Invariants for critical dimension groups and permutation-Hermite equivalence

Abstract Motivated by classification, up to order isomorphism, of some 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.

David Handelman

Outline
Motivated by classification of particular families of dense subgroups of \( \mathbb{R}^n \) as partially ordered \((\text{simple dimension})\) groups, we find two directed sets of invariants (in the form of finite sets of abelian groups, with some maps between them) for an equivalence relation on integer matrices that turns up occasionally in the study of lattice polytopes and commutative codes, among other places. Although the development 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. Then we say \( B \) is permutation-Hermite equivalent \((\text{or PHermite-equivalent, or PH-equivalent})\) to \( B' \) if there exist \( U \in \text{GL}(m, \mathbb{Z}) \) 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 \((\text{a fixed copy of})\) \( \mathbb{Z}^{1 \times n} \) as partially ordered subgroups of \( \mathbb{Z}^n \) (with the inherited ordering)—the row space of \( B, r(B) \), is the subgroup, and the order automorphisms of \( \mathbb{Z}^{1 \times n} \) are implemented by the permutation matrices (acting on the right). With this in mind, we can even define an equivalence relation on matrices \( B \in \mathbb{Z}^{m \times n} \) and \( B' \in \mathbb{Z}^{m' \times n} \), if we allow the additional operation of deleting a row of zeros any time it appears in the course of row reduction.

For an important subclass of matrices (suggested by the dimension group problem), we construct two families of invariants that are surprisingly effective. For example, the Smith normal form is an invariant, but a relatively crude one; but these 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 \( C := \begin{pmatrix} 1^{n-1} & a \\ 0 & d \end{pmatrix} \)—that is, an identity matrix of size \( n - 1 \), a column \( a \), and \( d = |\det B| \) (for example, if the elementary divisors of the matrix are square-free, then the Smith normal form is of this type; but the matrix need not be PH-equivalent to a matrix of the form of \( C \)). The latter forms are particularly amenable to complete classification for PH-equivalence. We also construct numerous examples with the expected weird properties.

The motivation came from classification of dense subgroups, \( G \), of \( \mathbb{R}^n \) that are free of rank \( n + 1 \), viewed as a partially ordered abelian group, the ordering obtained by restricting the strict ordering on \( \mathbb{R}^n \) to \( G \) (that is, nonzero \( g \in G \) is in the positive cone, \( G^+ \) iff each coordinate is a (strictly) positive real number); this defines (together with the embedding into \( \mathbb{R}^n \), which we often suppress in notation) a critical 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, \( G \to \text{Aff} S(G, u) \), for some order unit \( u \) will yield the desired dense embedding in \( \mathbb{R}^n \cong \text{Aff} S(G, u) \); different order units yield isomorphisms among the images).

\(^1\)Supported in part by a Discovery grant from NSERC.
Let $e_i$ denote the standard basis elements of $\mathbb{R}^n = \mathbb{R}^{1 \times n}$. A standard construction of a critical group, known as a basic critical group is the group $G = \langle e_1, e_2, \ldots, e_n; \sum \alpha_i e_i \rangle$ where $\alpha_i$ are real numbers such that that $\{1, \alpha_1, \ldots, \alpha_n\}$ is linearly independent over the rationals (this is equivalent to density of $G$ in $\mathbb{R}^n$). Basic critical groups are a useful source of examples, as in [BeH]. 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 $\Omega \subset \partial_c S(G, u)$ such that $|\Omega| = n - 1$ (that is, $\Omega$ misses exactly one of them), define $\ker \Omega = \cap_{r \in \Omega} r$. For any critical dimension group, the rank of $\ker \Omega$ will either be one or zero. We can thus write the kernel as $x_\Omega \mathbb{Z}$ where $x_\Omega$ is unique with respect to $\sigma(x_\Omega) \geq 0$ where $\sigma$ is the pure trace not in $\Omega$. Now form $E(G) := \sum_{\Omega} x_\Omega \mathbb{Z} \subset G$. Then $G$ is basic iff $G/E(G) \cong \mathbb{Z}$; when this occurs, all sets of pure traces are ugly (in the sense of [BeH]).

However, the converse of the latter statement is not correct, but yields 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) $G = \langle f_1, f_2, \ldots, f_n; (\alpha_1, \ldots, \alpha_n) \rangle \subset \mathbb{R}^n$ where the $f_i \in \mathbb{Z}^n$ ($\{f_1, \ldots, f_n\}$ is real linearly independent and $\{1, \alpha_1, \ldots, \alpha_n\}$ is rationally linearly independent: these are necessary and sufficient for $G$ to be dense in $\mathbb{R}^n$. Then $G$ is almost basic iff 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 $\Omega \subset \partial_c S(G, u)$ (this time, we allow arbitrary subsets, not 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—can only be pre-ordered, and does not inherit many properties from the original).

When the set $\Omega$ 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 $\mathbb{R}^{\Omega}$. 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).

Of course, we give a direct proof (avoiding dimension groups) that the resulting family of abelian groups and maps between them (the torsion parts of $G_\Omega/E(G_\Omega)$) as $\Omega$ varies over the direct set consisting of the subset of a finite set) is a PH-invariant.

The quotient maps are obtained by removing columns (those not in $\Omega$), and recalculating the invariant (or the torsion part) without using the irrational row. This turns out to be surprisingly easy, and also leads to a second family of PH-invariants (also indexed by subsets of $\{1, 2, \ldots, n\}$), corresponding to a dual operation.

A list of objects is an unordered tuple (equivalently, a set with multiplicities recorded). To distinguish between sets, ordered tuples, and lists, we use the notation $(a_1, a_2, a_3)$ for lists (I couldn’t find any notation in the literature for this).

**Introduction**

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

Now suppose we let $G$ inherit the usual topology from $\mathbb{R}^n$, and assume that the image of $G$
is dense. Suppose $G'$ is another group with the same properties (free of the same rank, a dense subgroup of $\mathbb{R}^n$, etc), and we want to decide whether $G$ and $G'$ are isomorphic as topological subgroups of $\mathbb{R}^n$. Any such isomorphism, by definition, must extend to a continuous, hence vector space, automorphism of $\mathbb{R}^n$, and these are given by the right action of $\text{GL}(n, \mathbb{R})$. Thus the classification of (dense) $G \subset \mathbb{R}^n$ up to topological isomorphism is given by orbits of $\text{GL}(m, \mathbb{Z}) \times \text{GL}(n, \mathbb{Z})$ acting on a subset of $\mathbb{R}^{m \times n}$ (corresponding to those matrices whose row space is dense in $\mathbb{R}^n$) in the obvious manner.

Finally, suppose we also impose the strict ordering on $\mathbb{R}^n$, making it into a simple dimension group, and by restriction, give a dense subgroup $G$ the structure of a partially ordered abelian group. By [EHS], it is also a simple dimension group, and every simple dimension group with no infinitesimals and exactly $n$ pure traces arises in this manner. Now we wish to determine the order-isomorphism class of such simple dimension groups. Every order-isomorphism $G \to G'$ (both embedded in $\mathbb{R}^n$ as dense subgroups and with the inherited strict ordering) will extend to an order-automorphism of $\mathbb{R}^n$ [H]. The order-automorphisms of the latter are given exactly by the weighted permutation matrices all of whose nonzero entries are positive: that is, they factor as $\Delta P$ where $\Delta$ is a positive diagonal matrix and $P$ is a permutation matrix. Let $P(n, \mathbb{R})^+$ denote the group of such weighted permutation matrices. Here the classification of $G$ (now viewed as simple dimension groups with ordering inherited from $\mathbb{R}^n$) is given by the orbits of $\text{GL}(m, \mathbb{Z}) \times P(n, \mathbb{R})^+$ on the subset of $\mathbb{R}^{m \times n}$ consisting of the matrices whose row space is dense.

We are specifically interested in the partially ordered case, with $m = n + 1$; that is $G$ is free of rank $n + 1$, and the embedding into $\mathbb{R}^n$ which determines the ordering and also the topology (the ordering determines the topology in any case) has dense image; these are called critical (dimension) groups.

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

The analogue of the third relation arises when we view the fixed $\mathbb{Z}^n$ as a partially ordered group, with the coordinatewise ordering, called simplicial. Subgroups inherit the partial ordering (but are 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 $\mathbb{Z}^n$. These are given precisely by permutation matrices. We arrive at an equivalence relation that frequently turns up (e.g., [R, R2, ALTPP, TSCS]), but has no name. So we give it one, at least restricted to square matrices.

Two matrices $B$ and $B'$ in $M_m \mathbb{Z}$ are PHermite-equivalent (or PH-equivalent for short) if there exist $U \in \text{GL}(n, \mathbb{Z})$ and a permutation matrix $P$ such that $UB = B'P$. (We could of course stick the $P$ to the right of $B$, but it is more convenient as given.)

We will see that for a large class of critical groups, the classification problem includes within it a PH-equivalence class question. We will develop invariants for PH-equivalence on a subclass of $M_n \mathbb{Z}$ (appropriate for critical groups), much finer than the usual elementary divisors. We also obtain (natural) density results for matrices that have a particularly tractible equivalent form; it turns out that for $n \geq 6$, more than 80% have this property, converging to $\zeta(2)\zeta(3)/\zeta(6) \cdot \zeta(2)\zeta(3)\zeta(4) \cdots \sim .845$ as $n \to \infty$.

Critical (simple dimension) groups have been a source of interesting examples in dimension groups, e.g., [EHS], [H], and particularly in [BeH], concerning properties of traces (good, ugly,
bad). The can be used to characterize classes of critical dimension groups.

Let \( G \) be an abelian group, free of rank \( n + 1 \), which is embedded as a dense subgroup of \( \mathbb{R}^n \). This embedding imposes both a topology (the relative one, inherited from \( \mathbb{R}^n \)), and a partial ordering, inherited from the strict ordering on \( \mathbb{R}^n \) (thus an element \( v \) in \( \mathbb{R}^n \) is in the positive cone if and only if \( v \) is zero, or if each of its components is strictly positive). The latter ordering makes the group into a simple dimension group, whose pure traces are precisely the coordinate functions (from \( \mathbb{R}^n \)). In the latter case, the ordering induces a metric, which yields the same topology as the inherited one.

If \( G \) is a simple dimension group, free of rank \( n + 1 \), with exactly \( n \) pure traces, then we call it a \textit{critical} (dimension group). These are precisely the partially ordered groups described in the previous paragraph, via any affine representation. If we view \( G \) merely as a topological group (free of rank \( n + 1 \), embedded as a dense subgroup of \( \mathbb{R}^n \)), with topology inherited from \( \mathbb{R}^n \), we call it \textit{topologically critical}.

In the case that \( n = 1 \), critical subgroups of \( \mathbb{R} \) are of the form \( \mathbb{Z} + r \mathbb{Z} \subset \mathbb{R} \), up to order isomorphism, and is well known that \( \mathbb{Z} + r \mathbb{Z} \cong \mathbb{Z} + r' \mathbb{Z} \) as either topological groups or ordered groups if and only if \( r \) is in the \( \text{PSL}(2, \mathbb{Z}) \)-orbit of \( r' \), the group acting by fractional linear transformations \([ES]\). However, the situation when \( n \geq 2 \) is much more complicated.

A special class of critical dimension groups, called \textit{basic} in \([\text{BeH}]\), is relatively easy to classify. Let \( \{e_i\} \) be the standard basis of \( \mathbb{Z}^n \subset \mathbb{R}^n \), and let \( \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n \) be such that the set \( \{1, \alpha_1, \ldots, \alpha_n\} \) is linearly independent over the rationals. Set \( G \) to be the subgroup of \( \mathbb{R}^n \) generated by \( \{e_i\}_{i=1}^n \cup \{\sum \alpha_i e_i\} \). This is automatically dense in \( \mathbb{R}^n \), and as an ordered group is critical. We call a critical group \textit{basic} if it is order-isomorphic to \( G \) for some choice of \( \alpha \) (the rational linear independence is necessary and sufficient for \( G \) to be dense).

All critical groups of rank two (that is, \( n = 1 \)) are automatically basic, but this fails drastically when \( n > 1 \), as we will see. However, if we fix \( n \), and consider classification of basic critical groups of rank \( n + 1 \), then the role of \( \text{PSL}(2, \mathbb{Z}) \) is performed by the much more elementary group, the semidirect product \( \mathbb{Z}^n \rtimes_{\Theta} (S_n \times \{\pm 1\}) \) (with obvious actions of the symmetric group and \( \pm 1 \)).

Basic critical groups are easily characterized in terms of ugly sets of pure traces, with an extra condition. This suggests a potentially larger class of critical groups, characterized entirely in terms of ugly sets of pure traces. These are given by the following construction. Let \( A \) be a rank \( n \) subgroup of \( \mathbb{Z}^n \), and let \( G \) be the subgroup of \( \mathbb{R}^n \) generated by \( A \) and \( \alpha \) (same \( \alpha \) as above); this will automatically be critical, and we call a critical \textit{almost basic} if it is order isomorphic to such a choice of \( A \) and \( \alpha \).

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 a reasonably well known equivalence relation on \( n \times n \) matrices, intermediate to Hermite and Smith. This has appeared before, e.g., in classification of lattice simplices \([R, \text{ALTPP}]\), and very recently in dealing with commutative codes \([\text{TSCS}]\). This equivalence relation has no name, so we give it one. Let \( B \) and \( B' \) be \( n \times n \) integer matrices; they are \textit{PHermite-equivalent} (or \textit{PH-equivalent} for short) if there exist \( U \in \text{GL}(n, \mathbb{Z}) \) and a permutation matrix \( P \) such that \( B' = UBP \).

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 three appendices. The first 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 4. The second 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. for size three matrices. The third appendix has exact formulas for PH-equivalence classes, with special attention to those with 1-block size \(n - 1\), when \(n = 3\).

A subset \(\{g_i\}\) of a torsion-free abelian group \(A\) is rationally linearly independent (or linearly independent over \(Q\)) if whenever \(\{n(i)\}\) is a collection of integers with \(n(i) = 0\) for all but finitely many \(i\), then \(\sum n(i)g_i = 0\) implies \(n(i) = 0\) for all \(i\). This is equivalent to the usual linear independence over the rationals of the set \(\{g_i\}\) as a subset of the divisible hull of \(A\), that is, \(A \otimes \mathbb{Z} Q\), a vector space over the rationals.

Statement of results

Section 1 contains the definition of the first form of the invariant its dual, together with their elementary properties. The second section contains sufficient conditions for a matrix \(B \in M_n \mathbb{Z}\) to be PH-equivalent to a form in which the 1-block size is \(n - 1\), and describes the (pseudo-)action of the permutation group \(S_{n+1}\) on these forms. Section 3 introduces two families of invariants (of which the initial ones are the biggest), and gives examples to show how fine these are; there are also more results on PH-equivalence to a matrix with 1-block size \(n - 1\).

Section 4 gives a density result for matrices with this last property, at least .8 for \(n \geq 6\) and converging up to \(\zeta(2) \zeta(3) / \zeta(6) \zeta(2) \zeta(3) \cdots \sim .845\) as \(n \to \infty\).

Sections 5–8 deal with critical groups, that is dense subgroups of \(\mathbb{R}^n\) that are free of rank \(n + 1\), equipped (except in section 5) with the strict ordering, making them into simple dimension groups. Section 5 contains a topological classification theorem, which for \(n \geq 3\) corresponds to the classification of a totally ordered subgroup of \(\mathbb{R}\). Basic critical dimension groups \([\text{BeH}]\) are characterized in section 6, within the class of critical dimension groups, by means of the invariant which lead to the development in section 1–4.

Almost basic critical dimension groups are introduced in section 7, and the principal result is that the classification of these reduces to PH-equivalence of integer matrices associated to them. When \(n = 1\), this is partly given by the action of \(\text{PSL}(2, \mathbb{Z})\); however, when \(n \geq 2\), the corresponding group is much smaller, a semi-direct product of \(S_n \times \{\pm 1\}\) acting on \(\mathbb{Z}^{n+1}\). Section 8 is a result on almost critical basic dimension groups that amounts to showing that the whole family of PH-invariants yields their counterparts for these dimension groups.

Appendix A (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 4. Appendix B suggests an asymptotic formula for the number of PH-equivalence classes of fixed determinant and size, and proves it when the determinant is square-free. Appendix C 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; first invariants
2 PH-equivalence for some terminal forms
3 A better way of proceeding: two families of invariants
4 Densities for PH-equivalence to 1-block size \(n - 1\)
5 Topological isomorphism for topologically critical groups
6 Basic critical dimension groups
7 Isomorphisms between almost critical groups
8 Unperforation of quotients
Appendix A A truncated reciprocal formula (joint with D Roy)
Appendix B Counting PH-equivalence classes
Appendix C Counting PH-equivalence classes in size 3

5
1 Permutation-Hermite equivalence; first invariants

Let $B$ and $C$ be $n \times n$ integer matrices ($B, C \in \mathbb{M}_n\mathbb{Z}$). We consider two very well known, and a lesser-known, equivalence relation possible between $B$ and $C$.

The matrices $B$ and $C$ are Hermite equivalent if there exists $U$ in $\text{GL}(n, \mathbb{Z})$ 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 $\mathbb{Z}$-elementary row operations (that is, permutations, multiplication of a row by $-1$, and adding a row to another). Normal forms have been well-studied.

Matrices $B$ and $C$ are Smith equivalent if there exist $U$ and $V$ in $\text{GL}(n, \mathbb{Z})$ 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 PH-hermite equivalent or PH-equivalent) if there exists $U$ in $\text{GL}(n, \mathbb{Z})$ and a permutation matrix $P$ such that $B = UCP$ In order words, $B$ and $C$ are obtainable from each other by $\mathbb{Z}$-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 $\mathbb{Z}^n$ 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 its row space, viewed as a subgroup of $\mathbb{Z}^n$. Left multiplication by elements of $\text{GL}(n, \mathbb{Z})$ has no effect on the row space—only the generating set for $r(B)$ is changed—and column permutations implement the order-automorphisms of $\mathbb{Z}^{1\times n}$ when the latter is given the usual coordinatewise partial ordering. It is helpful permit the matrices $B$ to be $m \times n$ with $m \geq n$; then elementary row operations are now implemented by elements of $\text{GL}(m, \mathbb{Z})$. These do not change the row space, and it useful to add another permitted operation: if at some point during a sequence of row and permitted column operations, a row becomes identically zero, then we delete it (and thus reduce the size). This obviously has no effect the row space, and will be useful in the development of our invariants.

While PH-equivalence is the same as classification of subgroups of $\mathbb{Z}^n$ up to order-automorphisms of the latter, it leaves open the question as to whether it is simply the classification of subgroups of $\mathbb{Z}^n$ as partially ordered abelian groups (with ordering inherited from the simplicial ordering). In other words, if $H, H' \subset \mathbb{Z}^n$ are subgroups of the same copy of $\mathbb{Z}^n$, and there is a group isomorphism $\phi : H \rightarrow H'$ that is an order isomorphism ($H$ and $H'$ having the partial orderings inherited from the inclusions in $\mathbb{Z}^n$), then $\phi$ can be extended to a order-automorphism of $\mathbb{Z}^n$, that is, a permutation.

Reduced forms for PH-equivalence have been obtained, but normal forms have not, as far as I could 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 $\text{cont}(v) = c$, if $c$ is the greatest common divisor of the nonzero entries (and if all the entries are zero, then $\text{cont}(v) = 0$). We say $v$ is unimodular (not to be confused with unimodal) if $\text{cont}(v) = 1$.

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

(a) rank $B = n$

(b) every column of $B$ is unimodular.

Observe that if $C$ is any element of $\mathbb{M}_n\mathbb{Z}$ with full rank, then there is a factorization $C = B\Delta$ where $B$ is weakly nonsingular and $\Delta$ is diagonal with positive integer entries thereon.

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

Given \( B \in NS \), 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 \( U_1 \in \text{GL}(n, \mathbb{Z}) \) such that the first column of \( U_1B \) 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 diagonal 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

\[
\begin{pmatrix}
I_s & Y \\
0 & D
\end{pmatrix},
\]

where \( D \) is an upper triangular matrix of size \( n - s \), whose diagonal entries all exceed one. If, in \( D \), 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 can be improved. We obtain a PHermite-reduced form from the following result of [TSCS], for convenience stated here only for full rank matrices.

**THEOREM 1.1** [TSCS, Theorem 4.1] Let \( B \in \text{M}_{n, \mathbb{Z}} \) be of full rank. Then there exists a PHermite-equivalent upper triangular matrix \( C \in \text{M}_{n, \mathbb{Z}^+} \), such that

(a) \( 0 < C_{ii} \leq C_{i+1,i+1} \) for all \( 1 \leq i < n \);
(b) \( 0 \leq C_{i,j} < C_{jj} \) for all \( i < j \);
(c) \( C_{ii} \leq \gcd \{ C_{sj} | i \leq s \leq j \} \) for all \( i < j \).

We say \( C \) is **PH-terminal** if it is in the form described in the theorem. **Terminal** comes from the feeling 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 \( B \in NS_n \), then it has at 1-block size at least one.

This is described in the reference as a normal form, but this is not the usual use of normal form, as two distinct matrices \( C \) and \( C' \) each satisfying the conditions can be PHermite-equivalent. As a trivial example from \( NS \), 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 \( \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus (1) \), 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 \( NS \) matrix, the terminal form has an identity block of some size in the upper left corner. If two terminal forms are PHermite-equivalent, it would be nice if the size of the
identity blocks were the same. The answer is no, and we will see that this phenomenon occurs fairly frequently, almost generically (Proposition 2.3). 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 \(C'\) 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 \(U \in \text{GL}(3, \mathbb{Z})\). So \(C\) and \(C'\) are PH-equivalent but with different block sizes for 1 (this turns out to be very common). We will look at this example and some relatives after we discuss our first invariant. First, we give a simple example to distinguish the three equivalence relations. Barely any calculation is required.

For each \(i = 1, 2, 3, 4\), set

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

Then

(i) Each \(B_i\) is in \(\mathcal{NS}\) and is in terminal form.

(ii) Every \(2 \times 2\) matrix with invariant factors \(\{1, 5\}\) is Hermite equivalent to one of \(B_i\)

(iii) all four are mutually Hermite-inequivalent.

(iv) \(B_2\) and \(B_3\) are PHermite equivalent, but there are no other PH-equivalences among these matrices.

(v) all four are mutually Smith equivalent, that is, their set of invariant factors is \(\{1, 5\}\).

Now we introduce the first group in our PH-invariant. 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 with the following properties:

(a) \(x_i = m(i)E_i\) where \(E_i\) is the \(i\)th standard basis element of \(\mathbb{Z}^{1 \times n}\) and \(m(i)\) is a positive integer

(b) \(x_i \in \sum f_j \mathbb{Z}\)

(c) whenever \(y \in \sum f_j \mathbb{Z}\) and \(y = kE_i\) for some \(k \in \mathbb{Z}\), then \(m(i) \divides |k|\).

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

Now form \(X(B) = \sum x_i \mathbb{Z} = \oplus x_i \mathbb{Z}\). 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 \(U \in \text{GL}(n, \mathbb{Z})\) and \(P\) is a permutation matrix. The row space of \(B\) is unaffected by the left action of \(\text{GL}(n, \mathbb{Z})\), and the list \(\{x_i\}\) is similarly unaffected by permutation of the columns.

It would be useless if we couldn’t compute with it, but it turns out to be rather easy to deal with.

Unless inconvenient, we write \(\mathbb{Z}_k\) (for \(k\) a positive integer) in place of \(\mathbb{Z}/k\mathbb{Z}\).

**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:

\[
B = \begin{pmatrix}
1 & 0 & 0 & \ldots & 0 & a_1 \\
0 & 1 & 0 & \ldots & 0 & a_2 \\
0 & 0 & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & 1 & a_{n-1} \\
0 & 0 & 0 & \ldots & 0 & d
\end{pmatrix}
\]

\[
B' = \begin{pmatrix}
1 & z_2 & z_3 & \ldots & z_{n-1} & z_n \\
0 & d_2 & 0 & \ldots & 0 & 0 \\
0 & 0 & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & d_{n-1} & 0 \\
0 & 0 & 0 & \ldots & 0 & d_n
\end{pmatrix}
\]
Then both $B$ and $B'$ are $N\Sigma$ matrices in terminal form. Moreover,

$$I(B) \cong \bigoplus_{i} \left( \mathbb{Z}/\left( \frac{d}{\gcd \{d,a_i\}} \right) \right),$$

and $I(B')$ is cyclic of order $\text{lcm} \{d_2,d_3,\ldots,d_n\}$.

**Remark.** That’s a big direct sum symbol—and a big solidus, too.

**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 $I(B) \cong \bigoplus_{i} \left( \mathbb{Z}/\left( \frac{d}{\gcd \{d,a_i\}} \right) \right)$.

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

$$E_1 = f_1 - \sum_{i\geq 2} \frac{z_i}{d_i} f_i$$

$$lE_1 = lf_1 - \sum_{i\geq 2} z_if_i$$

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 $\sum f_j\mathbb{Z}$, so that $x_1 = lE_1$. For $i > 2$, $x_i = f_i$. Hence a basis for $\sum_{i=1}^{n} x_i\mathbb{Z}$ 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 $d'$ 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 either $a = a'$ or $aa' \equiv 1 \mod d$ (that is, in $\mathbb{Z}/d\mathbb{Z}$, $[a] = [d]^{-1}$). The second choice comes from letting $P$ be the nontrivial permutation matrix, and working out the details. Here $I(B_{a,d}) \cong \mathbb{Z}/d\mathbb{Z}$, not very exciting.

