Morfismos, Vol. 21, No. 2, 2017, pp. 33–55

Enumeration of integer lattices by quotient group

Álvar Ibeas Martín

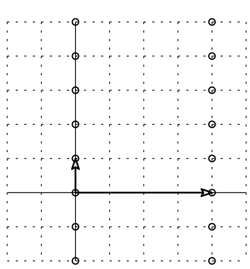
Abstract

Motivated by the enumeration of graph regular coverings, Kwak, Chun, and Lee gave a formula that counts the subgroups of a finitely generated free abelian group with a given finite quotient. This article examines that result from several viewpoints, providing an alternative proof with a plain combinatorial interpretation.

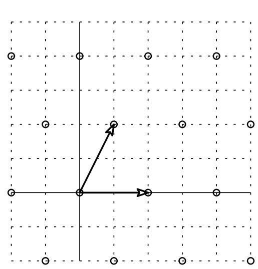
2010 Mathematics Subject Classification: 05E15, 20K27
Keywords and phrases: integer lattices, combinatorics

1 Introduction

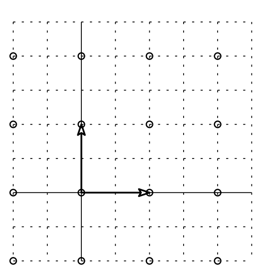
An *integer (point) lattice* in dimension r is a subgroup of the additive group $\mathbb{Z}^r$, equipped with the metric inherited from the Euclidean space $\mathbb{R}^r$. Such an object is conveniently set down by means of a *basis*: an integer matrix with r rows and linearly independent columns that generate the subgroup (elements of $\mathbb{Z}^r$ are treated as column vectors in this article). In symbols, if B is a d-column basis for lattice Λ, we have $\Lambda = B\mathbb{Z}^d = \{B\mathbf{v} \ : \ \mathbf{v} \in \mathbb{Z}^d\}$. We shall only consider full-dimensional lattices, i.e. those generated by square matrices. For example, here are three different lattices in $\mathbb{Z}^2$:



$\left[\begin{array}{c|c} 4 & 0 \\ 0 & 1 \end{array}\right]\mathbb{Z}^2$



$\left[\begin{array}{c|c} 2 & 1 \\ 0 & 2 \end{array}\right]\mathbb{Z}^2$



$\left[\begin{array}{c|c} 2 & 0 \\ 0 & 2 \end{array}\right]\mathbb{Z}^2$

Let us determine the quotient group (which must be abelian of order 4) for each of the three examples above. In the first two, a point in $\mathbb{Z}^2$ can be found whose order modulo the lattice is 4, so that the quotient is cyclic (C_4) in both cases. In contrast, the double of every point lies in the third lattice (which is indeed $2\mathbb{Z}^2$), so that the quotient is $C_2 \oplus C_2$ in this case (and in no other in dimension 2, see Lemma 4.1).

This paper focuses on the following enumeration problem: given a positive integer r and a finite abelian group G, how many lattices are there in dimension r whose quotient group is G? We look, therefore, for the cardinality of the set

$$\mathcal{L}_r(G) = \{\Lambda \subseteq \mathbb{Z}^r \ : \ \mathbb{Z}^r/\Lambda \cong G\}.$$

In other words, we are interested in counting lattices whose bases have a given Smith Normal Form. As the Euclidean metric is not relevant to this matter,[1] the problem can be phrased just in terms of subgroups of a finitely generated free abelian group.

The question above is settled by a theorem published by Kwak, Chun, and Lee [11, Thm. 3.4] and restated here as Theorem 5.2. These authors' aim was to enumerate graph regular coverings and used this result—put as the enumeration of connected coverings—as an intermediate step. Nevertheless, they have also pointed out [12, p. 125] the subgroup-enumerating reading of their study.

In spite of presenting such a plain statement, the mentions to the studied problem that we have found in the literature are scarce. This might be explained by the fact that Theorem 5.2 can be thought of as a straightforward corollary to the long-known result [5, 6, 19] which enumerates (through Equation (4)) subgroups of a given type in a finite abelian group. However, we have considered it worth to provide a detailed account of the topic.

Due to the structure properties of finite abelian groups, only finite abelian p-groups (i.e. with a prime-power order) need to be considered. These are conveniently described by means of integer partitions, as recalled in Section 3. Hence, the formula solving the addressed problem is parameterized by a positive integer r, a prime p, and an integer partition λ (with no more than r parts).

Delving further into that formula, we explore several ways to understand it. We start by analysing (in Section 6) a couple of special cases: when the quotient group is cyclic and when it is elementary abelian. In

[1] We will however turn to it to define dual lattices.

dimension 2, the cyclic case is enough to fully solve the problem; but this reduction is not extendable to an arbitrary dimension. When the quotient is an elementary abelian p-group, our problem is equivalent to finding subspaces of a vector space over a finite prime field.

