n t_j f_j + nm\alpha$; since $ng \in \sum f_j \mathbf{Z}$, we deduce $nm\alpha$ is in the span of f_j, which of course is impossible unless $nm = 0$, that is, $m = 0$. So $g \in \sum f_j \mathbf{Z}$, and thus $g + E(G) \in r(B)/X(B)$. $\square$

When G is basic, $G/E \cong \mathbf{Z}$, as is obvious from its matrix A representing it. When every proper subset of the pure trace space is ugly, then the torsion-free rank of G/E is one, but it may have torsion elements. If not every proper subset is ugly, then the torsion-free rank of G/E must exceed one, and there can also be torsion. The following is practically tautological.

Proposition 9.3. *Let G be a critical dimension group. Then G is basic if and only if $G/E(G) \cong \mathbf{Z}$.*

Proof. One way is trivial. Suppose $G/E \cong \mathbf{Z}$. Then $G \to G/E$ splits, and thus we may find $y \in G$ such that $E \oplus y\mathbf{Z} = G$. We can write $E = \bigoplus x_i \mathbf{Z}$, and since the rank of E is n, there are n of the x_i. Now each x_i vanishes at all the traces except τ_i; by replacing x_i by $-x_i$ if necessary, we can also assume that $\tau_i(x_i) > 0$. Set $u = \sum x_i$, so that $\tau_i(u) = \tau_i(x_i) > 0$ for all i. Thus u is an order unit. Now renormalize the traces with respect to u, that is, τ_i is replaced by $\sigma_i := \tau_i/\tau_i(x_i)$. Then $\sigma_i(x_j) = \delta_{ij}$ (Kronecker delta), and in the affine representation with respect to u, each x_j simply maps to the jth standard basis element. Now y (or more accurately $\hat{y}$) is a real linear combination of x_i, say $\hat{y} = \sum \alpha_i \hat{x}_i$. As G has dense range, it easily follows that $\{1, \alpha_1, \dots, \alpha_n\}$ is linearly independent over the rationals, and we have exhibited an order-isomorphic copy of G as a basic critical group. $\square$

With respect to Lemma 9.2 (i), the torsion part of $G/E(G)$ is determined by the elementary divisors of B^{op}.

Example 9.4. Examples illustrating Lemma 9.2 and Proposition 9.3.

For $n = 2$, set $f_1 = (1,1)$, $f_2 = (0,2)$, $f_3 = (\alpha, \beta)$, where $\{1, \alpha, \beta\}$ is linearly independent over the rationals, and set $G = \langle f_1, f_2, f_3 \rangle = \bigoplus f_i \mathbf{Z}$. The matrix A is already reduced as far as it can be (if we insist that the top 2×2 matrix have only integer entries),

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 2 \\ \alpha & \beta \end{pmatrix}.$$

Then $\ker \tau_1 = f_2 \mathbf{Z}$, so we set $x_1 = f_2$; $\ker \tau_2 = (2f_1 - f_2)\mathbf{Z}$, so we set $x_2 = 2f_1 - f_2$. But $\langle x_1, x_2 \rangle = \langle 2f_1, f_2 \rangle$, so $G/E \cong \mathbf{Z} \oplus \mathbf{Z}_2$; in particular, this dimension group is not basic. (It is the presence of the 1 in the $(1,2)$ entry, that ensures that we obtain 2-torsion; if $f_1 = (1,0)$ instead, then the group would be basic, since we could divide the second column by 2).

Now let $n = 3$, and define f_i to be the four rows of the matrix

$$\begin{pmatrix} 1 & 0 & 11 \\ 0 & 1 & 2 \\ 0 & 0 & 12 \\ \alpha & \beta & \gamma \end{pmatrix},$$

where $\{1, \alpha, \beta, \gamma\}$ is linearly independent over the rationals. Then $x_1 = 12f_1 - 11f_3$ (up to sign), $x_2 = 6f_2 - f_3$, and $x_3 = f_3$. The torsion subgroup of G/E, that is, $J(B^{\mathrm{op}})$, is isomorphic to $\mathbf{Z}_{12} \oplus \mathbf{Z}_6$, which has 72 elements, not the expected $12 = 1 \times 2 \times 6$. In particular, G is not basic.

We will see (in the next section) that the invariant really boils down to PH-equivalence, together with an action on the bottom row.

10. Isomorphisms between almost basic critical groups

A critical group of rank $n + 1$ is *almost basic* if it is order isomorphic to a dimension group G given by the matrix $\left(\begin{smallmatrix} B \\ \alpha \end{smallmatrix} \right)$, where $B \in \mathrm{M}_n \mathbf{Z}$; necessarily (in order to have dense image in $\mathbf{R}^n$), rank $B = n$ and $\{1, \alpha_1, \ldots, \alpha_n\}$ is linearly independent over the rationals. As above, we may assume that all the columns of B are unimodular, that is, $B \in \mathcal{NS}_n$. We will show (Theorem 10.1) that two almost basic groups (with corresponding (B, α) and (B', α')) are order isomorphic if and only if $B = UB'P$ (for some $U \in \mathrm{GL}(n, \mathbf{Z})$ and P a permutation matrix, i.e., B is PH-equivalent to B') and one of $\alpha \pm \alpha'P \in r(B)$.

We also obtain an internal characterization of almost basic among critical groups, independent of how it is realized: every subset of $\partial_e S(G, u)$ is ugly (Proposition 10.4).

Suppose r and s are irrational real numbers. Then the critical groups of rank 2 ($n = 1$), $\mathbf{Z} + r\mathbf{Z}$ and $\mathbf{Z} + s\mathbf{Z}$ with orderings inherited from the reals, are order-isomorphic if and only if r is in the $\mathrm{PGL}(2, \mathbf{Z})$-orbit of s—there exist integers a, b, c, d such that $|ad - bc| = 1$ and $r = (as + b)/(cs + d)$, see [5]. This follows from $(as + b)\mathbf{Z} + (cs + d)\mathbf{Z} = \mathbf{Z} + s\mathbf{Z}$ when $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \mathrm{GL}(2, \mathbf{Z})$. For $n > 1$ and basic critical groups, perplexingly, the role of $\mathrm{PGL}(2, \mathbf{Z})$ is replaced by the semi-direct product $\mathbf{Z}^n \times_{\pi \times \rho} (S_n \times \{\pm 1\})$, where S_n is the symmetric group. This is abelian by finite, rather different from $\mathrm{PGL}(2, \mathbf{Z})$. A similar, but somewhat more restrictive description for isomorphism classes of almost basic groups, follows from the same result.

Notation for the statement of the theorem. Let $B \in \mathrm{M}_n \mathbf{Z}$ be of rank n. Suppose $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbf{R}^{1 \times n}$ is such that $\{1, \alpha_1, \ldots, \alpha_n\}$ is linearly independent over the rationals. Form the augmented matrix $\mathcal{B} = \left(\begin{smallmatrix} B \\ \alpha \end{smallmatrix} \right) \in \mathbf{R}^{(n+1) \times n}$. Set $G_{B, \alpha}$ to be the subgroup of $\mathbf{R}^{1 \times n}$ generated by the rows of $\mathcal{B}$. Then $G_{B, \alpha}$

is a critical dimension group of rank $n + 1$. If the content of ith column of B is $\delta_i \in \mathbf{Q}$, then applying Δ^{-1} on the right, where $\Delta = \mathrm{diag}(\delta_1, \ldots, \delta_n)$, we see that $B'' := B\Delta^{-1}$ is still an integer matrix, but now in $\mathcal{NS}_n$, and $G_{B,\alpha} \cong G_{B'',\alpha\Delta^{-1}}$ as partially ordered abelian groups. Hence (at a cost of multiplying the entries of α by various fractions of the form $1/k$), we may assume that B is already in $\mathcal{NS}$.

Theorem 10.1. *Let $G_{B,\alpha}$ and $G_{B',\alpha'}$ be almost basic critical groups, where $B, B' \in \mathcal{NS}_n$. If they are order isomorphic, then there exists $C \in \mathrm{GL}(n+1, \mathbf{Z})$ and $\Delta P \in P(n, \mathbf{R})^+$ (with P a permutation matrix) such that $C\mathcal{B}\Delta P = \mathcal{B}'$. Moreover,*

- (i) *in the $(n, 1)$ partition of $C = \left(\begin{smallmatrix} U & c \\ r & t \end{smallmatrix}\right)$, we have that $c = (0, 0, \ldots, 0)^T \in \mathbf{Z}^{(n-1)\times 1}$, $U \in \mathrm{GL}(n, \mathbf{Z})$, and $t \in \{\pm 1\}$,*
- (ii) *$\Delta = I$ and $UBP = B'$,*
- (iii) *α' belongs to one of $\pm\alpha P + r(B)$.*

In particular, $G_{B,\alpha} \cong G_{B',\alpha'}$ if and only if (ii) and (iii) hold.

Remark. Condition (iii) says that one of $\alpha' \pm \alpha P$ belongs to the row space of B.

Proof. First, suppose that B and B' are in $\mathcal{NS}$, α is given (so that $G_{B,\alpha}$ is a critical group), and B is PH-equivalent to B'. Then it is elementary that $G_{B,\alpha} \cong G_{B',\alpha^\pi}$ (as partially ordered groups), where π effects a permutation of the entries. To see this, suppose $UBP = B'$, where $U \in \mathrm{GL}(n, \mathbf{Z})$ and P is a permutation matrix. Let $C = U \oplus 1$. Then

$$C \binom{B}{\alpha} P = \binom{UBP}{\alpha P} = \binom{B'}{\alpha P},$$

and of course, αP is just a permutation of α. By our usual construction, this yields an order isomorphism $G_{B,\alpha} \to G_{B',\alpha P}$.

Thus given full rank $B \in \mathrm{M}_n\mathbf{Z}$ and α such that $\{1\} \cup \{\alpha_i\}$ is linearly independent over the rationals, there exists a terminal $B'' \in \mathcal{NS}_n$ such that $G_{B,\alpha}$ is order isomorphic to $G_{B'',\alpha''}$ (where α'' is obtained from α by applying some weighted permutation to the latter).

Hence we may suppose that α and α' are given (and satisfy the usual rational linear independence condition), B and B' are terminal forms in $\mathcal{NS}_n$, and there is an order isomorphism $G_{B,\alpha} \to G_{B',\beta}$. We will show that (i)–(iii) hold.

The isomorphism entails that there exist $C \in \mathrm{GL}(n+1, \mathbf{Z})$ and a weighted permutation matrix with positive real entries (here factored as diagonal times permutation), ΔP, such that $C\mathcal{B}\Delta P = \mathcal{B}'$. Partitioning the matrices as we did before and writing $B = \left(\begin{smallmatrix} \mathrm{I}_s & X \\ 0 & \mathcal{D} \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} \mathrm{I}_{s'} & X' \\ 0 & \mathcal{D}' \end{smallmatrix}\right)$ in terminal form (thus $\mathcal{D}$ is upper triangular with positive increasing entries along the diagonal, none of them 1, etc.), we have

$$\begin{pmatrix} U & c \\ r & t \end{pmatrix} \left(\begin{pmatrix} \mathrm{I}_s & X \\ 0 & \mathcal{D} \\ & & \alpha \end{pmatrix} \right) \Delta P = \left(\begin{pmatrix} \mathrm{I}_{s'} & X' \\ 0 & \mathcal{D}' \\ & & \alpha' \end{pmatrix} \right).$$

Our objective is to show that the column $c = (c_1, \ldots, c_n)^T$ is zero, and we achieve this by exploiting the numerous zeros in the matrices. Then it is elementary that Δ must be the identity and $UBP = B'$, and moreover, $|\det U| = 1$ is immediate.

From the equation

$$\begin{pmatrix} U & c \\ r & t \end{pmatrix} \begin{pmatrix} B \\ \alpha \end{pmatrix} \Delta = \begin{pmatrix} B'P^{-1} \\ \alpha P^{-1} \end{pmatrix},$$

we obtain

$$(UB + c\alpha)\Delta = B'P^{-1}, \quad rB + t\alpha = \alpha'P^{-1}.$$

One of the columns of $B'P^{-1}$, say the hth, is the first standard column basis element. Hence for all i,

$$\big((UB)_{ih} + c_i\alpha_h\big)\delta_h = \begin{cases} 1 & \text{if } i = 1, \\ 0 & \text{if } i > 1. \end{cases}$$

Hence if $i > 1$, $(UB)_{ih} + c_i\alpha_h = 0$. As the first term and c_i are integers, and $\{1, \alpha_h\}$ is linearly independent over the rationals, we deduce $c_i = 0$ (and $(UB)_{ih} = 0$). Assume $c_1 \neq 0$; we will obtain a contradiction.

Write $U = \{\gamma_{ij}\}$. As the first column of B is the first standard basis element, we have $(UB)_{i1} = \gamma_{i1}$. Thus $(\gamma_{i1} + c_i\alpha_1)\delta_1 \in \mathbf{Z}$ (as these are the entries of a column of $B'P^{-1}$). Hence for $i > 1$, $\gamma_{i1} \in \delta_1^{-1}\mathbf{Z}$ (as the corresponding c_i are zero). If for some $i > 1$, $\gamma_{i1} \neq 0$, then δ_1 is rational. From $\gamma_{11} + c_1\alpha_1 \in \delta_1^{-1}\mathbf{Z}$ together with the rational linear independence of $\{1, \alpha_1\}$, we deduce $c_1 = 0$, a contradiction. Hence $\gamma_{i1} = 0$ for all $i > 1$.

Now consider the second column of UB; as B is upper triangular, $(CB)_{i2} = \gamma_{i1}B_{12} + \gamma_{22}B_{22}$ and $B_{22} \neq 0$. Hence

$$\gamma_{i1}B_{12} + \gamma_{i2}B_{22} + c_i\alpha_2 \in \frac{1}{\delta_2}\mathbf{Z}.$$

If $i > 1$, this simplifies to $\gamma_{i2}B_{22} \in \delta_2^{-1}\mathbf{Z}$; thus if $\gamma_{i2} \neq 0$ for some $i > 1$, then δ_2 is rational. Hence, $\gamma_{11}B_{12} + \gamma_{12}B_{22} + c_1\alpha_2 \in \delta_2^{-1}\mathbf{Z} \subset \mathbf{Q}$. As $c_1 \neq 0$, the rational linear independence of $\{1, \alpha_2\}$ is impossible, a contradiction. Hence $\gamma_{i2} = 0$ for $i > 1$.

Thus the first, second, and $(n+1)$st columns of the matrix $C \in \mathrm{GL}(n+1, \mathbf{Z})$ are

$$\begin{pmatrix} \gamma_{11} \\ 0 \\ 0 \\ \vdots \\ 0 \\ r_1 \end{pmatrix}, \quad \begin{pmatrix} \gamma_{12} \\ 0 \\ 0 \\ \vdots \\ 0 \\ r_2 \end{pmatrix}, \quad \begin{pmatrix} c_1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ t \end{pmatrix}.$$

These generate a subgroup of rank only two, so that $\mathrm{rank}\, C < n+1$. This final contradiction shows that $c_1 = 0$, and thus c is zero.

Thus $C = \left(\begin{smallmatrix} U & 0 \\ r & t \end{smallmatrix}\right)$, and so $1 = |\det C| = |t \det U|$. Then $t = \pm 1$ and $U \in \mathrm{GL}(n, \mathbf{Z})$ yielding (i) and of course the equations simplify to $UB\Delta = B'P^{-1}$.

Since B and B' are invertible in $\mathrm{M}_n\mathbf{Q}$, this forces $\delta_i \in \mathbf{Q}^+$ for all i. In particular, there exists an integer N such that $N\Delta$ is an integer matrix (with positive entries).

As B and B' have all their columns unimodular, so do UB (as $U \in \mathrm{GL}(n, \mathbf{Z})$) and $B'P^{-1}$. Thus the content of the ith column of $NUB\Delta$ is $N\delta_i$ while that of $NB'P^{-1}$ is just N. Hence $N\delta_i = N$, so $\Delta = \mathrm{I}$. Thus (finally)

$$UBP = B', \quad rB \pm \alpha P = \alpha'.$$

This yields (ii) and (iii), and the final statement is a consequence of this and the remarks early in the proof. $\qquad\square$

Proposition 10.2. *Let $n > 1$, $\alpha = (\alpha_1, \ldots, \alpha_n), \alpha' = (\alpha'_1, \ldots, \alpha'_n) \in \mathbf{R}^n$ be such that both $\{\alpha_i\}_{i=1}^n \cup \{1\}$ and $\{\alpha'_i\}_{i=1}^n \cup \{1\}$ are linearly independent over the rationals. The basic critical dimension groups G_α and $G_{\alpha'}$ (generated by $\{e_1, \ldots, e_n; \alpha\}$ and $\{e_1, \ldots, e_n; \alpha'\}$, respectively) are order isomorphic if and only if α' is in the orbit of α under the action of $\mathbf{Z}^n \times_{\Pi \times \rho} (S_n \times \mathbf{Z}_2)$.*

Proof. Here we have $B = B' = \mathrm{I}$, so the criterion of the theorem simplifies to $\alpha' \pm \alpha P \in \mathbf{Z}^{1 \times n}$. $\qquad\square$

Corollary 10.3. *Almost basic critical groups of rank at least three admit no nontrivial order-automorphisms.*

Proof. From $C\mathcal{B}\Delta P = \mathcal{B}$ (the order-automorphisms on a critical group automatically extend to order-automorphisms of the closure, $\mathbf{R}^n$, hence must be given by weighted permutation matrices), the preceding yields $\pm\alpha + rB = \alpha P$. If π is the permutation induced by P, and $\pi(i) = j \neq i$ for some i and j, then $\alpha_j \pm \alpha_i \in \mathbf{Z}$; but this contradicts the rational linear independence of $\{1, \alpha_i, \alpha_j\}$. Hence P is the identity. Thus, by the preceding, $B = UBP = UB$; as B is of full rank, this forces U to be the identity, and thus the only automorphism is the identity. $\qquad\square$

This contrasts with the critical groups discussed in [10]; those arose from integral orders in totally real fields with one real embedding discarded, and are classified by their ideal class structure. In those cases, there are plenty of order automorphisms, arising from some of the units in the number field.

For an abelian group J, the torsion-free rank of J, that is, the rank of J modulo its torsion subgroup, is denoted tf rank J.

Theorem 10.4. *Let G be a critical group of rank $n + 1$, with $n > 1$. Let u be any order unit for it. The following are equivalent:*

(a) *The torsion-free rank of $G/E(G)$ is one.*
(b) *For all $\sigma \in \partial_e S(G, u)$, the intersection $\cap_{\tau \in \partial_e S(G,u) \setminus \{\sigma\}} \ker \tau$ is nonzero.*
(c) *There exists a basic critical group G' such that $G \otimes \mathbf{Q}$ is order-isomorphic to $G' \otimes \mathbf{Q}$.*
(d) *Every proper subset of $\partial_e S(G, u)$ is ugly.*
(e) *G is almost basic.*

Proof. (a) if and only if (b): Property (b) is equivalent to rank $E(G) = n$ (since the sum $\sum x_i \mathbf{Z}$ is direct), which is equivalent to tf rank $G/E(G) = 1$.

(b) implies (c). For each i, there exists $x_i \in G$ unique with respect to the properties $\bigcap_{\tau_j \in \partial_e S(G,u) \setminus \{\tau_i\}} \ker \tau_j = x_i \mathbf{Z}$ and $\tau_i(x_i) > 0$. Then $E(G) := \sum x_i \mathbf{Z}$ is free of rank n and there exists $y \in G$ such that $G_0 = E(G) \oplus y\mathbf{Z}$ is of finite index in G. As G is dense in $\mathbf{R}^n$, so is G_0.

As a subgroup of G of rank less than $n+1$, $E(G)$ is discrete; being of rank n, any $\mathbf{Z}$-basis for it is also an $\mathbf{R}$-basis for $\mathbf{R}^n$. Hence there exist $\alpha_i \in \mathbf{R}$ such that $y = \sum \alpha_i x_i$. The density of G_0 in $\mathbf{R}^n$ entails that $\{1, \alpha_1, \ldots, \alpha_n\}$ is linearly independent over the rationals, and G_0 is a dimension group with respect to the strict ordering, which obviously agrees with the relative ordering inherited from G, and its pure traces are the restrictions of τ_i, which we will also call τ_i.

Set $u = \sum x_i$, so that $\tau_i(u) = \tau_i(x_i) > 0$ for all i. Thus u is an order unit in both G_0 and G. Normalize the traces of G_0 with respect to u—the pure traces are now $\tilde{\tau}_i$ given by $\tilde{\tau}_i(g) = \tau_i(g)/\tau_i(u)$. The normalized traces now satisfy $\tilde{\tau}_i(x_j) = \delta_{ij}$ (Kronecker delta). Hence the embedding $(G_0, u) \to \operatorname{Aff} S(G_0, u)$ realizes G_0 as a basic critical group.

Since G_0 is of finite index in G, $G_0 \otimes \mathbf{Q} = G \otimes \mathbf{Q}$.

(c) implies (d). For any trace τ on any dimension group G, $\ker \tau \otimes 1_{\mathbf{Q}} = (\ker \tau) \otimes \mathbf{Q}$. Thus $\operatorname{rank} \ker \tau = \operatorname{rank} \ker(\tau \otimes 1_{\mathbf{Q}})$. As G is critical, every subgroup of less rank than $n+1$ is discrete, and the result follows.

(d) implies (e). For a pure trace τ_i, let $\Omega(i)$ be the complement of $\{\tau_i\}$ in $\partial_e S(G, u)$. As $\Omega(i)$ is ugly, $\bigcap_{\tau \in \Omega(i)} \ker \tau$ is not zero, and being discrete and spanning $\Omega(i)^{\perp}$ over the reals, it must be rank one. As it is a subgroup of a free group, it is free, so it equals $x_i \mathbf{Z}$ for some $x_i \in G$, and we may assume $\tau_i(x_i)$ is positive. Now we are in a position to use the method of proof in (b) implies (c), coming up with a basic critical group G_0 of finite index in G. There thus exists an integer N such that $NG \subseteq G_0$, and NG is obviously order isomorphic to G, while $G_0 \subset \mathbf{Z}^n$. Any subgroup of a free group is free, so we can find the desired basis.