Next, consider variations on the earlier example. Set

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

We have, by the earlier result, \( I(B) = (\mathbb{Z}/(6/\gcd\{6, b\})\mathbb{Z}) \oplus (\mathbb{Z}/(6/\gcd\{6, c\})\mathbb{Z}) \). Hence if at least one of \( b \) or \( c \) is relatively prime to 6, then \( I(B) \) is not cyclic, and has \( \mathbb{Z}/6\mathbb{Z} \) as a proper quotient.

Now \( I(C_i) \cong \mathbb{Z}_6 \) since 6 = 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 \( B = \begin{pmatrix} 1_r & X_D \\ 0 & D \end{pmatrix} \) be in terminal form with \( D \) upper triangular, and whose diagonal entries satisfy \( 1 < d_{r+1} \leq d_{r+2} \leq d_n \). Set \( l = \text{lcm} \{d_i\} \).

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

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

\[
(\mathbb{Z}/l\mathbb{Z})^r \oplus \left( \bigoplus_{j=r+1}^{n-1} \mathbb{Z}/\text{lcm} \{d_{j+1}, d_{j+2}, \ldots, d_n\} \mathbb{Z} \right).
\]

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

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

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

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 \( B = \begin{pmatrix} 1_r & X_D \\ 0 & D \end{pmatrix} \) is in terminal form, and let \( d = \det B \). If \( I(B) \) has a quotient which is isomorphic to \( (\mathbb{Z}_d)^s \), then all terminal forms PH-equivalent to \( B \) must have 1-block size at least \( s \).

**Proof.** Suppose \( B' = \begin{pmatrix} 1_r & X_D' \\ 0 & D' \end{pmatrix} \) is a PH-equivalent terminal form with \( r < s \). In particular, \( \det B' = \det B = d \). All the factors that are quotients of \( \mathbb{Z}/\text{lcm} \{d'_j, \ldots, d'_n\} \) 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 \( (\mathbb{Z}_d)^r \) appearing as a factor, a contradiction.

**COROLLARY 1.5** Suppose \( B = \begin{pmatrix} 1_{n-1} & X_d \\ 0 & d \end{pmatrix} \) is in terminal form, and suppose each entry of the column \( X = (z_i)^T \) \( (1 \leq i \leq n - 1) \) satisfies \( \gcd(z_i, d) = 1 \). Then all terminal forms PH-equivalent to \( B \) have 1-block of size \( n - 1 \).

**Proof.** By Lemma 1.1, \( I(B) \cong (\mathbb{Z}_d)^{n-1} \), so the result follows from the preceding corollary.
Lemma 1.6 Let \( B \in \mathcal{NS} \), and suppose it has a terminal form with non-unital diagonal entries \( d_{r+1}, d_{r+2}, \ldots, d_n \). Then the exponent of \( I(B) \) divides \( \text{lcm}\{d_i\} \).

Proof. As in the previous arguments, \( x_i = m(i)E_i \), where \( m(i) \) divides \( \text{lcm}\{d_j\} \), and in particular, the coefficient of \( f_i \) in \( x_i \) divides \( m(i) \); but the least common multiple of these coefficients is exactly the exponent of \( I(B) \).

Lemma 1.7 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 \( m \geq 1 \). Then

(a) the exponent of \( I(B) \) is \( p^m \).

(b) 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. (a) Since the content of the last column is one, at least one entry must be relatively prime to \( p \), hence to \( p^n \). By Lemma 1.2, at least one of the direct summands in \( I(B) \) is \( \mathbb{Z}/p^n\mathbb{Z} \); hence the exponent is divisible by \( p^m \). By the preceding, \( p^m \) divides the exponent.

(b) If \( B \) is PH-equivalent to \( B' \) in terminal form with block size less than \( n - 1 \), then the non-one diagonal entries of the latter are powers of \( p \), and their product is the determinant, \( p^m \). Their lcm is thus strictly less than \( p^m \), and so the exponent of \( I(B') \neq p^m \), a contradiction.

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

It is convenient to introduce the notion of opposite here, in order to put the invariant(s) in a broader context.

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 \( I(B) = \mathbb{Z}^{1\times n}/\mathbb{Z}^{1\times n} B^{op} \), so that the elementary divisors of \( B^{op} \) yield \( I(B) \). To see this, we have a unique representation for each \( i \), \( x_i = \sum_j c_{ij} f_j \) with \( c_{ij} \in \mathbb{Z} \); since \( x_i \) is not a nontrivial multiple of any element of \( \sum f_j \mathbb{Z} \), it follows that the content of \( \{c_{ij}\}_{j=1}^n \) is one. 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 \( CT \) on the right by an element of \( \text{GL}(n, \mathbb{Z}) \), hence multiplies its transpose, \( C \), on the left by an element of \( \text{GL}(n, \mathbb{Z}) \). A column permutation applied to \( B \) multiplies the representation of the \( x_i \) by a row permutation of the matrix \( CT \), so induces a column permutation of \( C \).

So we can call \( C, B^{op} \), although it is really the PH-equivalence class of \( B^{op} \) that is of interest. In some cases (e.g., in some situations where the 1-block is of size \( n - 1 \), \( B^{op} \) turns out to be the transpose of the adjoint matrix of \( B \). 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 \( I(B) = \mathbb{Z}^n / r(B^{op}) \). 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, \( I(B^{op}) \) is determined solely from the elementary divisors of \( B \), and \( (B^{op})^{op} \) is PH-equivalent to \( B \). In general, \( |\det B| \neq |\det B^{op}| \); this occurs when \( |\det B| \neq |I(B)| \), and we have seen an example for which \( \det B = 8 \), but \( I(B) \cong \mathbb{Z}_8 \oplus \mathbb{Z}_2 \).
In [ALTPP], the authors 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 \( I^* \), and is \( |\det B^{\text{op}}| \); they also use \( B^* \), the dual matrix emanating from lattice polytopes, for what is called here \( B^{\text{op}} \). Among other things, they constructed very useful tables of numbers of isomorphism classes, and explicit generators, which turned out to be particularly useful for Appendix C.

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,

\[
0 \rightarrow r(B) \rightarrow \mathbb{Z}^{1 \times n} \rightarrow \mathbb{Z}^{1 \times n} / r(B) \rightarrow 0.
\]

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

\[
0 \rightarrow I(B) \rightarrow \oplus \mathbb{Z}_{m(i)} \rightarrow I(B^{\text{op}}) \rightarrow 0.
\]

**LEMMA 1.8** The following hold.

(a) \( |I(B)| \cdot |I(B^{\text{op}})| = \prod m(i) = |\det B^{\text{op}}| \cdot |\det B| \).

(b) The sets of prime divisors of each of \( |\det B|, |\det B^{\text{op}}|, |I(B)|, |I(B^{\text{op}})| \), and \( \prod m(i) \) are identical.

**Proof.** (a) is immediate from the short exact sequences and the identifications. (b) We may assume \( B \) is in terminal form, \( B = \begin{pmatrix} 1_k & X \\ 0 & D \end{pmatrix} \) where \( k \geq 1 \) and \( D \) is upper triangular, with diagonal entries \( d_{k+1}, \ldots, d_n > 1 \).

\[
E_i = \begin{cases} f_i - \frac{x_i}{d_{i+1}} - \sum_{l>0} \frac{s}{d_{k+l}} f_{k+l} & \text{if } 1 \leq i \leq k \\ f_i - \sum_{l>0} \frac{s}{d_{j+l}} f_j & \text{if } k+1 \leq i \leq n-1 \\ f_i & \text{if } i = n. \end{cases}
\]

For \( i \leq k \), the first line says that \( m(i) \) divides \( \text{lcm} \{ d_i \} \); for \( i > k \), we see that \( m(i) \) divides the least common multiple of a subset of \( \{ d_i \} \). In particular, if \( q \) is a prime dividing and of the \( m(i) \), then \( q \) divides \( |\det B| = \prod d_i \).

On the other hand, suppose \( q \) is a prime dividing one of the \( d_i \), and suppose that \( i \) is the smallest index with this property. At least one of the entries of the \( i \)th column must be relatively prime to \( q \) (since all columns have content 1), say the \( u \)th. If \( u > k \), then we have the relation \( E_u = f_u/d_u - \cdots - a_u f_i/d_i - \sum_{j>i} f_j/d_j \). The \( i \)th coordinate of \( E_u \) is zero since the only one of \( \{ u, u+1, \ldots, i \} \) for which \( q \) divides \( d_k \) is \( i \), and \( f_j \) contributes zero to the \( i \)th coordinate if \( j > i \), it follows that \( q \) divides \( m(u) \). If \( u \leq k \), the argument is the same, but we have \( E_u = f_u - \cdots \). In particular, \( q \) dividing \( \prod d_i = |\det B| \) implies \( q \) divides \( \prod m(i) \). But we have a bit more from this argument—\( q \) must also divide the determinant of \( B^{\text{op}} \), since the leading term of \( x_i \) is of the form \( af_i \), where \( q \) divides \( a \).

Thus far, we have that the numbers \( |\det B| \) and \( \prod m(i) \) have the same sets of prime divisors, and any prime dividing \( |\det B| \) divides \( |\det B^{\text{op}}| \). Interchanging \( B \) with \( B^{\text{op}} \) (which we cannot do

---

1 Unfortunately I came across this reference after I had established the notation for this paper, so that their \( I \) is \( |I(B^{\text{op}})| \), and their \( I^* \) is \( |I(B)| \).
via the \( m(i) \), since we have not shown that the opposite counterpart to \( \prod m(i) \) is the same, the prime divisors of \( |\det B| \) and \( |\det B^{op}| \) are the same. Now \( |\det B^{op}| = |I(B)| \) and \( |\det B| = |I(B^{op})| \) allows us to conclude.

**Remark.** The condition that the order be of prime power (in addition to being cyclic) is essential.

**COROLLARY 1.9** Suppose that \( B \in NS_n \) and \( I(B) \) is cyclic of prime power order, \( q^a \). Then

\[
\begin{pmatrix}
1 & \cdots & c(n) \\
1 & \cdots & q^{t(k+1)} \\
& \cdots & \\
& & q^{t(n)}
\end{pmatrix}
\]

is PH-equivalent to

\[
\begin{pmatrix}
1_{n-1} & C \\
0 & q^a
\end{pmatrix},
\]

where \( C = (a_1, a_2, \ldots, a_{n-1})^T \) where \( k = 1 + |\{i \mid a_i \equiv 0 \mod q\}| \).

**Proof.** Say \( I(B) \cong \mathbb{Z}_{q^a} \) for some prime \( a \) and prime \( q \). We work with \( B^{op} \), abbreviated \( B' \). Then \( \mathbb{Z}^{1 \times n}_{/r(B')} \cong I(B) \cong \mathbb{Z}_{q^a} \). Obviously \( \det B' = q^a \), so that when any terminal form for \( B \) can have only powers of \( q \) along the diagonal. Let \( B'' \) be a terminal form for \( B' \); then

\[
B'' = \begin{pmatrix}
1_k & X \\
0 & D
\end{pmatrix}
\]

where \( D = \begin{pmatrix}
q^{a(k+1)} & * \\
\vdots & \ddots \\
qu^{a(n)} & \end{pmatrix} \)

with \( 1 \leq a(k+1) \leq \cdots \leq a(n) \) and all the strictly upper triangular entries of \( D \) are either zero or divisible by a power of \( p \), but that power is less than the power appearing in the diagonal entry for that column. Obviously, we may assume that \( k < n - 1 \).

For any cyclic abelian group of prime power order, any pair of subgroups is comparable (that is, one of them is a subgroup of the other). Let \( G_i \) be the subgroup of \( \mathbb{Z}^{1 \times n}_{/r(B'')} \) generated by \( E_i \). Then either \( G_{n-1} \subset G_n \) or vice versa. Thus we have either

\[
E_n = \sum_{j=1}^{n} f_j c_j + \lambda E_{n-1} \quad \text{or}
\]

\[
E_{n-1} = \sum_{j=1}^{n} f_j c_j + \lambda E_n,
\]

where \( c(j), \lambda \in \mathbb{Z} \). Examining the first \( k \) coordinates, we immediately see that in either case, \( c_j = 0 \) for all \( 1 \leq j \leq k \). In the first case, the \( n \)th coordinate yields \( 1 = \sum_{j > k} (f_j, E_n)c_j \) (where \( (, ) \) denotes the usual inner product, that is, it is the \( n \)th coordinate of \( f_j \)). However, all the entries in
the final column of $D$ are divisible by $q$ or zero, yielding a contradiction. In the second case, the same argument applies to the $n-1$st coordinate, again a contradiction. Hence $k = n-1$, so that the terminal form, $B''$, has 1-block size $n-1$.

Now $B$ is PH-equivalent to $B''$, and the latter has the form given in the statement, as is easy to check.

2 PH-equivalence for some terminal forms

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 $a = (a_i)^T$ is in $\mathbb{Z}^{(n-1)\times 1}$ 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 the others at any time in a sequence of PH-equivalences, we may regard the $a_i$ as elements of $\mathbb{Z}_d$.

We wish to describe PH-equivalence for this class of matrices. Since the absolute value of the determinant is a PH-invariant for matrices in $NS$, we may fix the determinant, which of course is $d$; 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 conjugation of $B$ with 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 $(\mathbb{Z}_d)^{(n-1)\times 1}$ (that is, the columns $a$) induced by PH-equivalence between the corresponding $B_a$ (with $d$ fixed of course) is more complicated than merely permuting.

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 $y = (a_i) \in A^{n-1}$; 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 $\pi$ 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 $y'$, the obvious thing. Otherwise, there exists $j < n$ such that $\pi(j) = n$, so that the last coordinate of $\pi(y')$ is $a_j$ and $\pi$ 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 $\mathbb{Z}$—this time viewed additively—this is the Weyl group action of $S_{n+1}$ on the dual of the maximal torus of $SU(n+1)$.)

Denote this action $\Pi_{A,n} : S_n \to \text{Aut } A^{n-1}$. Now replace $A$ by $\mathbb{Z}_d^\times$, the group of (multiplicatively) invertible elements in $\mathbb{Z}_d$ (so $\phi(d) = |\mathbb{Z}_d^\times|$). Suppose that $a \in (\mathbb{Z}_d)^{n-1}$ consists of elements relatively prime to $d$, that is, members of $\mathbb{Z}_d^\times$. Then we will see that the PH-equivalence class of $B_a$ consists of a slightly twisted $S_n$-orbit of $a$ under $\Pi_{S_n}$.

However, if some of the entries of $a$ are zero divisors in $\mathbb{Z}_d$, then the situation becomes pear-shaped. 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 $\mathbb{Z}_d$, 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 equivalence classes, but instead a union of actions of various groups.

When $n = 2$, $B_a$ is PH-equivalent to $B'_a$ iff $ad' \equiv 1 \mod d$; this is easy, and can be done directly, since we are dealing only with the transposition matrix. 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, just arrange them 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 looks like these should generate a larger orbit, but they don’t. (So if all $a_i = -1$, it is not equivalent to anything else.) The orbit consists of \{(−$a_1a_2^{-1}$, ..., $a_j^{-1}$, ..., −$a_{n-1}a_{n-1}^{-1}$)\}, together with $(a_i)$ itself, and all their permutations.

To verify these claims, suppose $UB_aP = B_{a'}$. First, we note that if also $U_1B_aP = B_{a''}$ (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 $M_nQ$, $P = B_{a'}^{-1}U_1^{-1}B_{a''} = B_{a'}^{-1}U^{-1}B_{a''}$, whence $U^{-1}B_{a'} = U_1^{-1}B_{a''}$, so that $U_1U^{-1}B_{a'} = U_{a''}$. Set $V = U_1U^{-1} \in \text{GL}(n, \mathbb{Z})$. From the form of the $B$s (first $n - 1$ columns are standard basis elements), $V = \begin{pmatrix} I_{n-1} & X \\ 0 & t \end{pmatrix}$; since the lower right entries of both $B$s are $a, t = 1$, 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 $0 \leq a''/a, a' < d$, this forces $a' = a''$.

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

Let $B$ and $B'$ be matrices in $NS_n$, both in terminal form. Suppose there exists a permutation matrix $P$ together with $U \in \text{GL}(n, \mathbb{Z})$ such that $UB = B'P$; then we say $P$ is realizable over $B$ (in other words, there exists $B'$ in terminal form, etc).

Suppose that $B = \begin{pmatrix} 1_{n-1} & 0 \\ 0 & d \end{pmatrix}$; its 1-block is size $n - 1$. Let $\pi$ 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 $PQ$ is also realizable, so that the realizable permutation matrices form a coset space over $S_{n-1}$. However, this is fairly complicated.

For $a \in \mathbb{Z}^{(n-1) \times 1}$ such that $\text{cont} \{a, d\} = 1$, recall that $B_a = \begin{pmatrix} 1_{n-1} & a \\ 0 & d \end{pmatrix}$. We will determine precisely the permutation matrices $P$ such that there exist $a' \in \mathbb{Z}^{(n-1) \times 1}$ such that $B_{a'} = UB_a$ for some $U \in \text{GL}(n, \mathbb{Z})$. 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.)

For an integer $d > 1$, $\mathbb{Z}_d^*$ will denote the group of multiplicatively invertible elements in the ring $\mathbb{Z}_d$ (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 $xy \equiv 1 \mod d$.

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

\[
a'_{t} \equiv \begin{cases} -a_{\pi(t)}a_{\pi(n)}^{-1} & \text{if } t \neq \pi^{-1}(n) \\
a_{\pi(n)}^{-1} & \text{if } t = \pi^{-1}(n). \end{cases}
\]
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 to choices for terminal $B'$ that have a smaller
1-block, we can obtain more realizable $P$.

Remark. For $n = 3$, this type of action of the symmetric group was discussed in [R].

Proof. First, suppose that $UB_a = B_{a'}P$ for some $U \in \text{GL}(n, \mathbb{Z})$, and $\pi(n) \neq n$. Then the $i$th
column of $UB_a$ is $Ue_i$, except when $i = n$, in which case, it is $U(e_i')$. On the other hand, the $i$th
column of $B_{a'}P$ is the $\pi^{-1}$th column of $B_{a'}$, which is $e_{\pi^{-1}}$, unless $\pi(i) = n$, in which case it is
$\begin{pmatrix} a' \\ d \end{pmatrix}$.

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 $\begin{pmatrix} a' \\ d \end{pmatrix}$; let $(h_j)^T$ be the $n$th column of $U$. The basic vectors represented in the columns exclude $e_n$ and $e_{\pi(n)}$; hence in the $\pi(n)$ and $n$th rows of $U$, there are at most two nonzero entries, $a'_{\pi(n)}$ and $h_{\pi(n)}$, & $d$ and $h_n$, respectively.

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

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

$$a'_{\pi^{-1}(n)}a_{\pi(n)} + h_{\pi(n)}d = 1.$$

The second equation says that $a_{\pi(n)}$ is invertible modulo $d$, and $a'_{\pi^{-1}(n)} \equiv a_{\pi(n)} \pmod d$. 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, we can almost reconstruct $U$ from the equations; the $a_i'$ are defined up to
multiples of $d$ (so we can perform additional elementary row operations if necessary to ensure that
$0 \leq a_i' < d$. There is only one additional condition; $|\det U| = 1$ iff $|\det \begin{pmatrix} a_{\pi(n)} & h_{\pi(n)} \\ d & h_n \end{pmatrix}| = 1$, that is,

$$a_{\pi(n)}h_n - h_{\pi(n)}d = \pm 1,$$

which is easily arranged (since $a_{\pi(n)}$ is invertible modulo $d$).

The case that $\pi(n) = n$ has already been discussed.

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 $a_i = a_j \in \mathbb{Z}_d$, on taking a permutation $\pi$ such that $\pi(n) = i$,
the corresponding $a_i'$, 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.

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

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

iff $d = d'$ and either of $a' \equiv a \pm 1 \mod d$.

It also allows us to conclude that

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

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

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

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

Here is a more drastic family of examples, with minimal and maximal 1-blocks.

A useful PH-equivalence tool (found in [AALPT]) is that $C$ and $C'$ are PH-equivalent (via the permutation matrix $P$ or its inverse) iff $C'PC^{-1}$ has only integer entries. We use this frequently, without further comment.

**Proposition 2.2** Let $B = \begin{pmatrix} 1 & b \\ 0 & D \end{pmatrix}$ (below) be a terminal member of $\Lambda S_n$, and suppose $d_1 > 1$ with $d := \prod d_i$ such that $\gcd \{d_i, d_j\} = 1$ for all $i \neq j$. Then there exist $a_i$ divisible by $d/d_{n-i+1}$, such that

$$B := \begin{pmatrix} 1 & b_2 & b_3 & \ldots & b_n \\ 0 & d_2 & 0 & \ldots & 0 \\ 0 & 0 & d_3 & \ldots & 0 \\ \vdots & \vdots & 0 & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & d_n \end{pmatrix} \text{ is PH-equivalent to } \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & 0 & \ldots & 0 & a_2 \\ 0 & 0 & 1 & \ldots & 0 & a_3 \\ \vdots & \vdots & 0 & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & a_{n-1} \\ 0 & 0 & 0 & \ldots & 0 & d \end{pmatrix},$$

where the right matrix is in terminal form.

**Remark.** Both matrices are in terminal form; the left has 1-block size one, and the right has 1-block size $n - 1$.

**Remark.** Example 3.3 (fourth matrix) provides an example in terminal form wherein the diagonal entries are pairwise relatively prime, but the matrix is not PH-equivalent to any terminal form with 1-block size $n - 1$; the difference lies in the fact that the lower right block matrix is not diagonal, but merely triangular. This shows that the zeros there are essential to the statement of the result.

**Proof.** Call the right matrix $C$, and let $P$ be the permutation matrix corresponding to $i \leftrightarrow n+1-i$, that is, $P$ is the identity matrix turned by $90^\circ$ (we cannot use $\pi/2$ radians, since we have reserved $\pi$ for permutations). Then $P^{-1} = P$. For any selection of integers $a_i$, let $U_0 = BPC^{-1} \in \mathbb{M}_n \mathbb{Q}$. 17
Then $|\det U_0| = |\det B \det C^{-1}| = 1$; so if we can arrange that $U_0 \in M_n \mathbb{Z}$, then $U_0 \in \text{GL}(n, \mathbb{Z})$, and $U_0CP = B$, so that $C$ is PH-equivalent to $B$. Conveniently, $C$ is easy to invert, so

$$BPC^{-1} = \frac{1}{d} \begin{pmatrix} b_n & b_{n-1} & b_{n-2} & \cdots & b_2 & d_1 \\ d_2 & d_3 \\ \vdots \\ d_{n-1} & d_n \end{pmatrix} \begin{pmatrix} d & -a_1 & \cdots & -a_{n-1} \\ -a_2 & d & \cdots & \vdots \\ \vdots & \vdots & \ddots & -a_3 \\ -a_n & \cdots & \cdots & \cdots & 1 \end{pmatrix},$$

Thus necessary and sufficient for $BPC^{-1}$ to have only integer entries are the following conditions, obtained from the rightmost column of the product:

$$\sum_{i=2}^{n} b_i a_{n-i+1} \equiv 1 \mod d$$

$$\frac{d}{d_i} \text{ divides } a_{n-i+1} \text{ for } 2 \leq i \leq n.$$  

As $B$ is in terminal form, gcd \{\(b_i, d_i\)\} = 1 for 2 ≤ i ≤ n. In addition, from $d_i$ being pairwise relatively prime, it follows that gcd \{\(\frac{b_2d_2}{d_2}, \frac{b_3d_3}{d_3}, \ldots, \frac{b_n d_n}{d_n}; d\)\} = 1. To see this, write the elements as $b_2d_2 \cdots d_n, b_2b_3d_4 \cdots d_n, \ldots, d_2d_3 \cdots d_{n-1}d_n$. If $p$ is a prime dividing all of them, then there exists $j$ such that $p$ divides $d_j$. Since \(\{d_i\}\) are pairwise relatively prime, $p$ does not divide $d_i$ if $i \neq j$. Since $p$ divides $b_jd_j/d_j$, it follows that $p$ divides $b_j$, but this contradicts gcd \{\(b_j, d_j\)\} = 1.

Hence there exist integers $h_i$ and $h$ such that $hd + \sum_{i=2}^{n} h_i b_i d_i = 1$. Set $a_i = h_{n-i+1} d_i / d_{n-i+1}$, that is, $a_{n-i+1} = h_i d_i / d_i$, so that $\sum_{i=2}^{n} b_i a_{n-i+1} \equiv 1 \mod d$ and $d/d_i$ divides $a_{n-i+1}$ for $i = 2, \ldots, n$. If some $h_i d_i / d_i$ exceed $d$ or are negative, we can add or subtract multiplies of $d$ by an elementary row operation, and thus ensure that the resulting $0 \leq a_i < d$ (this is in order to guarantee that $C$ is in terminal form). This does not affect divisibility by $d/d_{n-i+1}$.

With initial 1-block size two (as opposed to one in the Proposition), the corresponding result fails, even with $n = 4$ (with respect to equivalence to a terminal form with 1-block size 3). For example, the matrix

$$B = \begin{pmatrix} 1 & 0 & 5 & 0 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix}$$

in $\mathcal{NS}_4$ has determinant $15 = 5 \cdot 3$, is in terminal form, and is not PH-equivalent to a terminal form with 1-block size three. We can use the method of the proof of 2.2. Suppose $B = UCP$ where $U \in \text{GL}(4, \mathbb{Z})$, $P$ is a permutation matrix, and $C$ is a terminal form with 1-block size three, then $U = BP^{-1}C^{-1}$ (the last factor is easy to determine). Since none of the rows of the upper right $2 \times 2$ block of $B$ has content one, it is straightforward to check that not all of the entries of the so-defined $U$ are integers. This example is decomposable (a direct sum of two $2 \times 2$ matrices each in terminal form), but a similar one can be constructed which is not decomposable.