Lattices with a given abelian p-group quotient can be recursively constructed drawing on the elementary abelian case. In this way, we contribute (in Section 7) an inductive proof for Theorem 5.2 which allows a combinatorial interpretation of its formula, according to which the sought lattices are classified as liftings of chains of subspaces in $(\mathbb{Z}/p\mathbb{Z})^r$ with dimensions prescribed by the quotient group.

Summing up, we count three approaches for proving the result we are dealing with. Apart from the interpretation sketched out in the previous paragraph, we have the original proof by Kwak, Chun, and Lee and the reduction to the subgroup-enumerating formula (4). In the closing section, the last two are presented in a unified fashion that boils down to the enumeration of epimorphisms from a finitely generated free abelian group to an abelian p-group.

2 Enumeration by volume

A characterization of a full-dimensional lattice Λ, alternative to the one given in the introduction, is that the quotient group is finite. In this case, the lattice *volume* is the index $[\mathbb{Z}^r : \Lambda]$. It equals the absolute value of the determinant of every lattice basis. This suggests the problem of counting $a_r(n)$, the number of integer lattices in $\mathbb{Z}^r$ with volume n [14, A128119, A160870].

When $r = 1$, there is exactly one lattice (namely, $n\mathbb{Z}$) for every volume n. When $r = 2$, $a_2(n) = \sigma(n)$, the sum of divisors of n. This can be proved describing a system of bases of lattices with volume n. To this end, since a lattice admits (infinitely) many bases, it will be useful to fix a canonical choice.

Two bases for the same lattice are related by a *unimodular matrix* (i.e. an integer matrix with an integer inverse), and conversely. In other words, a matrix is a basis of lattice $B\mathbb{Z}^r$ if and only if it is of the form BP, with $P \in \mathbb{Z}^{r\times r}$ and $|\det(P)| = 1$.

As a normalized basis, we adopt a variant of the Hermite form. Namely, an upper triangular matrix with nonnegative entries and positive diagonal elements (called *pivots*), each of them bigger than the rest of entries in its row. Now, the set of normalized bases for 2-dimensional lattices of volume n is

$$\left\{ \begin{pmatrix} d & b \\ 0 & n/d \end{pmatrix} \ :\ d \mid n, \quad 0 \leq b < d \right\}, \tag{1}$$

affording the statement $a_2(n) = \sigma(n)$.

The enumeration of normalized bases settles the question for arbitrary dimension as well. Namely, $a_r(n)$ can be expressed as the sum of $d_1^0 d_2^1 \cdots d_r^{r-1}$, extended over every factorization $n = d_1 \cdots d_r$ of the volume into r ordered factors: the pivots arranged from bottom to top. The following recursive expressions can be provided too:

$$a_r(n) = \sum_{d|n} \left(\frac{n}{d}\right)^{r-1} a_{r-1}(d) = \sum_{d|n} d \cdot a_{r-1}(d). \tag{2}$$

The first one is deduced from the observation that, in the Hermite Normal Form of a lattice with volume n, the bottom-right $(r-1) \times (r-1)$ block generates a lattice of volume d, for a certain divisor d of n. Moreover, the first pivot is n/d and every entry in the first row (shadowed in the left figure below) can take n/d different values. The other recurrence reflects the decomposition shown in the right figure, where each element on the shadowed column can take as many values as the corresponding pivot on the top-left block, and the pivot product is d (cf. [17, §63, Aufg. 13], [1, Appx. A]).

It can be proved from the expressions above that, for a fixed dimension, the amount of lattices of a given volume is a multiplicative function. As shown in the cited exercise from [17], as well as in [7, 20] (see also below),

$$a_r(p^e) = \begin{bmatrix} e+r-1 \\ e \end{bmatrix}_p \tag{3}$$

and the associated Dirichlet generating function is

$$\sum_{n \geq 1} \frac{a_r(n)}{n^s} = \zeta(s)\zeta(s-1)\cdots\zeta(s-r+1).$$

The bracket above stands for a Gaussian polynomial. Namely, we use the notation $[n]_p = 1+p+\cdots+p^{n-1} = \frac{p^n-1}{p-1}$, $[n]_p! = [n]_p[n-1]_p\cdots[2]_p$, $\left[{r \atop x_1,\ldots,x_{l+1}}\right]_p = \frac{[r]_p!}{[x_1]_p!\cdots[x_{l+1}]_p!}$ (where $r = x_1+\cdots+x_{l+1}$) for the p-analogue of multinomial coefficients, and $\left[{r \atop x}\right]_p = \left[{r \atop x,r-x}\right]_p$ for Gaussian polynomials. Note that the latter can be defined through any of the recurrences