(e) implies (a). Trivial. $\qquad \square$

Example 10.5. Critical dimension groups that are not almost basic, but such that all of whose pure traces τ_i are ugly and with all $\tau_i(G)$ equal.

Let r be a real number that is neither rational, quadratic, nor cubic over the rationals; that is, the set $\{1, r, r^2, r^3\}$ is linearly independent over the rationals. Let G be the subgroup of $\mathbf{R}^3$ spanned by

$$\left\{ E_1 := (1,1,1),\ E_2 := (1,1,r),\ E_3 := (1,r,0),\ E_4 = (r,0,0) \right\}.$$

The set of four 3×3 determinants of the spanning set is linearly independent over the rationals. Hence G is dense in $\mathbf{R}^3$, and thus with the strict ordering, is a critical group (of rank three).

The pure traces on G are the three coordinate maps, denoted τ_i. Then we see that $\tau_1(G) = \mathbf{Z} + r\mathbf{Z} = \tau_2(G) = \tau_3(G)$, free of rank two. In all three cases, the kernel is free of rank two, and since the affine representation is one to one,

and since the kernels are discrete subgroups, the corresponding pure traces are ugly. However, $\ker \tau_1 \cap \ker \tau_3 = \{0\}$; by Lemma 9.1, the subset $\Omega = \{\tau_1, \tau_3\}$ is not ugly. By Theorem 10.4 (d), G cannot be almost basic.

This leads to a class of non-basic critical groups free of rank $n + 1$ such that all $\tau_i(G)$ are equal and of rank two (hence all the pure traces are ugly). Pick r such that $\{1, r, \ldots, r^n\}$ is linearly independent over the rationals (that is, either r is transcendental or its algebraic degree is at least $n + 1$). Define the following elements of $\mathbf{R}^n$:

$$
\begin{aligned}
F_n &= \begin{pmatrix} r & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}, \\
F_{n-1} &= \begin{pmatrix} 1 & r & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}, \\
F_{n-2} &= \begin{pmatrix} 1 & 1 & r & \cdots & 0 & 0 & 0 \end{pmatrix}, \\
&\ \ \vdots \qquad\qquad\qquad \ddots \\
F_1 &= \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & r \end{pmatrix}, \\
F_0 &= \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 \end{pmatrix}.
\end{aligned}
$$

That is, F_i has $i - 1$ zeros (for $i \geq 1$), immediately preceded by r, which in turn is immediately preceded by enough ones to fill up the row. Let M_i be the $n \times n$ matrix obtained by deleting F_i, and throwing together the rest of the F_j. Then $\det M_0 = r^n$ and $|\det M_1| = r^{n-1}$ as is easily seen from the lower triangular forms. For $i > 1$, M_i is a block lower triangular matrix, and it is straightforward to check that $\det M_i = r^{n-i}(1 - r)^{i-1}$. (At one point, multiply the matrix $rN^T + I + N + N^2 + \cdots$ by $I - N$, creating an upper triangular matrix. See Lemma 10.6 below.) Next we claim that the set $\{r^n, r^{n-1}, r^{n-2}(1 - r), \ldots, r(1 - r)^{n-2}, (1 - r)^{n-1}\}$ spans $\sum_{i=0}^{n} r^i \mathbf{Q}$, which is easily checked by induction. Hence the set is linearly independent over the rationals.

Thus $G \equiv G(n, r)$ is a critical group of rank $n + 1$, so with the strict ordering inherited from $\mathbf{R}^n$ is a simple dimension group with n pure traces, the latter arising as the coordinate functions. Their value groups, that is, the ranges of the pure traces, are all equal to the rank two group, $\mathbf{Z} + r\mathbf{Z}$. In particular, their kernels are necessarily of rank $n - 1$ and discrete (the latter from being a critical group), and it easily follows that they are all ugly.

We have that $G(n, r) \subset (\mathbf{Q} + r\mathbf{Q})^n$ is of rank $n + 1$, and is dense in $\mathbf{R}^n$; we have assumed r does not satisfy a rational equation of degree n or less.

Now we can show that $G(n, r)$ is not almost basic; assume $n \geq 3$. It is an easy exercise to show that $\ker \tau_n$ has $\{F_2, F_3, \ldots, F_n\}$ as $\mathbf{Z}$-basis, and $\ker \tau_1$ is spanned by $\{F_{n-1} - F_0, F_{n-2} - F_0, \ldots, F_1 - F_0\}$. The intersection is spanned by $\{F_{n-1} - F_2, \ldots, F_3 - F_2\}$, which has only $n - 3$ elements. Thus $\ker \tau_1 \cap \ker \tau_n$ has rank $n - 3$. With $\Omega = \{\tau_1, \tau_n\}$, we see that Ω is not ugly by Lemma 9.1, and by Theorem 10.4 (d), $G(n, r)$ is not almost basic.

Lemma 10.6. *Let N be the lower triangular $k \times k$ matrix with ones in the $(j+1, j)$ entries and zeros every where else. Let r be any real number, and set $Q = rN^T + I + N + N^2 + \cdots$. Then $\det Q = (1-r)^{k-1}$.*

Proof. Multiply Q from the left by $I - N$ (which has determinant 1); the outcome is $I - rNN^T + rN^T$. Now NN^T is just the identity matrix less the first 1, so that $(I - N)Q$ is upper triangular, with diagonal entries $(1, 1-r, 1-r, \ldots, 1-r$. Hence $\det Q = (1-r)^{k-1}$. $\square$

When $n > 2$, the construction $G(n, r)$ does not yield a basic critical group, but we can still construct basic ones with the property that all the value groups of the pure traces are order isomorphic.

Example 10.7. Basic critical groups G such that all value groups, $\tau_i(G)$, are mutually order isomorphic.

Let r be a positive real number that satisfies no nontrivial integer polynomial of degree n or less. Then the set $\{1, r, r/(1+r), r/1 + 2r, \ldots, r/(1+(n-1)r)\}$ is linearly independent over the rationals. This is a routine exercise, which becomes trivial if we assume r is transcendental. Hence there is a basic critical group whose last row is $(r, 1/(1+r), \ldots, 1/(1+(n-1)r))$. The respective value groups of the pure traces are $\mathbf{Z} + r\mathbf{Z}, \mathbf{Z} + (r/(1+jr)\mathbf{Z}$ $(1 \le j \le n-1)$. But these are all isomorphic (multiply $\mathbf{Z} + (1/(1+jr)\mathbf{Z}$ by $1 + jr$; this is an order isomorphism to $(1 + jr)\mathbf{Z} + r\mathbf{Z} = \mathbf{Z} + r\mathbf{Z}$).

11. Unperforation of quotients

In this section, we want to ensure that the quotient pre-ordered groups of almost basic critical groups by kernels of subsets of $\partial_e S(G, u)$ are themselves almost basic; the crucial property is that these quotients are unperforated. The following result suggested and motivated the $\mathcal{J}(B)$ invariant of PH-equivalence.

Proposition 11.1. *Let G be an almost basic critical group of rank $n + 1$. Let $\Omega \subset \partial_e S(G, u)$, and define $L = \ker \Omega := \bigcap_{\tau \in \Omega} \ker \tau$. Then $G/\ker \Omega$, equipped with the quotient ordering, is an almost basic critical group with pure trace space Ω.*

This boils down to showing the quotient is unperforated, something that is obvious for basic critical groups (and the quotients are themselves basic critical groups), but not so obvious for almost basic ones. This provides an alternative path to the definition of $J((B^{\mathrm{op}})_\Omega)$ as the torsion subgroup of $G_\Omega/E(G_\Omega)$, where $G_\Omega = G/\ker \Omega$ (for $\Omega \subset \partial_e S(G, u)$, the latter identified with $\{1, \ldots, n\}$).

The following is a slight improvement on [2, App. B, Prop. 1 and 2], not covered by the results there.

Lemma 11.2. *Let (G, u) be a simple unperforated group with order unit, and let L be a convex subgroup of G such that G/L is torsion-free. Suppose that the closure of the image of L, $\overline{L}$, in $\mathrm{Aff}\, S(G, u)$, contains a subgroup of the form $D + P$, where D is a rational vector space and P is generated by nonnegative*

elements of Aff $S(G, u)$, *and* $\overline{L}/(D + P)$ *is torsion. Then, equipped with the quotient ordering, G/L is unperforated.*

Remark. For example, if G is basic, say with generators $\{e_i; \sum \alpha_j e_j\}$, and $L = \ker S$ (where $S \subset \{\tau_i\}$), then L is generated by $\{e_i\}_{\{i | \tau_i \notin S\}}$. Each e_i has image in Aff $S(G, u) = \mathbf{R}^n$ as e_i itself, which is nonnegative in the affine function space (of course, the e_i is not in the positive cone of G, since the ordering is the strict one). By [2, App. B], the quotient is nicely behaved.

Remark. The lemma above removes the density condition on $D + P$ (that it be dense in $\overline{L}$) [*op. cit.*], and replaces it with a different requirement. This is particularly useful when L is already discrete, hence closed in the affine representation; then $D = 0$, but P need only be a subgroup; this will automatically be closed, so that L need not equal P. But the lemma here says that sufficient for unperforation is that $\operatorname{rank} P = \operatorname{rank} L < \infty$, which is easy to verify for almost basic critical groups.

Proof. The convexity condition (which in the simple case boils down to $L \cap G^+ = \{0\}$) is sufficient to guarantee that the quotient pre-ordering is a partial ordering, that is, an element that is both positive and negative must be zero.

If $kg + L = L$, then torsion-freeness of the quotient entails $g \in L$. Hence we may assume that $kg + L \in (G/L)^+ \setminus \{0\}$.

Suppose $g \in G$ and k is a positive integer such that $kg + L \in G^+ \setminus \{0\}$. We may thus find $x \in L$ such that $kg + x$ is an order unit. Let

$$\epsilon = \inf_{\sigma \in S(G,u)} \sigma(kg + x) = \inf_{\sigma \in S(G,u)} (\widehat{kg + x})(\sigma) > 0.$$

There exists a positive integer N such that $N\widehat{x}$ is in the norm closure of $D + P$. Select an integer M to be determined (as a function of k and N).

We may find $d \in D$ and $p \in P$ such that $\|N\widehat{x} - d - p\| < \epsilon/M$. There exists (from the definition of D) $d' \in D$ such that $d = Nkd'$; so $\|N\widehat{x} - Nkd' - p\| < \epsilon/M$. We may write $p = p_1 - p_2$, where $p_i \geq 0$ and $p_i \in P$ (in particular, $p_i \in \overline{L}$).

There exists $f \in L$ such that $\|\widehat{f} - d'\| < \epsilon/M$ and $q_i \in L$ such that $\|\widehat{q_i} - p_i\| < \epsilon/M$. In particular, $\widehat{q_i} \geq -\epsilon \mathbf{1}/M$ as functions on $S(G, u)$.

Set

$$z = Nkg + Nkf + Nkq_1 = Nk(g + f + q_1).$$

If we can show $z \in G^+$, then as G itself is unperforated, it would follow that $g + f + q_1 \in G^+$, and so $g + L$ is in the positive cone of the quotient. So it suffices to show $z \in G^+$.

We have

$$z - N(kg + x) = Nkf + Nkq_1 - (Nx - Nkf - q_1 + q_2) - Nkf - q_1 + q_2$$
$$= Nkq_1 + q_2 - (Nx - Nkf - q_1 + q_2);$$

evaluating at $\sigma \in S(G, u)$,

$$\sigma(z) \geq N\sigma(kg + x) + Nk\sigma(q_1) + \sigma(q_2) - \|N\widehat{x} - Nk\widehat{f} - \widehat{q_1} + \widehat{q_2}\|$$

$$\geq N\epsilon - \frac{Nk\epsilon}{M} - \frac{\epsilon}{M} - \|N\widehat{x} - Nkd' - p\| - Nk\|\widehat{f} - d'\|$$
$$- \|\widehat{q_1} - p_1\| - \|\widehat{q_2} - p_2\|$$

$$\geq \epsilon\Big(N - \frac{Nk+1}{M} - \frac{1}{M} - \frac{Nk\epsilon}{M} - \frac{2}{M}\Big)$$

$$= \epsilon\Big(N - \frac{2Nk+4}{M}\Big).$$

If we select $M > 2k + 4/N$ (e.g., $M = 2k + 6$), $\widehat{z}$ is strictly positive, so that z is an order unit of G, and we are done. $\square$

Corollary 11.3. *Suppose G is a simple dimension group with an order unit u. Let L be a convex subgroup of G such that G/L is torsion-free and the image of L in $\operatorname{Aff} S(G, u)$ is discrete. Sufficient for G/L to be a simple dimension group (with respect to the quotient ordering) is that there exist a subgroup L_0 of L such that L/L_0 is torsion, and the image of L_0 is generated by its nonnegative elements (with respect to the usual ordering on $\operatorname{Aff} S(G, u)$). In this case, the trace space of $(G/L, u + L)$ is a closed face of $S(G, u)$.*

Proof. Since the image of L is discrete, its image is already closed in $\operatorname{Aff} S(G, u)$; the hypothesis ensures that $\widehat{L_0} = P$ satisfies $\widehat{L}/P$ is torsion, so the preceding applies with $D = 0$. Hence G/L is unperforated. Simplicity is automatic.

Since L/L_0 is torsion, if $\tau \in S(G, u)$ kills L_0, it automatically kills L. Hence $L^\vdash = L_0^\vdash$. Let $P^+ = P \cap \operatorname{Aff} S(G, u)^+$ (the latter with the usual, not the strict ordering), so that $P = P^+ - P^+$. Since L_0 maps to P, and $P^\vdash = (P^+)^\vdash$, we have that $L^\vdash$ is a (closed) face, call it F, of $S(G, u)$. In particular, F is a Choquet simplex.

Let ϕ be a trace of G/L; then ϕ induces a trace of G, with kernel containing L. Thus $\phi \in L^\vdash = F$. Conversely any element of F kills L and thus induces a trace on G/L. Hence the map $S(G/L, u + L) \to F$ is an affine bijection; it is obviously continuous, so by compactness of $S(G/L, u + L)$, it is an affine homeomorphism.

Select an element $h \in \operatorname{Aff} F$; this lifts to an element $j \in \operatorname{Aff} S(G, u)$. Given ϵ, there exists $g \in G$ such that $\|\widehat{g} - j\| < \epsilon$, that is, $\sup_{\sigma \in S(G, u)} |\sigma(g) - j(\sigma)| < \epsilon$. This implies $\sup_{\sigma \in F} |\sigma(g) - j(\sigma)| < \epsilon$, and together with the affine homeomorphism, this forces the image of G/L to be dense in $\operatorname{Aff} F$, hence in its affine representation (with respect to $u + L$). As G/L is unperforated and simple, its ordering must be the strict one inherited from affine functions on a Choquet simplex, and thus G/L is a dimension group. $\square$

Proof of Proposition 11.1. Let F be the face spanned by Ω (since $\operatorname{Aff} S(G, u)$ is a finite-dimensional simplex, it is simply the convex hull of Ω). By Proposition 10.4 (c), there exists a basic critical group G_0 of finite index in G (whose relative ordering agrees with its usual one). Then $\ker \Omega \cap G_0$ is generated by

elements with nonnegative image in Aff $S(G, u)$, and this is of finite index in ker Ω. By the result above, $G/\ker S$ is a simple dimension group, and its pure trace space is just the set of extreme points of F, which is Ω. $\qquad\square$

Connections to PH-equivalence. This was the starting point for the development of $(J(B_\Omega^{\mathrm{op}}))_{\Omega \subset S}$, the directed family of PH-invariants; when G is generated by the row space of B and α, then the torsion subgroup of $G_\Omega/E(G_\Omega)$ is $J((B_\Omega^{\mathrm{op}}))$.

For almost basic critical groups, $G_{B,\alpha}$, $G_{B',\alpha'}$, with $\binom{B}{\alpha}, \binom{B'}{\alpha'} \in \mathbf{R}^{n \times (n+1)}$ such that $B, B' \in \mathrm{M}_n\mathbf{Z}$ and $\det B, \det B' \neq 0$, we immediately reduce to the case that $B, B' \in \mathcal{NS}_n$, by factoring out a positive diagonal matrix, as in Section 7. Then by Theorem 10.1, $G_{B,\alpha}$ is order-isomorphic to $G_{B',\alpha'}$ if and only if B is PH-equivalent to B' and the permutation involved in the PH-equivalence sends α to α'.

Example 11.4. Examples illustrating the results.

If

$$\mathcal{B}_\alpha := \begin{pmatrix} 1 & 0 & 15 \\ 0 & 1 & 2 \\ 0 & 0 & 30 \\ \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} \quad \text{and} \quad \mathcal{B}'_{\alpha'} := \begin{pmatrix} 1 & 0 & 5 \\ 0 & 1 & 6 \\ 0 & 0 & 30 \\ \alpha'_1 & \alpha'_2 & \alpha'_3 \end{pmatrix},$$

given $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ (with $\{1, \alpha_1, \alpha_2, \alpha_3\}$ linearly independent over the rationals), there is no choice of $\alpha' = (\alpha_1, \alpha_2, \alpha_3)$ such that $G_{B,\alpha}$ is order isomorphic to $G_{B',\alpha'}$, since from Example 3.4 (first two matrices), B and B' are not PH-equivalent.

If we set $B = B'$ to be the leftmost example (the 3×3 integer matrix in $\mathcal{B}_\alpha$ above), and let $\alpha = (\sqrt{2}, \sqrt{3}, \sqrt{5})$ and $\alpha' = (\sqrt{3}, \sqrt{2}, \sqrt{5})$, then even though the integer matrix parts are the same, the resulting critical dimension groups are not order isomorphic. The permutation $\pi = (12)$ and its corresponding matrix $P = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \oplus (1)$ does not fix B, as follows from Proposition 2.1, with no invertible elements in the column (modulo $d = 30$).

Appendix A. A general duality result

This appendix gives fairly general duality results about orbits under natural actions, that appear in Section 6. Here R will be a not necessarily commutative ring (of course with 1), but not much additional effort is required to prove the corresponding results over noncommutative rings.

Let R be a ring, and $n > k$ be positive integers. A matrix with entries from a ring will be called *invertible* if it is square and two-sided invertible; sometimes we add *two-sided*, for emphasis. We follow [3] in saying an $n \times k$ matrix M is *completable* if there exists an $n \times (n-k)$ matrix W such that the $n \times n$ matrix $(W\ M)$ is invertible. Invertibility of this matrix is equivalent to the columns constituting an R-basis for $R_R^{n \times 1}$ (as a right R-module).

If instead, $n < k$, then we say M is *completable* if there exists a $(k-n) \times k$ matrix W such that the $k \times k$ matrix $\binom{W}{M}$ is invertible. If $n = k$, then completable is simply invertible.

These notions date back to the origins of K-theory.

The ring of $n \times n$ matrices will be denoted $\mathrm{M}_n R$, but the set of non-square rectangular matrices with k rows and n columns will be denoted $R^{k \times n}$. We denote by $\mathrm{GL}(k, R)$ (or simply $\mathrm{GL}(k)$ if no ambiguity will result) the group of invertible matrices in $\mathrm{M}_n R$. The group of invertible elements of R will be denoted $R^\times$.

The next two lemmas are obvious.

Lemma A.1. *Let $M \in R^{n \times k}$, with $n > k \geq 1$. The following are equivalent:*

    (a) *M is completable.*

    (b) *The set of columns of M can be enlarged to a basis of size n of $R^{n \times 1}$ as a right R-module.*

    (c) *There exists a right R-submodule L of $R^{n \times 1}$ that is free on $n - k$ generators such that $L \oplus M(R^{k \times 1}) = R^{n \times 1}$.*

Lemma A.2. *Let $M \in R^{n \times k}$, with $k > n \geq 1$. The following are equivalent:*

    (a) *M is completable.*

    (b) *The set of rows of M can be enlarged to a basis of size k of ${}_R R^{k \times 1}$ as a left R-module.*

    (c) *There exists a left R-submodule L of $R^{1 \times k}$ that is free on $k - n$ generators such that $L \oplus (R^{1 \times n})M = R^{1 \times k}$.*

Lemma A.3. *Let A, B, and C be respectively in $\mathrm{M}_{n-k}R$, $R^{(n-k) \times k}$, and $\mathrm{M}_k R$, with $C \in \mathrm{GL}(k, R)$, and set $E := \left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix} \right) \in \mathrm{M}_n R$. Then $A \in \mathrm{GL}(n - k, R)$ if and only if $E \in \mathrm{GL}(n, R)$.*

Proof. Suppose that E is invertible. Let U be the inverse of E; partitioned in the same way as E, we can write $U = \left(\begin{smallmatrix} Q & S \\ T & V \end{smallmatrix} \right)$, and we have

$$\begin{pmatrix} \mathrm{I}_{n-k} & 0 \\ 0 & \mathrm{I}_k \end{pmatrix} = UE = \begin{pmatrix} QA & QB + SC \\ TA & TV + VC \end{pmatrix}$$
$$= EU = \begin{pmatrix} AQ + BT & AQ + BT \\ CT & CV \end{pmatrix}.$$

From $CT = 0$ (second matrix, lower left) and invertibility of C (two-sided invertibility, that is), we deduce $T = 0$ (of the appropriate dimensions). From the upper left corners of each matrix, we then have $AQ = QA = \mathrm{I}_{n-k}$, so $A \in \mathrm{GL}(n - k, R)$.