Let $B$ denote the $n \times n$ integer matrix $\begin{pmatrix} 1_{n-1} & \alpha \\ 0 & d \end{pmatrix}$, with $d > 1$, where $\alpha = (a_1, \ldots, a_{n-1})^T \in \mathbb{Z}^{(n-1) \times 1}$, and assume $B$ is in terminal form. Thus cont $\{\alpha, d\} = 1$ and $0 \leq a_i < d$.

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 $C = \begin{pmatrix} 1_r & X \\ 0 & \text{diag}(d_{r+1}, \ldots, d_n) \end{pmatrix}$; also assume that $C \in \mathcal{NS}$, so that the content of any column is one. Here $X \in \mathbb{Z}^{r \times (n-r)}$. 

18
Let $P$ be a permutation matrix. We want to establish conditions (in terms of all the variables) so that $UB = CP$ for some $U \in \text{GL}(n, \mathbb{Z})$. Since det $B \neq 0$, $B^{-1}$ exists as an element of $M_n \mathbb{Q}$, and so existence of such a $U$ implies $CPB^{-1} \in M_n \mathbb{Z}$; but this is also sufficient as $|\text{det} CPB^{-1}| = 1$. As $B^{-1}$ is particularly easy to calculate, the conditions are not difficult to obtain.

Let $\pi$ denote the permutation corresponding to the action of $P$ on the right; that is, if right multiplication sends the $i$th column to the $j$th column, then $\pi(i) = j$. We have (zeros are omitted)

$$U_0 := CPB^{-1} = \frac{1}{d} \begin{pmatrix} I_r & X & d_{r+1} & d_{r+2} & \cdots & d_n \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \end{pmatrix} \begin{pmatrix} \frac{d}{d_{\pi^{-1}(t)}} & d & & & & -a_1 \\ & & \frac{d}{d_{\pi^{-1}(t)}} & d & & -a_2 \\ & & & \frac{d}{d_{\pi^{-1}(t)}} & & \vdots \\ & & & & \frac{d}{d_{\pi^{-1}(t)}} & -a_{n-1} \\ & & & & & 1 \end{pmatrix}.$$  

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

We calculate the $kn$ entry of the product for where $k > r$; set $t = \pi(k)$. By the preceding, $t \neq n$. The $k$th row of $CP$ is $d_k E_t$ (where $E_t$ are the standard basis elements of $\mathbb{Z}^r \times n$). Thus the $kn$ 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 $ln$ entries of the product for $l \leq r$; the crucial case is $m = \pi^{-1}(n)$. The $mn$ row of $CP$ has 1 as its final entry, zeros in the entries corresponding to $S$, and various $x$s (entries of $X$, too complicated to establish a notation for) in the entries corresponding to $T$. Then the $mn$ 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 $m$th row of $X$.

For $l \neq m$, the condition is a let-down. In this case, the $lt$ row of $CP$ has a one in the $\pi(l) \neq n$ position and various $x$s located in coordinates corresponding to $T$ (which does not include $n$). This yields that $-a_{\pi(l)} + \sum x_l, a_t$ is divisible by $d$. So we obtain the additional (semi-) condition.

(2½) every $a_s$ (for $s \in S \setminus \{n\}$) 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 (2½) is a consequence of (2). Moreover, conditions (1) and (2) imply something drastic about the $d_t$s, namely that they 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 $d_t$s 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 $d_t$s 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 $d_t$s); when $d$ is a power of single prime, this gives an alternative but much more tedious proof of Lemma 1.7, 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 with 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 $d_j$s.

Now suppose that $d$ and $a$, the partition $S \cup T$, 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 is straightforward.

As a consequence, we have the following result about non-stability of 1-block sizes.

**Proposition 2.3** Let $B$ belong to $\mathcal{NS}_n$ (where $n \geq 3$) with determinant $d$. Suppose that whenever $B'$ is a terminal form PH-equivalent to $B$, then $B'$ has 1-block size $n - 1$. Then $d$ is a power of a prime.

**3 A better way of proceeding: two families of invariants**

Here we develop many more PH-invariants, in fact two lattices of them. Fix $n$, and for $1 \leq i \leq n$, let $t_i : \mathbb{Z}^n \to \mathbb{Z}$ 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 $\Omega$ (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 to start with. By applying elementary (integer) row operations to $B$ with columns deleted, we can obtain a matrix of the form $\left( \begin{array}{c} C \\ 0 \end{array} \right)$ where $C$ is square of size $\Omega$. 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 $B_{\Omega}$.

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 $B$, $r(B) \subset \mathbb{Z}^n$, up to the restriction of the action of the permutation matrices acting on the right (that is, as column permutations). When we delete the columns not corresponding to elements of $\Omega$ and take the row space of the resulting matrix, and use that to define $r(B_{\Omega})$, without defining $B_{\Omega}(\Omega)$.

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

If $\Omega' \subset \Omega$, then there is a natural map $r(B_{\Omega}) \to r(B_{\Omega'})$ (between row spaces, viewed as subgroups respectively of $\mathbb{Z}^\Omega$ and $\mathbb{Z}^{\Omega'}$). The kernel of this map is $\cap_{j \notin \Omega} \ker t_j$. We claim that the kernel $\Omega$ is spanned by $\{x_i\}$ where $x_i$ is uniquely determined from $x_i \in \cap_{j \notin \Omega} \ker t_j$ and $t_i(x_i)$ is minimal among elements of $\cap_{j \notin \Omega} \ker t_j$. The corresponding $t_s$ for $B_{\Omega'}$ are simply $t_k$ with $k \in \Omega$. Since $x_i$ vanishes at all $t_j$s except $t_i$, its image in the row space of $B_{\Omega'}$ either vanishes at all the associated $t_s$ (so its image is zero) or, if $i \in \Omega'$, it vanishes at all but one. In that case, its image is an integer multiple of the corresponding $x_i$. Hence $X(B_{\Omega})$ maps to $X(B_{\Omega'})$, and thus we obtain a family of maps $I(B_{\Omega}) \to I(B_{\Omega'})$, one for each pair $(\Omega', \Omega)$ with $\Omega' \subset \Omega$.

Suppose that $\Omega' \subset \Omega$; we thus have an induced onto group homomorphisms $p_{\Omega', \Omega} : I(B_{\Omega}) \to I(B_{\Omega'})$. It is routine to verify that the maps are transitive (that is, if $\Omega'' \subset \Omega' \subset \Omega$, then $p_{\Omega', \Omega'} \circ p_{\Omega', \Omega} = p_{\Omega'', \Omega}$).

Now 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 $S$ together with a compatible family of group isomorphisms $I(B_{\Omega}) \to I(B_{\pi \Omega})$. This is trivial: if we apply an element of $\text{GL}(n, \mathbb{Z})$, the row space is unchanged, and we obtain the identity maps. If we permute columns, $\pi$ is the corresponding permutation, etc. We thus see that not only is $I(B)$ a PH-equivalence, but so is (for example), the set of maps $I(B) \to I(B_{\Omega})$ where we restrict the $\Omega$s to have the same cardinality.

**Lemma 3.1** The lattice of finite abelian groups $(I(B_{\Omega}))_{\Omega \in 2^S}$, together with the onto maps $p_{\Omega', \Omega} : I(B_{\Omega}) \to I(B_{\Omega'})$ whenever $\Omega' \subset \Omega$, is a PH-invariant for matrices $B$ in $\mathcal{NS}_n$. If $k \leq n$, then the list $(I(B_{\Omega}))_{|\Omega| = k}$ is also a PH-invariant.
Seemingly the most useful is the list of \( n \) \( \Omega \)s of cardinality \( n - 1 \), say \( \Omega(i) = S \setminus \{i\} \). Originally, the intent of developing \( B_{\Omega} \) was to find a finer invariant that \( I(B) \): even together with \(|\det B| \) (another PH-invariant) \( I(B) \) does not determine the family \( \{I(B_{\Omega})\} \), or even \( \{I(B_{\Omega(i)})\} \). More interestingly, those \( \Omega \) for which \( I(B_{\Omega}) = \{0\} \) play a particularly important role. For example, there exists \( \Omega \) of cardinality \( r \) such that \( I(B_{\Omega}) = \{0\} \) iff \( B \) is PH-equivalent to a terminal form whose 1-block size is at least \( r \). This is practically tautological, but provides a useful way of constructing interesting examples.

This yields a new family of PH-invariants, specifically, \( (I((B^{op})_{\Omega}))_{\Omega \in 2^S} \). In general \( (B_{\Omega})^{op} \) is not PH-equivalent to \( (B^{op})_{\Omega} \), 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, \( (B^{op})_{\Omega} \). However, I could not decide whether \( (I((B^{op})_{\Omega}))_{\Omega \in 2^S} \) is determined by \( (I(B_{\Omega}))_{\Omega \in 2^S} \), that is, whether for \( B, B' \in \mathcal{NS}_n \), such that \( (I(B_{\Omega})) \cong (I(B'_{\Omega})) \) (as a family) implies \( (I((B^{op})_{\Omega})) \cong (I((B'^{op})_{\Omega})) \).

Self-dual matrices, those in \( \mathcal{NS}_n \) for which \( B^{op} \) is PH-equivalent to \( B \), ought to be of interest. Among other things, self-duality forces \( B \) and \( B' \) to have the same elementary divisors. In the four-matrix example Example 3.3 (below), because \( \det B = 30 = |I(B)| \) and 30 is square-free, we have \( \det B^{op} = 30 \) and the elementary divisors are the same. If we take the leftmost matrix there, then we have

\[
B^{op} = \begin{pmatrix}
15 & 0 & 0 \\
0 & 2 & 0 \\
-1 & -1 & 1
\end{pmatrix}.
\]

It takes a few minutes to determine that

\[B^{op} \text{ is PH-equivalent to both } \begin{pmatrix} 1 & 1 & 14 \\ 0 & 2 & 0 \\ 0 & 0 & 15 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 15 \\ 0 & 1 & 14 \\ 0 & 0 & 30 \end{pmatrix} .\]

By Proposition 2.1, the latter is not PH-equivalent to any of the first three matrices in example 3.3, and since the fourth is not PH-equivalent to a terminal matrix with size two 1-block, it isn’t equivalent to that one either. The list of three \( (B^{op})_{\Omega(i)} \) are (using the rightmost matrix for computations) \( (\mathbf{z}_{15}, \mathbf{z}_{2}, 0) \), which is the same list as that of \( B \).

As a warm-up, we find an easy example for which \( I(B) \cong I(B') \) but they are distinguished by the families \( (I(B_{\Omega(i)})) \) and \( (I(B'_{\Omega(i)})) \). In this case, the absolute values of the determinants are unequal, so we already they cannot be PH-equivalent.

Set

\[
B = \begin{pmatrix}
1 & 0 & 1 \\
0 & 1 & 4 \\
0 & 0 & 8
\end{pmatrix} \quad \text{and} \quad B' = \begin{pmatrix}
1 & 1 & 1 \\
0 & 2 & 4 \\
0 & 0 & 8
\end{pmatrix} .
\]

Both are in \( \mathcal{NS}_4 \) and in terminal form, with \( \det B = 8 \) and \( \det B' = 16 \). It is easy to check that \( I(B) \cong \mathbf{z}_8 \oplus \mathbf{z}_2 \), and this also follows from Lemma 1.2. To calculate \( I(B') \), let \( f_i \) be the rows, and \( E_i \) the standard basis elements for \( \mathbb{Z}^{4 \times 3} \). Then \( E_1 = f_1 - f_2/2 + f_3/8 \), so \( x_1 = 8f_1 - 4f_2 + f_3 \); also \( E_2 = f_2 - f_3/2 \), so \( x_2 = 2f_2 - f_3 \), and of course, \( x_3 = f_3 \). So it remains to find the elementary divisors (or the Smith normal form) of the matrix

\[
\begin{pmatrix}
8 & 0 & 0 \\
-4 & 2 & 0 \\
1 & -1 & 1
\end{pmatrix} .
\]

The obvious column operations (which we are now allowed to do!) yield the Smith normal form of this matrix as \( \text{diag} (8, 2, 1) \). Thus \( I(B') \cong I(B) \).
For $i = 1$, $I(B'_{(2,3)})$ is obtained from the matrix $B$ with the first column removed, \( \begin{pmatrix} 0 & 1 & 4 \\ 1 & 0 & 8 \end{pmatrix} \); elementary row operations yield the $2 \times 2$ identity with third row consisting of zeros. So $I(B'_{(2,3)}) = \{0\}$. The same is obviously true with $I(B'_{(1,2)})$. It is a routine calculation to see that $I(B'_{(1,3)}) \cong \mathbb{Z}_4$. Hence the list $\{I(B_{(i)}(0))\}$ is $\{0, 0, \mathbb{Z}_4\}$.

On the other hand, none of the three choices for $I(B'_{(3)(j)})$ are zero. With $i = 3$, the outcome is obviously $\mathbb{Z}_2$, with $i = 2$ and $i = 1$, we have the row reductions

\[
\begin{pmatrix} 1 & 1 \\ 0 & 4 \\ 0 & 8 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 4 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 2 & 4 \\ 0 & 8 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 2 \\ 0 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 2 \\ 0 & 0 \end{pmatrix}
\]

so $I(B'_{(2)(3)}) \cong \mathbb{Z}_4$ and $I(B'_{(1)(3)}) \cong \mathbb{Z}_2$. Hence the list $\{I(B_{(3)(i)}(0))\}$ is different from $\{I(B'_{(3)(i)}(0))\} = \{\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_4\}$.

Examples to distinguish them with equal determinant will appear after a few remarks.

Suppose that $I(B_{\Omega}) = 0$ for some subset $\Omega \subset S$. Then for every $j \in \Omega$, the basis vector of $\mathbb{Z}_2^\Omega$, $e_{j,\Omega}$, belongs to the span of $X(B_{\Omega})$. This means that by elementary row operations along on $B_{\Omega}$, we can obtain the size $|\Omega|$ identity matrix. Elementary row operations obviously extend to $\mathbb{Z}^\Omega$, and when we apply them to $B$ itself, we obtain a matrix whose $\Omega \times \Omega$ block is the corresponding identity. Conjugating with a permutation will put it in the form $\begin{pmatrix} \mathbb{1}_{|\Omega|} & X \\ 0 & C \end{pmatrix}$. Now we can apply the procedure of [TSCS] to put $C$ itself in terminal form and then there is nothing to prevent additional 1s from appearing, so when we proceed to fix $X$ so that the $n \times n$ matrix is in terminal form, the identity block size may have become larger. Thus if $|\Omega| = r$ and $I(B_{\Omega}) = \{0\}$, then there exists a terminal form PH-equivalent to $B$ with 1-block size at least $r$.

If when we perform this transformation, the resulting matrix has 1-block size exceeding $r$, then it is easy to see that there exists an overset $\Omega_0 \supset \Omega$ such that $I(B_{\Omega_0}) = \{0\}$. There follows, PROPOSITION 3.2 Suppose $B \in \mathcal{NS}_n$ and there exists $\Omega \subset \{1, 2, \ldots, n\}$ such that $I(B_{\Omega}) = \{0\}$, but for all supersets $\Omega_0 \supset \Omega$, $I(B_{\Omega_0})$ is non trivial. Then there exists a terminal matrix $B'$, PH-equivalent to $B$, having 1-block size $|\Omega|$.

The converse is obvious.

EXAMPLES 3.3 (a) Four matrices in $\mathcal{NS}_3$, with the same elementary divisors ($\{1, 1, 30\}$), and in terminal form for which $I(B)$ are all isomorphic, but for which the lists, $\{I(B_{\Omega(i)}(0))\}$ are distinct, and not all are PH-equivalent to a terminal form with 1-block size two.

(b) A matrix $C \in \mathcal{NS}_6$ such that both $I(C)$ and $I(C^{op})$ are cyclic yet neither $C$ nor $C^{op}$ is PH-equivalent to a terminal form with 1-block size 5.

In the following, the calculations are very easy. Each of the four matrices has $\{1, 1, 30\}$ as its invariant factors.

\[
B = \begin{pmatrix} 1 & 0 & 15 \\ 0 & 1 & 2 \\ 0 & 0 & 30 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 5 \\ 0 & 1 & 6 \\ 0 & 0 & 30 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 10 \\ 0 & 0 & 30 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 5 \\ 0 & 0 & 15 \end{pmatrix}
\]

\[
\{I(B_{\Omega(i)}(0))\}_{i=1}^3 \cong \{\mathbb{Z}_{30}, \mathbb{Z}_{30}, \mathbb{Z}_{30}, \mathbb{Z}_{30}\}, \quad \{\mathbb{Z}_{15}, \mathbb{Z}_{2}, 0\}, \quad \{\mathbb{Z}_5, \mathbb{Z}_6, 0\}, \quad \{\mathbb{Z}_3, \mathbb{Z}_{10}, 0\}, \quad \{\mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_2\}
\]

All four lists (viewed as unordered) are different (although their product groups are all $\mathbb{Z}_{30}$), so that there are no PH-equivalences between any of them. Moreover, the list for the fourth example
contains no zero term; hence it is not PH-equivalent to a terminal matrix whose 1-block size is two.

(b) Setting $B$ to be the opposite of the fourth example, we calculate that $\det B = 30 = \det B^{op}$; hence we obtain a matrix such that $I(B)$ and $I(B^{op})$ are cyclic (since their orders are square-free), yet neither $B$ nor $B^{op}$ is PH-equivalent to a terminal form with 1-block size $n - 1$; compare this with Proposition 2.2. This example is also discussed in Appendix C.

**Lemma 3.4** Let $B \in \mathcal{NS}_n$ have a terminal form with a 1-block of size $n - 1$, such that the entries above $d = |\det B|$ are all relatively prime to $d$. Then $I(B) = (Z_d)^{n-1}$, and $I(B_{\Omega}) = 0$ for proper subsets $\Omega$ of $\{1,2,\ldots,n\}$.

This is elementary. More interesting is that the converse holds.

**Lemma 3.5** Suppose $B \in \mathcal{NS}_n$ and $I(B_{\Omega(i)}) = 0$ for all $i = 1,2,\ldots,n$. Then $B$ is PH-equivalent to a terminal matrix of the form described in the previous lemma.

**Remark.** Obviously $I(B_{\Omega(i)}) = 0$ for all $i$ entails $I(B_{\Omega}) = 0$ for all proper subsets $\Omega$, as the maps are onto.

**Remark.** The same method yields that if $|\Omega| > 1$ and $n \in \Omega$, then $I(B_{\Omega}) = 0$ iff $\gcd\{a_j\}_{j \in \Omega} \cup \{d\} = 1$.

**Proof.** Since there exists one $i$ such that $I(B_{\Omega(i)}) = 0$, $B$ is PH-equivalent to a terminal matrix of the form,

\[
\begin{pmatrix}
I_{n-1} & a \\
0 & d
\end{pmatrix}
\]

(necessarily $d = |\det B|$, since PH-equivalence preserves the absolute value of the determinant), where $a = (a_1, \ldots, a_{n-1})^T$ consists of nonnegative integers less than $d$ and $\gcd\{a,d\} = 1$. Suppose $p$ is a prime dividing both $d$ and $a_j$ for some $j$ (this includes the possibility that $a_j = 0$). By conjugating with an obvious permutation matrix (that fixes the $n$th coordinate), we may assume $j = n - 1$. Then the matrix relevant for calculating $I(B_{\Omega(n-1)})$ (delete the $n - 1$st column, creating an $n \times (n - 1)$ matrix) is

\[
\begin{pmatrix}
I_{n-2} & a' \\
0 & a_{n-1} \\
0 & d
\end{pmatrix}
\]

where $a' = (a_1, \ldots, a_{n-2})^T$. It is easy to check that the row space is of index $\gcd\{d,a_{n-1}\}$ in $\mathbb{Z}^{n-1}$ (alternatively: all $(n - 1) \times (n - 1)$ determinants are divisible by $p$). Hence $I(B_{\Omega(n-1)})$ has order divisible by $p$, so is not zero. This contradicts the assumption, whence $\gcd\{a_j,d\} = 1$ for all $j$.

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

(a) Then $B$ is equivalent to a terminal form with 1-block size $n - 1$ iff there exists $i \in S$ such that $I(B_{\Omega(i)}) = 0$.

(b) If $B = \begin{pmatrix} I_{n-1} & a \\ 0 & d \end{pmatrix}$ is a terminal form with 1-block size $n - 1$, where $a = (a_1, \ldots, a_{n-1})^T$, then

$$|\{j \leq n \mid I(B_{\Omega(j)}) = 0\}| = 1 + |\{i \leq n - 1 \mid \gcd\{a_i,d\} = 1\}|$$

**Proof.** (a) One direction follows from Proposition 3.2, the other is obvious. (b) If $j = n$, then $B_{\Omega(n)}$ contains the $(n - 1) \times (n - 1)$ identity, so $I(B_{\Omega(n)}) = \{0\}$. If $j < n$, then the same argument as in 3.5 yields that $I(B_{\Omega(j)}) = \{0\}$ iff $\gcd\{a_j,d\} = 1$. 

23
There is a dual to Lemma 3.5. If \( I(B) \) and all \( I(B_\Omega) \) are isomorphic to \( \mathbb{Z}_d \) for all subsets \( \Omega \) with more than one element, then \( B \) is PH-equivalent to a matrix of the form

\[
\begin{pmatrix}
1 & z_2 & z_3 & \cdots & z_n \\
0 & dI_{n-1}
\end{pmatrix},
\]

where \( \gcd \{ z_i, d \} = 1 \) for all \( i \). The converse is true as well.

If two matrices \( B, B' \in \mathcal{NS}_n \) are both in terminal form, and each has 1-block size \( n-1 \), then there is a relatively efficient procedure for deciding whether they are PH-equivalent. 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 much less), 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 for each \( i = 0, 1, \ldots, n-1 \), decide 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 \( i \)th column and testing whether the resulting row space is all of the standard copy of \( \mathbb{Z}^{n-1} \)—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 \( \gcd \) 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.

4 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 \( n-1 \). Although we give an explicit formula, valid for each \( n \), it is difficult to compute with; however, it converges (as \( n \to \infty \)) to

\[
\frac{\zeta(2) \cdot \zeta(3)}{\zeta(6)} \cdot \frac{1}{\zeta(2)\zeta(3)\zeta(4)\ldots} \sim .85
\]

This is almost double the likelihood that \( B \in M_n \mathbb{Z} \) has a Hermite normal form with at least \( n-1 \) ones [MRW]. The methods derive from that reference, with a few added twists.

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

Now suppose that \( B \in M_n \mathbb{Z} \) is PH-equivalent to a terminal form 1-block size at least \( n-1 \). Then for every prime \( p \), the matrix \( B + pM_n \mathbb{Z} \in M_n \mathbb{Z}_p \) has rank at least \( n-1 \). The converse fails—examples are ubiquitous. Let \( \mathcal{TF}_n \) denote the collection of matrices in \( M_n \mathbb{Z} \) PH-equivalent to a matrix with at least \( n-1 \) ones in its terminal form (for large \( n \), \( \mathcal{TF}_n \cap \mathcal{NS}_n \) 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 every prime \( p \), let \( \pi_p : M_n \mathbb{Z} \to M_n \mathbb{Z}_p \) 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 \( B \in M_n \mathbb{Z} \) 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
\[
\frac{1}{\psi((s+1)^2+2) \cdot \zeta((s+1)^2) \cdot \zeta((s+1)^2+1) \cdots \zeta(n)},
\]
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 \(f(z) = 1 - z^{-(s+1)^2+2} + O(z^{-(s+1)^2+3})\) (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 \(\mathcal{T}F_n\), 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 usual or somewhat stronger notion of natural density, as discussed, for example, in [MRW, Ma].

I confess that I am much more interested in the elegant formulas that come out of the manipulations of the product functions than checking that they actually represent anything like densities. However, 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. The use of inclusion-exclusion—a key tool in this context—really does have to be justified, although it is perfectly natural.

**Upper bound.** Fix integers \(s, n\) with \(n > (s+1)^2 + 1\) and let \(p\) be a prime. The normalized number of matrices in \(M_n \mathbb{Z}_p\) of rank at least \(n - s\) (that is, divided by the cardinality of \(M_n \mathbb{Z}_p\), which is \(p^{n^2}\)) is given by Landsberg’s theorem [L] (quoted in Appendix A) as
\[
\left(\prod_{i=1}^n (1 - z^i)\right) \left(1 + \sum_{1 \leq j \leq s} c_j(z)\right) = \left. \frac{z^{j^2} (1 - z^n)(1 - z^{n-1}) \cdots (1 - z^{n-j+1})}{(1 - z)^2(1 - z^2)^2 \cdots (1 - z^j)^2}\right|_{z = 1/p}
\]
where
\[
c_j(z) = \frac{z^{j^2}}{(1 - z)^2(1 - z^2)^2 \cdots (1 - z^j)^2},
\]
although for some computations we could take the simplified (and slightly less accurate)
\[
c_j \sim \frac{z^{j^2}}{(1 - z^2)(1 - z^2) \cdots (1 - z^j)^2}.
\]
By the Proposition A.2, the Maclaurin series of \(a_s = \prod_{i=1}^{(s+1)^2 - 1} (1 - z^i)\) \((1 + \sum_{1 \leq j \leq s} c_j(z))\) (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 \(M_n \mathbb{Z}_p\) is
\[
n_{s,p} := a_s \cdot \left. \prod_{i=1}^n (1 - z^i)\right|_{z = 1/p}
\]
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 \(n \rightarrow \infty\), the limiting value is
\[
\frac{1}{\prod_{j \geq (s+1)^2} \zeta(j)}.
\]
The case of interest occurs when \( s = 1 \), and an easy computation reveals that \( a_1 = 1 - z^6 \) (exactly!). Hence

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

(2)

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 [MRW] (with extremely 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 approaching squaring with each addition of 1 to \( s \)).

To check that the expressions \( \prod_p n_{p,1} \), (1), and (2) really do represent natural densities (that is, the number of \( B \in M_n \mathbb{Z} \) with all entries in \([-N,N]\) such that for every prime \( p \), the rank of \( \pi_p(B) \in M_n \mathbb{Z} \)) is at least \( n - s \), divided by \((2N)^n\), tends as \( N \to \infty \) to the corresponding expression, we note that the method of [MRW] works almost verbatim. Specifically, the Chinese remainder theorem argument in the proof of [MRW, Lemma 3] applies here, as does the argument of [MRW, Lemma 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 \( TF_n \cap NS_n \), there does not appear to be simple characterization of the set by properties modulo \( p \).

In particular, if \( n \geq 6 \), the density of matrices \( M \in M_n \mathbb{Z} \) 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 \( M \in TF_n \cap NS_n \).

Counting \( TF_n \cap NS_n \). First, we count the number of matrices \( b \in M_n \mathbb{Z}_p \) the 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 \( NS_n \cap TF_n \).) This is almost the same as a special case of [M; Corollary 7].

There are \( N_p = (p^n - 1)(p^p - p) \cdots (p - 1) \) 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 \( n \)th column is not zero is

\[
N_p \cdot \left( 1 + \frac{p^{n-1} - 1}{p^n - p^{n-1}} \right) = p^{n^2} \frac{(1 - 1/p)(1 - 1/p^2) \cdots (1 - 1/p^n)}{(1 - 1/p)(1 - 1/p^2) \cdots (1 - 1/p^n)} \cdot \frac{1 - 1/p^n}{1 - 1/p} = p^{n^2} \frac{(1 - 1/p^2) \cdots (1 - 1/p^n)(1 - p^n)}{1 - 1/p}.
\]

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

\[
(*) \quad \frac{1}{\zeta(2) \cdot \zeta(3) \cdots \zeta(n-1) \cdot \zeta(n)^2}.
\]
This differs from the natural density of matrices with Hermite normal form with at least $n - 1$ ones [Ma, Corollary 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 $\Phi$ is a subset of $\{1, 2, \ldots, n\}$, let $D_\Phi$ 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 $j$th column deleted is one. Clearly, if $|\Phi| = |\Phi'|$ and $D_\Phi$ has a natural density, then so does $D_{\Phi'}$, and their natural densities are equal.

This number is the natural density for this problem is practically immediate from the special case of [Ma, Corollary 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 the the final column be unimodular, so nonzero modulo every prime. This resulted in the extra factor of $\zeta(n)$. In op cit, the author used a stronger form of natural density (this is important for the use of inclusion-exclusion).

We have just shown that if $|\Phi| = 1$, then $D_\Phi$ has a natural density, given by the number in (*). Now $\cup D_\Phi$, where $\Phi$ 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.

The inclusion-exclusion formula now can be used (with caution). We will obtain a density for every $D_\Phi$. 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 iff the $i$th 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

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

$$= (1 - z)(1 - z^2) \cdots (1 - z^n) \left(1 + z(1 - z)^{s-2}\right)$$

Denote by $f_s$ the polynomial (now in the variable $z$) $(1 - z)(1 + z(1 - z)^{s-2})$; this is $(1 - z)(1 + z - (s-2)z^2 + \ldots)$, so $f_s = 1 - (s-1)z^2 + O(z^3)$. This permits us to define a function (which it turns out is 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 $p^{s-1} - (p-1)^{s-1} \neq p^s$ (this simplifies), it is easy to check that $F$ is analytic on a neighbourhood 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 neighbourhoods of the zeros; so $F$ is entire. Its zeros are precisely the set, $\{s \in \mathbb{C} \mid \exists$ prime $p$ such that $p^{s-1} = (p-1)^{s-2}\}$; this can be rewritten as

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

The reciprocals of the moduli of the zeros are thus square summable. Along any infinite strip $|\text{Im } z| < N$, there are only finitely many zeros, and if we could get rid of the zeros with imaginary
parts of absolute value exceeding $2p \ln p$, then the sum of the reciprocals of the remaining zeros is absolutely summable (since $\sum_p 1/p \ln p < \infty$).

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

$$F(0) = \prod_p \left( 1 + \frac{1}{p(p-1)} \right); \text{ this is } \zeta(2)\zeta(3)/\zeta(6) \sim 1.94, \text{ the Landau totient constant, again}$$

$$F(1) = 1$$

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

$$F(3) = \prod_p \left( 1 - \frac{2p-1}{p^3} \right); \text{ the carefree constant, } \sim .426 [M]$$

The values at the other integers (both positive and negative) have likely appeared before, but I couldn’t locate them in the huge literature on constants. The density of $D_\Phi$ (when $|\Phi| = s > 1$) is thus

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

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

For $s = 2$, the density of $D_\Phi$ is $1/(\zeta(2))^2 \zeta(3) \ldots \zeta(n)$. The exclusion-inclusion 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

$$\frac{n}{\zeta(n)} - \frac{(2)}{\zeta(2)} + \sum_{j=3}^{n} (-1)^{j-1} \binom{n}{j} F(j) \frac{\zeta(2) \ldots \zeta(n)}{\zeta(2) \zeta(3) \ldots \zeta(n)} \quad (***)$$

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 this mess. The denominator converges extremely rapidly, and has been calculated as around $1/.44$ for large (and not so large) $n$ [Ma]. Also, $\{F(j)\}_{j \in \mathbb{N}}$ 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

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

This converges uniformly on compact subsets of $|\text{Im } s| < \pi/\ln 2$. Viewed as a real function (that is, restricting $s$ to be real), each summand is the negative of a completely monotone function and $F$ is nonnegative on $\mathbb{R}$, so that $F$ is logarithmically completely monotone (meaning that $F > 0$ and $-F'/F$ is completely monotone) which implies $F$ is completely monotone.

With single-digit accuracy, I managed to approximate (with pencil and paper) the values of the expression in (***) 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 $(\zeta(2)\zeta(3)/\zeta(6)) \cdot 1/\zeta(2)\zeta(3) \cdots \sim .85$.

This suggests that the numerator of (***) 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

\[
D(n) := F(0) - nF(1) + \left( \frac{n}{2} \right) F(2) - \cdots + (-1)^n F(n) = \sum_{i=0}^{n} (-1)^n \left( \frac{n}{i} \right) F(i).
\]

We will show

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

This is equivalent to the numerator in (***) converging (in \( n \)) to \( F(0) = \zeta(2)\zeta(3)/\zeta(6) \).

A function \( f : \mathbb{R} \to \mathbb{R} \) is completely monotone if \((-1)^n f^{(n)}(r) \geq 0\) for all \( n \in \mathbb{Z}^+ \) and \( r \in \mathbb{R} \) (here \( f^{(n)} \) is the \( n \)th 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.

Let \( \Delta \) denote the usual difference operator, acting on functions on \( \mathbb{Z} \) or \( \mathbb{R} \), that is, \( \Delta f(k) = f(k+1) - f(k) \). If \( f : \mathbb{Z} \to \mathbb{R} \) satisfies \((-1)^n \Delta^n f(k) \geq 0\) for all \( n \in \mathbb{Z}^+ \) and \( k \in \mathbb{Z} \), then we say that \( f \) is completely monotone.

It is routine 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 completely elementary.

Now suppose that \( f : \mathbb{R} \to \mathbb{R} \) is completely monotone; then it is routine to see that \( f|\mathbb{Z} \) (or any other discrete subgroup) is completely monotone (in the sense of functions on \( \mathbb{Z} \)). By the higher order mean value theorem, given \( r \in \mathbb{R} \), and \( n \in \mathbb{Z}^+ \), there exists \( \xi \in [r, r+n) \) such that \( \Delta^n f(r) = f^{(n)}(\xi) \); setting \( r = k \in \mathbb{Z} \), 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.

The following is elementary, and presumably standard.

**Proposition 4.1** Suppose that \( f : \mathbb{Z} \to \mathbb{R} \) is completely monotone. Then for all \( k \in \mathbb{Z} \)

\[
\lim_{N \to \infty} \sum_{j=0}^{N} (-1)^j \Delta^j f(k) \quad \text{exists and equals} \quad f(k-1).
\]

**Remark.** Formally, this means that \( I + \sum_{j=1}^{\infty} (-1)^n \Delta^n = (I + \Delta)^{-1} \) (as would be expected from the power series expansion) when applied to completely monotone functions (and therefore to the vector space they span).

**Proof.** First, we claim that \( d_n(k) := (-1)^n \Delta^n f(k) \to 0 \) as \( n \to \infty \). Consider \( d_n(k-1) = d_n(k) + d_{n+1}(k-1) \); iterating this, we quickly see that since all \( d_n(n) \geq 0 \), we have \( d_n(k-1) \geq jd_{n+j}(k) \). As \( d_{n+j}(k) \geq 0 \), this forces \( d_{n+j}(k) = O(1/j) \); in particular, \( d_n(k) \to 0 \) as \( n \to \infty \).

Now apply \( I + \Delta \) to the expression on the left of the display; this yields \((I + (-1)^{N+1} \Delta^{N+1}) f(k) = f(k) + d_{N+1}(k) \to f(k) \). On the other hand, \((I + \Delta) f(k-1) = f(k) \).

Set \( g_N(l) := \sum_{i=0}^{N} d_i(l) \). Then \((I + \Delta) g_N(l) = f(l) + d_{N+1}(l) \), but also \((I + \Delta) g_N(l) = g_N(l+1) \).

Setting \( l = k-1 \), we have \( g(k) = f(k-1) + d_{N+1}(k-1) \); this says \(|g_N(k) - f(k-1)| \leq d_{N+1}(k-1) \), which goes to zero as \( N \to \infty \).

**Proposition 4.2** The restriction of \( F \) to \( \mathbb{R} \) is logarithmically completely monotone.

**Proof.** With \( \ln F \) given above, we note that \( F|\mathbb{R} \) is strictly positive, and the logarithmic derivative \( F'/F = (\ln F)' \) is a locally convergent (on compact subsets of the strip \(|\text{Im} z| < \pi/\ln 2 \)) sum of terms each of which is the negative of a completely monotone function.
COROLLARY 4.3 The natural density of matrices in $\mathcal{T}F_n \cap \mathcal{NS}_n$ 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. In fact, it also follows from the last two propositions that if $T(n)$ is the (strong) natural density of $\mathcal{T}F_n \cap \mathcal{NS}_n$, then $\{T(n)\}$ is increasing, 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.

Motivation. Why the emphasis on 1-block size $n - 1$ (for PH-equivalence classes of matrices in $\mathcal{NS}_n$)? For one thing, if $B$ and $B'$ are in terminal form with 1-block size $n$, we can easily decide (from Proposition 2.1) whether they are PH-equivalent (and the procedure can be made very fast).

For another, the condition that $B \in \mathcal{NS}_n$ have a terminal form with 1-block size $n$, for $n \geq 6$, has density at least .8 tending to .85...—meaning five out of six random matrices should have such a terminal form.

If we consider $s = 2$ 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 analogue of Proposition 2.1 for $n - 2$, describing the equivalence classes containing terminal form of this type).

For the classification, 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, we have an elementary lemma.

If $p$ is a prime and $m \in \mathbb{N}$, then $v_p(m) = r$ means that $p^r$ maximally divides $m$; this is the usual valuation.

LEMMA 4.4 Suppose that $B \in \mathcal{NS}_n$ is PH-equivalent to the terminal form

$$\begin{pmatrix} I_{n-1} & a \\ 0 & d \end{pmatrix}$$

where $a = (a_i)^T \in \mathbb{Z}^{(n-1)\times 1}$ and $\gcd\{a, d\} = 1$. Then $B^{op}$ is PH-equivalent to a terminal form with 1-block size $n - 1$ iff for every prime $p$ dividing $d$, there exists at most one (hence exactly one) nonzero $a_i$ such that $v_p(a_i) < v_p(d)$.

Proof. If $B$ is in the displayed terminal form, we may reorder the entries of the column $a$ (by conjugating with a permutation matrix) so that if there are any $i$ such that $a_i = 0$, they form an
initial segment; let \( l \) (possibly zero) denote the number. It is a routine computation that

\[
B^{op} = \begin{pmatrix}
I_l & \frac{d}{(d,a_l+1)} & \frac{d}{(d,a_{l+2})} & \cdots \\
0^l & -\frac{a_{l+1}}{(d,a_{l+1})} & -\frac{a_{l+2}}{(d,a_{l+2})} & \cdots & 1
\end{pmatrix}
\]

The second matrix is obtained by cyclically permuting the rows below the identity block, then correspondingly permuting the columns; if we order the as so that \( \gcd \{d, a_i\} \) are decreasing for \( l + 1 \leq i \leq n - 1 \), then the second matrix is in terminal form, although not a particularly nice one. If \( l = n - 2 \), its 1-block size is already \( n - 1 \), and there is nothing to do. Otherwise, \( l < n - 2 \).

Now \( B' \) has a terminal form with a 1-block size \( n - 1 \) iff there exists \( j \) such that \( I(B_{\Omega(j)}) = \{0\} \); in other words, iff there exists a column, which after its deletion, the resulting matrix has 1 as the gcd of the determinants of the square size \( n - 1 \) matrices. Let \( s_i = d/\gcd \{d, a_i\} \) and \( u_i = -a_i/\gcd \{d, a_i\} \). For all \( i \), \( \gcd \{s_i, u_i\} = 1 \)

Deleting any of the first \( l + 1 \) columns results in the gcd being the product of the diagonal entries, \( \prod s_i \). Removing the \( i \)th column with \( l + 2 \leq i \leq n - 1 \) results in a gcd of \( t_i := s_i^{-1} \prod_j s_j \). However, deleting the \( l + 1 \)st column results in the determinants, \( \{ \prod s_i, s_i^{-1} u_1, s_2^{-1} u_2, \ldots, s_n^{-1} u_n \prod s_i \} \). It is easy to check (since \( (s_i, u_i) = 1 \) for all relevant \( i \)) that this list has the same greatest common divisor as \( \{s_j^{-1} \prod s_i\}_{j= l+1}^n = \{t_j\} \).

Hence \( B' \) is \( \text{PFH-equivalent} \) to a terminal form with 1-block size \( n - 1 \) iff \( \gcd \{t_j\} = 1 \). Let \( p \) be a prime; if \( v_p(a_i) < v_p(d) \) for two values of \( i \) (with \( a_i \neq 0 \)), then \( p \) divides all the \( t_j \); the converse is clear.

The condition in the lemma seems rather restrictive, but it is not clear how to convert this into a likelihood estimate for both \( B \) and \( B^{op} \) having 1-block size \( n - 1 \).

We wish to obtain something like a natural density for columns \( \alpha := (a_1, \ldots, a_{n-1}, d)^T \in \mathbb{Z}^{n \times 1} \) with the following properties

(i) \( \text{cont}(\alpha) = 1 \)

(ii) \( d \geq 1 \)

(iii) for all primes \( p \), there exists at most one \( i \) such that \( v_p(a_i) < v_p(d) \).

Because of (i), the third condition means that if \( p \) divides \( d \), then \( v_p(a_i) = 0 \) for at most one \( i \), and for all other \( j \), \( v_p(a_j) \geq v_p(d) \). We do our (approximate) count over the box \([-N, N]^{n-1} \times [1, N] \), the last coordinate because of (iii). In fact, if we fix the value of \( d \), we obtain a nonzero density for the truncated columns \( \beta := (a_1, \ldots, a_{n-1})^T \) such that \( (\beta, d) \) satisfies the properties. However, when we allow \( d \) to vary, provided \( n \geq 4 \), the overall density is zero.

Let \( k \) be a nonnegative integer (which will be the number of distinct prime divisors of \( d \)); let \( S(k) \) denote \( \{1, 2, \ldots, k\} \). Define the following subcollection of \((2^S(k))^{n-1}\),

\[
\mathcal{N}(k, n - 1) = \{ \Omega := (\Omega_i)_{i=1}^{n-1} \mid \Omega_i \subseteq S(k); \cap \Omega_i = \emptyset; \ i \neq j \implies \Omega_i \cup \Omega_j = S(k) \}.
\]
It is immediate that \(|N(k, 2)| = 2^k\). There is an obvious recurrence relation obtained by deleting the first coordinate,
\[
|N(k, m)| = \sum_{\delta=0}^{k} \binom{k}{\delta} |N(k - \delta, m - 1)|
\]
(the notation \(\delta\) is supposed to indicate the defect, that is the cardinality of the complement of \(\Omega_1\)). We see that the function \(P(k, m) = m^k\) satisfies the same recurrence relation and agrees with \(|N|\) when \(m = 2\); so \(P = |N|\), and thus \(|N(k, m)| = m^k\). Since the cardinality of \(2^{S(k)} n^{-1}\) is \(2^{k(n-1)}\), \(N(k, n - 1)\) (of cardinality \((n - 1)^k\)) forms a very small subset of \((2^{S(k)})^{n-1}\)—but we will need the exact form of the cardinality later anyway.

Now let \(d > 1\) be a positive integer, and let \(w(d)\), denoted \(k\) at least temporarily, be the number of distinct prime divisors of \(d\). Factor \(d = \prod i = 1^k p^{m(i)}\) where \(p_1 < p_2 < \ldots\) and \(m(i) \geq 1\) for all \(i\). For \(\Omega \subset S(k)\), let \(d_{\Omega} = \prod_{j \in \Omega} p^{m(j)}\); thus \(d_\emptyset = 1\) and \(d_{S(k)} = d\). As usual \(\phi\) will denote the Euler totient function.

Associate to each \(\Xi \in N(k, n - 1)\) a number (depending on \(d\)—thus on \(k\)—and the large integer \(N\)), \(\text{wt}_{N, d}(\Xi) = 0\) if \(d > N\) and otherwise
\[
\text{wt}_{N, d}(\Xi) := \frac{1}{d^{n-1}} \prod_{i=1}^{n-1} \phi(d_{\Omega_i})
\]
\[
= \frac{\phi(d)}{d^{n-1}}.
\]

The conditions in the definition of \(N\) guarantee that the set \(\{d_{\Omega_i}\}\) is pairwise relatively prime, and their product is just \(d\); hence the second line, and the result that the weight does not depend on the choice of \(\Xi\).

On defining \(f_N(d) = \sum_{\Xi \in N(w(d), n-1)} \text{wt}_{N, d}(\Xi)\), we have \(f_d = |N(w(d), n - 1)| \phi(d)/d^{n-1} = (n - 1)^w(d) \phi(d)/d^{n-1}\) if \(d \leq N\) and zero otherwise.

Now we claim that if \(N^{-1} \sum_{d \leq N} f_N(d)\) converges (as \(N \to \infty\)), then the limit is the natural density of the set. In other words, if
\[
\lim_{N \to \infty} \frac{1}{N} \sum_{d \leq N} \frac{(n - 1)^w(d) \phi(d)}{d^{n-1}}
\]
exists and equals \(s\), then \(s\) is the natural density of the set of columns satisfying (i–iii) above. Note in particular, that the thing being summed is multiplicative (in the number-theoretic sense, that if \(a\) and \(b\) are coprime, then the value at \(ab\) is just the product of the values at \(a\) and \(b\)).

To see this, consider the set of columns satisfying (i–iii), and fix \(d > 1\), with \(d = \prod_{j=1}^{k} p^{m(i)}\). To each such column \((a_i; d)^T\), associate an element of \(\mathcal{N}\) as follows. If \(p_j\) divides \(a_i\), then \(p_j^{m(j)}\) divides it; let \(\Omega_i\) be the subset of \(\{1, 2, \ldots, k\}\) such that \(p_j\) divides \(a_i\). Then conditions (i–iii) entail that \(\Xi := (\Omega_i)_{i=1}^{n-1}\) belongs to \(\mathcal{N}(w(d), n - 1)\). Conversely, given \(\Xi \in \mathcal{N}(k, n - 1)\), there exists a column \((a_i; d)^T\) to which \(\Xi\) is associated: define \(a_i = \prod_{j \in \Xi} p_j^{m(j)}\), and verify that the column satisfies (i–iii).

Now in the cube \((-N, N)^{n-1}\), we count the number of possible columns \((a_i)^T\) so that when \(d\) is adjoined, the resulting column satisfies (i–iii); equivalently, for each \(\Xi \in \mathcal{N}(k, n - 1)\), we count the number of columns in the cube which are associated to \(\Xi\).
In the \(i\)th coordinate, \(a_i = d_{\Omega_i} \cdot t_i\), where \((t_i, p_j) = 1\) for all \(j \in \Omega_i^c\) (we allow higher powers of \(p_j\) in \(a_i\) than in \(d\)). For large \(N\), the number of such \(a_i\) is

\[
\frac{2N}{d_{\Omega_i}} \cdot \frac{\phi(d_{\Omega_i})}{d_{\Omega_i}} \left( 1 + O \left( \frac{1}{N} \right) \right) = \frac{2N}{d} \phi(d_{\Omega_i}) \left( 1 + O \left( \frac{1}{N} \right) \right).
\]

Normally, we would put an ceiling or floor functions around the expression, but as we are taking limits as \(N \to \infty\), this is unnecessary. The number of the columns \((a_i)^T\) is thus up to multiplication by \(1 + O(n/N)\), the product

\[
\left( \frac{2N}{d} \right)^{n-1} \prod_{i=1}^{n-1} \phi(d_{\Omega_i}) = \left( \frac{2N}{d} \right)^{n-1} \phi(d).
\]

(As \(\Omega_i \cup \Omega_j = S\) for distinct \(i\) and \(j\), it follows that the numbers \(\{d_{\Omega_i}\}\) are pairwise relatively prime.) As this is true for every choice of \(\Xi \in \mathcal{N}(w(d), n - 1)\), the total number of the truncated columns \((a_i)^T\) is thus

\[
(2N)^{n-1} |\mathcal{N}(w(d), n - 1)| \frac{\phi(d)}{d^{n-1}} = (2N)^{n-1} (n - 1)^{w(d)} \frac{\phi(d)}{d^{n-1}};
\]

normalizing (dividing by \((2N)^{n-1}\)), and letting \(N \to \infty\), we obtain a density with \(d\) fixed for the choices of \(\beta \in \mathbb{Z}^{(n-1) \times 1}\) such that \((\beta, d)\) satisfies (i–iii),

\[
\frac{(n - 1)^{w(d)} \phi(d)}{d^{n-1}}.
\]

Now we allow \(d\) to vary over \([2, N]\), and we obtain

\[
\frac{1}{N} \sum_{2 \leq d \leq N} \frac{(n - 1)^{w(d)} \phi(d)}{d^{n-1}};
\]

this should converge as \(N \to \infty\), and if it does, the limit is the density. But more is true: if \(n \geq 4\), the sum (without the \(1/N\) factor) converges—in particular, the overall density is zero.

Now make a change of notation, replacing \(n - 1\) by \(s\) and \(d\) by \(n\). Let \(w\) be the number of distinct prime divisors function, and set (for suitable \(s \in \mathbb{C}\)),

\[
G(s) = \sum_{n=0}^{\infty} \frac{s^{w(n)} \phi(n)}{n^s}.
\]

This is not quite a Dirichlet series (because of the power of \(s\) appearing in the numerator), but the argument is multiplicative. For \(s\) fixed but with \(\text{Re} s > 1\), \(|s^{w(n)} \phi(n)| = o(n^{1+\epsilon})\) for all \(\epsilon > 0\). Hence the sum converges (uniformly on compact sets) on \(\text{Re} s > 2\) (it diverges at \(s = 2\), so the latter is the abscissa of convergence).

To see all this, we recall some standard techniques from Dirichlet series. Let \(c : \mathbb{N} \to \mathbb{C}\) be a multiplicative function (that is, \(c(mn) = c(m)c(n)\) whenever \(\gcd m, n = 1\)). The following is well known and easy to verify.

**PROPOSITION** Let \(c : \mathbb{Z} \to \mathbb{C}\) be multiplicative. Provided both sides converge absolutely,

\[
\sum_{n \in \mathbb{N}} c(n) = \prod_p \left( \sum_{j=0}^{\infty} c(p^j) \right).
\]
We say that \( c : \mathbb{N} \to \mathbb{C} \) is a special multiplicative function if it is multiplicative and for all primes \( p \), for all \( j \geq 1 \),
\[
\frac{c(p^{j+1})}{c(p^j)} := r(p)
\]
is independent of \( j \), and in addition, \( |r(p)| < 1 \). This property is stronger than multiplicative, but weaker than completely multiplicative. For example, \( \phi(p^{j+1})/\phi(p^j) = p \), so both \( 1/\phi \) and \( n \mapsto \phi(n)/n \) are special multiplicative functions. The relevant example is \( c_s(n) = s^{w(n)}\phi(d)/d^s \) if \( \Re s > 1 \), where \( w \) is the number-of-distinct-prime-divisors function (we will actually need \( \Re s > 2 \) for convergence of the series and products).