Conversely, suppose that A is invertible. Multiply E on the left by $A^{-1} \oplus C^{-1} \in \mathrm{GL}(n, R)$, resulting in $\left(\begin{smallmatrix} \mathrm{I}_{n-k} & A^{-1}B \\ 0 & I_k \end{smallmatrix} \right)$; this has inverse $\left(\begin{smallmatrix} \mathrm{I}_{n-k} & -A^{-1}B \\ 0 & I_k \end{smallmatrix} \right)$, so E is a product of two invertible matrices, hence is invertible. $\square$

A ring R is *stably finite* if for all matrix rings $\mathrm{M}_n R$ and elements $x \in \mathrm{M}_n R$, x is right invertible implies x is invertible. This is a two-sided condition, and is equivalent to onto right module homomorphisms $x \colon R^{n \times 1} \to R^{n \times 1}$ always being isomorphisms, or equivalently, if the left module homomorphism ${}_R R^{1 \times n} \leftarrow {}_R R^{1 \times n} \colon x$ is onto, then x is an isomorphism.

The ring R has the property that *stably free modules are free* (SFF) if whenever $R^n \cong R^k \oplus Q$ as right R-modules, then Q is free. This property is also right/left symmetric. This property also hearkens back to the origins of K-theory, e.g., what was formerly Serre's conjecture, now known as the Quillen–Suslin theorem.

Finally, R has *invariant basis number* (IBN) if $R^m \cong R^n$, as right R-modules implies $m = n$. This is again left/right symmetric, and it is easy to check that stably finiteness implies IBN. The reverse implication is well known not to be true; e.g., the ring generated by the unilateral shift and its transpose (defined on $l^2(\mathbf{Z}^+)$) has the IBN property but is not stably finite. However, SFF and IBN together imply stable finiteness. (*Proof*: Suppose that the right R-module homomorphism $x\colon R^n \to R^n$ is onto. It splits since the image is free; this yields $R^n \cong R^n \oplus Q$ for the module $Q = \ker x$. SFF implies that Q is free, and IBN entails that it must be free on zero generators, hence zero. So x is an isomorphism.)

For the computations in Section 6, we only deal with rings of the form $R = \mathbf{Z}_d$. All of these, and $\mathbf{Z}$ itself, satisfy both SFF and stable finiteness (the latter being trivial, since the rings are commutative).

Kaplansky [14, p. 498] had a limited definition of *Hermite rings.* Lam [15, p. 26] defines Hermite to mean a ring satisfying SFF. Cohn [3, Section 0.4] refers to a ring satisfying SFF and IBN as an Hermite ring (Charles Hermite was French, so the initial H is pronounced as a stop, requiring *an*, not *a*; this practise is adopted in [14] and many subsequent papers). To avoid confusion, particularly in view of the main subject of this paper, we will not use this term at all, nor IBN.

Sometimes, to emphasize the chirality of a module (left or right) over the ring R, we place a subscripted R beside it: thus $_R Q$ means Q considered as a left module, and Q_R means as a right R-module.

Lemma A.4. *Let R be a stably finite ring satisfying SFF. Suppose $n > k$ are positive integers. Let $M \in R^{n \times k}$. The following are equivalent:*

  (a) *The set of columns of M is a right R-module basis for a free direct summand of $R_R^{n \times 1}$.*
  (b) *There exists $W \in R^{n \times (n-k)}$ such that $U \coloneqq (W \quad M) \in \mathrm{GL}(n, R)$.*
  (c) *The left R-submodule of $_R R^{1 \times n}$ spanned by the rows of M is all of $_R R^{1 \times n}$.*

Remark. It is not sufficient (in (c)) that the row space be free on k generators; $R = \mathbf{Z}$ yields an example.

Remark. The right versus left hypotheses are important (unless R is commutative), as shown in Example A.5.

Proof. (a) implies (b). Let V be the (right) submodule of $R^{n \times 1}$ spanned by the columns of V; by hypothesis, it is free with k generators, and there exists a submodule X of $R^{n \times 1}$ such that $R^{n \times 1} = X \oplus V$. Since V is free, SFF implies that X is free, and stable finiteness guarantees that it is free on $n - k$

generators. Label them $w_1, w_2, \ldots, w_{n-k}$, and let W be the resulting $n \times (n-k)$ matrix (whose ith column is w_i). From the direct sum decomposition, the set of columns of $U = (W \ M)$ is a basis for $R^{n \times 1}$. Thus the map $U \colon R^{n \times 1} \to R^{n \times 1}$ is a homomorphism of right R-modules which is onto. Stable finiteness now yields that U is (two-sided) invertible.

(b) implies (c). Given $U = (W \ M)$ invertible, define the map of left modules, $_R R^{1 \times n} \leftarrow {_R R^{1 \times n}} : U$ (given by right multiplication of course, hence the weird notation). This is an isomorphism (since U is invertible). Now consider the images of M and W separately. Identifying $_R R^{1 \times (n-k)}$ and $_R R^{1 \times k}$ with respectively the submodules of $_R R^{1 \times n}$ having zeros in the bottom k positions and zeros in the top $n - k$ positions, we have that the respective ranges satisfy $(_R R^{1 \times n})W \subset {_R R^{1 \times (n-k)}}$ and $(_R R^{1 \times n})M \subset {_R R^{1 \times (k)}}$. Since U (as a homomorphism of left modules) is onto, the sum of the two ranges is all of $(_R R^{1 \times n})$, and since the respective images have zero intersection, it follows that $(_R R^{1 \times n})M = {_R R^{1 \times (k)}}$. But this is precisely condition (c).

(c) implies (b). Again, view M as a left module homomorphism $_R R^{1 \times k} \leftarrow {_R R^{1 \times n}} : M$. Hypothesis (c) says that M is onto, so the map splits. Hence there exists $V \in R^{k \times n}$ such that VM is the identity on $_R R^{1 \times k}$ (one of the peculiarities of left module homomorphisms is that they compose in the correct order, unlike what we are used to with right modules). Moreover, we have a direct sum decomposition $_L \ker M \oplus Z = {_R R^{1 \times n}}$, where $_L \ker M$ is the kernel of M as a left module homomorphism, and Z is obtained from the splitting, and moreover, left multiplication by M induces an isomorphism $_R R^{1 \times k} \leftarrow Z$.

As in the proof of (a) implies (b), SFF and stable finiteness imply that $_L \ker M$ is free on $n - k$ generators. Identifying $_R R^{1 \times k}$ with the submodule of $_R R^{1 \times n}$ consisting of elements whose leftmost $n - k$ entries are zero (and similarly $_R R^{1 \times (n-k)}$ with the obvious complementary submodule), we define $W \in R^{n \times (n-k)}$ acting (on the right of course) as an isomorphism $_R R^{1 \times (n-k)} \leftarrow {_L \ker M}$, and zero on Z.

Now define the $n \times n$ matrix $U = (W \ M)$, and observe that its range (as a left module homomorphism) is all of $_R R^{1 \times n}$. As R is stably finite, this implies that U is invertible.

(b) implies (a). Let Z be the inverse of $U = (W \ M)$. Invertibility entails that the set of columns of U is a basis for $R^{n \times 1}$. Let V_1 be the right R-module span of the set of columns of W, and V_2 the span of the set of columns of M.

Then $R^{n \times 1} = V_1 + V_2$; from the fact that the set of all columns is a basis, we have $R^{n \times 1} = V_1 \oplus V_2$. Since any subset of a basis is itself a basis for the submodule it generates, we have that V_2 is free, necessarily on the k generators arising from the columns of M. $\square$

Suppose that $n > k$. Define the following subsets of rectangular matrices over R:

$$C(n, k) = \big\{ M \in R^{n \times k} \mid M \text{ is completable} \big\},$$
$$C'(n, k) = \big\{ M \in R^{k \times n} \mid M \text{ is completable} \big\},$$

$$F(n, k) = \left\{ M \in R^{n \times k} \;\middle|\; \begin{array}{l} M \text{ contains a set of } k \text{ rows} \\ \text{whose corresponding matrix is invertible} \end{array} \right\},$$

$$F'(n, k) = \left\{ M \in R^{k \times n} \;\middle|\; \begin{array}{l} M \text{ contains a set of } k \text{ columns} \\ \text{whose corresponding matrix is invertible} \end{array} \right\},$$

$$F_i(n, k) = \left\{ M \in R^{n \times k} \;\middle|\; \begin{array}{l} M \text{ contains exactly } i \text{ sets of } k \text{ rows} \\ \text{whose corresponding matrix is invertible} \end{array} \right\}$$
$$\text{for each } i = 1, 2, \ldots, \tbinom{n}{k},$$

$$F'_i(n, k) = \left\{ M \in R^{k \times n} \;\middle|\; \begin{array}{l} M \text{ contains exactly } i \text{ sets of } k \text{ columns} \\ \text{whose corresponding matrix is invertible} \end{array} \right\}$$
$$\text{for each } i = 1, 2, \ldots, \tbinom{n}{k}.$$

If R is a local ring (in the not necessarily commutative setting, this means that R modulo its Jacobson radical is a division ring), then $C(n, k) = F(n, k)$. It is probably true that $C(n, k) = F(n, k)$ for *some* $n > k$ implies that R is local.

It can happen that some of the $F_i(n, k)$ are empty when i is at or near the maximum. For example, if R is the finite field $\mathbf{Z}_p$ with p prime, then with $n = 5$ and $k = 2$, $\binom{5}{2} = 10$, and $F_{10}(5, 2)$ is empty for $p = 2$ or 3, while $F_9(5, 2)$ is empty if $p = 2$. However if R is an infinite field, then $F_{\binom{n}{k}}(n, k)$ is generic (and if the field is $\mathbf{R}$ or $\mathbf{C}$, its complement in $F(n, k)$ is just a union of lower dimensional varieties).

Set $\mathcal{D}_n$ to be the group of invertible diagonal $n \times n$ matrices with entries from $R^\times$ (the group of invertible elements of R), and let $\mathcal{P}_n$ denote the group of $n \times n$ permutation matrices (regarded as elements of $\mathrm{GL}(n, R)$). The group they generate (consisting of weighted permutation matrices), will be denoted $W(n)$. Then $W(n)$ acts from the left on each of the sets $C(n, k), F(n, k), F_i(n, k)$ and $\mathrm{GL}(k, R)$ acts on the right, yielding a $W(n) \times \mathrm{GL}(k, R)$ action; similarly, $\mathrm{GL}(n, R)$ acts from the left on $C'(n, k), F'(n, k), F'_i(n, k)$, yielding an action of $\mathrm{GL}(k, R) \times W(n)$ on each of these.

We see that $F(n, k) = \bigcup F_i(n, k)$ $(i = 1, 2, \ldots, \binom{n}{k})$, and it is not difficult to see that $F(n, k) \subset C(n, k)$ (below). We denote their orbit spaces by replacing the roman capital letters by their script forms, e.g., $\mathcal{C}(n, k), \mathcal{C}'(n, k)$, etc.

We will obtain what amounts to duality by showing that there exists a natural bijection $\mathcal{F}(n, k) \to \mathcal{F}'(n, n - k)$, which restricts to dualities $\mathcal{F}_i(n, k) \to \mathcal{F}'_i(n, n - k)$ for each $i = 1, \ldots, \binom{n}{k}$ (conveniently, $\binom{n}{k} = \binom{n}{n-k}$). Here the corresponding groups implementing the actions are $W(n) \times \mathrm{GL}(k, R)$ and $\mathrm{GL}(n - k, R) \times W(n)$. When R is commutative (or more generally admits an anti-automorphism), there are bijections $\mathcal{F}'_i(n, n - k) \to \mathcal{F}_i(n, n - k)$ (determined by composing the anti-automorphism with transpose), yielding bijections $\mathcal{F}_i(n, k) \to \mathcal{F}_i(n, n - k)$; if the anti-automorphism is either the identity or involutive, these are dualities.

For $C(n, k)$, at the moment, the situation requires an additional hypothesis, namely, that R be stably finite and satisfy SFF (even if R is commutative). Then there is a duality $\mathcal{C}(n, k) \to \mathcal{C}'(n, n - k)$ that extends the duality

$\mathcal{F}(n,k) \rightarrow \mathcal{F}'(n, n-k)$, and the same comments about the presence of an anti-automorphisms apply.

My colleagues, Kirill Zaynullin and Damien Roy, pointed out that if $R = F$ is a field, then one of the dualities, $\mathcal{F}(n,k) \rightarrow \mathcal{F}(n, n-k)$, is implied by the usual Grassmannian duality $\mathrm{Gr}(k,n) \rightarrow \mathrm{Gr}(n-k, n)$. To see this, pick $M \in F^{n \times k}$; its columns form a basis for a k-dimensional subspace of $F^{n \times 1}$; the right action by $\mathrm{GL}(k, F)$ (given by elementary column operations) has no effect on the subspace, and the duality takes the transpose and looks at its kernel.

If R is commutative, we will see that the dualities $\mathcal{F}(n,k) \rightarrow \mathcal{F}(n, n-k)$ and $\mathcal{F}_i(n,k) \rightarrow \mathcal{F}_i(n, n-k)$ are implemented by $[M] \rightarrow [N]$, where the columns of N constitute a right basis for the kernel of the map $M^T : R^{n \times 1} \rightarrow R^{k \times 1}$. This is particularly simple, as $M^T N = 0$ if and only if $N^T M = 0$. However, if R is not commutative, the transpose does not do what we expect. For example, at one point in the argument of the commutative case, we would use the obvious fact that if $g \in \mathrm{M}_k R$ is invertible, then so is g^T. This is no longer the case in the noncommutative situation; in fact, it is almost never true. Example A.5 illustrates this. This is a minor modification of an example in [9], the main result of which is that a ring R in which the transpose of invertibles is always invertible, must be commutative modulo its Jacobson radical.

Example A.5 ([9]). Suppose R is a ring and there exist elements $x, y \in R$ such that $xy - yx$ is invertible (in R). Then there exists $g \in \mathrm{GL}(2, R)$ such that g^T is a two-sided zero divisor in $\mathrm{M}_2 R$.

Set $g = \left(\begin{smallmatrix} 1 & x \\ y & xy \end{smallmatrix}\right)$. Elementary column operations (using *right* multiplications) reveal that g is invertible, in fact even a product of elementary matrices; explicitly,

$$ g^{-1} = \begin{pmatrix} 1 + xe^{-1}y & -xe^{-1} \\ -e^{-1}y & e^{-1} \end{pmatrix} = \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -y & 1 \end{pmatrix}, $$

where $e = xy - yx$. However, $g^T = \left(\begin{smallmatrix} 1 & y \\ x & xy \end{smallmatrix}\right)$ kills the column $\left(\begin{smallmatrix} -y \\ 1 \end{smallmatrix}\right)$ and the row $(-x \ 1)$, so $a := \left(\begin{smallmatrix} -y \\ 1 \end{smallmatrix}\right)(-x \ 1) = \left(\begin{smallmatrix} yx & -y \\ -x & 1 \end{smallmatrix}\right)$ satisfies $a g^T = g^T a = 0$.

Any division ring which is not commutative admits such a pair x, y, as does any ring containing a full set of matrix units (e.g., $x = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$), and similar examples for larger sets of matrix units).

In particular, we must avoid the temptation to use the transpose. We avoid it by sometimes considering matrices as left R-module homomorphisms, acting on the right. (An alternative is to use the opposite ring of R; however, I found this extremely confusing.) We use the weird but logical notation, $_R Q_2 \leftarrow {}_R Q_1 : x$, to denote the left module homomorphism x from Q_1 to Q_2, the subscripted R on the left of the names of the modules emphasizing the fact that they are left modules.

First, we show that $F(n,k) \subset C(n,k)$. Pick $M \in F(n,k)$; there exists a permutation $P \in \mathcal{P}_n$ such that the bottom k rows of PM constitutes an invertible matrix, $g \in \mathrm{GL}(k, R)$. Then $PMg^{-1} = \left(\begin{smallmatrix} X \\ I_k \end{smallmatrix}\right)$. Set $W_0 = \left(\begin{smallmatrix} I_{n-k} \\ 0 \end{smallmatrix}\right)$

(where the zero matrix is size $k \times (n-k)$). Then $h := (W_0 \quad PMg^{-1})$ is invertible
(by the lemma about upper triangular matrices if and only if), and set $W = P^{-1}W_0$, and $U = (W \ M)$. Then $PU(\mathrm{I}_{n-k} \oplus g^{-1}) = h$, so $U = P^{-1}h(\mathrm{I}_{n-k} \oplus g)$
is a product of invertibles, hence is invertible. Thus $M \in C(n, k)$. The same
argument (*not* using the transpose) works to show $F'(n, k) \subset C'(n, k)$.

To construct the map on equivalence classes, pick $M \in C(n, k)$, and view
M as a homomorphism of left modules, $_R R^{1 \times k} \leftarrow {}_R R^{1 \times n} \ M$ (it acts by right
multiplication, of course). Denote its kernel $_L \ker M$. By Lemma A.3 ((a)
implies (c)), the image of M is all of $_R R^{1 \times k}$, so the map splits; in particu-
lar, $_L \ker M$ is a direct summand, and there exists a submodule Q such that
$R^{1 \times n} = {}_L \ker M \oplus Q$, and the restriction to Q of right multiplication by M is
an isomorphism $R^{1 \times k} \leftarrow Q$. In particular, Q is free on k generators as a left
module. Now we make the assumption,

(∗) $_L \ker M$ is free (as a left R-module) on $n - k$ generators.

(We will see later that this applies if either $M \in F(n, k)$ or R satisfies SFF
and stable finiteness.) Pick a basis with $n - k$ generators, $\{r_1, r_2, \ldots, r_{n-k}\} \subset R^{1 \times n}$. Let N be the $(n - k) \times n$ matrix whose ith row is r_i. We will show that
the assignment $M \to N$ (which is highly dependent on choices of bases) yields
a well-defined map $[M] \mapsto [N]$ on the orbit spaces.

First, we claim that $N \in C'(n, n - k)$. But this is easy: let W be the
$k \times n$ matrix consisting of a k-element basis for Q. Then the rows of $V := \binom{W}{N}$ constitute an n element basis for $_R R^{1 \times n}$, and it is immediate that V is
invertible.

Next, if we choose a different $(n - k)$-element basis for $_L \ker M$ and corre-
sponding N', there exists $g \in \mathrm{GL}(n - k, R)$ such that $gN = N'$ (express each
element of one basis as a *left* linear combination of the elements of other basis;
the matrices of coefficients are mutually inverse).

If we replace M by wMh, where $w \in W(n)$ and $h \in \mathrm{GL}(k)$, we observe
that $_L \ker(wMh) = {}_L \ker(wM) = (_L \ker M)w^{-1}$. Thus if we choose a basis for
$_L \ker wM$, (s_i), and form the matrix N (whose rows are the s_i, then $N := Nw$
will have rows constituting a basis for $_L \ker M$ (recall that $W(n)$ acts on the
right of rows, multiplying by a weighted permutation matrix). Thus if M
belongs to the $W(n) \times \mathrm{GL}(k)$-orbit of M_0, then any choice for N (that is,
whose rows form a basis) will belong to the $\mathrm{GL}(n - k) \times W(n)$ orbit of (any
choice of) N_0, and $N \in C'(n, n - k)$.

All this was under the assumption (∗). Now assume that $M \in F(n, k)$; we
claim that (∗) holds. By assumption, there exists $P \in \mathcal{P}_n$ and $g \in \mathrm{GL}(k, R)$
such that $M_0 := PMg^{-1} = \binom{X}{I_k}$. It is an easy computation (essentially
column-reduced echelon form, but with noncommuting entries) that $_L \ker M_0$
is spanned as a left R-module by the rows,

$$\left\{ \left(-e_j; X_{j,n-k+1}, X_{j,n-k+2}, \ldots, X_{j,n} \right) \right\}_{j=1}^{n-k}$$

(where e_j is the jth standard basis element of $_R R^{1 \times (n-k)}$), and the module is
clearly free on these generators, and a direct summand (with complementary

basis $\{E_s\}_{s=n-k+1}^n$, where $\{E_i\}$ is the standard basis for ${}_R R^{1\times n}$. In particular, $(*)$ holds.

But we have more: $N \in F'(n, n-k)$, and if we choose the displayed basis, then $N = \left({-\mathrm{I}_{n-k} \atop X}\right)$, which clearly belongs to $F'(n, n-k)$.

Thus the assignment, $\phi \colon [M] \to [N]$, sends $\mathcal{F}(n, k) \to \mathcal{F}'(n-k)$. If $M \in F_i(n, k)$, for each of the i sets of k rows yielding an invertible matrix, there exists a distinct permutation matrix P such that PM has that particular set of k rows moved to the bottom (of course different permutations can yield the same subset of i rows), and we easily see from the preceding explicit form that for each, there is a corresponding subset of $n-k$ columns in N. This yields a one to one map from the sets of k rows of M constituting an invertible matrix to the sets of $n-k$ columns of N yielding an invertible matrix. To show it is a bijection, we work in reverse.

Begin with $N \in C'(n, n-k)$, and consider the map of right modules, $\mathbf{N} \colon R^{n\times 1} \to R^{(n-k)\times 1}$. By Lemma A.4 (a), it is onto, so the map splits, and we have a direct sum decomposition of right modules, $\ker N \oplus Q = R^{1\times n}$, with the restriction of N to Q being an isomorphism with $R^{1\times(n-k)}$. If $\ker N$ is free on k generators, then we send N to any matrix whose set of k columns is a basis for $\ker N$ (in parallel with what we did before). Now suppose $N \in F(n, n-k)$; by applying a permutation matrix and pre-multiplying it by an element of $\mathrm{GL}(n-k)$, we may assume that $hNP = \left({-\mathrm{I}_{n-k} \atop X}\right)$. Then $\ker hNP = \ker NP = P^{-1}\ker N$, and we see that the kernel is spanned by the rows of $\left({X \atop I_k}\right)$. It follows that if N came from an $M \in F(n, k)$, then we recover M up to the action of $W(n) \times \mathrm{GL}(k)$.

In particular, this yields an inverse map $[N] \mapsto [M]$, and we obtain that ϕ is a bijection $\mathcal{F}(n, k) \to \mathcal{F}'(n, n-k)$; moreover, parallel arguments show that the inverse map sends $\mathcal{F}'_i(n, n-k) \to \bigcup_{j\geq i}\mathcal{F}_j(n, k)$. Combined with the previous, we must have $\phi(\mathcal{F}_i(n, k)) = \mathcal{F}'_i(n, n-k)$.