**Proposition** If \( c \) is a special multiplicative function, then for every prime \( p \),
\[
\sum_{j=0}^{\infty} c(p^j) = 1 + \frac{c(p)}{1 - r(p)}.
\]

*Proof. A trivial geometric series argument; for \( j \geq 1 \), \( c(p^j) = r(p) c(p)^{j-1} \), so
\[
\sum_{j=0}^{\infty} c(p^j) = 1 + c(p) \sum_{j=1}^{\infty} r(p)^{j-1} = 1 + \frac{c(p)}{1 - r(p)}.
\]

**Corollary** Let \( c : \mathbb{N} \to \mathbb{C} \) be a special multiplicative function. Provided both sides converge absolutely,
\[
\sum_{n \in \mathbb{N}} c(n) = \prod_p \left(1 + \frac{c(p)}{1 - r(p)}\right).
\]

If we take (for fixed \( s \)), \( c_s \) defined above, then it is special if \( \Re s > 1 \), and the relevant sums and products are
\[
\sum_{n \in \mathbb{N}} s^{w(n)}\phi(n)/n^s \quad \text{and} \quad \prod_p \left(1 + s \cdot \frac{p-1}{p} \cdot \frac{1}{p^{s-1}}\right).
\]

It is routine to verify that \( |s^{w(n)}\phi(n)| = o(n^{1+\epsilon}) \) for all \( \epsilon > 0 \); hence the sum converges absolutely if \( \Re s > 2 \) (and also, if \( s = 2 \), the sum diverges; so the abscissa of convergence is 2, although this is not a Dirichlet series). Since \( \prod_p (1 - 1/p^{1+\delta}) \) converges for all \( \delta > 0 \), the condition \( \Re s > 2 \) is also sufficient for convergence of the product on the right.

Hence, for \( \Re s > 2 \),
\[
G(s) := \sum_{n \in \mathbb{N}} s^{w(n)}\phi(n)/n^s = \prod_p \left(1 + s \cdot \frac{p-1}{p} \cdot \frac{1}{p^{s-1}}\right),
\]
and the resulting function (of \( s \)) is analytic on this half-plane. (The trivial zeros arising from the product realization of \( G \), are rather difficult to determine!)

For example, \( G(3) = \prod_p (1 + 3/p^{p+1}) \), which has probably turned up before; if it helps to recognize it, \( G(3)/\zeta(2) = \prod_p (1 + (2p-3)/p^3) \).

**5 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 [H]. Suppose \( G \to V \) and \( H \to W \) are group homomorphisms from abelian groups
to ordered real Banach spaces. We say \( f : G \to H \) is continuous if there exists continuous and linear \( F : V \to W \) 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 \( \mathbb{R}^n \) is topologically critical of rank \( k + 1 \) if it is free of rank \( n + 1 \) and dense. Any subgroup of lesser rank of a topologically critical group is discrete. In this section (only), when we regard \( g \in G \) as an element of \( \mathbb{R}^k \), we denote it \( \tilde{g} \). Associated to a topologically critical group is an isomorphism class of rank \( n + 1 \) subgroups of \( \mathbb{R} \), \( \text{TO}(G) \), defined as follows. Select any ordered \( \mathbb{Z} \)-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 \( \mathbb{R}^n \); hence we can write \( \tilde{g}_{n+1} = \sum \alpha_i g_i \). It is easy to check that \( \{1, \alpha_i\} \) is rationally linearly independent, and so we may form the subgroup of \( \mathbb{R} \), \( \mathbb{Z} + \sum \alpha_i \mathbb{Z} \), of rank \( n + 1 \). Every topologically critical subgroup of \( \mathbb{R}^n \) is topologically isomorphic to the group generated by \( \{e_i; \sum e_j \alpha_j\} \) (where \( e_i \) are the standard basis elements of \( \mathbb{R}^n \)) by this construction (for example, see [H]).

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

Let \( \text{TO}(G) \) denote the isomorphism class of \( \mathbb{Z} + \sum \alpha_i \mathbb{Z} \subset \mathbb{R} \), that is, with respect to continuous maps (alternatively, we may view the group as a totally ordered group, and use order-preserving group isomorphisms; the resulting equivalence classes are the same, since in this case, any continuous map is either order-preserving or its negative is).

**Lemma 5.1** Suppose \( G \) and \( H \) are topologically critical groups such that \( \text{TO}(G) \cong \text{TO}(H) \). Then \( H \) and \( G \) are continuously isomorphic.

**Proof.** Suppose \( \{\alpha_i\}_{i=0}^{n} \) and \( \{\beta_i\}_{i=1}^{n+1} \) are subsets of \( \mathbb{R} \) that are linearly independent over the rationals, and \( \alpha_{n+1} = 1 = -\beta_{n+1} \), and moreover, \( \sum \alpha_i \mathbb{Z} = \sum \beta_i \) (as subgroups of \( \mathbb{R} \)). Let \( G = \langle e_i; e_{n+1} := \sum_{i=1}^{n} \alpha_i e_i \rangle \) be the (dense) subgroup of \( \mathbb{R}^n \), where \( \{e_i\}_{i=1}^{n} \) is the standard basis for \( \mathbb{R}^n \). Then there exist \( \{h_i\}_{i=1}^{n} \) such that \( G = \sum h_i \mathbb{Z} \) 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 \( \alpha_i = \sum_{t=0}^{n+1} \beta_i a_{i,t} \). Complete \( (a_{i,t}) \) 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 \( j = 1, 2, \ldots, n + 1 \),

\[
h_j = \sum_{i=1}^{n} a_{i,j} g_i
\]

(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,\[
\begin{align*}
h_{n+1} &= \sum_{i=1}^{n+1} a_{i,n+1} g_i \\
&= \sum_{i=1}^{n} (a_{i,n+1} + a_{n+1,n+1} \alpha_i) g_i + (a_{n+1,n+1} \alpha_i) g_i; \quad \text{on the other hand,}
\end{align*}
\]
\[
\sum_{i=1}^{n} \beta_i h_i = \sum_{i=1}^{n} \beta_i \sum_{i=1}^{n+1} a_{i,t} g_i \\
&= \sum_{i=1}^{n} \beta_i \left( \sum_{i=1}^{n} a_{i,t} g_i + \alpha_i \beta_t a_{n+1,t} \right) \\
&= \sum_{i=1}^{n} g_i \cdot \left( \sum_{i=1}^{n} a_{i,t} \beta_t + 0 \right) \\
&= \sum_{i=1}^{n} g_i \cdot (\alpha_i - \beta_{n+1} a_{i,n+1}).
\]

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

Since \(\sum \alpha_i Z = \sum \beta_i Z\), 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 \(\sum h_j Z = \sum g_j Z\), and the rank condition guarantees that the sums are direct.

6 Basic critical dimension groups

A dimension group is a direct limit of simplicial (partially ordered abelian) groups; see [G], the standard reference for partially ordered abelian groups, for far more information than can be given here. By [EHS], a partially ordered abelian group \(G\) is a dimension group if and only if it is unperforated (for \(n \in \mathbb{N}\) and \(g \in G\), \(ng \geq 0\) entails \(g \geq 0\)) and satisfies Riesz interpolation (for \(a_i, b_j \in G\) with \(i, j \in \{1, 2\}\) and \(a_i \leq b_j\) 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 \(n \in \mathbb{N}\) 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 \(\tau\) is simply \(\tau(G)\), its set of values.

The real vector space consisting of convex-linear continuous (affine) real-valued functions \(f : S(G,u) \to \mathbb{R}\) is denoted \(\text{Aff} S(G,u)\). 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 \(u\), \(\tilde{\cdot} : (G,u) \to \text{Aff} S(G,u)\) given by \(g \mapsto \tilde{g}\), where \(\tilde{g}(\tau) = \tau(g)\) for \(\tau \in S(G,u)\). This imposes a pseudo-norm topology on \(G\), which is a norm if the affine map 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 \(G \to \text{Aff} S(G,u)\) (with respect to any or equivalently all choices of order unit \(u\)) has dense range, and \(G^+ \setminus \{0\}\) consists of \(\{g \in G \mid \tilde{g} \text{ is strictly positive}\}\). 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, $\text{Aff} S(G,u)$ can be identified with $\mathbb{R}^n$ for some integer $n$, with the coordinate functions being identified with the pure traces (possibly with some normalization required). The strict ordering on $\mathbb{R}^n$ or $\text{Aff} S(G,u)$ 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 $\mathbb{R}^n$ equipped with the strict ordering. The pure traces are just (up to renormalization) the coordinate maps.

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 $\mathbb{R}^n$, and since the partial ordering determines the topology (the affine representation is automatically one to one here), it is also topologically critical.

We are interested in classification of critical groups. It turns out 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 $\mathbb{R}^n$ (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 $\alpha_i$ are real numbers. For a subgroup so generated, density is equivalent to the set $\{1, \alpha_1, \ldots, \alpha_n\}$ being rationally linearly independent. 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 [BeH], we translated Akin’s notion of good measure on a Cantor set to dimension groups, and were able use these to illustrate various properties of good and non-good traces. Following [BeH], we say trace $\tau$ 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 $\tau^+ := \{h \in \text{Aff} S(G,u) \mid h(\tau) = 0\}$.

This lead to the definition of ugly for a trace on a dimension group; $\tau$ is ugly if $\ker \tau$ has discrete image in $\text{Aff} S(G,u)$ and the trace $\tau \otimes 1_\mathbb{Q}$ on $G \otimes \mathbb{Q}$ is good.

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

(i) $\Omega$ 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 $a - a' \in \ker \Omega := \cap_{e \in \Omega} \ker \tau$ and $a' \leq b$

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

These are not equivalent to the definitions in general; the restriction to $\Omega \subseteq \partial_e S(G,u)$ allowed considerable simplification. Among other things, these correspond to faces in $S(G,u)$. For critical groups in general 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 $\tau$, $\text{rank} \tau(G) = 2$, and this forces all the pure traces to be ugly. Conversely, the pure trace $\tau$ is ugly if $\text{rank} \tau(G) = 2$. There are examples (for every $n \geq 2$, that is, rank at least 3) of critical groups 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).

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 rational. Let $G$ be the subgroup of $\mathbb{R}^3$ spanned by $\{E_1 := (1,1,1), E_2 := (1,1,r), E_3 := (1,r,0), E_4 := (r,0,0)\}$. The set of four $3 \times 3$ determinants of the spanning set is rationally linearly independent. Hence $G$ is dense in $\mathbb{R}^3$, and thus with the
strict ordering, is a critical group (of rank three).

The pure traces on $G$ are the three coordinate maps, denoted $\tau_i$. Then we see that $\tau_1(G) = \mathbb{Z} + r\mathbb{Z} = \tau_2(G) = \tau_3(G)$, 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, as we will see later, $G$ is not 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 rank two (hence all the pure traces are ugly). Pick $r$ such that $\{1, r, \ldots, r^n\}$ is rationally linearly independent (that is, either $r$ is transcendental or its algebraic degree is at least $n + 1$). Define elements of $\mathbb{R}^n$

$$F_n = (r \ 0 \ 0 \ \ldots \ 0 \ 0 \ 0)$$
$$F_{n-1} = (1 \ r \ 0 \ \ldots \ 0 \ 0 \ 0)$$
$$F_{n-2} = (1 \ 1 \ r \ \ldots \ 0 \ 0 \ 0)$$
$$\vdots$$
$$F_1 = (1 \ 1 \ 1 \ \ldots \ 1 \ 1 \ r)$$
$$F_0 = (1 \ 1 \ 1 \ \ldots \ 1 \ 1 \ 1)$$

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 $F_j$s. 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 $rN^T + I + N + N^2 + \ldots$ by $I - N$, creating an upper triangular matrix. See the lemma 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 $\sum_{i=0}^n r^i\mathbb{Q}$, which is easily checked by induction. Hence the set is rationally linearly independent.

Thus $G \equiv G(n, r)$ is a critical group of rank $n + 1$, so with the strict ordering inherited from $\mathbb{R}^n$, 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, $\mathbb{Z} + r\mathbb{Z}$. 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 will soon show that if $n > 2$, then $G(n, r)$ is not basic (or even satisfy a more general property, almost basic).

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

**LEMMA 6.1** Let $N$ be the lower triangular $k \times k$ matrix with $1$s in the $(j + 1,j)$ entries and zeros everywhere else. Let $r$ be any number, and set $Q = rN^T + I + N + N^2 + \ldots$. 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 $\det Q = (1 - r)^{k-1}$. 

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 $\Omega$ simplifies to (i) $\ker \Omega := \cap_{\tau \in \Omega} \ker \tau$ is discrete, and (b) $\ker \Omega \otimes \mathbb{Q}$ is dense in $\Omega^\perp = \{h \in \text{Aff} S(G, u) \mid h|\Omega \equiv 0\}$ ($\Omega$ can be replace by the face it spans).

When $(G, u)$ is critical of rank $n + 1$, and $\Omega \subset \partial_e S(G, u)$, then it is fairly easy to decide whether $\Omega$ is ugly. First, every subgroup of rank $n$ or less is automatically discrete, hence any $\mathbb{Z}$-linearly independent subset is real linearly independent. Second, if $\Omega \subset \partial_e S(G, u)$, then $\Omega^\perp$ has
(real) dimension exactly \(n - |\Omega|\) (the set of pure traces is a dual basis for \(\text{Aff}_S(G, u)\)). The following is then immediate. Note that 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.

**LEMMA 6.2** Let \((G, u)\) be a critical group of rank \(n\), and let \(\Omega\) be a proper set of pure traces. Then \(\Omega\) is ugly iff \(\text{rank ker } \Omega = n - |\Omega|\).

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

In the examples above, \(r\) is a real number that satisfies no nonconstant rational polynomial of degree \(n\) or less, and we formed the group \(G(n, r) \subset \mathbb{R}^n\). These are critical dimension groups with the interesting property that for all pure traces \(\tau\), \(\tau(G)\) 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 \(\tau\) varies over the pure traces.

Moreover, in these examples, we have that \(\text{rank } \tau(G) = 2\), so that \(\text{rank ker } \tau = n - 1\); thus all pure traces are ugly, just as in the case of basic critical groups. However, if \(n \geq 3\), \(\text{rank } (\text{ker } \tau_1 \cap \text{ker } \tau_n) = n - 3 \neq n - 2\); specifically, a \(\mathbb{Z}\)-basis for the intersection is \(\{F_n - F_2, F_{n-1} - F_2, \ldots, F_3 - F_2\}\).

Hence there exists a two-element subset of the pure trace space that is not ugly, so that if \(n \geq 3\), these critical groups are not basic.

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

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

As in the earlier sections, let \(P(n, \mathbb{R})^+\) denote the group 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 \(\Delta\) is a diagonal matrix with only strictly positive real entries along the diagonal. The group of order-automorphisms of \(\mathbb{R}^{1 \times n}\) with respect to either the strict or the usual ordering is just \(P(n, \mathbb{R})^+\), and since any order isomorphism between critical groups (necessarily of the same rank) extends uniquely to an order automorphism of \(\mathbb{R}^{1 \times n}\) (after identifying the two sets of pure traces), we have that the order isomorphisms between critical groups are determined by right actions of \(P(n, \mathbb{R})^+\).

So we can act on \(A\) from the left by \(\text{GL}(n + 1, \mathbb{Z})\) and from the right by \(P(n, \mathbb{R})^+\). 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 the top \(n \times n\) part is just the identity, then the critical dimension group is basic.

We illustrate this with a simple example, the case \(n = 2\) of \(G(n, r)\). Here \(r\) is a real number that is not quadratic or rational. Let \(G = \langle (r, 0), (1, r), (1, 1) \rangle \subset \mathbb{R}^2\). 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 (observe that \(\{1, 1/r, 1/(r - 1)\}\) is linearly independent over \(\mathbb{Q}\) iff \(\{1, r, r^2\}\) is).
required $n \geq 3$. It also satisfies the property that $\tau(G)$ are mutually isomorphic as $\tau$ varies over the pure trace space.

Suppose $A$ is partitioned as $A = \begin{pmatrix} B & \alpha \end{pmatrix}$, where $B$ is an $n \times n$ matrix (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 $\text{GL}(n, \mathbb{Z})$ to be those of $\text{GL}(n, \mathbb{Z}) \times \{1\}$, that is, perform only elementary row operations not affecting the bottom row, $B$. 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 rationally linearly independent.

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 $\alpha$ is multiplied by a rational at the same time). Hence we may assume that $B \in \text{NS}_n$.

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

We investigate the converse. For any critical dimension group with pure trace space $\partial_x S(G, u) = \{\tau_i\}$, 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, $\pm x_i$). Now form $E \equiv E(G) := \sum x_i \mathbb{Z}$ where the $i$ varies over those such that $J_i$ is not zero.

Now form $E(G) = \sum x_i \mathbb{Z}$ where the $x_i$ are defined both above and in terms of the traces (they are the same); the latter ensures that the isomorphism $G \to G'$ induces a group isomorphism $E(G) \to E(G')$, and thus yields an isomorphism $G/E(G) \to G'/E(G)$. In particular, the torsion parts are respectively isomorphic. We claim that this induces an isomorphism $\text{tor}(G/E(G)) \to I(B)$. We are not done yet, since $G = (\sum f_j \mathbb{Z}) \oplus \alpha \mathbb{Z}$ as abelian groups.

It suffices to show that $r(B)/X(B)$ (a subgroup of $G/E(G)$) is exactly the torsion part of $G/E(G)$ (and similarly with $C$ replacing $B$). Since the former is torsion, 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 $ng \in \sum f_j \mathbb{Z}$ (as the $x_i \in \sum f_j \mathbb{Z}$). On the other hand, since $\{f_j\} \cup \{\alpha\}$ is a $\mathbb{Z}$-basis for $G$, we may write $g$ uniquely as $\sum nt_j f_j + n\alpha$, so that $ng = \sum nt_j f_j + n\alpha$; since $ng \in \sum f_j \mathbb{Z}$, we deduce $n\alpha$ is in the span of $f_j$, which of course is impossible unless $nm = 0$, that is, $m = 0$. So $g \in \sum f_j \mathbb{Z}$, and thus $g + E(G) \in r(B)/X(B)$. Of course, the same works with $C$ replacing $B$.

First, $\sum x_i \mathbb{Z} = \oplus x_i \mathbb{Z}$ (routine). Next, $E$ and $G/E$ are invariants for order isomorphism; that is, any order isomorphism between critical dimension groups $G_1 \to G_2$ maps $E(G_1)$ isomorphically (as abelian groups, of course) onto $E(G_2)$, so that the induced map on their cokernels $G_1/E(G_1) \to G_2/E(G_2)$ is also an isomorphism.

When $G$ is basic, $G/E \cong \mathbb{Z}$, 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.

**Lemma 6.3** Let $G$ be a critical dimension group. Then $G$ is basic iff $G/E(G) \cong \mathbb{Z}$. 

40
Proof. One way is trivial. Suppose $G/E \cong \mathbb{Z}$. Then $G \to G/E$ splits, and thus we may find $y \in G$ such that $E \oplus y\mathbb{Z} = G$. We can write $E = \oplus x_i \mathbb{Z}$, 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 $\tau_i$; 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, $\tau_i$ 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 $j$th 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 $\{1, \alpha_1, \ldots, \alpha_n\}$ is rationally linearly independent, and we have exhibited an order-isomorphic copy of $G$ as a basic critical group.

In the examples we just computed, we see that the torsion-free part is rank one (also follows from the fact that all proper sets of pure traces are ugly). The torsion part is determined by the elementary divisors in the final form. Here is a simple example. 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 $G = \langle f_1, f_2, f_3 \rangle = \oplus f_i \mathbb{Z}$. The matrix $A$ is already reduced as far as it can be (if we insist that the top 2-by-2 matrix has only integer entries),

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

Then $\ker \tau_1 = f_2 \mathbb{Z}$, so we set $x_1 = f_2$; $\ker \tau_2 = (2f_1 - f_2) \mathbb{Z}$, so we set $x_2 = 2f_1 - f_2$. But $\langle x_1, x_2 \rangle = \langle 2f_1, f_2 \rangle$, so $G/E \cong \mathbb{Z} \oplus \mathbb{Z}_2$; 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

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

where $\{1, \alpha, \beta, \gamma\}$ is rationally linearly independent. Then $x_1 = 12f_1 - 11f_3$ (up to sign), $x_2 = 6f_2 - f_3$, and $x_3 = f_3$. Then the torsion subgroup of $G/E$, that is, $I(B)$, is isomorphic to $\mathbb{Z}_{12} \oplus \mathbb{Z}_6$, which has 72 elements, not the expected $12 = 1 \times 2 \times 6$.

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

When $n = 2$, we saw an example of a basic critical group such that $\tau(G)$ are all isomorphic as $\tau$ varies over all (two) pure traces. When $n > 2$, the corresponding construction $G(n, r)$, does not yield a basic critical group, but we can still construct basic ones with this property.

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 rationally linearly independent. This is an easy 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 $\mathbb{Z} + r \mathbb{Z}$, $\mathbb{Z} + (r/(1+jr)) \mathbb{Z}$ ($1 \leq j \leq n-1$). But these are all isomorphic (multiply $\mathbb{Z} + (1/(1+jr)) \mathbb{Z}$ by $1+jr$; this is an order isomorphism to $(1+jr) \mathbb{Z} + r \mathbb{Z} = \mathbb{Z} + r \mathbb{Z}$).

7 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 $\begin{pmatrix} B \\ a \end{pmatrix}$ where $B \in M_n \mathbb{Z}$; necessarily (in order to have dense image in $\mathbb{R}^n$),

41
rank $B = n$ and $\{1, \alpha_1, \ldots, \alpha_n\}$ is rationally linearly independent. As above, we may assume that all the columns of $B$ are unimodular, that is, $B \in \mathcal{NS}_n$. We will show that two almost basic groups (with corresponding $(B, \alpha)$ and $(B', \alpha')$) are order isomorphic iff $B = UB'P$ (with $U \in \text{GL}(n, \mathbb{Z})$ and $P$ a permutation matrix, i.e., $B$ is $\text{PH}$-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, that is, every subset of $\partial_1 S(G, u)$ is ugly.

Suppose $r$ and $s$ are irrational real numbers. Then the critical groups of rank $2 (n = 1)$, $\mathbb{Z} + rz \mathbb{Z}$ and $\mathbb{Z} + sz \mathbb{Z}$ with orderings inherited from the reals, are order-isomorphic iff $r$ is in the $\text{PGL}(2, \mathbb{Z})$-orbit of $s$, that is, there exist integers $a, b, c, d$ such that $|ad - bc| = 1$ and $r = (as + b)/(cs + d)$ [ES?]. This easily follows from $(as + b)\mathbb{Z} + (cs + d)\mathbb{Z} = \mathbb{Z} + sz \mathbb{Z}$ when $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}(2, \mathbb{Z})$. For $n > 1$ and basic critical groups, rather perplexingly, the role of $\text{PGL}(2, \mathbb{Z})$ is replaced by the semi-direct product $\mathbb{Z}^n \times \pi \times \rho (S_n \times \{\pm 1\})$ where $S_n$ is the symmetric group. This is abelian by finite, rather different from $\text{PGL}(2, \mathbb{Z})$. 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 $B \in M_n \mathbb{Z}$ be of rank $n$. Suppose $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^{1 \times n}$ is such that $\{1, \alpha_1, \ldots, \alpha_n\}$ is rationally linearly independent. Form the augmented matrix $B = \begin{pmatrix} B \\ \alpha \end{pmatrix} \in \mathbb{R}^{(n+1) \times n}$. Set $G_{B,\alpha}$ to be the subgroup of $\mathbb{R}^{1 \times n}$ generated by the rows of $B$. Then $G_{B,\alpha}$ is a critical dimension group of rank $n + 1$. If the content of $i$th column of $B$ is $\delta_i \in \mathbb{Q}$, then applying $\Delta^{-1}$ on the right, where $\Delta = \text{diag} (\delta_1, \ldots, \delta_n)$, 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 $\alpha$ by various fractions of the form $1/k$), we may assume that $B$ is already in $\mathcal{NS}$.

**Theorem 7.1** 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 $C \in \text{GL}(n+1, \mathbb{Z})$ and $\Delta P \in \text{P}(n, \mathbb{R})^+$ (with $P$ a permutation matrix) such that $C' B \Delta P = B'$. Moreover,

1. In the $n, 1$ partition of $C = \begin{pmatrix} U & C \end{pmatrix}$, $C = (0, 0, \ldots, 0)^T \in \mathbb{Z}^{(n-1) \times 1}$, $U \in \text{GL}(n, \mathbb{Z})$, and $t \in \{\pm 1\}$.
2. $\Delta = 1$ and $UBP = B'$.
3. $\alpha'$ is one of $\pm \alpha P + rB$.

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

$$C \begin{pmatrix} B \\ \alpha \end{pmatrix} P = \begin{pmatrix} UBP \\ \alpha P \end{pmatrix} = \begin{pmatrix} B' \\ \alpha P \end{pmatrix},$$

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

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

Hence we may suppose that $\alpha$ and $\alpha'$ 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 $G_{B,\alpha} \rightarrow G_{B',\beta}$. We will show (i–iii) hold.
The isomorphism entails there exist \( C \in \text{GL}(n+1, \mathbb{Z}) \) and a weighted permutation matrix with positive real entries (here factored as diagonal times permutation), \( \Delta P \), such that \( C' \Delta P = B' \).

Partitioning the matrices as we did before and writing \( B = \begin{pmatrix} 1_s & X \\ 0 & \mathcal{D} \end{pmatrix} \) and \( B' = \begin{pmatrix} 1_{s'} & X' \\ 0 & \mathcal{D}' \end{pmatrix} \), in terminal form (thus \( \mathcal{D} \) is upper triangular with positive increasing entries along the diagonal, none of the them 1, etc)

\[
\begin{pmatrix} U & c \\ r & t \end{pmatrix} \begin{pmatrix} I_s & X \\ 0 & \mathcal{D} \end{pmatrix} \Delta P = \begin{pmatrix} I_{s'} & X' \\ 0 & \mathcal{D}' \end{pmatrix}.
\]

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 \( \Delta \) 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,

\[
(UB + c\alpha)\Delta = B'P^{-1} \quad \text{and} \quad rB + t\alpha = \alpha'P^{-1}.
\]

One of the columns of \( B'P^{-1} \), say the \( h \)th, is the first standard column basis element. Hence for all \( i \),

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

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 rationally linearly independent, 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 \((UB)_{11} = \gamma_{11}\). Thus \((\gamma_{11} + c_i\alpha_1)\delta_1 \in \mathbb{Z} \) (as these are the entries of a column of \( B'P^{-1} \)). Hence for \( i > 1 \), \( \gamma_{11} \in \delta_1^{-1}\mathbb{Z} \) (as the corresponding \( c_i \) are zero). If for some \( i > 1 \), \( \gamma_{11} \neq 0 \), then \( \delta_1 \) is rational. From \( \gamma_{11} + c_1\alpha_1 \in \delta_1^{-1}\mathbb{Z} \) together with rational linear independence of \( \{1, \alpha_1\} \), we deduce \( c_1 = 0 \), a contradiction. Hence \( \gamma_{11} = 0 \) for all \( i > 1 \).

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

\[
\gamma_{i1}B_{12} + \gamma_{i2}B_{22} + c_1\alpha_2 \in \frac{1}{\delta_2}\mathbb{Z}.
\]

If \( i > 1 \), this simplifies to \( \gamma_{i2}B_{22} \in \delta_2^{-1}\mathbb{Z} \); thus if \( \gamma_{i2} \neq 0 \) for some \( i > 1 \), then \( \delta_2 \) is rational. Hence, \( \gamma_{i1}B_{12} + \gamma_{i2}B_{22} + c_1\alpha_2 \in \delta_2^{-1}\mathbb{Z} \subset \mathbb{Q} \). As \( c_1 \neq 0 \), 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 \( C \in \text{GL}(n+1, \mathbb{Z}) \) are

\[
\begin{pmatrix} \gamma_{11} \\ 0 \\ \vdots \\ r_1 \end{pmatrix}, \begin{pmatrix} \gamma_{12} \\ 0 \\ \vdots \\ r_2 \end{pmatrix}, \begin{pmatrix} c_1 \\ 0 \\ \vdots \\ t \end{pmatrix}.
\]
These generate a subgroup of rank only two, so that rank \( C < n + 1 \). This final contradiction shows that \( c_1 = 0 \), and thus \( c \) is zero.

Thus \( C = \left( \begin{array}{cc} U & 0 \\ r & t \end{array} \right) \), and so \( 1 = |\det C| = |t \det U| \). Thus \( t = \pm 1 \) and \( U \in \text{GL}(n, \mathbb{Z}) \), and of course the equations simplify to \( UB\Delta = B'P^{-1} \). Since \( B \) and \( B' \) are invertible in \( M_n \mathbb{Q} \), this forces \( \delta_i \in \mathbb{Q}^{-} \) 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 \( U \in \text{GL}(n, \mathbb{Z}) \)) and \( B'P^{-1} \). Thus the content of the \( i \)th column of \( NUB\Delta \) is \( N\delta_i \) while that of \( NBP^{-1} \) is just \( N \). Hence \( N\delta_i = N \), so \( \Delta = I \). Thus (finally)

\[
UBP = B' \\
rB \pm \alpha P = \alpha'.
\]

This yields (i–iii), and the final statement is a consequence of this and the remarks early in the proof.

**PROPOSITION 7.2** Let \( n > 1 \), \( \alpha = (\alpha_1, \ldots, \alpha_n), \alpha' = (\alpha'_1, \ldots, \alpha'_n) \in \mathbb{R}^n \) 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 \( G_{\alpha} \) and \( G_{\alpha'} \) (generated by \( \{e_1, \ldots, e_n, \alpha\} \) and \( \{e_1, \ldots, e_n; \alpha'\} \) respectively) are order isomorphic iff \( \alpha' \) is in the orbit of \( \alpha \) under the action of \( \mathbb{Z}^n \times_{\Pi \times \rho} (S_n \times \mathbb{Z}_2) \).

**Proof.** Here \( B = B' = 1 \), so the criterion of the theorem simplifies to \( \alpha' \pm \alpha P \in \mathbb{Z}^{1 \times n} \).

**COROLLARY 7.3** Almost basic critical groups of rank at least three admit no nontrivial order-automorphisms.

**Proof.** From \( C B \Delta P = B \) (the order-automorphisms on a critical group automatically extend to order-automorphisms of the closure, \( \mathbb{R}^n \), hence must be given by weighted permutation matrices), the preceding yields \( \pm \alpha + rB = \alpha P \). If \( \pi \) is the permutation induced by \( P \), and \( \pi(i) = j \neq i \) for some \( i \) and \( j \), then \( \alpha_j \pm \alpha_i \in \mathbb{Z} \); but this contradicts 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.

This contrasts with the critical groups discussed in [H]; those arise 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.

**PROPOSITION 7.4** 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 \( \sigma \in \partial_eS(G, u) \), the intersection \( \cap_{\tau \in \partial_eS(G, u) \setminus \{\sigma\}} \ker \tau \) is nonzero.
(c) there exists a basic critical group \( G' \) such that \( G \otimes \mathbb{Q} \) is order-isomorphic to \( G' \otimes \mathbb{Q} \).
(d) every proper subset of \( \partial_eS(G, u) \) is ugly.
(e) \( G \) is order-isomorphic to a dimension group \( G'' \subset \mathbb{R}^n \) with the strict ordering such that the latter has a \( \mathbb{Z} \)-basis \( \{E_1, E_2, \ldots, E_n, E_{n+1}\} \) for which for all \( i \leq n \), \( E_i \in \mathbb{Z}^n \subset \mathbb{R}^n \) \((G \text{ is almost basic})\).

**Remark.** The last formulation says that the \((n + 1) \times n \) matrix representing \( G' \), \( A \), has the form \( \begin{pmatrix} B & 0 \\ \alpha \end{pmatrix} \) where \( B \) is an \( n \times n \) integer matrix, necessarily with nonzero determinant; this is a restatement of the definition of almost basic.
Proof. (a) iff (b): Property (b) is equivalent to rank $E(G) = n$ (since the sum $\sum x_iZ$ is direct), which is equivalent to $\text{frank}G/E(G) = 1$.

(b) implies (c). For each $i$, there exists $x_i \in G$ unique with respect to the properties $\cap_{r \in \partial_0S(G,u) \setminus \{r_i\}} \ker \tau_j = x_iZ$ and $\tau_i(x_i) > 0$. Then $E(G) := \sum x_iZ$ is free of rank $n$ and there exists $y \in G$ such that $G_0 = E(G) \oplus yZ$ is of finite index in $G$. As $G$ is dense in $\mathbb{R}^n$, so is $G_0$.

As a subgroup of $G$ of rank less than $n + 1$, $E(G)$ is discrete; being of rank $n$, any $\mathbb{Z}$-basis for it is also an $\mathbb{R}$-basis for $\mathbb{R}^n$. Hence there exist $\alpha_i \in \mathbb{R}$ such that $y = \sum \alpha_i x_i$. Density of $G_0$ in $\mathbb{R}^n$ entails that $\{1, \alpha_1, \ldots, \alpha_n\}$ be rationally linearly independent, 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 $\tau_i$, which we will also call $\tau_i$.

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 $(G_0, u) \rightarrow \text{Aff}S(G_0, u)$ realizes $G_0$ as a basic critical group.

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

(c) implies (d). For any trace $\tau$ on any dimension group $G$, $\ker \tau \otimes 1_Q = (\ker \tau) \otimes Q$. Thus rank $\ker \tau = \ker(\tau \otimes 1_Q)$. 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 $\tau_i$, let $\Omega(i)$ be the complement of $\{\tau_i\}$ in $\partial_0S(G,u)$. As $\Omega(i)$ is ugly, $\cap_{r \in \Omega(i)} \ker \tau$ 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 $x_iZ$ 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 $G_0 \subseteq \mathbb{Z}^n$. Any subgroup of a free group is free, so we can find the desired basis.

(e) implies (a). Trivial.

8 Unperoration 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 $\partial_0S(G,u)$ are themselves almost basic; the crucial property is that these quotients are unperforated. We will prove the following. This construction is what motivated the $I(B_\Omega)$ invariants of PH-equivalence.

PROPOSITION 8.1 Let $G$ be an almost basic critical group of rank $n + 1$. Let $\Omega \subset \partial_0S(G,u)$, and define $L = \ker \Omega := \cap_{r \in \Omega} \ker \tau$. Then $G/\ker \Omega$, equipped with the quotient ordering, is an almost basic critical group with pure trace space $\Omega$.

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 $I(B_\Omega)$ as the torsion subgroup of $G_\Omega/E(G_\Omega)$ where $G_\Omega = G/\ker \Omega$ (for $\Omega \subset \partial_0S(G,u)$, the latter identified with $\{1, \ldots, n\}$).

The following is a slight improvement on [BeH, Appendix B, Propositions 1 and 2], not covered by any of the results there.

LEMMA 8.2 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 $\text{Aff}S(G,u)$ contains a subgroup of the form $D + P$, where $D$ is a rational vector space and $P$ is generated by nonnegative elements of $\text{Aff}S(G,u)$, 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 $\{ e_i \}_{\tau_i \in S}$. Each $e_i$ has image in $\text{Aff} S(G, u) = \mathbb{R}^n$ 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 [BeH, Appendix B], the quotient is nicely behaved.

The lemma above removes the density condition on $D + P$ (that it be dense in $\hat{L}$) [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 rank $P = \text{rank} L$, 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 $kg + L$ is a nonzero element of the positive cone.

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

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

There exists $\hat{f} \in L$ such that $\| \hat{f} - d' \| < \epsilon / M$ and $q_1 \in L$ such that $\| \hat{q}_1 - p_1 \| < \epsilon / M$. In particular $\hat{q}_1 \geq -\epsilon 1 / M$ 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

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

$$= Nkq_1 + q_2 - (Nx - Nkf - q_1 + q_2)$$

$$\leq N \sigma(kg + x) = N \sigma(q_1) + \sigma(q_2) - N\|N\tilde{x} - Nk\tilde{f} - \hat{q}_1 + \hat{q}_2\|$$

$$\geq N\epsilon - \frac{Nk\epsilon}{M} - \frac{\epsilon}{M} - \|N\tilde{x} - Nkd' - p\| - Nk\|\hat{f} - d'\| - \|\hat{q}_1 - p_1\| - \|\hat{q}_2 - p_2\|$$

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

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

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

**COROLLARY 8.3** 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 $\text{Aff} S(G, u)$ 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 $\text{Aff} S(G, u)$). In this case, the trace space of $(G/L, u + L)$ is a closed face of $S(G, u)$.  

46
Proof. Since the image of $L$ is discrete, its image is already closed in $\text{Aff} S(G,u)$; the hypothesis ensures that $\tilde{L}_0 = P$ satisfies $\tilde{L}/P$ 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 $L^+ = L_0^+$. Let $P^+ = P \cap \text{Aff} S(G,u)^+$ (the latter with the usual, not the strict ordering), so that $P = P^+ - P^+$. Since $L_0$ maps to $P$, and $P^+ = (P^+)^+$, we have that $L^+$ is a (closed) face, call it $F$, of $S(G,u)$. In particular, $F$ is a Choquet simplex.

Let $\phi$ be a trace of $G/L$; then $\phi$ induces a trace of $G$, with kernel containing $L$. Thus $\phi \in L^+ = F$. 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 $h \in \text{Aff} F$; this lifts to an element $j \in \text{Aff} S(G,u)$. Given $\epsilon$, there exists $g \in G$ such that $\|g - j\| < \epsilon$, 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 $\text{Aff} F$, 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.

COROLLARY 8.4 If $G$ is an almost basic critical group and $\Omega \subset \partial_c S(G,u)$, then $G/\ker \Omega$ is a simple dimension group whose pure trace space is $\Omega$.

Proof. Let $F$ be the determined spanned by $S$ (since $\text{Aff} S(G,u)$ is a finite dimensional simplex, it is simply the convex hull of $\Omega$). By Proposition 7.4(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 $\text{Aff} S(G,u)$, and this is of finite index in $\ker \Omega$. 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 $\Omega$.

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

For almost basic critical groups, $G_{B,\alpha}, G_{B',\alpha'}$ with $\left(\begin{array}{c} B \\ \alpha \end{array}\right), \left(\begin{array}{c} B' \\ \alpha' \end{array}\right) \in \mathbb{R}^{n \times (n+1)}$ such that $B, B' \in M_n \mathbb{Z}$ 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 7.1, $G_{B,\alpha}$ is order-isomorphic to $G_{B',\alpha'}$ iff $B$ is PH-equivalent to $B'$ and the permutation involved in the PH-equivalence sends $\alpha$ to $\alpha'$.

For example, if

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

given $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ (with $\{\alpha_1, \alpha_2, \alpha_3\}$ rationally linearly independent), 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 3.3 (first two matrices), $B$ and $B'$ are not PH-equivalent.

If we set $B = B'$ to be the leftmost example in Example 3.3 (the $3 \times 3$ integer matrix in $B_{\alpha}$ 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, because the
permutation $\pi = (12)$ and its corresponding matrix $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ does not fix $B$, as follows from Proposition 2.1, with no invertible elements in the column (modulo $d = 30$).

**Appendix A. A truncated reciprocal formula**

*David Handelman & Damien Roy*

Fix a prime $p$. The following goes back to 1893.

**THEOREM A.1** [L] The number of rank $n - s$ matrices in $\text{GL}(n, \mathbb{Z}_p)$ is

$$C_s := \frac{\left((p^n - 1) \ldots (p^n - p^{n-s-1})\right)^2}{(p^n - s - 1) \cdot (p^{n-s} - p) \ldots (p^{n-s} - p^{n-s-1})}.$$ 

Now we can prove the result of this section. The limiting case of this is the identity [HW, 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 A.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

$$\left(\prod_{i=1}^{(s+1)^2-1} (1 - z^i)\right) \cdot \left(1 + \sum_{j=1}^{s} \frac{z^j}{(1 - z)(1 - z^2) \ldots (1 - z^s)}\right)$$

and

$$\left(\prod_{i=1}^{(s+1)^2-1} (1 - z^i)\right) \cdot \left(1 + \sum_{j=1}^{s} \frac{z^j(1 - z^n)(1 - z^n - 1) \ldots (1 - z^{-j+1})}{(1 - z)(1 - z^2) \ldots (1 - z^s)}\right)$$

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 $2s$ 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,

$$C_s = \frac{N_p}{\prod_{i=0}^{n-1} (p^n - p^i)} \cdot \frac{\left((p^n - 1) \ldots (p^n - p^{n-s-1})\right)^2}{(p^n - s - 1) \cdot (p^{n-s} - p) \ldots (p^{n-s} - p^{n-s-1})}$$

$$= N_p \cdot \frac{(p^n - 1) \ldots (p^n - p^{n-s-1})}{(p^n - p^{n-s})(p^n - p^{n-s+1}) \ldots (p^n - p^{n-1}) \cdot ((p^n - s - 1)(p^{n-s} - p) \ldots (p^{n-s} - p^{n-s-1}))}$$

$$= p^{n^2} \cdot \frac{N_p}{p^{n^2}} \cdot \frac{p^{(n-s)(n-s-1)/2}((p^n - 1)(p^{n-1} - 1) \ldots (p - 1)) \cdot ((p^n - s - 1)(p^{n-s} - 1) \ldots (p - 1))}{p^{(n-s)(n-s-1)/2}((p^n - 1)(p^{n-1} - 1) \ldots (p - 1)) \cdot (p^{s+1} - 1)}; \ \text{divide by } p^{n^2} \text{ and set } z = 1/p;$$

$$\frac{C_s}{p^{n^2}} = \frac{N_p}{p^{n^2}} \cdot \frac{z^2(1 - z^n)(1 - z^{n-1}) \ldots (1 - z^{n+s+1})}{(1 - z)(1 - z^2) \ldots (1 - z^s)^2} = \left(\prod_{i=1}^{n} (1 - z^i)\right) \cdot c_s(z).$$
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 terms 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 ($\{0, 1/2, 1/3, \ldots\}$), 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

$$\frac{z^i}{(1 - z)^2 \cdots (1 - z^i)^2} \times (1 - z^n)(1 - z^{n-1}) \cdots (1 - z^{n-s+1}).$$

When we expand this in its Maclaurin expansion, we see that $c_i = z^i + 2z^{i+1} + \text{terms of higher order}$. 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 $m_p \cdot c_i$ where $t > s$. It follows immediately that the smallest degree term in the Maclaurin expansion of what is missing is $z(s+1)^2 + 2z(s+1)^2 + \text{terms of higher order}$. Thus $E_s := \sum_{i=0}^{s} c_i - \sum_{i>s} c_i = 1 - z(s+1)^2 - 2z(s+1)^2 + \text{terms of higher order}$. Now truncate $m$ at $(s + 1)^2 - 1$, that is, $m_s = \prod_{i \leq (s+1)^2 - 1}(1 - z^i)$. Then

$$m - m_s = m_s \cdot ((1 - z(s+1)^2)(1 - z(s+1)^1) \cdots - 1)$$

$$= m_s \cdot (-z(s+1)^2 - z(s+1)^2 + 1 - z(s+1)^2 + 2 + \cdots)$$

$$= -z(s+1)^2(1 + z + z^2 + \cdots) \cdot (1 - z)(1 - z^2)(1 - z^3) \cdots$$

$$= -z(s+1)^2(1 - z^2 + \cdots); \quad \text{so}$$

$$m_s = m + z(s+1)^2(1 - z^2 + \cdots).$$

Now we have

$$m_s \cdot E_s = m + z(s+1)^2(1 - z^2 + \cdots) \cdot \left(\sum_{i=0}^{n} c_i - \sum_{i>s} c_i \right)$$

$$= 1 - m \sum_{i>s} c_i + \left(z(s+1)^2(1 - z^2 + \cdots) \right) E_s$$

$$= 1 - ((1 - z)(1 - z^2) \cdots (c_{s+1} + \cdots)) + \left(z(s+1)^2(1 - z^2 + \cdots) \right) (1 + z + 2z^2 + \cdots)$$

$$= 1 - (1 - z - z^2 + z^3 + \cdots)z(s+1)^2(1 + 2z + 5z^2 + \cdots) + z(s+1)^2(1 + z + z^2 + \cdots)$$

$$= 1 - z(s+1)^2((1 + z + 2z^2 + \cdots) - (1 + z + z^2 + \cdots))$$

$$= 1 - z(s+1)^2 + 2 + \cdots.$$

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.

The simpler expression (the first one) does not involve $n$ and product behaves as $1 - z(s+1)^2 + 2(1 + O(z))$ 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 [HW, 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 B. Counting PH-equivalence classes

In [ALTPP], the authors compiled tables of PH-equivalence isomorphism types, based on (what amounts to) \( d = |\det B| \) and \( |\det B^{\text{op}}| \) for \( n = 3 \) and 4. Using Proposition 2.1, one can obtain explicit formulas for the the numbers of equivalence classes that contain a terminal form with 1-block size \( n \) of determinant \( d \), and subdivide it according to the possible values of \( |\det B^{\text{op}}| \). Aside from the complicated nature of the expressions, these only deal with 1-block size \( n - 1 \).

In this appendix, we see that the lower bound obtained for the number of PH-classes of \( C \in NS_n \) of determinant \( d \) obtained in Lemma B.1,

\[
F_n(d) := \frac{\phi \ast J_2 \ast \cdots \ast J_{n-1}}{n!}
\]

is asymptotically correct (with an error estimate of a factor \( O(1/d) \)), 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.

First, we obtain an easy lower bound (that is probably an asymptotic one in \( d \) for fixed \( n \)) on the number of PH-equivalence classes of matrices in \( NS_n \) with determinant \( \pm d \).

A matrix \( C \) is called weakly terminal, if it is in Hermite normal form and belongs to \( NS \); 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 implements \( \pi \) as a permutation of the set of columns. There exists \( U \equiv U_P \in \text{GL}(n, \mathbb{Z}) \) 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 \( U \in \text{GL}(n, \mathbb{Z}) \), 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 \( NS \) 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 \( C \in NS_n \).

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 \( I(C_{\Omega(i)}) \) are all distinct. The obvious action of \( P \) (acting on the columns) implements a permutation of the \( n \)-tuple, \((I(\Omega(1)), I(\Omega(2)), \ldots, I(\Omega(n)))\) (the subsequent left action by the unimodular matrix does not affect the order of these groups). If \( I(C_{\Omega(i)}) \) 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 \( \pi \) as a column permutation. Then a weakly terminal matrix \( C \in NS_n \) is fixed by \( \pi \) (or
\( P = P_n \) iff \( CPC^{-1} \) has only integer entries. For a subgroup \( H \) of \( S_n \) and a positive integer \( d \), let \( Z(H)(d) \) 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 \( \pi \), we use the notation \( Z(\pi)(d) \). The cardinality of \( Z(\pi)(d) \) is denoted \( S(\pi)(d) \) (and similarly for subgroups \( H \)). The function \( d \mapsto S(\pi)(d) \) is multiplicative (in the number-theoretic sense) for all \( \pi \).

There is an obvious procedure for counting PH-equivalence classes. First, we count all the weakly terminal matrices of fixed determinant \( d \) (done in xxx). 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. Then the remainder is divided by \( n! \) and added to the number of PH-equivalence classes with smaller orbits. 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 \( S(\pi)(d) \) for every \( \pi \in S_n \); since the matrices with orbit size less than \( n! \) must be in \( Z(\pi) \) for some non-identity \( \pi \in S_n \), we can easily obtain an upper bound for the number of PH-equivalence classes. This will verify the conjecture below when \( d \) is square-free.

Recall the definition of the \( k \)th Jordan totient, \( J_k(n) = n^k \prod_{p \mid n} (1 - p^{-k}) \). 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 a \( d \) in the bottom entry. Recall that for multiplicative functions \( f \) and \( g \), \( f \ast g \), the convolution, is defined by \((f \ast g)(t) = \sum_{x \mid d} f(x)g(d/x)\), and is multiplicative; moreover, \( f \ast g = g \ast f \). There is an identity for constructing \( J_k \), namely if \( \xi_k \) is the multiplicative function \( n \mapsto n^k \phi(n) \), then \( \xi_k \ast \xi_k \ast \cdots \ast \xi_1 \ast \phi = J_k \). (The Dirichlet series for the function on the left telescopes.)

**Lemma B.1** Let \( d \) be a positive integer. For \( n > 1 \), the number of weakly terminal \( n \times n \) matrices of determinant \( d \) is

\[
(\phi \ast J_2 \ast \cdots \ast J_{n-1})(d).
\]

**Proof.** This simple proof is by induction on \( n \). If \( n = 2 \), we are counting the matrices \( \begin{pmatrix} 1 & a \\ 0 & d \end{pmatrix} \) where \( 0 \leq a < d \) 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 \( n \)th 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 thus have \( H_{n-1}(t) = (\phi \ast J_2 \ast \cdots \ast J_{n-2})(t) \) by the induction hypothesis, and

\[
H_n(d) = \sum_{x \mid d} J_{n-1}(x)H_{n-1}(d/x)
\]

\[
= (J_{n-1} \ast H(n-1))(d) = (H_{n-1} \ast J_{n-1})(d)
\]

\[
= (\phi \ast J_2 \ast \cdots \ast J_{n-1})(d),
\]

completing the induction. \( \blacksquare \)

It follows immediately that \((\phi \ast J_2 \ast \cdots \ast J_{n-1})(d)/n! \) is a lower bound for the number of PH-equivalence classes of matrices in \( \mathcal{NS}_n \) of determinant \( \pm d \).
CONJECTURE For a positive integer, the number of PH-equivalence classes of matrices in \( NS_n \), having determinant \( \pm d \) is

\[
\frac{1}{n!} (\phi * J_2 * \cdots * J_{n-1})(d) \cdot \left(1 + O\left(\frac{1}{d}\right)\right).
\]

We have already seen, via Lemma B.1, that this expression (without the big Oh term) is a lower bound.

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 \( \pi \) 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 weird action of \( P \), that is, \( C P C^{-1} \in M_n \mathbb{Z} \).

Let \( K(\pi) \) denote the number of cycles in the decomposition of the permutation \( \pi \) associated to \( P \); fixed points of course are 1-cycles, so are counted. Then \( K(\pi) \) is just the co-rank of the matrix \( I - P \), that is, \( n = \text{rank}(I - P) + K(\pi) \), 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 \( \pi \in S_n \). Then for all \( \epsilon > 0 \),

\[
\frac{S(\pi)(d)}{S(I)(d)} = o\left(d^{K(\pi) - n + \epsilon}\right),
\]

where \( S(I)(d) \) is just the number of weakly terminal matrices of size \( n \) and of determinant \( d \).

Without \( \epsilon \), the specific conjecture fails (in Appendix C, we will see that when \( n = 3 \) and \( \pi \) is a 3-cycle, then \( S(\pi)(d)/S(I)(d) \) is infinitely greater than \( d^{-2} \)).