For the action of $W(n) \times \mathrm{GL}(k, R)$ on $F(n, k)$ or $C(n, k)$, we define the *stabilizer* of a point, M, to be the subgroup of $\mathcal{P}_n$ consisting of

$$\left\{P \in \mathcal{P}_n \mid PDMg = M \text{ for some } D \in \mathcal{D}_n \text{ and } g \in \mathrm{GL}(k)\right\}$$

(and similarly with respect to the actions on $F'(n, k)$ and $C'(n, k)$). It is easy to check that this is a subgroup of $\mathcal{P}_n$ (which we typically identify with S_n), with the usual properties of stabilizers, e.g., if M and M' are in the same $W(n) \times \mathrm{GL}(k)$ orbit, then the stabilizer of M is isomorphic to that of M' via an inner automorphism of $\mathcal{P}_n$ (of course, the word *inner* is only significant if $n = 6$).

Thus far, we have most of the following.

Proposition A.6. *Let R be any ring and $n > k \geq 1$. Then the map ϕ induces bijections $\mathcal{F}_i(n, k)) \to \mathcal{F}'_i(n, n-k)$ for each of $i = 1, 2, \ldots, \binom{n}{k}$. Moreover, it induces isomorphisms on the stabilizers.*

Proof. We have already seen that ϕ is a bijection. Select M in $F(n, k)$, and construct $N \in F^{n\times(n-k)}$ such that $M^T N$ is zero, as in the definition of ϕ. Suppose

P belongs to the stabilizer of M; then $PDMg = M$ for $(D, g) \in \mathcal{D} \times \mathrm{GL}(k)$. Thus $M^T (D^T)^{-1} PN = 0$. Since the columns of N constitute a basis for $\ker M^T$, it follows there exists $h \in \mathrm{GL}(n - k)$ such that $(D^T)^{-1} PNh = N$. Since we can write $(D^T)^{-1} P = P(P^{-1}(D^T)^{-1} P)$ and the second factor is diagonal, we have that P belongs to the stabilizer of N. It follows, by interchanging M and N, that their stabilizers are equal. $\qquad\square$

It is clear from the definitions that an $n \times k$ matrix of the form $U(X) := \binom{X}{\mathrm{I}_k}$ belongs to $F(n, k)$, and moreover, every orbit in $F(n, k)$ contains a matrix of this form. More interestingly, such a matrix $U(X)$ belongs to $F_m(n, k)$, where $m = \binom{n}{k}$, if and only if all $s \times s$ submatrices of X are invertible, for all $s = 1, 2, \ldots, k$. In particular, all the entries of X have to be invertible (corresponding to $s = 1$), and if $k > 1$, then all matrices of the form

$$\begin{pmatrix} x_{i(1),j(1)} & x_{i(1),j(2)} \\ x_{i(2),j(1)} & x_{i(2),j(2)} \end{pmatrix}$$

($s = 2$) have to be invertible as well. There are thus $\sum_{j=1}^{k} \binom{n-k}{j} \binom{k}{j} = \binom{n}{j} - 1$ conditions.

Proposition A.7. *Let R be a stably finite ring satisfying SFF. Then the map ϕ induces a bijection $\mathcal{C}(n, k) \to \mathcal{C}'(n, n - k)$.*

Proof. First, we show that $(*)$ holds; that is, if $M \in C(n, k)$, then $_L \ker M$ is free on $n - k$ generators. As in the proof above, we have that $_R R^{1 \times n} = {}_L \ker M \oplus Q$ where Q is a free left R-module (because the restriction of right multiplication by M to Q is an isomorphism with $_R R^{1 \times k}$). By SFF, $_L \ker M$ is free, and by stable finiteness, it can only be free on $n - k$ generators. Hence $(*)$ holds.

Therefore the corresponding N exists, and we showed above that $N \in C'(n, n - k)$. In particular, ϕ is a well-defined map $\mathcal{C}(n, k) \to \mathcal{C}'(n, n - k)$. Now we can work in reverse to show it is a bijection. Pick $Z \in C'(n, n - k)$; write $\ker Z \oplus Q = R^{n \times 1}$ as right R-modules, with Z restricted to Q being an isomorphism. Then Q is free, so SFF implies $\ker N$ is free, and stable finiteness yields freeness on exactly k generators; pick such a basis. Define M to be the matrix whose ith column is the ith basis element. It is easy to check that if we construct the corresponding N, the R-module span of its rows will be that of N, and both being bases, they are bases for the same submodule, hence there exists $g \in \mathrm{GL}(n - k)$ such that $gN = N$. This shows that the map $\mathcal{C}'(n, n - k) \to \mathcal{C}(n, k)$ is the inverse to ϕ. $\qquad\square$

Suppose that R is commutative, or more generally, admits an anti-automorphism ψ (for commutative rings, we can take the identity; if R is a *-ring, we can take *). Then there is a (relatively) natural map (depending on ψ) $\mathcal{C}'(n, n - k) \to \mathcal{C}(n, n - k)$ (and corresponding maps on the F): send M to $\psi(M)^T$ (defining ψ on matrices entrywise). So composing this with ϕ, we obtain bijections $\mathcal{F}_i(n, k) \to \mathcal{F}_i(n, n - k)$ (and if R satisfies SFF and is stably finite, on the corresponding $\mathcal{C}$s).

In particular, if R is commutative, and we take the identity as ψ, the columns of N are given by a basis for $\ker M^T$, where we regard $M^T \colon R^{n \times 1} \to R^{k \times 1}$ as a homomorphism of right modules. Then $M^T N = 0$ and thus $N^T M = 0$, and we quickly see that the map ϕ really does behave like a duality. Similarly, if we assume that ψ is involutive (as in *-rings), then there is a natural duality $\mathcal{F}(n,k) \to \mathcal{F}'(n, n-k) \to \mathcal{F}(n,k)$ implemented via $\ker(M^*)^T$.

If, however, ψ is just an anti-automorphism, there are still mutually inverse bijections $\mathcal{F}(n,k) \to \mathcal{F}'(n, n-k)$ and vice versa, but they are not really the same (the first is implemented by $\ker \psi(M)^T$, the reverse by $\ker \psi^{-1}(M^T)$).

Suppose that $k = 2$, $n = 5$, and $F = \mathbf{Z}_p$ for a prime p. We note that the orbit space of $F_{10}(5,2)$ can be interpreted as the orbit space of the collection of 5 (distinct)-element subsets of 1-dimensional projective space over $\mathbf{Z}_p$, $\mathcal{P}_1$, acted upon by $\mathrm{PGL}(2, \mathbf{Z}_p)$. Since $\mathrm{PGL}(2, \mathbf{Z}_p)$ acts 3-transitively on $\mathcal{P}_1$, it is easy to check that it acts transitively on $F_{10}(5,2)$ if $p = 5$ or 7 (but not for any larger prime—the order of $F_{10}(5,2)$ does not divide that of $\mathrm{PGL}(2, \mathbf{Z}_p)$ if $p > 7$). In particular, the result above shows that $\mathrm{PGL}(3, \mathbf{Z}_7)$ acts transitively on $F_{10}(5,3)$—something that is routine to check with a computer (it suffices to show that the stabilizer of one or any point has at most six elements), but extremely tedious to check by hand.

Appendix B. A truncated reciprocal formula

David Handelman & Damien Roy

The rather casually obtained upper bound on density in the beginning of Section 7 stems from the result in this section.

Fix a prime p. The following goes back to 1893.

Theorem B.1 ([16])**.** *The number of rank $n - s$ matrices in $\mathrm{GL}(n, \mathbf{Z}_p)$ is*

$$C_s := \frac{\left((p^n - 1) \cdots (p^n - p^{n-s-1})\right)^2}{(p^{n-s} - 1) \cdot (p^{n-s} - p) \cdots (p^{n-s} - p^{n-s-1})}.$$

The limiting case of this is the identity [13, 19.7], due to Euler. However, we cannot obtain the result below simply by truncation, since there is a bonus of an extra bit in the exponent of the error term.

Proposition B.2. *Let n, s be positive integers, with $n > (s+1)^2 + 1$, and let z be a variable. Then as functions analytic on the open unit disk, we have that*

$$\left(\prod_{i=1}^{(s+1)^2 - 1} (1 - z^i) \right) \left(1 + \sum_{j=1}^{s} \frac{z^{j^2}}{(1-z)^2(1-z^2)^2 \cdots (1-z^s)^2} \right)$$

and

$$\left(\prod_{i=1}^{(s+1)^2 - 1} (1 - z^i) \right) \left(1 + \sum_{j=1}^{s} \frac{z^{j^2}(1-z^n)(1-z^{n-1}) \cdots (1-z^{n-j+1})}{(1-z)^2(1-z^2)^2 \cdots (1-z^s)^2} \right)$$

are polynomials, and their Maclaurin expansions are

$$1 - z^{(s+1)^2+2} + \text{ higher order terms.}$$

Proof. Since $(s+1)^2 - 1 \geq 2s$, it follows that all the denominators of the right factor are eliminated by the left (count the multiplicities of the various roots of unity that are zeros of the denominators, and do the same for the first 2 terms in the product on the left). Hence the polynomial assertion is verified.

With $N_p = \prod_{i=0}^{n-1}(p^n - p^i)$ being the number of invertible matrices, we have

$$C_s = \frac{N_p}{\prod_{i=0}^{n-1}(p^n - p^i)} \cdot \frac{\left((p^n - 1)\cdots(p^n - p^{n-s-1})\right)^2}{(p^{n-s} - 1)\cdot(p^{n-s} - p)\cdots(p^{n-s} - p^{n-s-1})}$$

$$= N_p \cdot \frac{(p^n - 1)\cdots(p^n - p^{n-s-1})}{\left((p^n - p^{n-s})(p^n - p^{n-s+1})\cdots(p^n - p^{n-1})\right)}$$

$$\cdot \frac{1}{\left((p^{n-s} - 1)(p^{n-s} - p)\cdots(p^{n-s} - p^{n-s-1})\right)}$$

$$= p^{n^2} \cdot \frac{N_p}{p^{n^2}} \cdot \frac{p^{(n-s)(n-s-1)/2}(p^n - 1)(p^{n-1} - 1)\cdots(p^{s+1} - 1)}{p^{n(n-1)/2}\left((p^s - 1)(p^{s-1} - 1)\cdots(p - 1)\right)}$$

$$\cdot \frac{1}{\left((p^{n-s} - 1)(p^{n-s-1} - 1)\cdots(p - 1)\right)}$$

$$= p^{n^2} \cdot \frac{N_p}{p^{n^2}} \cdot \frac{p^{(n-s)(n-s-1)/2}(p^n - 1)(p^{n-1} - 1)\cdots(p^{n-s+1} - 1)}{p^{n(n-1)/2}\left((p^s - 1)(p^{s-1} - 1)\cdots(p - 1)\right)^2};$$

divide by p^{n^2} and set $z = 1/p$ to obtain

$$\frac{C_s}{p^{n^2}} = \frac{N_p}{p^{n^2}} \cdot \frac{z^{s^2}(1 - z^n)(1 - z^{n-1})\cdots(1 - z^{n-s+1})}{(1 - z)^2(1 - z^2)^2\cdots(1 - z^s)^2} := \left(\prod_{i=1}^{n}(1 - z^i)\right) \cdot c_s(z).$$

Set $c_0 = 1$, and let $m(z) = \prod_{i=1}^{n}(1 - z^i)$. We see that each $c_s(z)$ is analytic on the unit disk; moreover, for each prime p, $m(1/p)\sum_{j=0}^{n} c_j(1/p) = 1$, since the unnormalized forms count the total number of matrices; this equality is also true at $z = 0$. Since each of the factors is analytic on the open disk, and the product agrees with the constant function 1 on a limit point ($\{0, 1/2, 1/3, \dots\}$), it follows that the product, $m \cdot (\sum_{j=0}^{n} c_j)$ is 1 on the unit disk. We use this to determine some Maclaurin coefficients. Each c_i is expressed as

$$\frac{z^{i^2}}{(1 - z)^2 \cdots (1 - z^i)^2} \times (1 - z^n)(1 - z^{n-1})\cdots(1 - z^{n-s+1}).$$

When we expand this in its Maclaurin expansion, we see that $c_i = z^{i^2} + 2z^{i^2+1} +$ terms of higher order. Now suppose that $s^2 \leq n$, and consider the truncated sum, $\sum_{i=0}^{s} c_i$. The missing terms are of the form $m_p \cdot c_t$, where $t > s$. It follows immediately that the smallest degree term in the Maclaurin expansion of what is missing is $z^{(s+1)^2} + 2z^{(s+1)^2} + 1$. Thus $E_s := \sum_{i=0}^{n} c_i - \sum_{i>s} c_i = 1 - z^{(s+1)^2} - 2z^{(s+1)^2} + 1 + \text{terms of higher order.}$

Now truncate m at $(s+1)^2 - 1$, that is, $m_s = \prod_{i \le (s+1)^2 - 1}(1 - z^i)$. Then

$$
\begin{aligned}
m - m_s &= m_s \cdot \big((1 - z^{(s+1)^2})(1 - z^{(s+1)^2+1}) \cdots - 1\big) \\
&= m_s \cdot \big(- z^{(s+1)^2} - z^{(s+1)^2+1} - z^{(s+1)^2+2} + \cdots\big) \\
&= -z^{(s+1)^2}(1 + z + z^2 + \cdots) \cdot (1 - z)(1 - z^2)(1 - z^3) \cdots \\
&= -z^{(s+1)^2}(1 - z^2 + \cdots);
\end{aligned}
$$

so

$$
m_s = m + z^{(s+1)^2}(1 - z^2 + \cdots).
$$

Now we have

$$
\begin{aligned}
m_s \cdot E_s &= m + z^{(s+1)^2}(1 - z^2 + \cdots) \cdot \Big(\sum_{i=0}^{n} c_i - \sum_{i>s} c_i\Big) \\
&= 1 - m \sum_{i>s} c_i + \big(z^{(s+1)^2}(1 - z^2 + \cdots)\big)E_s \\
&= 1 - \big((1 - z)(1 - z^2) \cdots (c_{s+1} + \cdots)\big) \\
&\quad + \big(z^{(s+1)^2}(1 - z^2 + \cdots)\big)(1 + z + 2z^2 + \cdots) \\
&= 1 - (1 - z - z^2 + z^3 + \cdots)z^{(s+1)^2}(1 + 2z + 5z^2 + \cdots) \\
&\quad + z^{(s+1)^2}(1 + z + z^2 + \cdots) \\
&= 1 - z^{(s+1)^2}\big((1 + z + 2z^2 + \cdots) - (1 + z + z^2 + \cdots)\big) \\
&= 1 - z^{(s+1)^2+2} + \cdots .
\end{aligned}
$$

This is exactly the desired assertion for the more complicated product. For the less complicated (first) product, from $n - j + 1 + j^2 > (s+1)^2 + 2$ (this is equivalent to $n + 1 > (s+1)^2 + 2$), the extra terms in the numerator of the right-hand term do not contribute to any Maclaurin series terms of degree less than or equal $(s+2)^2 + 2$, so the first product has the same Maclaurin expansion up to that degree. $\qquad\square$

The simpler expression (the first one) does not involve n and the product behaves as $1 - z^{(s+1)^2+2}(1 + \boldsymbol{O}(z))$ without reference to n. If we let $s \to \infty$, then the left function converges uniformly on compact subsets of the open unit disk to the Euler function, and since the latter has no zeros, it follows that the infinite sum on the right also converges uniformly on compact subsets, so is also analytic on the open disk; necessarily, the limit is the reciprocal of the Euler function, giving yet another proof of the identity [13, 19.7]. For all values of s that we could calculate with, the coefficients of the higher order terms oscillate in a particularly interesting way, and the maximum increases as s does, according to *Maple*.

Appendix C. Counting PH-equivalence classes

In [1], Atanasov et al. compiled tables of PH-equivalence isomorphism types, based on (what amounts to) $d = |\det B|$ and $|\det B^{\mathrm{op}}|$ for $n = 3$ and 4. Using Proposition 2.1, one can obtain explicit formulas for the numbers of equivalence classes that contain a terminal form with 1-block size $n - 1$ of determinant d, and subdivide it according to the possible values of $|\det B^{\mathrm{op}}|$. Aside from the complicated nature of the expressions, these only deal with 1-block size $n - 1$.

The usual (Jordan) totients are denoted $J_1 = \phi$, J_2, J_3, ...

In this appendix, we will see that the lower bound obtained for the number of PH-classes of $C \in \mathcal{NS}_n$ of determinant d obtained in Lemma C.1,

$$F_n(d) := \frac{(\phi * J_2 * \cdots * J_{n-1})(d)}{n!},$$

is asymptotically (in d) correct (with an estimate having a factor $1 + \boldsymbol{O}(d^{-1})$), when d is square-free. We do this by showing that the vast majority of the S_n-orbits on weakly terminal matrices (defined below) of determinant d are of full size, that is, $n!$, via estimates (and in some cases, exact formulas) for numbers of matrices fixed by an arbitrary permutation.

A matrix C is called *weakly terminal*, if it is in Hermite normal form and belongs to $\mathcal{NS}$; in particular, it is upper triangular, and its $(1,1)$ entry is 1. It is quite easy to count the weakly terminal matrices of given size and determinant.

Let C be a weakly terminal matrix of size n, let $\pi \in S_n$ be a permutation, and let $P \equiv P_\pi$ be the permutation matrix right multiplication by which implements π as a permutation of the set of columns. There exists $U \equiv U_P \in \mathrm{GL}(n, \mathbf{Z})$ such that $C_P := UCP$ is in Hermite normal form, and in fact, given P, C_P is unique. If C' and C'' are weakly terminal matrices such that $C' = UCP$ for some permutation matrix P and $U \in \mathrm{GL}(n, \mathbf{Z})$, and $C'' = U''CP$ (same permutation matrix), then $C'' = U''(U^{-1}C'P^{-1})P = U''U^{-1}C'$, so that C'' is Hermite equivalent to C'—but both are in Hermite normal form, so must be equal.

Since the property of being in $\mathcal{NS}$ is preserved by Hermite equivalence, it follows that $\{C_P\}_{P \in S_n}$ is a finite set consisting of weakly terminal elements, and an orbit, under the action of S_n. Moreover, this orbit must contain at least one terminal matrix (since every matrix is PH-equivalent to a terminal matrix, and terminal implies weakly terminal). Thus the orbits of the form $\{C_P\}_{P \in S_n}$ (with C varying over weakly terminal matrices) are in bijection with the PH-equivalence classes of $C \in \mathcal{NS}_n$.

In particular, for fixed weakly terminal C (weakly terminal is required, since otherwise C_P is not necessarily uniquely determined) is an S_n-space. The difficulty in counting arguments is that the orbits need not all be full, that is, there will be some fixed points—$C_P = C$ for some nontrivial permutation matrix P.

One case in which the orbit will be full (of cardinality $n!$) occurs when the $J(C_{\Omega(i)})$ are distinct (that is, mutually nonisomorphic as abelian groups). The obvious action of P (acting on the columns) implements a permutation of the

n-tuple, $(J(C_{\Omega(1)}), J(C_{\Omega(2)}), \ldots, J(C_{\Omega(n)}))$ (the subsequent left action by the unimodular matrix does not affect the order of these groups). If the $J(C_{\Omega(i)})$ are distinct, this action is just the permutation representation of S_n on a set with n elements. It follows that the orbit of the action $C \mapsto C_P$ is full.

For $\pi \in S_n$, let $P \equiv P_\pi$ denote the permutation matrix right multiplication by which implements π as a column permutation. Then a weakly terminal matrix $C \in \mathcal{NS}_n$ is fixed by π (or $P \equiv P_\pi$) if and only if CPC^{-1} has only integer entries. For a subgroup H of S_n and a positive integer d, let $\mathcal{Z}(H)(d)$ denote the set of all weakly terminal matrices of determinant d that are fixed by all elements of H. When H is the cyclic group generated by π, we use the notation $\mathcal{Z}(\pi)(d)$. The cardinality of $\mathcal{Z}(\pi)(d)$ is denoted $\mathcal{S}(\pi)(d)$ (and similarly for subgroups H). The function $d \mapsto \mathcal{S}(\pi)(d)$ is multiplicative (in the number-theoretic sense) for all π.

There is an obvious procedure for counting PH-equivalence classes. First, we count all the weakly terminal matrices of fixed determinant d (done in Lemma C.1). Then we count the number of weakly terminal matrices whose orbits are not full, and subtract them off, keeping track of the number of PH-equivalence classes they constitute, and apply Burnside's lemma. When $n = 3$, it is barely possible to do this, but for larger sizes, obtaining the exact number seems horrible. (In fact, when $n = 3$, we obtain a convenient subdivision into various cases with 1-block size two, and the remainder; this goes most smoothly when d is square-free.)

However, for n arbitrary and d prime (and thus for d square-free), we can obtain relatively explicit formulas for $\mathcal{S}(\pi)(d)$ for every $\pi \in S_n$; since the matrices with orbit size less than $n!$ must be in $\mathcal{Z}(\pi)$ for some non-identity $\pi \in S_n$, we obtain an upper bound for the number of PH-equivalence classes via Burnside's lemma. This will verify the conjecture below when d is square-free.

Recall the definition of the kth Jordan totient, $J_k(n) = n^k \prod_{p|n}(1 - p^{-k})$. Then $J_1 = \phi$, J_k is multiplicative (in the number-theoretic sense), and $J_k(d)$ counts the number of content one columns of size $k + 1$ with d in the bottom entry, and all the other entries belonging to $\{0, 1, \ldots, d-1\}$. Recall that for multiplicative functions f and g, the convolution, $f * g$, is defined by $(f * g)(d) = \sum_{x|d} f(x)g(d/x)$, and is multiplicative; moreover, $f * g = g * f$. There is an identity for constructing J_k, namely, if ξ_k is the multiplicative function $n \mapsto n^k \phi(n)$, then $\xi_{k-1} * \xi_{k-2} * \cdots * \xi_1 * \phi = J_k$. (The Dirichlet series for the function on the left telescopes.)

Lemma C.1. *Let d be a positive integer. For $n > 1$, the number of weakly terminal $n \times n$ matrices of determinant d is*

$$(\phi * J_2 * \cdots * J_{n-1})(d).$$

Proof. This simple proof is carried out by induction on n. If $n = 2$, we are counting the matrices $\left(\begin{smallmatrix} 1 & a \\ 0 & d \end{smallmatrix}\right)$, where $0 \le a < d$ and $(a, d) = 1$—the number of choices for a is obviously $\phi(d)$.

For $n > 2$, given a weakly terminal matrix C, say with (n, n) entry x (which divides d, as the matrix is upper triangular), deleting the last row and

column, yields a weakly terminal matrix of size $n - 1$, and with determinant d/x; moreover the nth column has content one. Conversely, given a weakly terminal matrix of size $n - 1$ and a content one column of size n, we created a weakly terminal matrix of size n by attaching the column, and embroidering $n - 1$ zeros on the bottom, and of course the determinant multiples.

If $H_j(t)$ denotes the number of weakly terminal matrices of size j and determinant t, we then have $H_{n-1}(t) = (\phi * J_2 * \cdots * J_{n-2})(t)$, by the induction hypothesis, and

$$
\begin{aligned}
H_n(d) &= \sum_{x \mid d} J_{n-1}(x) H_{n-1}(d/x) \\
&= (J_{n-1} * H(n - 1))(d) \\
&= (H_{n-1} * J_{n-1})(d) \\
&= (\phi * J_2 * \cdots * J_{n-1})(d),
\end{aligned}
$$

completing the induction. $\qquad\square$

Set $F(n, d) = (\phi * J_2 * \cdots * J_{n-1})(d)$. It follows immediately that $F(n, d)/n!$ is a lower bound for the number of PH-equivalence classes of matrices in $\mathcal{NS}_n$ of determinant $\pm d$.

Conjecture. For d a positive integer, the number of PH-equivalence classes of matrices in $\mathcal{NS}_n$ having determinant $\pm d$ is

$$
\frac{(\phi * J_2 * \cdots * J_{n-1})(d)}{n!} \cdot \left(1 + \frac{c}{d}(1 + \boldsymbol{o}(1))\right)
$$

for some constant c.

Theorem C.2. *If $n \geq 3$ is fixed and d is square-free, then the number of PH-equivalence classes of matrices in $\mathcal{NS}_n$ of determinant $\pm d$ is given by*

$$
\mathcal{PH}(n, d) = \frac{(\phi * J_2 * \cdots * J_{n-1})(d)}{n!}\left(1 + \frac{\binom{n}{2}}{d}\left(1 + \boldsymbol{O}\left(\frac{1}{d^{1-\epsilon}}\right)\right)\right)
$$

In Appendix D, we will show that the estimate is true for arbitrary d when $n = 3$.

One way to proceed, and even obtain a slightly sharper result is as follows. Fix n, then d, and a permutation $\pi \in S_n$, and its corresponding matrix P (right multiplication by which implements π as a column permutation). We wish to obtain an asymptotic estimate for the number of weakly terminal $n \times n$ matrices C of determinant d invariant under the action of P, that is, $CPC^{-1} \in \mathrm{M}_n \mathbf{Z}$.

Let $K(\pi)$ denote the number of cycles in the decomposition of the permutation π associated to P; fixed points of course are 1-cycles, so they are counted. Then $K(\pi)$ is just the co-rank of the matrix $\mathrm{I} - P$, that is, $n = \mathrm{rank}(\mathrm{I} - P) + K(\pi)$, as it simply counts the algebraic and geometric multiplicities (they are the same for permutation matrices) of 1 as an eigenvalue of P.

Motivated by the counting arguments above, the following is likely to be true.

Specific Conjecture. Let $\pi \in S_n$ be a non-transposition. Then for all $\epsilon > 0$,

$$\frac{\mathcal{S}(\pi)(d)}{F(n,d)} = \boldsymbol{o}(d^{K(\pi)-n+\epsilon}).$$

Without ϵ, the specific conjecture fails (in Appendix D, we will see that when $n = 3$ and π is a 3-cycle, then $\mathcal{S}(\pi)(d)/\mathcal{S}(\mathrm{I})(d)$ is infinitely greater than d^{-2}).

If the specific conjecture were true, the conjecture preceding it would follow (as we will see when we discuss $\mathcal{S}(\pi)$ when π is a transposition). Of course, it would be sufficient to prove this when d is restricted to powers of primes.

Presumably, this is part of a theory of an arithmetic version of varieties, corresponding to subvarieties having measure zero when imbedded in a variety.

Lemma C.3. *Let H be a subgroup of S_n, and $\pi \in S_n$. Then for all $d > 0$,*

$$\mathcal{S}(H)(d) = \mathcal{S}(\pi H \pi^{-1})(d).$$

Proof. Fix d, and let Q be the permutation matrix representing π. Select a permutation matrix P that corresponds to an element of H, and suppose weakly terminal C is fixed under the action of P, that is, $CPC^{-1} \in \mathrm{M}_n\mathbf{Z}$. There exists $U \equiv U_{C,Q} \in \mathrm{GL}(n,\mathbf{Z})$ such that UCQ^{-1} is in Hermite normal form; since both left multiplication by elements of $\mathrm{GL}(n,\mathbf{Z})$ and right multiplication by permutation matrices preserve $\mathcal{NS}_n$, UCQ^{-1} is itself weakly terminal, and of the same determinant as C (it is of the same absolute determinant, but being in Hermite normal form, the determinant is positive). In addition, $U_{C,Q}$ is unique (with respect to the property that UCQ^{-1} is in Hermite normal form), as $\det C = d \neq 0$.

Next, we observe that

$$UCQ^{-1}(QPQ^{-1})QC^{-1}U^{-1} = U(CPC^{-1})U^{-1} \in \mathrm{M}_n\mathbf{Z}.$$

Since this is true for every P corresponding to an element of H, we have a set map $\mathcal{Z}(H)(d) \to \mathcal{Z}(\pi H \pi^{-1})(d)$, given by $C \mapsto U_{C,Q}CQ^{-1}$. Since C is itself weakly terminal, it follows that $U_{UCQ^{-1},Q^{-1}}$ must be $U_{C,Q}^{-1}$, so the corresponding map $\mathcal{Z}(\pi H \pi^{-1})(d)) \to \mathcal{Z}(H)(d)$ is the inverse of the original. This shows that $C \mapsto U_{C,Q}CQ^{-1}$ is a bijection. $\square$

Define for each positive integer k, $\mathcal{N}_k \colon \mathbf{N} \to \mathbf{N}$ via

$$\mathcal{N}_k(d) = \big|\big\{z \in \mathbf{Z}_d \mid z^k = 1\big\}\big|.$$

The Chinese remainder theorem implies that for each k, the function $\mathcal{N}_k$ is multiplicative. The following is routine, and follows from $\mathbf{Z}_{p^m}^*$ being cyclic of order $p^{m-1}(p-1)$ when p is odd, and isomorphic to $\mathbf{Z}_{2^{m-2}} \times \mathbf{Z}_2$ when $p = 2$ (with the interesting convention that $\mathbf{Z}_{2^{-1}} \times \mathbf{Z}_2$ is the trivial group).

If p is a prime and $m \in \mathbf{N}$, then $v_p(m) = r$ means that p^r maximally divides m; this is the usual valuation.

Lemma C.4. *For a prime p,*

$$\mathcal{N}_k(p^m) = p^{\min\{v_p(k),m-1\}} \cdot \begin{cases} \gcd\{p-1,k\} & \text{if } p \text{ is odd, or } p^m = 2 \\ 2 & \text{if } p = 2 \text{ and } m \geq 2. \end{cases}$$

If k is an odd prime, then $\ln \mathcal{N}_k(d) \leq |\{p|d \mid p \equiv 1 \bmod k\}| \cdot \ln k$, and in general, $\mathcal{N}_k(d) \leq 2k^{w(d)+1}$, although the latter is almost always a gross overestimate.

Let $\pi \in S_n$, and let $i \in \{1, 2, \ldots, n\}$ (n will be fixed). Define the *orbit of i with respect to π, $\mathcal{O}_\pi(i)$* (or $\mathcal{O}(i)$ if π is understood), to be $\{\pi^k(i)\}_{k \in \mathbf{Z}}$.

For $\pi \in S_n$, let P_π (or P if π is understood) be the corresponding permutation matrix that implements the action of π on the columns of $n \times n$ matrices by right multiplication. If C is weakly terminal, then C is fixed by the action of π (or P) if CPC^{-1} has only integer entries: explicitly, CP^{-1} is put in Hermite normal form by a matrix $U \in \mathrm{GL}(n, \mathbf{Z})$, that is, UCP^{-1} is in Hermite normal form; then $UCP^{-1} = C$ if and only if $U = CPC^{-1}$, which is equivalent (since the determinant of the right side is plus or minus one) to CPC^{-1} having only integer entries.

We will determine $\mathcal{S}(\pi)(d)$ exactly, when d is square-free. We obtain a formula involving some of the orbits of π and their cardinalities, relating to Jordan totients. It is explicit enough that we can easily verify the specific conjecture for square-free d.

As before fix n and fix d as well. Let $2 \leq j \leq n$, and let

$$u = \left(a_1, a_2, a_3, \ldots, a_{j-1}, d, 0, 0, \ldots, 0\right)^T \in \mathbf{Z}^n$$

such that $0 \leq a_i < d$ and $\gcd\{d, a_1, \ldots, a_{j-1}\} = 1$. Let $C \equiv C(j, u)$ be the weakly terminal matrix whose jth column is u, and whose ith column for $i \neq j$ is the standard basis elements $E_i \in \mathbf{Z}^n$. In other words, $C - \mathrm{I}$ has exactly one nonzero column, and it is $u - E_j$. Note that C so constructed is automatically weakly terminal.

Define

$$V_j \equiv V_j(d) = \left\{ C \in \mathrm{M}_n\mathbf{Z} \ \middle| \ \begin{array}{l} \det C = d,\ C \text{ is weakly terminal,} \\ \text{the only nonzero column of } C - \mathrm{I} \text{ is the } j\text{th} \end{array} \right\}.$$

The definition forces the jth column to be of the form u as given above.

Given $\pi \in S_n$, we will determine the number of matrices $C \in V_j$ such that C is invariant under π, that is, for which $CP_\pi C^{-1} \in \mathrm{M}_n\mathbf{Z}$. If $d = p$, a prime, then every weakly terminal C of determinant d is in V_j for some j, so we obtain $\mathcal{S}(\pi)(p)$ as a sum over $j = 2, \ldots, n$ of these numbers. This yields a formula for $\mathcal{S}(\pi)(d)$ when d is square-free. The formula is sufficiently explicit to determine asymptotic behavior (that is, for large, square-free d).

Begin with $C \equiv C(j, u) \in V_j$, and $P \equiv P_\pi$. The ith column of CP is given by

$$(CP)_i = \begin{cases} E_{\pi^{-1}(i)} & \text{if } i \neq \pi(j), \\ u = \sum_{l \leq j-1} a_l E_l + dE_j & \text{if } i = \pi(j). \end{cases}$$

Thus the entries are given by

$$(CP)_{i,m} = \begin{cases} 1 & \text{if } i \neq \pi(j) \text{ and } i = \pi(m), \\ 0 & \text{if } i \neq \pi(j) \text{ and } i \neq \pi(m), \\ a_m & \text{if } i = \pi(j) \text{ and } m < j, \\ d & \text{if } i = \pi(j) \text{ and } m = j, \\ 0 & \text{if } i = \pi(j) \text{ and } m > j. \end{cases}$$

Extend the definition of a_i, so that $a_j = d$ and $a_l = 0$ if $l > j$. We will usually write πk rather than $\pi(k)$ (unless ambiguity may result) from now on. We can thus write the mth row of CP, $(CP)^{(m)}$, as

$$(CP)^{(m)} = a_m e_{\pi j} + \begin{cases} e_{\pi m} & \text{if } m \neq j, \\ 0 & \text{if } m = j. \end{cases}$$

(We are using the convention that E_i represent the standard basic columns, while e_i represent the standard basic rows, so that $e_k E_l$ is the matrix product whose outcome is δ_{kl}.)

Now C^{-1} is calculated easily by factoring C into a product of a diagonal matrix and a unipotent. The outcome is that all the columns of C^{-1} except the jth are just the standard basic columns, and the jth column is

$$d^{-1}(-a_1, \ldots, -a_{j-1}, 1, 0, 0, \ldots, 0)^T.$$

In particular, $(C^{-1})_j = d^{-1}(E_j - \sum_{i \leq j-1} a_i E_i)$.

We see immediately that CPC^{-1} has only integer entries if and only if its jth column does. We calculate the entries of the jth column:

$$(CPC^{-1})_{m,j} = (CP)^{(m)}(C^{-1})_j$$

$$= \begin{cases} \dfrac{-a_m a_{\pi j}}{d} + \begin{cases} -\dfrac{a_{\pi m}}{d} & \text{if } m, \pi m \neq j, \\ 0 & \text{if } m = j, \\ \dfrac{1}{d} & \text{if } m \neq j \text{ and } \pi m = j, \end{cases} & \text{if } \pi j \neq j, \\[4ex] \dfrac{a_m}{d} + \begin{cases} \dfrac{-a_{\pi m}}{d} & \text{if } m \neq j, \\ 0 & \text{if } m = j, \end{cases} & \text{if } \pi j = j. \end{cases}$$

Now we count the π-invariant matrices in V_j. First suppose that $\pi(j) = j$. Then the conditions for all the entries to be integers boil down to $a_{\pi m} \equiv a_m \bmod d$ for all $m \neq j$. Hence, if $m \neq j$, then $a_m \neq 0$ implies $a_i \neq 0$ for all $i \in \mathcal{O}(m)$. Thus $a_m \neq 0$ entails $\mathcal{O}(m) \subseteq \{1, 2, \ldots, j-1\}$. Conversely, if $\mathcal{O}(m) \subseteq \{1, 2, \ldots, j-1\}$, we can put any value in we like for a_m, and the same value for a_i as i varies over the orbit of m. The only constraint is that the resulting column u must have content one. The number of such columns is thus exactly $J_{s(j)}(d)$ (the Jordan totient), where $s(j)$ is the number of orbits that are contained in $\{1, 2, \ldots, j-1\}$.

So if $\pi(j) = j$, the number of matrices in $V_j(d)$ that are fixed by the action of π is exactly $J_{s(j)}(d)$. (If $s(j) = 1$, $J_1 = \phi$, the usual totient; if $s(j) = 0$, the outcome is zero.)

Now suppose that $\pi(j) \neq j$. First, we consider conditions arising from the coefficients corresponding to $\mathcal{O}(j)$, the orbit of j itself. Suppose the orbit of j has $k > 1$ elements, so that if $m = \pi j$, then $m, \pi m, \ldots, \pi^{k-2}m$ are distinct from each other and j, and all but the last one satisfies $\pi s \neq j$ (if $k = 2$, then all we have is $\{m\}$).

For $k > 3$, we deduce $a_m^2 \equiv -a_{\pi m}$, and then $a_{\pi m}a_m \equiv -a_{\pi^2 m}$, until we reach $a_{\pi^{k-3}m}a_m \equiv -a_{\pi^{k-2}m}$, and finally, $a_{\pi^{k-2}m} \equiv -1$. We can rewrite these as functions of a_m, obtaining $a_{\pi m} \equiv -a_m^2$, $a_{\pi^2 m} \equiv a_m^3$, and for $r \leq k - 2$, $a_{\pi^r m} \equiv (-a_m)^{r+1}$, and finally $(-a_m)^k \equiv 1 \mod d$. So we have $\mathcal{N}_k(d)$ choices for a_m, and every other a_i for $i \in \mathcal{O}(j) \setminus \{j\}$ is determined by the choice of a_m.

For $k = 2$ and $k = 3$, the same result applies (and is easily checked); the indexing was confusing.

Now we come to a_m for $m \notin \mathcal{O}(j)$. Then the equations become $a_{\pi m} \equiv -a_m a_{\pi j}$, $a_{\pi^2 m} \equiv a_m a_{\pi j}^2$, and in general $a_{\pi^r m} = a_m(-a_{\pi j})^r$ (this is true for all r). Thus the choice of $a_{\pi j}$ (which has to be a kth root of unity in $\mathbf{Z}_d$) and the choice of a_m will determine the rest of the a_i for $i \in \mathcal{O}(m)$. However, there are constraints on the choice of a_m if $k(m) := |\mathcal{O}(m)|$ is not divisible by $k = |\mathcal{O}(j)|$. Write $k(m) = ck + f$, with $c \geq 0$ and $0 \leq f < k$. Then $a_m \equiv a_{\pi^{k(m)}m} \equiv a_m(-a_{\pi j})^{k(m)} \equiv a_{\pi^f m} \equiv a_m(-a_{\pi j})^f$. Hence $a_m(1 - (-a_{\pi j})^j) \equiv 0 \mod d$.

Set $z = -a_{\pi j}$, so that $z^k \equiv 1 \mod d$. The restriction, that $a_m(1 - z^f) \equiv 0$, is trivial if $z^f \equiv 1$. At this point, for simplicity, we assume that d is a prime. In that case, $1 - z^f$ is a zero divisor if and only if $z^f \equiv 1$, and a_m can be anything; otherwise, $a_m = 0$ is forced. Moreover, if $z^f \equiv 1$, then the remaining a_i, determined by $a_{\pi^r m} = a_m(-a_{\pi j})^r$, are consistent with the conditions for invariance. Hence there are exactly $\gcd\{f, p - 1\} = \gcd\{k(m), k, p - 1\}$ selections for $a_{\pi j}$ for which we obtain p choices for a_m, and for all the rest $(\mathcal{N}_k(p) - \gcd\{k(m), k, p - 1\})$, there is exactly one choice, $a_i = 0$ for all i in the orbit of m. If k divides $k(m)$, then the latter does not occur (as $f = 0$).

Now we can count the number of matrices in $V_j(p)$ fixed by π, for p prime.

(a) If $\pi j = j$, there are $J_{s(j)}(p)$, where $s(j)$ is the number of π-orbits in $\{1, 2, \ldots, j - 1\}$.

(b) Suppose $\pi j \neq j$. If $\mathcal{O}(j)$ is not contained in $\{1, 2, \ldots, j\}$, then there are zero choices. Assuming $\mathcal{O}(j) \subseteq \{1, 2, \ldots, j\}$ (that is, $j = \max \mathcal{O}(j)$), select z in $\mathbf{Z}_p^*$ with order dividing $|\mathcal{O}(j)|$, and set $a_{\pi j} = -z$. For each of the $s(j)$ orbits in $\{1, 2, \ldots, j - 1\}$, we select m in the orbit, and either set a_m to zero (if $z^{|\mathcal{O}(m)|} \neq 1$) or let it be arbitrary (if $z^{|\mathcal{O}(m)|} = 1$), and define the a_i for other $i \in \mathcal{O}(m)$ according to the formulas. The constraint that the column must have content one is automatically satisfied, since $a_{\pi j} \equiv -z$ is relatively prime to p.

For z fixed, the number of choices (with $a_{\pi j} \equiv -z$) is thus (provided $\mathcal{O}(j) \subset \{1, 2, \ldots, j\}$)

$$p^{|\{\mathcal{O}(m) | \mathcal{O}(m) \subset \{1,2,\ldots,j\} \text{ and } z^{|\mathcal{O}(m)|} \equiv 1 \mod p\}|}.$$

Now we sum this over all choices for z, of which there are $\gcd\{|\mathcal{O}(j)|, p - 1\}$ (the number of kth roots of unity in $\mathbf{Z}_p^*$).

Finally, we observe that if d is prime, then the set of weakly terminal matrices in $\mathrm{M}_n\mathbf{Z}$ of determinant d is simply $\dot{\bigcup}_{j=2}^n V_j(p)$, since a matrix in Hermite normal form with prime determinant can only have one column that is not the corresponding standard basis element. This leads to the following expression. Recall that $s(j) \equiv s(j, \pi)$ is the number of π-orbits that are contained in $\{1, 2, \dots, j-1\}$.

Proposition C.5. *Let $\pi \in S_n$. Then for a prime p, the number of weakly terminal matrices of determinant p fixed by π is given by*

$$\mathcal{S}(\pi)(p) = \sum_{\substack{2 \leq j \leq n \\ \pi j = j}} J_{s(j,\pi)}(p)$$

$$+ \sum_{\substack{2 \leq j \leq n \\ \pi j \neq j \\ \mathcal{O}_\pi(j) \subseteq \{1,2,\dots,j\}}} \sum_{\substack{z \in \mathbf{Z}_p^* \\ z^{|\mathcal{O}_\pi(j)|} = 1}} p^{|\{\mathcal{O}(m)|\mathcal{O}(m) \subset \{1,2,\dots,j\} \text{ and } z^{|\mathcal{O}(m)|} \equiv 1 \bmod p\}|}.$$

Proof of Theorem C.2. If π is a transposition, then by Lemma C.3, we may assume that $\pi = (12)$. In that case, there are $n - 2$ fixed points, and $s(j, \pi) = j - 2$ for $j \geq 3$. The second sum in Proposition C.5 reduces to the case that $j = 2$, and there are exactly two solutions to $z^2 \equiv 1 \bmod p$ if p is odd ($z \equiv \pm 1$), and just one if $p = 2$. So we obtain

$$\sum_{l=1}^{n-2} J_l(p) + \begin{cases} 2 & \text{if } p \text{ is odd,} \\ 1 & \text{if } p = 2. \end{cases}$$

The left sum is $p^{n-2} + p^{n-3} + \cdots + p - (n-2) = (p^{n-1} - 1)/(p-1) - n + 1$; perhaps unsurprisingly, this is $\phi_1 * J_2 * \cdots * J_{n-2}(p)$. It is easy to see than any nonidentity permutation other than a transposition will have leading term at most p^{n-3}.