If the specific conjecture were true, the conjecture preceding it would follow, since \( \phi * J_2 * \cdots * J_{n-1} \geq d^{n-1} \) and \( K(\pi) < n \) for any \( \pi \) other than the identity. Of course, it would be sufficient to prove this when \( d \) is restricted to powers of primes.

What makes the specific conjecture plausible is an elementary observation. The weakly terminal matrix \( C \) is \( P \)-invariant iff \( C P C^{-1} \) has only integer entries, which in turn is equivalent to \( C(I - P)C^{-1} = I - C P C^{-1} \) having only integer entries. The matrix \( C(I - P) \) has rank \( n - K(P) \), and we expect that the smaller the rank, the fewer conditions will be imposed, hence the greater the number of solutions, but that the conditions imposed will reduce the exponent of \( d \) appearing in the number of solutions.

Presumably, this is part of a theory of an arithmetic version of varieties, corresponding to subvarieties having measure zero when imbedded in a variety.

We will show that the conjecture is true when is limited to square-free \( d \).

**Lemma B.2** Let \( H \) be a subgroup of \( S_n \), and \( \pi \in S_n \). Then for all \( d > 0 \),

\[
S(H)(d) = S(\pi H \pi^{-1})(d).
\]

**Proof.** Fix \( d \), and let \( Q \) be the permutation matrix representing \( \pi \). 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, \( C P C^{-1} \in M_n \mathbb{Z} \). There exists \( U \equiv U_{C,Q} \in \text{GL}(n, \mathbb{Z}) \) such that \( U C Q^{-1} \) is in Hermite normal form; since both left multiplication by elements of \( \text{GL}(n, \mathbb{Z}) \) 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, \( UCQ \) 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

\[
UCQ^{-1}(QPQ^{-1})QC^{-1}U^{-1} = U(CPC^{-1})U^{-1} \in M_n \mathbb{Z}.
\]

Since this is true for every \( P \) corresponding to an element of \( H \), we have a set map \( \mathcal{Z}(H)(d) \rightarrow \mathcal{Z}(\pi H \pi^{-1})(d) \) given by \( C \mapsto UCQ \). Since \( C \) is itself weakly terminal, it follows that \( U_{UCQ^{-1},QC^{-1}} \) must be \( U_{C,Q}^{-1} \), so the corresponding map \( \mathcal{Z}(\pi H \pi^{-1})(d) \rightarrow \mathcal{Z}(H)(d) \) is the inverse of the original. This shows that \( C \mapsto UCQ \) is a bijection.

Define for each positive integer \( k \), \( \mathcal{N}_k : \mathbb{N} \rightarrow \mathbb{N} \) via

\[
\mathcal{N}_k(d) = |\{z \in \mathbb{Z}_d \mid z^k = 1\}|.
\]

The Chinese remainder theorem implies that for each \( k \), the function \( \mathcal{N}_k \) is multiplicative. The following is routine, and follows from \( \mathbb{Z}^*_p \) being cyclic of order \( p^{n-1}(p-1) \) when \( p \) is odd, and isomorphic to \( \mathbb{Z}_{2m-2} \times \mathbb{Z}_2 \) when \( p = 2 \) (with the interesting convention that \( \mathbb{Z}_{2-1} \times \mathbb{Z}_2 \) is the trivial group).

**Lemma B.3** For a prime \( p \),

\[
\mathcal{N}_k(p^m) = p^{\min\{\nu_p(k),m-1\}} \cdot \begin{cases} \gcd\{p-1,k\} & \text{if } p \text{ is odd, or } p^m = 2 \\ 2 & \text{if } p = 2 \text{ and } m \geq 2. \end{cases}
\]

If \( k \) is an odd prime, then \( \ln \mathcal{N}_k(d) \leq |\{p|d| p \equiv 1 \mod k\}| \cdot \ln k \), 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 \( \pi \), \( \mathcal{O}_\pi(i) \) (or \( \mathcal{O}(i) \) if \( \pi \) is understood), to be \( \{\pi^k(i)\}_{k \in \mathbb{Z}} \).

For \( \pi \in S_n \) and \( P_\pi \) (or \( P \) if \( \pi \) is understood) the corresponding permutation matrix that implements the action of \( \pi \) on the columns of \( n \times n \) matrices by right multiplication. For \( C \) weakly terminal, then \( C \) is fixed by the action of \( \pi \) (or \( P \)) if \( CPC^{-1} \) has only integer entries: explicitly, \( CP^{-1} \) is put in Hermite normal form by a matrix \( U \in \text{GL}(n, \mathbb{Z}) \), that is, \( UCQ^{-1} \) is in Hermite normal form; then \( UCQ^{-1} \) is \( C \) iff \( U = CPC^{-1} \), which is equivalent (since the determinant of the right side is 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 \( \pi \) 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 \( u = (a_1,a_2,a_3,\ldots,a_{j-1},d,0,0,\ldots,0)^T \in \mathbb{Z}^n \) such that \( 0 \leq a_i < d \) and \( \gcd\{d,a_1,\ldots,a_{j-1}\} = 1 \). Let \( C = C(j,u) \) be the weakly terminal matrix whose \( j \) column is \( u \), and whose \( i \)th column for \( i \neq j \) is the standard basis elements \( E_i \in \mathbb{Z}^n \). In other words, \( C - I \) has exactly one nonzero column, and it is \( u - E_j \). Note that \( C \) so constructed is automatically weakly terminal.

Define

\[
V_j \equiv V_j(d) = \{C \in M_n \mathbb{Z} \mid \det C = d; C \text{ is weakly terminal; the only nonzero column of } C - I \text{ is the } j\text{th.}\}
\]

The definition forces the \( j \)th column to be of the form \( u \) as given above.

53
Given $\pi \in S_n$, we will determine the number of matrices $C \in V_j$ such that $C$ is invariant under $\pi$, that is, for which $CPC^{-1} \in M_n\mathbb{Z}$. If $d = p$, a prime, then every weakly terminal $C$ of determinant $d$ is in $V_j$ for some $j$, so we obtain $S(\pi)(p)$ as a sum over $j = 2, \ldots, n$ of these numbers. This then yields a formula for $S(\pi)(d)$ when $d$ is square-free. The formula is sufficiently explicit to determine asymptotic behaviour (that is, for large, square-free $d$).

Begin with $C \equiv C(j, u) \in V_j$, and $P \equiv P_\pi$. The $i$th 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 $a_\pi$, so that $a_j = d$ and $a_l = 0$ if $l > j$. We will usually write $\pi k$ rather than $\pi(k)$ (unless ambiguity may result) from now on. We can thus write the $m$th 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 basis rows, so that $e_k E_l$ is the matrix product whose outcome is $\delta_{kl}$.)

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 $j$th are just the standard basic columns, and the $j$th column is $d^{-1}(-a_1, \ldots, -a_{j-1}, 1, 0, 0, \ldots, 0)^T$. In particular, $(C^{-1})_j = d^{-1} \left( E_j - \sum_{i < j} a_i E_i \right)$.

We see immediately that $CPC^{-1}$ has only integer entries iff its $j$th column does. We calculate the entries of the $j$th column.

$$(CPC^{-1})_{m,j} = (CP)^{(m)}(C^{-1})_j = \begin{cases} -\frac{a_m a_\pi^j}{d} & \text{if } m, \pi m \neq j \\ \frac{a_m}{d} & \text{if } m = j \text{ and } \pi m = j \\ \frac{a_m a_\pi^j}{d} & \text{if } m \neq j \text{ and } \pi m = j \\ 0 & \text{if } m = j. \end{cases}$$

Now we count the $\pi$-invariant matrices in $V_j$. First suppose that $\pi(j) = j$. Then the conditions for all the entries to be integers boil down to $a_{\pi m} \equiv a_m \mod d$ 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 \( \pi \) is exactly \( J_{\pi(j)}(d) \). (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 \( O(j) \), 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 \( s \) have \( \{m\} \)).

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 \( a_{\pi^{k-2} m} a_m \equiv -a_{\pi^{k-3} m} \), and finally, \( a_{\pi^{k-2} m} = -1 \). 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 \( N_k(d) \) 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 \( a_{\pi m} \equiv -a_{\pi^2 m} \), \( a_{\pi^2 m} \equiv a_m a_{\pi^2 m} \), and in general \( a_{\pi^r m} = a_m (a_{\pi^r m})^r \) (this is true for all \( r \)). Thus the choice of \( a_{\pi^r m} \) (which has to be a \( k \)th root of unity in \( \mathbb{Z}_d \)) 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 \( a_m \equiv a_{\pi^{k(m)} m} \equiv a_m (a_{\pi^{r+1}})^{k(m)} \equiv a_{\pi m} \equiv a_m (a_{\pi^r m})^{f} \) mod \( d \). Hence \( a_m (1 - (a_{\pi^r m})^f) \equiv 0 \) mod \( d \).

Set \( z = -a_{\pi^r m} \), 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 \( z^f \equiv 1 \), 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 \( a_{\pi^r m} = a_m (a_{\pi^r m})^r \), are consistent with the conditions for invariance. Hence there are exactly \( \gcd \{f, p - 1\} \) selections for \( a_{\pi^r m} \) for which we obtain \( p \) choices for \( a_m \), and for all the rest \( (N_k(p) - \gcd \{k(m), k, p - 1\}) \), 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 \( \pi \), for \( p \) prime.

(a) If \( \pi j = j \), there are \( J_{\pi(j)}(p) \), where \( s(j) \) is the number of \( \pi \)-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 \( z \in \mathbb{Z}_p^* \) with order dividing \( |\mathcal{O}(j)| \), and set \( a_{\pi^r m} = -z \). 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 \( a_{\pi^r m} = -z \) is relatively prime to \( p \).

For \( z \) fixed, the number of choices (with \( a_{\pi^r m} = -z \)) is thus (provided \( \mathcal{O}(j) \subseteq \{1, 2, \ldots, j\} \))

\[
\prod_{\mathcal{O}(m) \subseteq \{1, 2, \ldots, j - 1\}} \frac{z^{|\mathcal{O}(m)|} \equiv 1 \mod p}{p^{|\mathcal{O}(j)|}}.
\]

Now we sum this over all choices for \( z \), of which there are \( \gcd \{|\mathcal{O}(j)|, p - 1\} \) (the number of \( k \)th roots of unity in \( \mathbb{Z}_p^* \)).

Finally, we observe that if \( d \) is prime, then the set of weakly terminal matrices in \( M_n \mathbb{Z} \) of determinant \( d \) is simply \( U_{n-1} V_j(p) \), 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 \( \pi \)-orbits that are contained in \( \{1, 2, \ldots, j - 1\} \)
PROPOSITION B.4 Let \( \pi \in S_n \). Then for a prime \( p \),
\[
S(\pi)(p) = \sum_{\{2 \leq j \leq n | \pi j = j\}} J_{\pi j}(p) + \sum_{\{2 \leq j \leq n | \pi j \neq j \text{ and } O_{\pi j} \subseteq \{1, 2, \ldots, j\}\}} \sum_{\{z \in \mathbb{Z}^* \mid |z^{O_{\pi j}}| = 1\}} p\{\{O(m) \mid O(m) \subseteq \{1, 2, \ldots, j-1\} \text{ and } z^{\{O(m)\} \equiv 1 \mod p}\}\}.
\]

If \( \pi \) is a transposition, then by Lemma B.2, 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 reduces to the case that \( j = 2 \), and there are exactly two solutions to \( z^2 \equiv 1 \mod p \) if \( p \) is odd \((z \equiv \pm 1)\), and just one if \( p = 2 \). So we obtain
\[
\sum_{l=1}^{n-2} J_l(p) + \left\{ \begin{array}{ll}
2 & \text{if } p \text{ is odd} \\
1 & \text{if } p = 2.
\end{array} \right.
\]

The left sum is just \( p^{n-2} + p^{n-3} + \cdots + p - (n-2) = (p^{n-1} - 1)/(p-1) - n + 1 \); perhaps unsurprisingly, this is \( \phi_1 * J_2 * \cdots * J_{n-2}(p) \). It is easy to see that any nonidentity permutation other than a transposition will have leading term at most \( p^{n-3} \).

If \( \pi \) 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 \( \mathcal{N}_n \), denoted \( \mathcal{P}\mathcal{H}(n, d) \), when \( d \) is square-free. We see that \( \bigcup_{\pi \neq I} \mathcal{Z}(\pi)(d) \) consists of the weakly terminal matrices (of determinant \( \pi \)) 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 \( d \). Obviously,
\[
\mathcal{P}\mathcal{H}(n, d) \leq \frac{F(n, d) - \mid\bigcup_{\pi \neq I} \mathcal{Z}(\pi)(d)\mid}{n!} + \sum_{\pi \neq I} S(\pi)(d).
\]

This is rather coarse, as it disregards the orbit sizes of the elements in \( \bigcup_{\pi \neq I} \mathcal{Z}(\pi)(d) \) (which are typically \( n!/\text{order of } \pi \)), as well as the overlap. We know that if \( \pi \) is a transposition, then \( S(\pi)(p)/F(n, p) \leq 1/p \); hence for \( d \) square-free, \( S(\pi)(d)/F(n, d) \leq 1/d \), and if \( \pi \) is not a transposition, then \( S(\pi)(p)/F(n, p) \leq 1/p^{2-\epsilon} \) for all \( \epsilon > 0 \), hence \( S(\pi)(d)/F(n, d) \leq 1/d^{2-\epsilon} \). There are \((n^2 - n)/2\) transpositions, so we obtain
\[
\frac{F(n, d)}{n!} - \mathcal{P}\mathcal{H}(n, d) \leq \frac{F(n, d)}{n!} \left( 1 + \frac{n!}{d} \left( \frac{n^2 - 2}{2} + \frac{n!}{d^{1-\epsilon}} \right) \right)
\]
for all \( \epsilon > 0 \). This is not effective until \( d \gg n^2 n! \), but it does yield \( \mathcal{P}\mathcal{H}(n, d) = \frac{F(n, d)(1 + O(d^{-1}))}{n!} \). It can probably refined to the form obtained by replacing the two occurrences of \( n!/d \) by \( n/d \).

COROLLARY B.5 If \( d \) is square-free and \( n \geq 3 \), then the number of PH-equivalence classes of matrices in \( \mathcal{N}_n \) of determinant \( \pm d \) is given by
\[
\mathcal{P}\mathcal{H}(n, d) = \frac{(\phi * J_2 * \cdots * J_{n-1})(d)}{n!} \left( 1 + O \left( \frac{1}{d} \right) \right)
\]

Appendix C: 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 $NS(1)$. 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).

For $n = 3$, the number of PH-equivalence classes is

\[
\phi \ast J_2(d) - 3(S(23)(d) - S(S_3)(d)) - (S(132)(d)) - S(S_3)(d) - S(S_3)(d) = \frac{1}{6} \phi \ast J_2(d) + \frac{3}{2} S(23)(d) + 2S(132)(d).
\]

This follows from inclusion-exclusion, $S(\pi)$ is the same for any transposition $\pi$ (Lemma B.2), and if $\pi, \pi'$ are distinct transpositions or $\pi$ is a transposition and $\pi'$ is a three-cycle, then $Z(\pi) \cap Z(\pi') = Z(S_3)$.

If $m > 1$ and $p$ is a prime,

\[
(\phi \ast J_1) (p^m) = (p^{m-2}(p+1)^2 + 1)p^{m-1}(p-1) = p^{2m}(1 + \frac{1}{p} - \frac{1}{p^2} - \frac{1}{p^3} - \frac{1}{p^{m+1}} + \frac{1}{p^m})
\]

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 $d^2 \prod_{p|d} (p+1)(1/1 - 1/p^2))$. At $2^m$, the outcome is asymptotically $9 \cdot 2^{2m-3}(1 - O(2^{-m})$.

Now $\phi \ast J_2(p^m) = p^{2m} + p^{2m-1} + \ldots$, so $\phi \ast J_2(d) = d^2 \prod_{p|d} (1 + 1/p + 1/p^2 + \ldots)$. We will find that $S(12)(p^m) = p^m + p^{m-1} - \ldots$, except for $p = 2$, when it begins $3 \cdot 2^m/4$ rather than $2^m$, so $S(12)(d) \leq d \prod_{p|d} (1 + 1/p + 1/p^2 \pm \ldots)$ and $S(132)(d) = O(d^\epsilon)$ 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 $n-1$ bounded below by max $\{(d - \phi(d))^{m-1}, \phi(d)^{-1}\}$.

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 determinant $d$ when the latter is square-free (and $n = 3$).

Let $w, w', w'' : N \to C$ 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 $9N$). Each of them is additive (in the number-theoretic sense), so each of $3w, 3w'$, and $3w''$ is multiplicative.

We also define $M_2, M : N \to C$ by setting, for $d = \prod_{p|d} p^{m(p)}$,

\[
M_2(d) = \begin{cases} 
1 & \text{if } m(2) = 0 \\
2 & \text{if } m(2) = 1 \\
6 & \text{if } m(2) = 2 \\
3 \cdot 2^{m-2} + 4 & \text{if } m(2) \geq 3.
\end{cases}
\]

\[
M(d) = \prod_{\text{odd } p|d} (p^{m(p)} + 1)
\]

\[
57
\]
Obviously, $\mathcal{M}$ and $\mathcal{M}_2$ are multiplicative, but not completely multiplicative.

Recall $\mathcal{N}_3(d)$ denote the number of solutions to the polynomial $X^3 - 1 = 0$ in $\mathbb{Z}_d$. 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 completely elementary.

**LEMMA C.1** $\mathcal{N}_3 = 3^{w' + w''}$.

**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 $\mathbb{Z}_d^*$ of exponent three or 1. If $p \equiv 2 \mod 3$, $|\mathbb{Z}_d^*| = \phi(p^m) = p^{m-1}(p-1)$ 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 $p \equiv 1 \mod 3$, $\mathbb{Z}_d^*$ 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 $m = 1$, $\mathbb{Z}_3^*$ is order two, so $\mathcal{N}_3(3) = 1 = 3^{w'(3)+w''(3)}$; if $m \geq 2$, then $\mathbb{Z}_d$ is cyclic of order $2 \cdot 3^{m-1}$, hence has a unique subgroup of order 3, and thus $\mathcal{N}_3(d) = 3 = 3^{w'(d)+w''(d)}$.

**LEMMA C.2** Let $p$ be a prime, and $m$ a positive integer. The number of solutions $(y,k)$ to the equations $Y^2 - 1 = 0$ and $K(Y+1) = 0$ in $\mathbb{Z}_{p^m}$ 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 $\mathbb{Z}_{p^m}/p^{m-1}\mathbb{Z} \cong \mathbb{Z}_p$ and the latter is embedded in the former, if $y^2 = 1$, then we can write $y = w + p^s$ for some 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 $\mathbb{Z}_p$, the only solutions are $\pm 1$, so $w = \pm 1$. Thus $1 = y^2 = 1 + p^s(\pm 2 + p^s2)$. As $(p,s) = 1$, we must have $p^m$ divides $p^s(\pm 2 + p^s2)$.

If $p$ is odd, then $\pm 2 + p^s2$ is invertible in $\mathbb{Z}_{p^m}$, which forces $y = \pm 1$. When $y = -1$, we can set $k$ to be any element of $\mathbb{Z}_{p^m}$, 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 $\mathbb{Z}_4$, $\pm 1$ (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 $2^t(\pm 2 + p^s2^t)$. 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, $\{(2^{m-1} - 1,k)\}$. 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.

By the Chinese remainder theorem, the number of solutions $(k,y) \in (\mathbb{Z}_d)$ of the equations $Y^2 = 1$ and $K(Y+1) = 0$ 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 \( C^{-1} = \frac{1}{egx} \begin{pmatrix} egx & -a & ayg - be \\ 0 & gx & -gy \\ 0 & 0 & e \end{pmatrix} \in M_3Q, \)
where all of \( \{a, b, e, g, y\} \) are nonnegative and \( \leq a < e, y < x, b < gx, \) 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 \( (I(C_{\mathfrak{R}(i)})^3) \) 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), \( (Z_{(\delta, g, x)}, Z_g, Z) \) where \( \delta = ayg - be \) (the determinant of the upper right block), if for example \( \pi = (23) \) or \( (132) \) and \( C \) is invariant under the action of \( \pi \) (meaning that \( CP\pi C^{-1} \in M_3Z \)), then we must have \( e = g \).

Define the multiplicative functions, \( \chi_2 \) and \( \mathcal{P} \),
\[ \chi_2 \text{ is the indicator function of the set of square integers and } \mathcal{P}(d) = \chi_2(d) \cdot \phi(\sqrt{d}). \]

**Lemma C.3** For \( d \) a positive integer, the number of weakly terminal \( 3 \times 3 \) matrices of determinant \( d \) that are invariant under a transposition \( \pi \in S_3 \) is
\[ S(\pi)(d) = (\mathcal{P} \ast \mathcal{M})(d). \]

**Proof.** By Lemma B.2, we may assume \( \pi = (23) \). Since \( d \mapsto S(\pi)(d) \) is multiplicative, we reduce to the case that \( d = p^m \) for some prime \( p \). Taking the generic matrix \( C \), examine the conditions equivalent to \( CPC^{-1} \in M_3Z \). As in the comment above, we must have \( e = g \), so we write \( d = e^2x = p^m \), with \( e = p^m \) and \( x = p^r \) where \( r = m - 2n \). The constraints are \( (a, p) = 1 = (b, p) \) if \( n > 0 \), and \( (y, p) = 1 \) if \( r > 0 \) (and if \( n = 0 \), then \( a = 0 \), etc).

Calculating the matrix product, we see that the conditions for integrality of \( CPC^{-1} \) are precisely,
\[ a \equiv b \mod p^n, \quad y^2 \equiv 1 \mod p^r, \quad (a - b)(y + 1) \equiv 0 \mod p^{n+r}. \]
If \( n = 0 \) (so \( r = m \)), then \( a = 0 \), and the conditions simplify to \( y^2 \equiv 1 \mod p^n \) and \( b(y + 1) \equiv 0 \mod p^m \), where both \( b, y \) are defined modulo \( p^m \). By Lemma C.2, the number of solutions \( (a, b, y) = (0, b, y) \) to this is \( \mathcal{M}(p^m) \).

If \( n > 0 \), we write \( b = a + kp^n \) where \( k < p^r \) (so if \( r = 0 \), then \( k = 0 \)). Then the equations reduce to \( k(y + 1) \equiv 0 \mod p^r \) and \( y^2 \equiv 1 \mod p^r \). When \( r = 0 \), then \( y = 0 \) and \( k = 0 \), so there are \( \phi(p^n) \) choices for \( (a, b, y) = (a, a, 0) \) arising from \( a \) being relatively prime to \( p^n \). When \( r > 0 \), then we may apply Lemma C.2 again, and obtain \( \mathcal{M}(p^r) \) solutions for \( (k, y) \); since \( a \) varies freely over numbers relatively prime and less than \( p^n \), we obtain \( \phi(p^n)\mathcal{M}(p^r) = \phi(p^n)\mathcal{M}(p^{m-2n}) \), and this is even valid if \( r = 0 \) (which only occurs when \( m \) is even), as \( \mathcal{M}(1) = 1 \).

The total number of solutions is thus given by
\[ \mathcal{M}(p^n) + \sum_{1 \leq m \leq n/2} \phi(p^n)\mathcal{M}(p^{m-2n}) = \sum_{0 \leq j \leq m} (\chi_2(p^j) \cdot \phi(p^{j/2}) \cdot \mathcal{M}(p^{n-j})) = (\mathcal{P} \ast \mathcal{M})(p^m). \]

This isn’t 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 C.4  
(a) If $p$ is an odd prime and $\pi$ is a transposition, then
\[ S(\pi)(p^m) = (P \ast M)(P^m) = p^m + p^{m-1} + 1 + \begin{cases} p^{m/2} - p^{m/2-1} & \text{if } m \text{ is even} \\ -p^{(m-1)/2} & \text{if } m \text{ is odd.} \end{cases} \]

(b) For $p = 2$,
\[ S(\pi)(2^m) = (P \ast M)(2^m) = \begin{cases} 2 & \text{if } m = 1 \\ 7 & \text{if } m = 2 \\ 12 & \text{if } m = 3 \text{ and is odd} \\ 2^m + 2m^3 + 2m^2 - 1 & \text{if } m \geq 4 \text{ and is even} \\ 2^m + 2m^3 + 2(m-1)^2 + 2(m-3)/2 & \text{if } m \geq 5 \text{ and is odd.} \end{cases} \]

Proof. When $p$ is odd and $s > 0$, $M(p^s) = p^s + 1$ and $M(1) = 1$. Taking into account the latter, we have
\[
S(\pi)(p^m) = \sum_{0 \leq n \leq m/2} \phi(p^n)p^{m-2n} + \sum_{0 \leq n < m/2} \phi(p^n)
= p^m + 1 + (p - 1) \sum_{1 \leq n \leq m/2} p^{m-n-1} + 2^{(m-1)/2]
= p^m + 1 + \begin{cases} (p - 1)\frac{p^{m-1} - p^{m/2-1}}{p - 1} + p^{m/2} & \text{if } m \text{ is even} \\ (p - 1)\frac{p^{m-1} - p^{(m-1)/2}}{p - 1} & \text{if } m \text{ is odd.} \end{cases}
= p^m + p^{m-1} + 1 + \begin{cases} p^{m/2} - p^{m/2-1} & \text{if } m \text{ is even} \\ -p^{(m-1)/2} & \text{if } m \text{ is odd.} \end{cases}
\]

When $p = 2$, the computation is more complicated because of the definition of $M(2^r)$. 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.