If π is a cycle of order n, then the count is hardly anything, just $\mathcal{N}_n(p) = \gcd\{n, p-1\}$.

Now we make some crude estimates for the number of PH-equivalence classes of determinant $\pm d$ matrices in $\mathcal{NS}_n$, denoted $\mathcal{PH}(n, d)$, when d is square-free. We see that $\bigcup_{\pi \neq \mathrm{I}} \mathcal{Z}(\pi)(d)$ consists of the weakly terminal matrices (of determinant d) whose orbit size is strictly less than $n!$. Let $F(n, d) = (\phi * J_2 * \cdots * J_{n-1})(d)$, the number of weakly terminal matrices of size n and determinant d. Let T be the set of transpositions in S_n, together with the identity element. By Burnside's lemma (actually the lemma that is not Burnside's) and Lemma C.3,

$$\mathcal{PH}(n, d) = \frac{F(n, d) + \sum_{\pi \neq \mathrm{I}} \mathcal{S}(\pi)(d)}{n!}$$

$$= \frac{F(n, d) + \binom{n}{2}\mathcal{S}(12)(d) + \sum_{\pi \in S_n \setminus T} \mathcal{S}(\pi)(d)}{n!}.$$

We know that if π is any of the $\binom{n}{2}$ transpositions, then $\mathcal{S}(\pi)(p)/F(n,p) \le 1/p$; hence for d square-free, $\mathcal{S}(\pi)(d)/F(n,d) \le 1/d$, and if π is not a transposition, then $\mathcal{S}(\pi)(p)/F(n,p) \le \boldsymbol{O}(1/p^{2-\epsilon})$ (as $d \to \infty$) for all $\epsilon > 0$, hence $\mathcal{S}(\pi)(d)/F(n,d) \le 1/d^{2-\epsilon}$. Thus

$$\frac{F(n,d)}{n!}\left(1 + \frac{\binom{n}{2}}{d}(1 - \boldsymbol{o}(1))\right) \le \mathcal{PH}(n,d) \le \frac{F(n,d)}{n!}\left(1 + \frac{\binom{n}{2}}{d} + \frac{n!}{d^{2-\epsilon}}\right)$$

for all $\epsilon > 0$. This is not effective until $d \gg n!$, but it does yield the conjecture (for square-free d). $\qquad\square$

For general d (not assumed to be square-free), we can obtain results for transpositions. For each integer $k > 1$, define the function $\mathcal{M}_k \colon \mathbf{N} \to \mathbf{N}$ via

$$\mathcal{M}_k(d) = \left|\left\{(a,t_1,t_2,\ldots,t_{k-1}) \in \mathbf{Z}_d^k \mid a^2 = 1 \text{ and for all } i, t_i(a+1) = 0\right\}\right|.$$

By the Chinese remainder theorem, each $\mathcal{M}_k$ is multiplicative.

We also define the multiplicative function $\mathcal{P}_k(d) \colon \mathbf{N} \to \mathbf{Z}^+$, via

$$\mathcal{P}_k(d) = \begin{cases} J_k(\sqrt{d}) & \text{if } d \text{ is a square,} \\ 0 & \text{if } d \text{ is not a square.} \end{cases}$$

Informally, $\mathcal{P}_k(d) = \chi_2(d) \cdot J_k(\sqrt{d})$, where χ_2 is the indicator function of the set of square integers.

Lemma C.6. *For p a prime,*

$$\mathcal{M}_k(p^m) = \begin{cases} p^{m(k-1)} + 1 & \text{if } p \text{ is odd,} \\ 2^{k-1} & \text{if } p^m = 2, \\ 2^{2(k-1)} + 2^{k-1} & \text{if } p^m = 4, \\ 2^{m(k-1)} + 2^{(m-1))(k-1)} + 2^k & \text{if } 8 \text{ divides } p^m. \end{cases}$$

Proof. If $a = -1$, then there are $p^{m(k-1)}$ choices for $(t_1,\ldots,t_{k-1})$. If $a = 1$ and p is odd, as 2 is invertible in $\mathbf{Z}_d$, we must have $t_i = 0$, that is, just one solution. When p is odd, the solutions to $a^2 = 1$ are exactly ± 1, hence we have a total of $p^{m(k-1)} + 1$ solutions.

If $p = 2$ and $a = 1$, the number of t such that $2t \equiv 0 \bmod 2^m$ is 2; hence this case accounts for 2^{k-1} solutions. When $m \ge 3$, there are two other roots of $a^2 = 1$, $2^{m-1} \pm 1$. When $a = 2^{m-1} - 1$, the equations reduce to $2^{m-1}t_i \equiv 0 \bmod 2^m$, so there are $2^{(m-1)(k-1)}$ solutions. When $a = 2^{m-1} + 1$, the equations become $2(1 + 2^{m-2})t_i \equiv 0 \bmod 2^m$, and as the middle factor is invertible, there are just 2^{k-1} solutions.

When $p^m = 2$, $a = 1$ is the only square root of 1, so there are 2^{k-1} (preceding paragraph, first line) solutions, as indicated in the statement of the result. If $p^m = 4$, then there are two roots of 1, ± 1; we have $2^{2(k-1)}$ solutions from $a = -1$ (first line of first paragraph) plus 2^{k-1} solutions arising from $a = 1$ (first line of second paragraph).

Finally, if $p^m = 2^m$ with $m \ge 3$, we have $2^{m(k-1)} + 2^{k-1} + 2^{(m-1)(k-1)} + 2^{k-1}$ solutions, arising, respectively, from $a = -1, 1, 2^{m-1} - 1, 2^{m-1} + 1$. $\qquad\square$

Recall that we have abbreviated $(\phi * J_2 * \cdots * J_{n-1})(d)$ to $F(n, d)$.

Lemma C.7. *Let $\pi \in S_n$ be a transposition, with $n > 2$. For d a positive integer, the number of $n \times n$ weakly terminal matrices of determinant d that are invariant under π is*

$$\mathcal{S}(\pi)(d) = \big(\phi * J_2 * \cdots * J_{n-3} * \mathcal{P}_{n-2} * \mathcal{M}_{n-1}\big)(d).$$

Proof. As $d \mapsto S(\pi(d))$ is multiplicative, we may assume $d = p^m$. By Lemma C.3, we may assume that π interchanges $n - 1$ and n. Fix (k, l) with $k + l \leq m$, and let C be a weakly terminal matrix whose last two diagonal entries are p^k and p^l, respectively. Denote the entries above the diagonal by $a_{i,j}$ as usual; for convenience, denote $a_{n-1,n} = a$. Let P be the permutation matrix corresponding to π, that is, right multiplication by it implements the interchange of the last two columns. Then $I - P = 0_{n-2} \oplus \left(\begin{smallmatrix} 1 & -1 \\ -1 & 1 \end{smallmatrix}\right)$.

The condition that C is π-invariant is equivalent to $CPC^{-1} \in \mathrm{M}_n\mathbf{Z}$, equivalently, $C(I - P)C^{-1} \in \mathrm{M}_n\mathbf{Z}$. To calculate $(I - P)C^{-1}$, we need only calculate the bottom 2×2 block of C^{-1}, which is found in a matter of seconds to be $p^{-(k+l)}\left(\begin{smallmatrix} p^l & -a \\ 0 & p^k \end{smallmatrix}\right)$. Thus, letting C_0 be the upper $n - 2$ square block of C,

$$C(I-P)C^{-1} = \frac{1}{p^{k+l}} \begin{pmatrix} C_0 & a_{1,n-1} & a_{1,n} \\ & a_{2,n-1} & a_{2,n} \\ & \vdots & \vdots \\ & a_{n-2,n-1} & a_{n-2,n} \\ 0 & p^k & a \\ 0 & 0 & p^l \end{pmatrix} \left(0_{n-2} \oplus \begin{pmatrix} p^l & -(a + p^k) \\ -p^l & a + p^k \end{pmatrix}\right).$$

This multiplies easily (we can ignore C_0), and we deduce necessary and sufficient conditions for all the entries to be integers:

(i) for all $1 \leq j \leq n - 2$, $a_{j,n} \equiv a_{j,n-1} \bmod p^k$,
(ii) for all $1 \leq j \leq n - 2$, $(a_{j,n} - a_{j,n-1})(a + p^k) \equiv 0 \bmod p^{k+l}$,
(iii) $a \equiv 0 \bmod p^k$,
(iv) $p^{2l} \equiv 0 \bmod p^{k+l}$,
(v) $p^{2k} \equiv a^2 \bmod p^{k+l}$.

From (iv), we must have $k \leq l$. We may write $a = p^k a_0$ by (iii), with $a_0 < p^{l-k}$ (as C is weakly terminal). Then (v) yields $a_0^2 \equiv 1 \bmod p^{l-k}$. By (i), we may write $a_{j,n} = a_{j,n-1} + t_j p^k$, for some $t_j < p^{l-k}$. Then (ii) translates to $t_j(1 + a) \equiv 0 \bmod p^{l-k}$. Conversely, if $l > k$, given $a_0^2 = 1$ and t_j satisfying $t_j(1+a) = 0$, then for each choice of $(a_{1,n-1}, a_{2,n-1}, \ldots, a_{n-2,n-1})^T$, we obtain a fixed point of π. If $l = k > 0$, then $a = 0$, and $t_i = 0$ for all i, so we obtain exactly one solution for each $(a_{1,n-1}, a_{2,n-1}, \ldots, a_{n-2,n})^T$. Finally, if $l = k = 0$, there is only once choice.

The arbitrary weakly terminal matrix in the upper block, C_0, is of determinant p^{m-k-l} and size $n - 2$; thus there are $F(n - 2, p^{m-k-l})$ choices for C_0. For the $(n - 1)$st column, there are no constraints on the entries (assuming $k \leq l$), so there are $J_{n-2}(p^k)$ choices (since the column has to be unimodular).

Finally, once the $(n-1)$st column entries are determined, we have, by the previous paragraph, $\mathcal{M}_{n-1}(p^{l-k})$ choices. Hence the number of weakly terminal matrices is (on setting $t = l - k$)

$$
\begin{aligned}
\mathcal{S}(\pi)(p^m) &= \sum_{k+l\le m,\ k\le l} F(n-2, p^{m-k-l}) J_{n-2}(p^k) \mathcal{M}_{n-1}(p^{l-k}) \\
&= \sum_{2k+t\le m} F(n-2, p^{m-2k-t}) J_{n-2}(p^k) \mathcal{M}_{n-1}(p^t) \\
&= \sum_{K+t\le m} F(n-2, p^{m-K-t}) \mathcal{P}_{n-2}(p^K) \mathcal{M}_{n-1}(p^t) \\
&= \big((\phi * J_2 * \cdots * J_{n-3}) * \mathcal{P}_{n-2} * \mathcal{M}_{n-1}\big)(p^m)
\end{aligned}
$$

The third line is obtained from the second line via the observation that if K is odd, then $P_{n-2}(p^K) = 0$. $\square$

If $n = 3$, the result is $\mathcal{P}_1 * \mathcal{M}_2$, and if $n = 4$, the result is $\phi * \mathcal{P}_2 * \mathcal{M}_3$ ($J_1 = \phi$ and J_0 is the constant function). So for π a transposition, $\mathcal{S}(\mathrm{I}) - \mathcal{S}(\pi) = (\phi * J_2 * \cdots * J_{n-3}) * (J_{n-2} * J_{n-1} - P_{n-2} * \mathcal{M}_{n-1})$, which is sufficient to show $\mathcal{S}(\pi)(d)/F(n,d) = \boldsymbol{O}(1/d)$. So the conjecture (for general d) would be true if the specific conjecture were true (as it almost certainly is).

Appendix D. Counting PH-equivalence classes of size 3

Here we obtain exact counts for various situations involving the PH-equivalence classes when the matrix size is 3, without assuming the determinants are square-free (as always, we are assuming the matrices are in $\mathcal{NS}$). For example, those equivalence classes that contain a terminal matrix with 1-block size two can be subdivided into three interesting subcases, and we can count each. As a result, we show that in terms of PH-equivalence classes, those of fixed determinant with a 1-block size two matrix are generically swamped by those not containing one, even when we restrict to square-free determinant (generally, for determinant d, the larger $\sum_{p|d} 1/p$ is, the smaller is the ratio of 1-block size two equivalence classes to the rest).

Theorem D.1. *The number of PH-equivalence classes $\mathcal{PH}(3,d)$ satisfies*

$$
1 + \frac{3}{d} \le \frac{\mathcal{PH}(3,d)}{(\phi * J_2)(d)/6} \le 1 + \frac{3\zeta(2)}{d} + \boldsymbol{o}\Big(\frac{1}{d^{2-\epsilon}}\Big)
$$

for all $\epsilon > 0$.

This of course is close to the conjecture of Appendix C with $n = 3$. The little oh term is presumably redundant.

For $n = 3$, again by Burnside's lemma, the number of PH-equivalence classes is

$$
\text{(5)} \qquad \frac{\phi * J_2(d) + 3\mathcal{S}(23)(d) + 2\mathcal{S}(132)(d)}{6}.
$$

If $m > 1$ and p is a prime,

$$(\phi * J_2)(p^m) = (p^{m-2}(p+1)^2 + 1)p^{m-1}(p-1)$$

$$= p^{2m}\left(1 + \frac{1}{p} - \frac{1}{p^2} - \frac{1}{p^3} - \frac{1}{p^{m+1}} + \frac{1}{p^m}\right)$$

At $m = 1$, the outcome is simply $p - 1 + p^2 - 1 = (p-1)(p+2)$. Hence as a function of d, it is a bit less than $d^2 \prod_{p|d}(p+1)(\prod_{p|d}(1 - 1/p^2))$. At $d = 2^m$, the outcome is asymptotically $9 \cdot 2^{2m-3}(1 - \boldsymbol{O}(2^{-m}))$

Now $\phi * J_2(p^m) = p^{2m} + p^{2m-1} + \cdots$, so $\phi * J_2(d) = d^2 \prod_{p|d}(1 + 1/p + 1/p^2 + \cdots)$. We will find that $\mathcal{S}(12)(p^m) = p^m + p^{m-1} - \cdots$, except for $p = 2$, when it begins $3 \cdot 2^m/4$ rather than 2^m, so $\mathcal{S}(12)(d) \le d \prod_{p|d}(1 + 1/p + 1/p^2 \pm \cdots)$ and $\mathcal{S}(132)(d) = \boldsymbol{o}(d^\epsilon)$ for all $\epsilon > 0$; both of these will result from exact expressions.

There are relatively straightforward asymptotic estimates, for example, with fixed n, the number of equivalence classes of terminal forms with 1-block size $n - 1$ is bounded below by

$$\frac{\max\{(d - \phi(d))^{n-1}, \phi(d)^{n-1}\}}{n!}.$$

However, there are some cases (with $n = 3$), wherein the formulas become quite simple. If d is a prime or a product of two distinct primes, automatically all terminal forms have 1-block size $n - 1$. More generally, we obtain exact numbers of PH-equivalence classes for fixed absolute determinant d when $n = 3$.

Let $w, w', w'' : \mathbf{N} \to \mathbf{C}$ be defined, respectively, by $w(d)$ is the number of distinct prime divisors of d, $w'(d)$ is the number of distinct prime divisors of d that are congruent to 1 modulo 3, and $w''(d)$ is 1 if 9 divides d, otherwise it is zero (so w'' is the indicator function of $9\mathbf{N}$). Each of them is additive (in the number-theoretic sense), so each of 3^w, $3^{w'}$ and $3^{w''}$ is multiplicative.

We also define $\mathcal{M}_2, \mathcal{M} : \mathbf{N} \to \mathbf{C}$ by setting, for $d = \prod_{p|d} p^{m(p)}$,

$$\mathcal{M}_2(d) = \begin{cases} 1 & \text{if } m(2) = 0, \\ 2 & \text{if } m(2) = 1, \\ 6 & \text{if } m(2) = 2, \\ 3 \cdot 2^{m-2} + 4 & \text{if } m(2) \ge 3, \end{cases}$$

$$\mathcal{M}(d) = \mathcal{M}_2(d) \prod_{\text{odd } p|d} (p^{m(p)} + 1).$$

Obviously, $\mathcal{M}$ and $\mathcal{M}_2$ are multiplicative, but not completely multiplicative.

Recall that $\mathcal{N}_3(d)$ denotes the number of solutions to the polynomial $X^3 - 1 = 0$ in $\mathbf{Z}_d$. On replacing X by $-X$, we see that $\mathcal{N}_3$ also counts the solutions to $X^3 = -1$. By the Chinese remainder theorem, the function $\mathcal{N}_3$ is multiplicative. The following is elementary.

Lemma D.2. *We have* $\mathcal{N}_3 = 3^{w'+w''}$.

Proof. Both sides are multiplicative, so it suffices to show equality for $d = p^m$, with p prime. The set of solutions to $X^3 - 1 = 0$ is a subgroup of $\mathbf{Z}_d^*$ of exponent 3 or 1. If $p \equiv 2 \bmod 3$, $|\mathbf{Z}_d^*| = \phi(p^m) = p^{m-1}(p-1)$ is relatively prime to 3, so the solution is unique. In this case, $\mathcal{N}_3(p^m) = 1 = 3^{w'(d)+w''(d)}$. If $p \equiv 1 \bmod 3$, $\mathbf{Z}_d^*$ is cyclic of order $p^{m-1}(p-1)$; the latter is divisible by 3, and as the group is cyclic, it has a unique subgroup of order three. Hence $\mathcal{N}_3(p^m) = 3 = 3^{w'(d)+w''(d)}$.

Finally, if $p = 3$, with $m = 1$, $\mathbf{Z}_3^*$ is order two, so $\mathcal{N}_3(3) = 1 = 3^{w'(3)+w''(3)}$; if $m \geq 2$, then $\mathbf{Z}_d$ is cyclic of order $2 \cdot 3^{m-1}$, hence has a unique subgroup of order 3, and thus $\mathcal{N}_3(d) = 3 = 3^{w'(d)+w''(d)}$. $\qquad\square$

Lemma D.3. *Let p be a prime, and m a positive integer. The number of solutions (y, k) to the equations $y^2 - 1 = 0$ and $(y + 1)k = 0$ in $\mathbf{Z}_{p^m}$ is*

$$\mathcal{M}(p^m) = \begin{cases} p^m + 1 & \text{if } p \text{ is odd,} \\ 2 & \text{if } p^m = 2, \\ 6 & \text{if } p^m = 4, \\ 3 \cdot 2^{m-1} + 4 & \text{if } p = 2 \text{ and } m \geq 3. \end{cases}$$

Proof. Since $\mathbf{Z}_{p^m}/p^{m-1}\mathbf{Z}_{p^m} \cong \mathbf{Z}_p$ and the latter is embedded in the former, if $y^2 = 1$, then we can write $y = w + p^t s$ for some $w \in \{0, 1, 2, \ldots, p-1\}$, $1 \leq t \leq m - 1$ (so if $m = 1$, the second summand disappears), and $(p, s) = 1$ with $1 \leq s \leq p - 1$, or $y = w$. In the field $\mathbf{Z}_p$, the only solutions are ± 1, so $w = \pm 1$. Thus $1 = y^2 = 1 + p^t s(\pm 2 + p^t s^2)$. As $(p, s) = 1$, we must have p^m divides $p^t(\pm 2 + p^t s^2)$.

If p is odd, then $\pm 2 + p^t s^2$ is invertible in $\mathbf{Z}_{p^m}$, which forces $y = \pm 1$. When $y = -1$, we can set k to be any element of $\mathbf{Z}_{p^m}$, so we obtain p^m choices, $(-1, k)$. When $y = 1$, $y + 1 = 2$ is invertible modulo p and thus modulo p^m, and so the only choice is $(1, 0)$. Hence there are $p^m + 1$ solutions.

If $p = 2$ and $m = 1$, then obviously $y = 1$ and then k can be anything, i.e., we obtain two solutions, $\{(1, 0), (1, 1)\}$. If $m = 2$, there are two square roots of unity in $\mathbf{Z}_4$, ± 1 (or $\{1, 3\}$ if you prefer); if $y = -1$, we obtain the four solutions $(-1, k)$, while if $y = 1$, there are only two, $\{(1, 0), (1, 2)\}$. Thus when $m = 2$, there are a total of 6 solutions.

If $p = 2$ and $m \geq 3$, there are now four square roots of 1, $y = \pm 1 + 2^{m-1}u$, where $u \in \{0, 1\}$, as follows easily from 2^m dividing $2^t(\pm 2 + p^t s^2)$. If $y = -1$, we have the 2^m solutions $\{(-1, k)\}$; if $y = 2^{m-1} - 1$, then $y + 1 = 2^{m-1}$, so we obtain 2^{m-1} solutions, $\{(2^{m-1} - 1, 2j)\}_{0 \leq j < 2^{m-1}}$. If $y = 1 + 2^{m-1}u$, then $y + 1 = 2(1 + 2^{m-2}u)$; as the second factor is a unit (since $m \geq 3$), it follows that in order that $k(y + 1) = 0$, we must have 2^{m-1} divides k. Hence in both cases, there are only two solutions.

Thus if 8 divides p^m, we must have $2^m + 2^{m-1} + 4$ solutions in total. $\qquad\square$

By the Chinese remainder theorem, the number of solutions $(k, y) \in (\mathbf{Z}_d)^2$ of the equations $Y^2 = 1$ and $(Y + 1)K = 0$ is $\mathcal{M}(d)$.

Now we determine $\mathcal{S}(23)(p^m)$ and $\mathcal{S}(132)(p^m)$. The generic weakly terminal matrix is given by

$$C = \begin{pmatrix} 1 & a & b \\ 0 & e & gy \\ 0 & 0 & gx \end{pmatrix},$$

and its inverse is

$$C^{-1} = \frac{1}{egx} \begin{pmatrix} egx & -a & ayg - be \\ 0 & gx & -gy \\ 0 & 0 & e \end{pmatrix} \in M_3\mathbf{Q},$$

where all of $\{a, b, e, g, y\}$ are nonnegative and $a < e$, $y < x$, $b < gx$, and $\gcd\{a, e\} = \gcd\{b, g\} = \gcd\{x, y\} = 1$ (by convention, $\gcd\{0, m\} = m$). When we have a permutation acting on C, it also acts on the triple $(J(C_{\Omega(i)}))_{i=1}^3$ by permuting according to its action on the columns. Since the three invariants for the generic matrix are, in order (that is, deleting the first column, then deleting the second column), $(\mathbf{Z}_{(\delta, gx)}, \mathbf{Z}_g, \mathbf{Z}_e)$, where $\delta = agy - be$ (the determinant of the upper right block), if for example $\pi = (23)$ or (132) and C is invariant under the action of π (meaning that $CP_\pi C^{-1} \in M_3\mathbf{Z}$), then we must have $e = g$.

Define the multiplicative functions, χ_2 and $\mathcal{P}$: χ_2 is the indicator function of the set of square integers and $\mathcal{P}(d) = \chi_2(d) \cdot \phi(\sqrt{d})$.

Lemma D.4. *For d a positive integer, the number of weakly terminal 3×3 matrices of determinant d that are invariant under a transposition $\pi \in S_3$ is*

$$\mathcal{S}(\pi)(d) = (\mathcal{P} * \mathcal{M})(d).$$

Proof. This is Lemma C.7. □

This is not useful unless we can describe the resulting convolution product. The formula below when $p = 2$ is obtained by considering a number of special cases, and then summing geometric series; it did not seem worthwhile to transcribe the tedious argument.

Lemma D.5. *Suppose π is a transposition.*

(a) *If p is an odd prime, then*

$$\mathcal{S}(\pi)(p^m) = (\mathcal{P} * \mathcal{M})(p^m)$$
$$= p^m + p^{m-1} + 1 + \begin{cases} p^{m/2} - p^{m/2-1} & \text{if } m \text{ is even,} \\ -p^{(m-1)/2} & \text{if } m \text{ is odd.} \end{cases}$$

(b) *If $p = 2$, then*

$$\mathcal{S}(\pi)(2^m) = (\mathcal{P} * \mathcal{M})(2^m)$$

$$= \begin{cases} 2 & \text{if } m = 1, \\ 7 & \text{if } m = 2, \\ 12 & \text{if } m = 3, \\ 2^m + 2^{m-3} + 2^{m/2} - 1 & \text{if } m \geq 4 \text{ and is even}, \\ 2^m + 2^{m-3} + 2^{(m-1)/2} + 2^{(m-3)/2} & \text{if } m \geq 5 \text{ and is odd.} \end{cases}$$

Proof. When p is odd and $s > 0$, $\mathcal{M}(p^s) = p^s + 1$ and $\mathcal{M}(1) = 1$. Taking into account the latter, we have

$$\mathcal{S}(\pi)(p^m) = \sum_{0 \leq n \leq m/2} \phi(p^n) p^{m-2n} + \sum_{0 \leq n < m/2} \phi(p^n)$$

$$= p^m + 1 + (p-1) \sum_{1 \leq n \leq m/2} p^{m-n-1} + p^{\lfloor (m-1)/2 \rfloor}$$

$$= p^m + 1 + \begin{cases} (p-1)\dfrac{p^{m-1} - p^{m/2-1}}{p-1} + p^{m/2} & \text{if } m \text{ is even}, \\ (p-1)\dfrac{p^{m-1} - p^{(m-1)/2}}{p-1} & \text{if } m \text{ is odd}. \end{cases}$$

$$= p^m + p^{m-1} + 1 + \begin{cases} p^{m/2} - p^{m/2-1} & \text{if } m \text{ is even}, \\ -p^{(m-1)/2} & \text{if } m \text{ is odd}. \end{cases}$$

When $p = 2$, the computation is more complicated because of the definition of $\mathcal{M}(2^r)$. Fortunately, there is still massive cancellation, and after a battle keeping track of the limits of summation, we obtain the result in the statement of the lemma. $\square$

In particular, the number of invariant C is $d \cdot \prod_{p | d, \, p \text{ odd}}(1 + 1/p \pm \cdots) \cdot \alpha(m(2))$, where α is the function obtained in the last lemma, divided by $2^{m(2)}$ (for $m \geq 4$, $\alpha(m) = 1 + 1/8 + \cdots$; the dependence on the exponent, m, is tiny if m is large).

Now to deal with $\mathcal{Z}(132)(d)$, the set of weakly terminal matrices invariant under the permutation matrix corresponding to (123) or (132). This is fairly horrible, but is not as bad as it could be. It is marginally better to use (132), rather than (123) (the groups they generate are the same, but the computations are a bit less tedious in the former case).

$\mathcal{S}(\pi)(d)$ *with* $\pi = (132)$. From the column action, we have $e = g = (\delta, gx)$ (the last equality, in the presence of the first, is equivalent to $(\delta, x) = 1$), so $d = e^2 x$. The equations are then

$$-a^2 + b \equiv 0 \bmod e, \quad ay - b - y^2 \equiv 0 \bmod x, \quad a^2 y - ab - by + 1 \equiv 0 \bmod ex.$$

Rewrite the third one as $(a^2 - b)y + 1 - ab \equiv 0 \bmod ex$. Taking this modulo e, we obtain $ab \equiv 1 \bmod e$, which, in combination with the first, yields $a^3 \equiv 1 \bmod e$ (and also $b^3 \equiv 1 \bmod e$). Write $b = a^2 + ke$, where k is defined modulo x.

Plugging this into the second and third equations yields

$$-key + 1 - ab \equiv 0 \bmod ex, \quad y^2 - ay + a^2 + ke \equiv 0 \bmod x.$$

The former yields $-key - a^3 - ake + 1 \equiv 0 \bmod ex$, so $ke(y+a) \equiv 1 - a^3 \bmod ex$. Multiplying the second displayed equation by $y + a$ yields $ke(y+a) \equiv -(y^3 + a^3) \bmod x$, whence $y^3 \equiv -1 \bmod x$. Since $e \mid (ab - 1)$, we also have $-ky \equiv (1 - ab)/e \bmod x$. In particular, if $x \neq 1$, then k (and thus b) is uniquely determined by y modulo x.

We recall from Lemma D.2 that each $X^3 \pm 1 = 0$ has three distinct solutions in $\mathbf{Z}_{p^m}$ if and only if $p \equiv 1 \bmod 3$ or $9 \mid p^m$, and otherwise each has one.

Now set $d = p^m$, $e = x^n$, and $x = p^r$ with $2n + r = m$. First, suppose that $n = 0$, so $r = m$, and the equations boil down to $a = 0$, $y^3 \equiv -1 \bmod p^m$, $b \equiv y^2 \bmod p^m$ (so b is determined by y), and $by \equiv -1 \bmod x$, but the last is a consequence of the second last.

If $p \equiv 2 \bmod 3$ or $p^m = 3$, then $y^3 \equiv -1$ entails $y \equiv -1 \bmod p^m$. Hence $b \equiv 1 \bmod p^m$, so there is exactly one solution for $(a, b, y) = (0, 1, -1)$. If $p \equiv 1 \bmod 3$ or $9 \mid p^m$, there are three choices for y, and thus a total of three choices for (a, b, y) when $n = 0$.

Now suppose that $n > 0$. If $r = 0$, then $m = 2n$, and the only conditions imposed are $a^3 \equiv 1 \bmod p^n$, $y = 0$ and $b \equiv a^2 \bmod p^n = ex$. Hence we obtain three solutions for (a, y, b) if $p \equiv 1 \bmod 3$ or $9 \mid p^m$ (since b is determined by a), and 1 otherwise.

Finally, suppose that $n, r > 0$, so that $1 \leq n < m/2$. Here y is defined modulo $p^r = x$ and b is defined modulo $p^{n+r} = ex$. We have $a^3 \equiv 1 \bmod p^n$, and we can write $b = a^2 + kp^n$ (where k is defined modulo p^r). We also have $y^3 \equiv -1 \bmod p^r$, that is, $(-y)^3 \equiv \bmod p^r$.

If $p \equiv 2 \bmod 3$, then $a = 1$ (defined modulo p^n) and $y = -1$ (defined modulo p^r), and thus $kp^n \equiv 1 + 1 + 1 \bmod p^r$. This forces (since both n and r are positive) $p = 3$, a contradiction, so that in this case, there are no solutions.

If $p^m = 3$, then $n + r = 1$, contradicting $n, r > 0$.

If $p \equiv 1 \bmod 3$ or $9 \mid p^m$, there are three choices for a, and also for y. However, they are not independent of each other. Modulo p, either $y + a$ is 0 (which corresponds to taking the same cube root of ± 1) or invertible. But if $p \mid (y+a)$, as in the previous paragraph, we obtain $kp^n \equiv -(y^2 - ay + a^2) \bmod p^r \equiv -3a^2 + pX \bmod p^r$. This yields a contradiction, unless $p = 3$—and in that case, we have $m \geq 2$, so either $r = 1$ (in which case k has three values), or $n = 1$ and $r > 1$, and in that case k is uniquely determined.

Finally, if $p \equiv 1 \bmod 3$ or $9 \mid p^m$ and $y + a \neq 0 \bmod p$, then there are six choices for (a, y), namely, so that $y + a$ is invertible modulo p, hence modulo any power of p, and for each of these, the equation $k(y+a) \equiv (1 - a^3)/e \bmod p^r$ uniquely determines k.

Now we count all these possibilities. Let $H(t)$ be 1 if t is odd, and 2 if t is even. If $p \equiv 2 \bmod 3$, there are zero solutions for $n, r > 0$, giving us a total of 1 solution (arising from $n = 0$) plus an additional 1 if and only if m is even. So the formula is $H(m(p))$.

If $p \equiv 1 \bmod 3$, we obtain 3 solutions from the case $n = 0$ plus an additional 3 if m is even ($r = 0$), plus $\sum_{1 \le n < m/2} 6 = 6\lfloor (m-1)/2 \rfloor$. Here the formula is $6\lfloor (m(p)-1)/2 \rfloor + 3H(m(p))$. This is $3(m(p)-1) + 6 = 3(m(p)+1)$ if $m(p)$ is even, and $3(m(p)-1) + 3 = 3m(p)$ if $m(p)$ is odd, so we can rewrite the expression as $3(m(p) + H(m(p)) - 1)$.

Now we look at the totals for the various situations. We recall $r = m - 2n$, so that $r = 0$ entails m is even and $r = 1$ entails m is odd. If $p \equiv 2 \bmod 3$, then

$$\mathcal{S}(132)(p^m) = 1 + 0 + H(m) - 1 = H(m).$$

If $p \equiv 1 \bmod 3$, then

$$\mathcal{S}(132)(p^m) = 3 + \sum_{1 \le n < m/2} 6 + 3(H(m) - 1)$$

$$= 3 + 6 \left\lfloor \frac{m-1}{2} \right\rfloor + 3(H(m) - 1)$$

$$= \begin{cases} 3m + 3 & \text{if } m \text{ is even,} \\ 3m & \text{if } m \text{ is odd.} \end{cases}$$

If $p^m = 3$, then

$$\mathcal{S}(132)(3) = 1.$$

Finally, if $p = 3$ and $m \ge 2$,

$$\mathcal{S}(132)(3^m) = 3 + \sum_{1 \le n < m/2} 6 + 3(H(m) - 1) + 1$$

$$= \begin{cases} 3m + 4 & \text{if } m \text{ is even,} \\ 3m + 1 & \text{if } m \text{ is odd.} \end{cases}$$

We can combine these in one gigantic formula,

$$\mathcal{S}(132)(d) = 2^{|\{p|d \,|\, p \equiv 2 \bmod 3; \, m(p) \text{ even}\}|} \cdot 3^{w'(d)}$$

$$\times \prod_{p|d, \, p \equiv 1 \bmod 3} (m(p) + H(m(p)) - 1) \cdot \begin{cases} 1 & \text{if } m(3) \le 1, \\ 3m(3) + 4 & \text{even } m(3) > 0, \\ 3m(3) + 1 & \text{odd } m(3) > 1. \end{cases}$$

It is not necessary for the counting formula, but a similar computation (much easier than the others) reveals that the number of S_3-invariant weakly terminal matrices of determinant d is

$$\mathcal{S}(S_3)(d) = 2^{w(d)} \cdot \begin{cases} 1 & \text{if } m(3) = 0, \\ \frac{m(3)+1}{2} & \text{if } m(3) > 0. \end{cases}$$

In particular, $\mathcal{Z}(123)(d) = \mathcal{Z}(S_3)(d)$ if and only if d is a square all of whose prime divisors are congruent to 1 modulo 3, and in that case, the cardinality is $2^{w(d)}$.

Equation (5) at the beginning of this section now yields the number of PH-equivalence classes of $C \in \mathcal{NS}_3$ with determinant $\pm d$:

$$\mathcal{PH}(3, d) \coloneqq \frac{(\phi * J_2)(d) + 3(\mathcal{P} * \mathcal{M})(d) + 2\mathcal{S}(132)(d)}{6}.$$

The last term is too complicated to expand compactly, but it is given explicitly above. When d is square-free, the formula simplifies considerably, and we will discuss this later.

We see from Lemma D.5 and the formula for $\phi * J_2$ that $(1-1/p^2)\mathcal{S}(23)(p^m) \leq (\phi * J_2)(p^m)/p^m$, so $\mathcal{S}(23)(d)/(\phi * J_2(d) \leq \zeta(2)/d$. And similarly, $\mathcal{S}(132)(d) = \boldsymbol{o}(d^{-2+\epsilon}) \cdot \phi * J_2(d)$. The number of PH-equivalence classes $\mathcal{PH}(3, d)$ thus satisfies

$$1 + \frac{3}{d} \leq \frac{\mathcal{PH}(3, d)}{(\phi * J_2)(d)/6} \leq 1 + \frac{3\zeta(2)}{d} + \boldsymbol{o}\Big(\frac{1}{d^{2-\epsilon}}\Big)$$

for all $\epsilon > 0$. This completes the proof of Theorem D.1.

1-block size two PH-equivalence classes. We now investigate the number of PH-equivalence classes of fixed absolute determinant that contain a 1-block size two weakly terminal (and thus terminal) matrix, so that we can compare them with the total number of PH-equivalence classes. This time, the set of matrices that we are looking at are not invariant under the action of S_3, so somewhat different methods are used.

So fix $d > 1$, and consider the PH-equivalence classes having a 1-block size two terminal form. We perform operations within the ring $\mathbf{Z}_d$. The third column of one of these terminal forms is

$$\begin{pmatrix} a_1 \\ a_2 \\ d \end{pmatrix},$$

where the ideal generated by $\{a_1, a_2\}$ is $\mathbf{Z}_d$ (when we regard a_i as elements of $\mathbf{Z}_d$), and $0 \leq a_i < d$ (when we regard a_i as integers).

Now we count the number of PH-equivalence classes of matrices $B \in \mathcal{NS}_3$ with absolute determinant d, having a terminal form with 1-block size two.

Recall the multiplicative function $w' : \mathbf{N} \to \mathbf{Z}^+$; $w'(d)$ is the number of distinct prime divisors of d that are congruent to 1 modulo 3.

Case 1: $J(B^{\mathrm{op}}) \cong \mathbf{Z}_d^2$. In this case, by Corollary 1.4 (even without the hypothesis that B has 1-block size 2), B has a terminal form,

$$\begin{pmatrix} 1 & 0 & a_1 \\ 0 & 1 & a_2 \\ 0 & 0 & d \end{pmatrix},$$

where $\gcd\{a_1, d\} = \gcd\{a_2, d\} = 1$. We now view the entries of the truncated column $(a_1, a_2)^T$ as elements of $\mathbf{Z}_d^*$. The equivalence class of such a truncated

column, renamed $(x, y)^T$, is given by

$$\left\{ \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} y \\ x \end{pmatrix}, \begin{pmatrix} x^{-1} \\ -x^{-1}y \end{pmatrix}, \begin{pmatrix} -x^{-1}y \\ x^{-1} \end{pmatrix}, \begin{pmatrix} -xy^{-1} \\ y^{-1} \end{pmatrix}, \begin{pmatrix} y^{-1} \\ -xy^{-1} \end{pmatrix} \right\}.$$

Most of these equivalence classes have size six, but some have size 1, 2, or 3. We count the latter, and then obtain a fairly simple formula for the number of equivalence classes.

1a. *Equivalence class size* 1. There is only one element with this property, explicitly $(-1, -1)^T$.

1b. *Equivalence class size* 3. An inspection of the six possible elements in the equivalence class reveals that the only such with exactly three elements are those of the form

$$\left\{ \begin{pmatrix} x \\ x \end{pmatrix}, \begin{pmatrix} -1 \\ x^{-1} \end{pmatrix}, \begin{pmatrix} x^{-1} \\ -1 \end{pmatrix} \right\},$$

provided $x \neq -1$. There are thus $\phi(d) - 1$ equivalence classes here, covering $3\phi(d) - 3$ elements.

1c. *Equivalence classes of size* 2. These are of the form

$$\left\{ \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \right\},$$

where $\alpha^3 = -1$, $\beta = -\alpha^2$ and $\alpha \neq -1$. To count the number of choices for α (and β), we first observe that if p is a prime exceeding 3, then the equation $z^3 = -1$ has a solution other than -1 in $\mathbf{Z}_p$ if and only if -3 is a square modulo p, equivalently, if and only if $p \equiv 1 \bmod 3$, and when this occurs, the solutions are distinct. It is easy to verify that these properties hold for any power of p as well.

If $p = 3$, then -1 is the only solution to $z^3 = -1$ modulo 3, but modulo any higher power of 3, there are exactly 3 distinct solutions: modulo p^m, the solutions are $\{p^{m-1} - 1, 2p^{m-1} - 1, -1\}$, including -1.

If $p = 2$, then there is only one solution to $z^3 = -1$ modulo 2^m.

Write $d = 3^{m(3)} \cdot \prod_{p \in P} p^{m(p)} \prod_{q \in Q} q^{m(q)}$, where P is the set of primes congruent to one modulo three, and Q is the set of primes (including 2) congruent to two modulo three. By the Chinese remainder theorem, the number of solutions (including -1) to the equation $z^3 = -1$ is thus $3^{|P|} \cdot 3^a$, where $a = 0$ if $m(3) \leq 1$ and otherwise equals 1. After discarding the solution $x = -1$ (which is in 1a), the number of columns covered is $3^{w'(d) + a} - 1$, accounting for half as many equivalence classes.

The remaining columns (out of the original $\phi(d)^2$) have six-element equivalence classes. Hence the total number of equivalence classes is

$$\frac{\phi(d)^2 - 1 - (3\phi(d) - 3) - (3^{w'(d)+a} - 1)}{6} + 1 + (\phi(d) - 1) + \frac{3^{w'(d)+a} - 1}{2}$$

$$= \frac{\phi(d)^2 + 3\phi(d) + 2 \cdot 3^{w'(d)+a}}{6},$$

where $a = 0$ if $m(3) \leq 1$, and 1 otherwise.

This is worth stating as a result on PH-equivalence classes.

Proposition D.6 (Case 1)**.** *For d a fixed positive integer, the number of PH-equivalence classes of matrices $B \in \mathcal{NS}_3$ with $|\det B| = d$ and $|J(B^{\mathrm{op}})| = d^2$ is*

$$\frac{\phi(d)^2 + 3\phi(d) + 2 \cdot 3^{w'(d)+w''(d)}}{6}.$$

Proof. The only thing we have to note is that if $|J(B^{\mathrm{op}})| = |\det B|^2$ for $B \in \mathcal{NS}_3$, then, by Lemma 1.3 and Corollary 1.4, B has a terminal form of the type discussed in case 1 above (it also follows that $J(B^{\mathrm{op}}) \cong (\mathbf{Z}_d)^2$). $\qquad\square$

Case 2: *Exactly one of $\{a_1, a_2\}$ is invertible modulo d.* In this case, $a_1 \not\equiv a_2 \bmod d$. By Proposition 2.1, the equivalence classes are then of the form

$$\left\{ \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x^{-1} \\ -x^{-1}y \end{pmatrix}, \begin{pmatrix} y \\ x \end{pmatrix}, \begin{pmatrix} -x^{-1}y \\ x^{-1} \end{pmatrix} \right\},$$

where $x \in \mathbf{Z}_d^*$ and $y \notin \mathbf{Z}_d^*$. The only possible equivalence classes with fewer than four elements are those with two, and this occurs if and only if $x = x^{-1}$ and $y = -x^{-1}y$; this reduces to $x^2 = 1$ and $(1+x)y = 0$. By Lemma D.3, the number of choices for (x, y) is $\mathcal{M}(d)$.

Now the only case in which y can be a unit occurs when $x = -1$, and in that case y can be anything. So to obtain the number of solutions in which y is a nonunit, we simply subtract $\phi(d)$ from $\mathcal{M}(d)$. The number of solutions to $x^2 = 1$ and $(1+x)y = 0$ for $(x, y) \in \mathbf{Z}_d^* \times (\mathbf{Z}_d \setminus \mathbf{Z}_d^*)$ is thus

$$N_2(d) \coloneqq \mathcal{M}(d) - \phi(d).$$

All of the other possible $2\phi(d) \cdot (d - \phi(d))$ columns have four-element equivalence classes; hence the total number of equivalence classes for case 2 is

$$\frac{2\phi(d) \cdot (d - \phi(d)) - 2N_2(d)}{4} + N_2(d) = \frac{\phi(d) \cdot (d - \phi(d)) + N_2(d)}{2}.$$

Proposition D.7 (Case 2)**.** *The number of PH-equivalence classes corresponding to exactly one of (a_1, a_2) being invertible modulo d is*

$$\frac{\phi(d) \cdot (d - \phi(d) - 1) + \mathcal{M}(d)}{2}.$$

Case 2 corresponds to all the situations in which $J(B^{\mathrm{op}})$ contains a proper direct summand isomorphic to $\mathbf{Z}_d$ but $|J(B^{\mathrm{op}})| < d^2$. The remainder are covered by case 3.