In particular, the number of invariant $C$ is $d \cdot \prod_{p | d, p \text{ odd}} (1 + 1/p \pm \ldots) \cdot \alpha(v_2(d))$ where $\alpha_2$ is the function obtained in the last lemma, divided by $2^{v_2(d)}$ (for $m \geq 4$, $\alpha_2(m) = 1 + 1/8 + \ldots$; the dependance on the exponent, $m$, is tiny if $m$ is large).

Now to deal with $Z(132)(d)$, 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 lighter in the former case).

$S(\pi)(d)$ 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 $d = e^2x$. The equations are then
\[-a^2 + b \equiv 0 \mod e; \quad ay - b - y^2 \equiv 0 \mod x; \quad a^2y - ab - by + 1 \equiv 0 \mod ex.\]

Rewrite the third one as $(a^2 - b)y + 1 - ab \equiv 0 \mod ex$. Taking this modulo $e$, we obtain $ab \equiv 1 \mod e$, which in combination with the first, yields $a^3 \equiv 1 \mod e$ (and also $b^3 \equiv 1 \mod e$). Write $b = a^2 + ke$, where $k$ is defined modulo $x$. Plugging this into the second and third equations yields
\[-key + 1 - ab \equiv 0 \mod ex; \quad y^2 - ay + a^2 + ke \equiv 0 \mod x.\]

The former yields $-key - a^3 - ake + 1 \equiv 0 \mod ex$, so $ke(y + a) \equiv 1 - a^3 \mod ex$. Multiplying the second displayed equation by $y + a$ yields $ke(y + a) \equiv -(y^3 + a^3) \mod x$, whence $y^3 \equiv -1$.
mod $x$. Since $e|(ab - 1)$, we also have $-ky \equiv (1 - ab)/e \mod x$. In particular, if $x \neq 1$, then $k$ (and thus $b$) is uniquely determined by $y$ modulo $x$.

We recall from Lemma C.1 that $X^3 \pm 1 = 0$ each has three distinct solutions in $\mathbb{Z}_{p^m}$ iff $p \equiv 1 \mod 3$ or $9|p^m$, 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 $a = 0$, $y^3 \equiv -1 \mod p^m$, $b \equiv y^2 \mod p^m$ (so $b$ is determined by $y$), and by $y \equiv -1 \mod x$, but the last is a consequence of the second last.

If $p \equiv 2 \mod 3$ or $p^m = 3$, then $y^3 \equiv -1$ entails $y \equiv -1 \mod p^m$. Hence $b \equiv 1 \mod p^m$, so there is exactly one solution for $(a, b, y) = (0, 1, -1)$. If $p \equiv 1 \mod 3$ or $9|p^m$, 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 $a^3 \equiv 1 \mod p^n$, $y = 0$, and $b \equiv a^2 \mod p^n = ex$. Hence we obtain three solutions for $(a, y, b)$ if $p \equiv 1 \mod 3$ or $9|p^m$ (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 $a^3 \equiv 1 \mod p^n$, and we can write $b = a^2 + kp^n$ (where $k$ is defined modulo $p^r$). We also have $y^3 \equiv -1 \mod p^r$, that is, $(-y)^3 \equiv \mod p^r$.

If $p \equiv 2 \mod 3$, then $a = 1$ (defined modulo $p^n$) and $y = -1$ (defined modulo $p^r$), and thus $kp^n \equiv 1 + 1 + 1 \mod p^r$. 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 $p \equiv 1 \mod 3$ or $9|p^m$, 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 $\pm 1$) or invertible. But if $p|(y + a)$, as in the previous paragraph, we obtain $kp^n \equiv -(y^2 - ay + a^2) \mod p^r \equiv -3a^2 + pX \mod p^r$. 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 $p \equiv 1 \mod 3$ or $9|p^m$ and $y + a \neq 0 \mod p$, 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 $k(y + a) \equiv (1 - a^3)/e \mod p^r$ 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 $p \equiv 2 \mod 3$, there are zero solutions for $n, r > 0$, giving us a total of 1 solution (arising from $n = 0$) plus an additional 1 iff $m$ is even. So the formula is $H(m(p))$ (recall that $H(m)$ is 1 if $m$ is odd and 2 if $m$ is even).

If $p \equiv 1 \mod 3$, we obtain 3 solutions from the case $n = 0$ plus an additional 3 if $m$ is even ($r = 0$), plus $\sum_{1 \leq n < m/2} 6 = 6[(m - 1)/2]$. Here the formula is $6[(m(p) - 1)/2] + 3H(m(p))$. 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 $p \equiv 2 \mod 3$, then

$$S(132)(p^m) = 1 + 0 + H(m) - 1 = H(m).$$

If $p \equiv 1 \mod 3$, then

$$S(132)(p^m) = 3 + \sum_{1 \leq n < m/2} 6 + 3(H(m) - 1)$$

$$= 3 + 6\left(\frac{m - 1}{2}\right) + 3(H(m) - 1)$$

$$= \begin{cases} 3m + 3 & \text{if } m \text{ is even} \\ 3m & \text{if } m \text{ is odd}. \end{cases}$$
If \( p^m = 3 \), then
\[
S(132)(3) = 1.
\]

Finally, if \( p = 3 \) and \( m \geq 2 \),
\[
S(132)(3^m) = 3 + \sum_{1 \leq n < m/2} 6 + 3(H(m) - 1) + 1
\]
\[
= \begin{cases} 
3m + 4 & \text{if } m \text{ is even} \\
3m + 1 & \text{if } m \text{ is odd}.
\end{cases}
\]

We can combine these in one gigantic formula,
\[
S(132)(d) = 2 \left\lfloor \frac{d}{|p| \mod 3; m(p) \text{ even}} \right\rfloor, 3^{w(d)} \prod_{p|d, \ p \equiv 1 \mod 3} (m(p) + H(m(p)) - 1) \cdot \begin{cases} 
1 & \text{if } m(3) \leq 1 \\
3m(3) + 4 & \text{even } m(3) > 0 \\
3m(3) + 1 & \text{odd } m(3) > 1
\end{cases}
\]

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 is
\[
S(S_3)(d) = 2^{w(d)} \cdot \begin{cases} 
1 & \text{if } m(3) = 0 \\
\frac{m(3) + 1}{2} & \text{if } m(3) > 0.
\end{cases}
\]

where \( m(3) \) is the multiplicity of 3 in the prime factorization of \( d \). In particular, \( Z(123)(d) = Z(S_3)(d) \) iff \( d \) is a square all of whose prime divisors are congruent to 1 modulo 3, and in that case, their cardinality is \( 2^{w(d)} \).

Equation (1) at the beginning of this section now yields the number of \( PH \)-equivalence classes of \( C \in NS_3 \) with determinant \( \pm d \):
\[
PH(3, d) := \frac{(\phi * J_1)(d) + 3(P * M)(d) + 2S(132)(d)}{6}.
\]

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 C.4 and the formula for \( \phi * J_2 \) that \( (1 - 1/p^2)S(23)(p^m) \leq (\phi * J_2)(p^m)/p^m \), so \( S(23)(d)/(\phi * J_2(d) \leq \zeta(2)/d \). And similarly, \( S(132)(d) = o(d^{-2+\epsilon}) \cdot \phi * J_2(d) \). The number of \( PH \)-equivalence classes, \( PH(3, d) \) thus satisfies
\[
1 + \frac{3}{d} \leq \frac{PH(3, d)}{(\phi * J_2)(d)/6} \leq 1 + \frac{3\zeta(2)}{d} + o \left( \frac{1}{d^{2-\epsilon}} \right)
\]
for all \( \epsilon > 0 \). This of course more than verifies the Conjecture of Appendix B, when \( n = 3 \). The little oh term may be unnecessary.

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 \( d > 1 \) (the case of \( d = 1 \) is trivial), and consider the PH-equivalence classes having a 1-block size two terminal form. We perform operations within the ring \( \mathbb{Z}_d \). The third column of one of these terminal forms is

\[
\begin{pmatrix}
 a_1 \\
 a_2 \\
 d
\end{pmatrix},
\]

where the the ideal generated by \( \{a_1, a_2\} \) is \( \mathbb{Z}_d \) (when we regard \( a_i \) as elements of \( \mathbb{Z}_d \)), and \( 0 \leq a_i < d \) (when we regard \( a_i \) as integers).

Now we count the number of 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 \( w' : \mathbb{N} \to \mathbb{Z}^+ \); \( w'(d) \) is the number of distinct prime divisors of \( d \) that are congruent to 1 modulo 3.

**Case 1:** \( I(B) \cong \mathbb{Z}_d^2 \). 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 \( \mathbb{Z}_d^* \). The equivalence class of such a truncated column, renamed \( (x, y)^T \), is given by

\[
\left\{ \begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x^{-1} \\ -x^{-1}y \end{pmatrix}, \begin{pmatrix} -y^{-1} \\ -xy^{-1} \end{pmatrix}, \begin{pmatrix} y^{-1} \\ -xy^{-1} \end{pmatrix} \right\}.
\]

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 \( \alpha^3 = -1, \beta = -\alpha^2, \text{ and } \alpha \neq -1 \). To count the number of choices for \( \alpha \) (and \( \beta \)), we first observe that if \( p \) is a prime exceeding 3, then the equation \( z^3 = -1 \) has a solution other than \( -1 \) in \( \mathbb{Z}_p \) iff \( -3 \) is a square modulo \( p \), equivalently iff \( p \equiv 1 \mod 3 \), 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 \( d = 3^\nu(3) \cdot \prod_{p \in P} p^{\nu(p)} \cdot \prod_{q \in Q} q^{\nu(q)} \) 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

\[
\phi(d)^2 - 1 - (3\phi(d) - 3) - (3^{w'(d)+a} - 1) = \frac{1+3\phi(d)+2\cdot3^{w'(d)+a}}{6},
\]

where \(a = 0\) if \(m(3) \leq 1\), and \(1\) otherwise.

This is worth stating as a result on PH-equivalence classes.

PROPOSITION C.5 (Case 1) For \(d\) a fixed positive integer, the number of PH-equivalence classes of matrices \(B \in NS_3\) with \(|\det B| = d\) and \(|I(B)| = d^2\) 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 \(|I(B)| = |\det B|^2\) for \(B \in NS_3\), 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 \(I(B) \cong (Z_d)^2\)).

Case 2: Exactly one of \(\{a_1, a_2\}\) is invertible modulo \(d\). In this case, \(a_1 \not\equiv a_2 \mod d\). By 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 \(x \in Z_d^*\) and \(y \not\in Z_d^*\). The only possible equivalence classes with fewer than four elements are those with two, and this occurs iff \(x = x^{-1}\) and \(y = -x^{-1}y\); this reduces to \(x^2 = 1\) and \((1+x)y = 0\).

By Lemma C.2, the number of choices for \((x, y)\) is \(M(d)\).

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 the displayed expression. The number of solutions to \(x^2 = 1\) and \((1+x)y = 0\) for \((x, y) \in Z_d^* \times (Z_d \setminus Z_d^*)\) is thus

\[
N_2(d) := M(d) - \phi(d)
\]

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

\[
\frac{2\phi(d) \cdot (d - \phi(d)) - 2N_2(d)}{4} + N_2(d) = \frac{\phi(d) \cdot (d - \phi(d)) + N_2(d)}{2}.
\]

If \(d\) is odd, the expression simplifies; \(N_2(d) = d\left(\prod_{p|d}(1+p^{-m(p)}) - \prod_{p|d}(1-1/p)\right)\), and if \(d\) is also square-free, \(N_2(d)\) has the rather nice form, \(d\left(\prod_{p|d}(1+1/p) - \prod_{p|d}(1-1/p)\right)\).

PROPOSITION C.6 (Case 2) The number of PH-equivalence classes corresponding to case 2 is

\[
\frac{\phi(d) \cdot (d - \phi(d) - 1) + M(d)}{2}.
\]
Case two corresponds to all the situations in which \(|I(B)|\) contains a proper direct summand isomorphic to \(\mathbb{Z}_d\) but \(|I(B)| < d^2\), and some of the possibilities with \(I(B) \cong \mathbb{Z}_d\). The remainder are covered by case 3.

**Case 3:** Both \(a_1\) and \(a_2\) are nonunits in \(\mathbb{Z}_d\). Since \(B \in \mathcal{NS}_3\), we also have to have \(\gcd\{a_1,a_2,d\} = 1\), equivalently, that in \(\mathbb{Z}_d\), 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 \(\mathbb{Z}_d\)), each with \(\gcd\{x,d\}, \gcd\{y,d\} > 1\), and of course, \(1 \leq x, y \leq d - 1\) (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 \(\Omega\) of \(S\), write \(d_\Omega = \prod_{i\in\Omega} p_i^{m(i)}\) and \(D_\Omega = \prod_{i\in\Omega} p_i\). Thus \(d_\emptyset = D_\emptyset = 1\), \(d_S = d\), and \(D := D_S = \prod_{p|d} p\).

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) \(\Omega_i \neq \emptyset\)

(ii) \(\Omega_1 \cap \Omega_2 = \emptyset\)

(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 \((\Omega_1,\Omega_2)\), 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 \((\Omega_1,\Omega_2)\) is the product,

\[
\frac{d}{D_{\Omega_1}} \prod_{j \in \Omega_1^c} \left(1 - \frac{1}{p_j}\right) \cdot \frac{d}{D_{\Omega_2}} \prod_{j \in \Omega_2^c} \left(1 - \frac{1}{p_j}\right) = \frac{d^2}{D_{\Omega_1 \cup \Omega_2}} \cdot \prod_{p|d} \left(1 - \frac{1}{p}\right) \cdot \prod_{j \in \Omega_1^c \cap \Omega_2^c} \left(1 - \frac{1}{p_j}\right).
\]

Now let \(\Omega\) be a subset of \(S\), say with \(|\Omega| = s\); the number of ways of writing it as a disjoint union of \(\Omega_1\) and \(\Omega_2\) (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 \(f(x) = \prod_{p|d}(1 + x/(p - 1))\).
The total number of truncated columns is thus
\[
\phi(d)^2 \sum_{s=2}^{k} (2^s - 2) \sum_{|\Omega|=s} \frac{1}{\phi(D_{\Omega})} = \phi(d)^2 \left( 1 + \sum_{s=0}^{k} (2^s - 2) \sum_{|\Omega|=s} \frac{1}{\phi(D_{\Omega})} \right)
\]
\[
= \phi(d)^2 \left( 1 + f(2) - 2f(1) \right)
\]
\[
= \phi(d)^2 \left( 1 + \prod_{p|d} \left( 1 + \frac{2}{p-1} \right) - 2 \prod_{p|d} \left( 1 + \frac{1}{p-1} \right) \right)
\]
\[
= \phi(d)^2 \left( \prod_{p|d} (p+1) - 2 \prod_{p|d} p + \prod_{p|d} (p-1) \right)
\]
\[
= d\phi(d) \left( \prod_{p|d} \left( 1 + \frac{1}{p} \right) - 2 + \prod_{p|d} \left( 1 - \frac{1}{p} \right) \right)
\]

The number of equivalence classes for case three is half of this.

PROPOSITION C.7 (Case 3) The number of PH-equivalence classes of \(B \in \mathcal{NS}_3\) with \(|\det B| = d\) corresponding to case 3 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 \(d\) 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 \(\epsilon\), 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 \(d\) (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

\[
\lim_{j \to \infty} \frac{\text{number of case 3 PH-equivalence classes for } B \in \mathcal{NS}_3 \text{ with } |\det B| = d(j)}{d(j)^2} = \frac{1}{2\zeta(2)}.
\]

For case 2 with the same sequence, the number of PH-equivalence classes is asymptotic to \(\phi(d)d/2\), which is much smaller. With case 1, the number is about \(\phi^2(d)/6\), much 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 $I(B^{op}) \cong \mathbb{Z}_d$; however, there are also examples as part of case 2 with the same property (case 2 examples with $I(B^{op}) \cong \mathbb{Z}_d$ 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 C.8** 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 terminal form with 1-block size two.

**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.** Suppose $p < q$. Let $B' \in \mathcal{NS}_3$ be a terminal form for $B$; if it has 1-block size less than 2, then it must be of the form $(1 \times X \times D)$ where $D = \begin{pmatrix} * & 0 \\ 0 & q \end{pmatrix}$; since the form is terminal, the * entry must be zero (since $p \leq \gcd\{q,*\}$, and the latter is 1 if $0 < * < q$). Now 2.2 applies. 

Adding the results from case 1, case 2, and case 3 yields the next result, without referring to the general horrible formula (1).

**Proposition C.9** Suppose the positive integer $d$ is of one of the following forms, $d = p, 2p, pq$ where $p$ and $q$ are odd primes. Then the number of PH-equivalence classes of $B \in \mathcal{NS}_3$ such that $|\det B| = d$ is

$$
\begin{align*}
\frac{p^2 + 4p + 1 + 2 \cdot 3^{w'(p)}}{6} & \quad \text{if } d = p \\
\frac{2p^2 + 5p - 1 + 3^{w'(d)}}{3} & \quad \text{if } d = 2p \\
\frac{\phi(d)(3d - 2\phi(d) + 3) + 2 \cdot 3^{w'(d)}}{6} + d + 1 & \quad \text{if } d = pq,
\end{align*}
$$

where $w'(d)$ is the number of distinct prime divisors of $d$ that are congruent to 1 modulo 3.

Interestingly, the number of equivalence classes with $|\det B| = 2p$ is itself divisible by $p$ iff $p \equiv 2 \mod 3$. It would be really interesting if this could be proved without reference to the formula.

There is one more bit of low-hanging fruit.

**Proposition C.10** 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

$$
\frac{p^4 + p^3 + 2p^2 + p + 1 + 2 \cdot 3^{w'(d)}(1 + 3^{w'(d)})}{6} \quad \text{if } p = 2
$$

$$
\frac{7}{ } \quad \text{if } p \neq 2.
$$

**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 the latter, \((1, p, p)\). Then the terminal form must be

\[
B' := \begin{pmatrix} 1 & b_1 & b_2 \\ 0 & p & 0 \\ 0 & 0 & p \end{pmatrix},
\]

where \(1 \leq b_i < p\) 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 \(I(B_{\pi(i)})\) is \(\mathbb{Z}_p\), a trivial computation. Hence \(B'\) (and thus \(B\)) is not \(\phi\)-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 \(\phi\)-equivalent to a 1-block size two terminal form, with determinant \(p\), corresponding to case 1 of the latter class:

\[
B'^{op} = \begin{pmatrix} p & 0 & 0 \\ -b_1 & 1 & 0 \\ -b_2 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -b_2 \\ 0 & 1 & -b_2 \\ 0 & 0 & p \end{pmatrix}.
\]

(The \(\phi\)-equivalence was implemented by conjugation with the permutation matrix that transposes 1 and 3.) Thus \(^{op}\) implements a bijection between the current matrices and the matrices covered by case 1 for \(d = p\), and of course, this bijection preserves \(\phi\)-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 [ALPPT]. 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 [ALTPP] 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 C.8, there will be \(\phi\)-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 \(\prod_{p|d}(\phi * J_2)(p) = \prod_{p|d}(p^2 + p - 2) = \phi(d)d\prod_{p|d}(1 + 2/p)\). For \(\pi\) a transposition, by Lemma C.4, \(S(\pi)(d) = \prod_{p|d} S(\pi)(p) = d\prod_{p|d; p\neq 2}(1 + 1/p)\), and \(S(123)(d) = 3^{w'(d)}\). Thus for square-free \(d\),

\[
\mathcal{P}(3, d) = \frac{d\phi(d)\prod_{p|d}(1 + 2/p) + 3d\prod_{p|d; p\neq 2}(1 + 1/p) + 2 \cdot 3^{w'(d)}}{6}.
\]

(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 C.12 against Table 1 in [ALPPT] (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 $6^{-1} \phi(d) \prod_{p\mid d}(p + 2) \cdot (1 + O(1/d))$. 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 C.10).

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 4, the difference operator $\Delta$, defined by $\Delta f(x) = f(x + 1) - f(x)$.

**PROPOSITION C.11** Let $d$ be a square-free integer. The number of PH-equivalence classes of $C \in N\mathcal{S}_3$ with $|\det C| = d$ and $C$ is not equivalent to a terminal form with 1-block size two is

$$\frac{\phi(d)\Delta^3 f_d(-1)}{6},$$

where $f_d(x) = \prod_{p\mid d}(x + p)$.

The factor $\phi(d)$ likely arises from an action of $\mathbb{Z}_d^*$ on the equivalence classes, presumably $(b, y) \mapsto (b, y)z$ as $z$ varies over $\mathbb{Z}_d^*$ (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 $\sum_{p\mid d} 1/p$ is large, is $\prod_{p\mid d}(p + 2)$. We obtain that if $d(m)$ is a sequence of square-free integers such that $\sum_{p\mid d(m)} 1/p \to \infty$ as $m \to \infty$, then

$$\frac{|\{\text{PH-equivalence classes of } C \in N\mathcal{S}_3 \text{ with } |\det C| = d(m), \text{ no terminal form with 1-block size two}\}|}{|\{\text{PH-equivalence classes } C \in N\mathcal{S}_3, |\det C| = d(m), \text{ a terminal form 1-block size two}\}| \cdot \prod_{p\mid d(m)}(1 + 1/p)} \to \frac{1}{3^3}.$$

If $d$ is a product of one or two primes, then $\Delta^3 f_d(-1) = 0$, consistent with Proposition C.9. 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 $\mathbb{Z}_d^*$ is just that of $\mathbb{Z}_d^*$ on itself. For example, with $d = 30$, we take

$$C = \begin{pmatrix} 1 & 1 & 4 \\ 0 & 2 & 5 \\ 0 & 0 & 15 \end{pmatrix}; \quad C^\text{op} \sim \begin{pmatrix} 1 & 2 & 4 \\ 0 & 3 & 5 \\ 0 & 0 & 10 \end{pmatrix} := D.$$

Both are in terminal form, with $\{I(C); I(C_{\Omega(i)}) \cong (\mathbb{Z}_3; \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_2) \cong \{I(D); I(D_{\Omega(i)})\}$. Hence neither is PH-equivalent to a terminal form with 1-block size two. The 8 PH-equivalence classes of determinant $\pm 30$ matrices in $N\mathcal{S}_3$ 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.

It is also (now) easy to check that $C^\text{op}$ is not PH-equivalent to $C$. By calculating the ordered triples $(I(C_{\Omega(i)})$ and $(I(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).

**References**

[ALPPT] A Atanasov, C Lopez, A Perry, N Proudfoot, M Thaddeus, *Resolving toric varieties with Nash blow-ups*, preprint (year?).
[BeH] S Bezuglyi & D Handelman, *Measures on Cantor sets: the good, the ugly, the bad*, Trans Amer Math Soc (to appear).

[EHS] EG Effros, David Handelman, & Chao-Liang Shen, *Dimension groups and their affine representations*, Amer J Math 102 (1980) 385–407.

[ES] EG Effros & Chao-Liang Shen, *Dimension groups and finite difference equations*, J Operator Theory 2 (1979) 215–231.

[G] KR Goodearl, *Partially ordered abelian groups with interpolation*, Mathematical Surveys and Monographs, 20, American Mathematical Society, Providence RI, 1986.

[GH] KR Goodearl & David Handelman, *Metric completions of partially ordered abelian groups*, Indiana Univ J Math 29 (1980) 861–895.

[H] D Handelman, *Free rank n + 1 dense subgroups of \( \mathbb{R}^n \) and their endomorphisms*, J Funct Anal 46 (1982), no. 1, 1–27.

[H1] David Handelman, *Positive polynomials and product type actions of compact groups*, Mem Amer Math Soc 54 (1985), 320, xi+79 pp.

[H2] David Handelman, *Positive polynomials, convex integral polytopes, and a random walk problem*, Lecture Notes in Mathematics, 1282, Springer–Verlag, Berlin, 1987, xii+136 pp.

[HW] GH Hardy & EM Wright, *Theory of Numbers*, likely a pirated edition.

[L] G Landsberg, *ber eine Anzahlbestimmung und eine damit zusammenhangende Reihe*, J Reine Angew Math 111 (1893) 87–88.

[Ma] G Maze, *Natural density distribution of Hermite normal forms of integer matrices*, arXiv:1009.4826v2 (2011); to appear J Number Theory.

[MRW] G Maze, J Rosenthal, & U Wagner, *Natural density of rectangular unimodular integer matrices*, arXiv:1005.3967v2 (2010).

[M] P Moree, *Counting carefree couples*, http://arxiv.org/abs/math.NT/0510003 (2005).

[R] B Reznick, *Lattice point simplices*, Discrete Math 60 (1986), 219–242.

[R2] B Reznick, *Clean lattice tetrahedra*, http://de.arxiv.org/pdf/math/0606227.pdf

[TSCS] C Toressan, JE Strapasson, SIR Costa, RM Siquera, *Optimum commutative group codes*, ArXiv:1205.4067v2 (2013)

**Constants references**

- **Carefree constant** [M]: \[ \prod_p \left( 1 - \left( 2p - 1 \right)/p^3 \right) \]

- **Landau’s totient constant** [M]: \[ \zeta(2)\zeta(3)/\zeta(6) = \prod_p \left( 1 + 1/p(p - 1) \right) \]

Mathematics Department, University of Ottawa, Ottawa ON K1N 6N5, Canada; dehsg@uottawa.ca & droy@uottawa.ca