Case 3: *Both a_1 and a_2 are nonunits in $\mathbf{Z}_d$.* This can be restated as $J(B_{\Omega(i)})$ is not zero for exactly two choices of i. Since $B \in \mathcal{NS}_3$, we also have to have $\gcd\{a_1, a_2, d\} = 1$, equivalently, that in $\mathbf{Z}_d$, the ideal generated by $\{a_1, a_2\}$ is the improper one.

So let $(x, y)^T$ correspond to such a truncated column; for most of this, we regard them as integers (rather than elements of $\mathbf{Z}_d$), each with $\gcd\{x, d\}$, $\gcd\{y, d\} > 1$, and of course, $1 \le x, y \le d - 1$ (we cannot have $x = 0$, $y = 0$, or $x = y$, since $\gcd\{x, y, d\} = 1$). All the equivalence classes here consist of

exactly two elements (the column and its flip), so it is simply a matter of counting the number of pairs, and dividing by two.

First, we note that if $w(d) = 1$ (that is, d is a power of a single prime), then there are no equivalence classes. So we assume $k := w(d) \geq 2$, and write $d = \prod_{i=1}^{k} p_i^{m(i)}$, and $S = \{1, 2, \ldots, k\}$. For a subset Ω of S, write $d_\Omega = \prod_{i \in \Omega} p_i^{m(i)}$ and $D_\Omega = \prod_{i \in \Omega} p_i$. Thus $d_\varnothing = D_\varnothing = 1$, $d_S = d$, and $D := D_S = \prod_{p \mid d} p$.

For an eligible truncated column $(x, y)^T$, we may write uniquely $x = D_{\Omega_1} \cdot t_1$, $y = D_{\Omega_2} \cdot t_2$, subject to the following conditions:

(i) $\Omega_i \neq \varnothing$,
(ii) $\Omega_1 \cap \Omega_2 = \varnothing$,
(iii) for all $p \in \Omega_i^c$, $\gcd\{t_i, p\} = 1$.

We see that since $1 \leq x, y < d$, we have $1 \leq t_i < d/D_{\Omega_i}$. If we fix the ordered pair (Ω_1, Ω_2), then the number of choices for t_i is

$$\frac{d}{D_{\Omega_i}} \prod_{j \in \Omega_i^c} \left(1 - \frac{1}{p_j}\right).$$

Thus the number of eligible truncated columns corresponding to fixed (Ω_1, Ω_2) is the product

$$\frac{d}{D_{\Omega_1}} \prod_{j \in \Omega_1^c} \left(1 - \frac{1}{p_j}\right) \cdot \frac{d}{D_{\Omega_2}} \prod_{j \in \Omega_2^c} \left(1 - \frac{1}{p_j}\right)$$
$$= \frac{d^2}{D_{\Omega_1 \cup \Omega_2}} \cdot \prod_{p \mid d} \left(1 - \frac{1}{p}\right) \cdot \prod_{j \in \Omega_1^c \cap \Omega_2^c} \left(1 - \frac{1}{p_j}\right)$$
$$= d\phi(d) \frac{\prod_{j \in \Omega_1^c \cap \Omega_2^c} (1 - \frac{1}{p_j})}{D_{\Omega_1 \cup \Omega_2}}$$
$$= \phi(d)^2 \cdot \frac{1}{\phi(D_{\Omega_1 \cup \Omega_2})}.$$

Now let Ω be a subset of S, say with $|\Omega| = s$; the number of ways of writing it as a disjoint union of Ω_1 and Ω_2 (maintaining the ordering), with neither being the empty set, is zero if $s \leq 1$, and otherwise

$$\sum_{i=1}^{s-1} \binom{s}{i} = 2^s - 2.$$

Define the polynomial $f(x) = \prod_{p \mid d}(1 + x/(p-1))$.

The total number of truncated columns is thus

$$\phi(d)^2 \sum_{s=2}^{k} (2^s - 2) \sum_{|\Omega|=s} \frac{1}{\phi(D_\Omega)} = \phi(d)^2 \left(1 + \sum_{s=0}^{k} (2^s - 2) \sum_{|\Omega|=s} \frac{1}{\phi(D_\Omega)}\right)$$
$$= \phi(d)^2 \left(1 + f(2) - 2f(1)\right)$$

$$= \phi(d)^2 \left(1 + \prod_{p|d}\left(1 + \frac{2}{p-1}\right) - 2\prod_{p|d}\left(1 + \frac{1}{p-1}\right) \right)$$

$$= \frac{\phi(d)^2}{\phi(D)} \left(\prod_{p|d}(p+1) - 2\prod_{p|d}p + \prod_{p|d}(p-1) \right)$$

$$= d\phi(d) \left(\prod_{p|d}\left(1 + \frac{1}{p}\right) - 2 + \prod_{p|d}\left(1 - \frac{1}{p}\right) \right).$$

The number of equivalence classes for case three is half of this.

Proposition D.8 (Case 3)**.** *The number of PH-equivalence classes of $B \in \mathcal{NS}_3$ with $|\det B| = d$ with both a_1 and a_2 being non-invertible modulo d is*

$$\frac{d\phi(d)}{2} \left(\prod_{p|d}\left(1 + \frac{1}{p}\right) - 2 + \prod_{p|d}\left(1 - \frac{1}{p}\right) \right).$$

When $\sum_{p|d} 1/p$ is large, the two rightmost summands are small compared to $\prod(1 + 1/p)$; in that case, this is asymptotic with (provided we choose ds so that $\sum_{p|d} 1/p$ becomes arbitrarily large)

$$\frac{d^2}{2} \prod_{p|d}\left(1 - \frac{1}{p^2}\right).$$

Given ϵ, there exists N such that $\sum_{p \geq N} 1/p^2 < \epsilon$; hence given M, we can find $d \equiv d(\epsilon)$ such that $\sum_{p|d} 1/p^2 < \epsilon$ and $\prod_{p|d}(1 + 1/p) > M$. It follows that the least upper bound for the number of equivalence classes is at least $d^2/2$ (and we can choose square-free d to asymptotically reach this). On the other hand, initially, we only have a choice of $(d - \phi(d))^2/2$ columns, so this is the best possible (and note that $\phi(d)/d \to 0$ for these sequences).

This means that case 3 overwhelms the other two cases (asymptotically) for the appropriate choice of ds (with large numbers of prime divisors). On the other hand, with few prime divisors (or simply small $\sum_{p|d} 1/p$), cases 1 and 2 together are dominant. With just one prime divisor, case 3 is empty.

An amusing example occurs when $d(j)$ is the product of the first j primes. Then

$$\lim_{j \to \infty} \frac{N_j}{d(j)^2} = \frac{1}{2\zeta(2)}.$$

where N_j is the number of case 3 PH-equivalent classes for $B \in \mathcal{NS}_3$ with $|\det B| = d(j)$. For case 2 with the same sequence, the number of PH-equivalence classes is asymptotic to $\phi(d)d/2$, which is smaller. With case 1, the number is about $\phi^2(d)/6$, smaller still. So in the display we could replace "case 3" by PH-equivalence classes that contain a terminal form with 1-block size two.

If B is classified in case 3, then $I(B^{\mathrm{op}}) \cong \mathbf{Z}_d$; however, there are also examples as part of case 2 with the same property (case 2 examples with $I(B^{\mathrm{op}}) \cong \mathbf{Z}_d$ automatically have the property that B^{op} also has a terminal form with 1-block size two; however, not all case 3 classes satisfy this).

There are a couple of situations in which we can go directly to the number of PH-equivalence classes, without requiring the restriction to those with 1-block size $n - 1$.

Lemma D.9. *If $B \in \mathcal{NS}_3$ and $d := |\det B|$ is either a prime or of the form pq for distinct primes p and q, then B is PH-equivalent to a terminal form with 1-block size 2.*

Remark. We have seen that the conclusion can fail if d is a product of three distinct primes, in fact, $d = 30 = 2 \cdot 3 \cdot 5$, and of course, it can also fail if $d = p^2$.

Proof. This is a special case of Proposition 3.9. $\square$

Adding the results from case 1, case 2 and case 3, we obtain the next result, without referring to the general horrible formula (5).

Proposition D.10. *Suppose the positive integer d is of one of the following forms, $d = p, 2p, pq$, where p and q are distinct odd primes. Then the number of PH-equivalence classes of $B \in \mathcal{NS}_3$ such that $|\det B| = d$ is*

$$\frac{p^2 + 4p + 1 + 2 \cdot 3^{w'(p)}}{6} \qquad \qquad \text{if } d = p,$$

$$\frac{2p^2 + 5p - 1 + 3^{w'(d)}}{3} \qquad \qquad \text{if } d = 2p,$$

$$\frac{\phi(d)(3d - 2\phi(d) + 3) + 2 \cdot 3^{w'(d)}}{6} + d + 1 \quad \text{if } d = pq,$$

where $w'(d)$ is the number of distinct prime divisors of d that are congruent to 1 modulo 3.

The number of equivalence classes with $|\det B| = 2p$ is itself divisible by p if and only if $p \equiv 2 \bmod 3$.

There is one more bit of low-hanging fruit.

Proposition D.11. *If p is a prime, then the number of PH-equivalence classes of $B \in \mathcal{NS}_3$ with $|\det B| = p^2 := d$ is given by the number of PH-equivalence classes for 1-block size two of determinant d (cases 1 and 2 for $d = p^2$) plus the number of PH-equivalence classes for case 1 with $d = p$. This is*

$$7 \qquad \qquad \text{if } p = 2,$$

$$\frac{p^4 + p^3 + 2p^2 + p + 1 + 2 \cdot 3^{w'(d)}(1 + 3^{w''(d)})}{6} \quad \text{if } p \neq 2.$$

Proof. Let $B \in \mathcal{NS}_3$ have determinant $\pm p^2$. Any of its terminal forms has diagonal either $(1, 1, p^2)$ or $(1, p, p)$. In the former case, it has a terminal form with 1-block size two, so is covered by cases 1, 2 and 3; however, for a power of prime, case 3 is empty.

Suppose that the diagonal is $(1, p, p)$. Then the terminal form must be

$$B' := \begin{pmatrix} 1 & b_1 & b_2 \\ 0 & p & 0 \\ 0 & 0 & p \end{pmatrix},$$

where $1 \le b_i < p$ and $\gcd\{b_1, p\} = \gcd\{b_2, p\} = 1$ (recall the condition in the terminal form that the diagonal entry in the second row from the bottom must be less than or equal to the greatest common divisor of the bottom diagonal entry and the entry immediately above; this explains the zero in the $(2, 3)$ position). Now for $i = 1, 2, 3$, each of $I(B_{\Omega(i)})$ is $\mathbf{Z}_p$, a trivial computation. Hence B' (and thus B) is not PH-equivalent to a terminal form with 1-block size two, so these equivalence classes are disjoint from the former case.

However, if we calculate B'^{op}, we find that it is PH-equivalent to a 1-block size two terminal form, with determinant p, corresponding to case 1 of the latter class:

$$B'^{\mathrm{op}} = \begin{pmatrix} p & 0 & 0 \\ -b_1 & 1 & 0 \\ -b_2 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -b_2 \\ 0 & 1 & -b_2 \\ 0 & 0 & p \end{pmatrix}.$$

(The PH-equivalence was implemented by conjugation with the permutation matrix that transposes 1 and 3.) Thus $^{\mathrm{op}}$ implements a bijection between the current matrices and the matrices covered by case 1 for $d = p$, and of course, this bijection preserves PH-equivalence classes. Hence the number of equivalence classes arising from terminal forms with diagonal $(1, p, p)$ is the same as the number from case 1 of the equivalence classes with $d = p$.   □

The function w'' is nonzero only when $p = 3$; in that case, the outcome is $138/6 = 23$, which of course agrees with the entry for $I = 9$ in [1]. For $p > 3$, the expression simplifies (?) to

$$\frac{p^4 + p^3 + 2p^2 + p + 1 + 4 \cdot 3^{w'(d)}}{6}.$$

I was relieved to find that for $p = 5$ ($w'(d) = 0$) and $p = 7$ ($w'(d) = 1$), this yields 135 and 477 respectively, agreeing with the table entries for $I = 25$ and 49.

Table 1 of [1] was particularly useful in checking examples in order to see whether the formulas were very likely correct! With other values of d than those covered in Lemma D.9, there will be PH-equivalence classes that contain no terminal forms with 1-block size 2.

When $n = 4$, formulas are still possible, but it would take a lot of *Sitzfleisch* to work out all the possible equivalence classes and their quantities.

The formulas simplify considerably when we consider only square-free choices for d; for example, the number of weakly terminal matrices with determinant fixed, is

$$\prod_{p \mid d} (\phi * J_2)(p) = \prod_{p \mid d} (p^2 + p - 2) = \phi(d) d \prod_{p \mid d} (1 + 2/p).$$

For π a transposition, by Lemma D.5,

$$\mathcal{S}(\pi)(d) = \prod_{p \mid d} \mathcal{S}(\pi)(p) = d \prod_{p \mid d; p \neq 2} (1 + 1/p) \quad \text{and} \quad \mathcal{S}(123)(d) = 3^{w'(d)}.$$

Thus for *square-free d*,

$$\mathcal{PH}(3,d) = \frac{d\phi(d)\prod_{p|d}(1+\frac{2}{p}) + 3d\prod_{p|d;p\neq 2}(1+\frac{1}{p}) + 2\cdot 3^{w'(d)}}{6}.$$

(Recall $w'(d)$ is the number of distinct prime divisors of d that are congruent to 1 modulo 3.)

The middle term is $3\prod_{p|d}(1+p)$ if d is odd and $2\prod_{p|d}(1+p)$ if d is even. I tested the formula in Corollary D.1 against Table 1 in [1] (recalling that their I is our d) for values of $d = 30, 42, 70, 102, 105, 154, 165, 182, 186, 190, 195, 210$, as well as numerous choices of primes and products of two primes. Agreement was complete—so I am confident that the formula is correct! (This is somewhat miraculous, as the formula is a sum of four formulas, each rather delicate.)

The first term is by far the largest, so the number is $6^{-1}\phi(d)\prod_{p|d}(p+2)\cdot(1+\boldsymbol{O}(1/d))$. This is the same as $(\phi*J_2(d))/6$ for square-free d. This is also true if d is restricted to squares of primes (Proposition D.11).

Something rather startling occurs when we subtract from this the number of PH-equivalence classes that contain a 1-block size two matrix (the latter is the sum of the three numbers obtained from cases 1, 2 and 3). Recall from Section 7, the difference operator Δ, defined by $\Delta f(x) = f(x+1) - f(x)$.

Proposition D.12. *Let d be a square-free integer. The number of PH-equivalence classes of $C \in \mathcal{NS}_3$ with $|\det C| = d$ and C not equivalent to a terminal form with 1-block size two is*

$$\frac{\phi(d)\Delta^3 f_d(-1)}{6},$$

where $f_d(x) = \prod_{p|d}(x+p)$.

The factor $\phi(d)$ likely arises from an action of $\mathbf{Z}_d^*$ on the equivalence classes, presumably $(b,y) \mapsto (b,y)z$ as z varies over $\mathbf{Z}_d^*$ (a similar phenomenon exists for the number obtained in case 3). The appearance of the third difference operator is rather mysterious. The dominant term in $\Delta^3 f_d(-1)$, at least when $\sum_{p|d} 1/p$ is large, is $\prod_{p|d}(p+2)$. We obtain that if $d(m)$ is a sequence of square-free integers such that $\sum_{p|d(m)} 1/p \to \infty$ as $m \to \infty$, then

$$\frac{N_m^-}{N_m^+ \cdot \prod_{p|d(m)}(1+1/p)} \to \frac{1}{3},$$

where N_m^+ (resp. N_m^-) is the number of PH-equivalence classes of $C \in \mathcal{NS}_3$ with $|\det C| = d(m)$, with (resp. without) a terminal form with 1-block size two.

If d is a product of one or two primes, then $\Delta^3 f_d(-1) = 0$, consistent with Proposition D.10. If $d = pqr$, a product of three primes, then $\Delta^3 f_d(-1) = 6$, so the number of PH-equivalence classes not equivalent to a terminal form with 1-block size two is $\phi(d)$, and in fact, the action of $\mathbf{Z}_d^*$ is just that of $\mathbf{Z}_d^*$ on itself.

For example, with $d = 30$, we take

$$C = \begin{pmatrix} 1 & 1 & 4 \\ 0 & 2 & 5 \\ 0 & 0 & 15 \end{pmatrix}, \quad C^{\mathrm{op}} \sim \begin{pmatrix} 1 & 2 & 4 \\ 0 & 3 & 5 \\ 0 & 0 & 10 \end{pmatrix} =: D.$$

Both are in terminal form, with

$$[\![J(C); J(C_{\Omega(i)})]\!] \cong [\![\mathbf{Z}_{30}; \mathbf{Z}_3, \mathbf{Z}_5, \mathbf{Z}_2]\!] \cong [\![J(D); J(D_{\Omega(i)})]\!].$$

Hence neither is PH-equivalent to a terminal form with 1-block size two. The 8 PH-equivalence classes of determinant ± 30 matrices in $\mathcal{NS}_3$ with no terminal form having 1-block size two are obtained by multiplying the $(b, gy)^T$ truncated column, $(2, 5)^T$, by the integers relatively prime to 30, that is, $1, 7, 11, 13, 17, 19, 23, 29$ (that these are all primes is not entirely a coincidence), and then reducing modulo 15.

More is true: C^{op} is not PH-equivalent to C (even though their invariants are identical). By calculating the ordered triples $(J(C_{\Omega(i)}))$ and $(J(D_{\Omega(i)}))$, we see that if C were PH-equivalent to D, then the relevant permutation matrix P would have to correspond to the transposition (13). But a simple computation reveals that with this P, DPC^{-1} has non-integer coefficients (specifically, the $(1, 3)$ entry is $1/6$).

Constants' References

carefree constant: (see `http://oeis.org/A065463` and [19])

$$\prod_p (1 - (2p - 1)/p^3).$$

Landau's totient constant: (see `http://oeis.org/A082695`)

$$\zeta(2)\zeta(3)/\zeta(6) = \prod_p (1 + 1/p(p - 1)).$$

References

[1] A. Atanasov et al., Resolving toric varieties with Nash blowups, Exp. Math. **20** (2011), no. 3, 288–303. MR2836254

[2] S. Bezuglyi and D. Handelman, Measures on Cantor sets: the good, the ugly, the bad, Trans. Amer. Math. Soc. **366** (2014), no. 12, 6247–6311. MR3267010

[3] P. M. Cohn, *Free ideal rings and localization in general rings*, New Mathematical Monographs, 3, Cambridge University Press, Cambridge, 2006. MR2246388

[4] E. G. Effros, D. E. Handelman and Chao Liang Shen, Dimension groups and their affine representations, Amer. J. Math. **102** (1980), no. 2, 385–407. MR0564479

[5] E. G. Effros and C. L. Shen, Dimension groups and finite difference equations, J. Operator Theory **2** (1979), no. 2, 215–231. MR0559606

[6] K. R. Goodearl, *Partially ordered abelian groups with interpolation*, Mathematical Surveys and Monographs, 20, American Mathematical Society, Providence, RI, 1986. MR0845783

[7] K. R. Goodearl and D. E. Handelman, Metric completions of partially ordered abelian groups, Indiana Univ. Math. J. **29** (1980), no. 6, 861–895. MR0589651

[8] P. A. Grillet, Directed colimits of free commutative semigroups, J. Pure Appl. Algebra **9** (1976/77), no. 1, 73–87. MR0422461

[9] R. N. Gupta et al., Rings over which the transpose of every invertible matrix is invertible, J. Algebra **322** (2009), no. 5, 1627–1636. MR2543626

[10] D. Handelman, Free rank $n + 1$ dense subgroups of $\mathbf{R}^n$ and their endomorphisms, J. Funct. Anal. **46** (1982), no. 1, 1–27. MR0654462

[11] D. Handelman, Positive polynomials and product type actions of compact groups, Mem. Amer. Math. Soc. **54** (1985), no. 320, xi+79 pp. MR0783217

[12] D. E. Handelman, *Positive polynomials, convex integral polytopes, and a random walk problem*, Lecture Notes in Mathematics, 1282, Springer, Berlin, 1987. MR0914972

[13] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford, at the Clarendon Press, 1954. MR0067125

[14] I. Kaplansky, Elementary divisors and modules, Trans. Amer. Math. Soc. **66** (1949), 464–491. MR0031470

[15] T. Y. Lam, *Serre's conjecture*, Lecture Notes in Mathematics, Vol. 635, Springer, Berlin, 1978. MR0485842

[16] G. Landsberg, Ueber eine Anzahlbestimmung und eine damit zusammenhängende Reihe, J. Reine Angew. Math. **111** (1893), 87–88. MR1580299

[17] G. Maze, Natural density distribution of Hermite normal forms of integer matrices, J. Number Theory **131** (2011), no. 12, 2398–2408. MR2832832

[18] G. Maze, J. Rosenthal and U. Wagner, Natural density of rectangular unimodular integer matrices, Linear Algebra Appl. **434** (2011), no. 5, 1319–1324. MR2763589

[19] P. Moree, Counting carefree couples, Math. Newsl. **24** (2014), no. 4, 103–110. MR3241593

[20] B. Reznick, Lattice point simplices, Discrete Math. **60** (1986), 219–242. MR0852110

[21] B. Reznick, Clean lattice tetrahedra, arXiv:math/0606227v1 [math.CO] (2006)

[22] C. Torezzan et al., Optimum commutative group codes, Des. Codes Cryptogr. **74** (2015), no. 2, 379–394. MR3302663

David Handelman
University of Ottawa, Mathematics Department
Ottawa ON K1N 6N5, Canada
E-mail: `dehsg@uottawa.ca`