$$\begin{bmatrix} x+y \\ x,y \end{bmatrix}_p = \sum_{i=0}^{x} p^i \begin{bmatrix} i+y-1 \\ i,y-1 \end{bmatrix}_p = \sum_{i=0}^{x} p^{(x-i)y} \begin{bmatrix} i+y-1 \\ i,y-1 \end{bmatrix}_p (\text{if } y>0)$$

and the boundary conditions $\left[{x \atop x,0}\right]_p = \left[{y \atop 0,y}\right]_p = 1$. Therefore, (3) follows from any of the recurrences in (2) and the boundary conditions $a_r(p^0) = a_1(p^e) = 1$.

Our aim is studying the refined enumeration of lattices by their quotient group. For instance, the three examples listed in the introduction lie among the $7 = \sigma(4)$ two-dimensional lattices with volume 4. As we have already pointed out, all of the seven give a cyclic quotient except the third example (see Figure 3). Let us recall some facts about the kind of groups that we will come across as quotients.

3 Finite abelian groups

There are two standard structure results for finite abelian groups. On the one hand, every such an object can be uniquely decomposed as the direct sum of cyclic groups $C_{d_1} \oplus \cdots \oplus C_{d_l}$ such that $1 < d_l \mid \cdots \mid d_1$. The orders of these components are called *invariant factors*. If B is a basis of a lattice $\Lambda \subseteq \mathbb{Z}^r$ such that $\mathbb{Z}^r/\Lambda$ has an invariant factor decomposition as above, there exist unimodular matrices P, Q such that $PBQ = \operatorname{diag}(d_1, \ldots, d_l, \underbrace{1, \ldots, 1}_{r-l})$, the *Smith Normal Form* of B.

On the other hand, a finite abelian group can be written as the direct sum of abelian groups with a prime-power order (i.e. finite abelian p-groups). It is sufficient to take these into account for the sake of the enumeration dealt with in this article (see Lemma 5.1). As for these components, every finite abelian p-group is itself (in a unique way, except for the ordering) the direct sum of cyclic groups $C_{p^{\lambda_i}}$. For every occurring exponent λ_i, let x_i be the number of copies present in the decomposition. Thus, every finite abelian group takes the form

$$\bigoplus_p G_p(\lambda), \quad \text{where } G_p(\lambda) = C_{p^{\lambda_1}}^{x_1} \oplus \cdots \oplus C_{p^{\lambda_l}}^{x_l}.$$

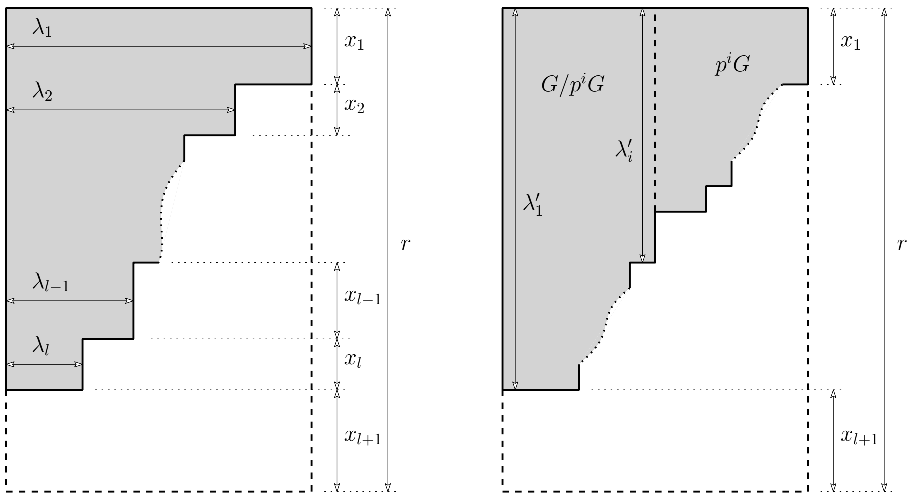


Figure 1: Partition $(\lambda; r) = (\lambda_1^{x_1}, \ldots, \lambda_l^{x_l}, 0^{x_{l+1}})$

Arranging the set of occurring exponents in the decreasing order ($\lambda_1 > \cdots > \lambda_l > 0$) leads to the identification of a finite abelian p-group with its *type*: the integer partition $\lambda = (\lambda_1^{x_1}, \ldots, \lambda_l^{x_l})$, written here in exponential notation. A partition is conveniently displayed by means of its associated Young diagram (see Figure 1).

The order of $G_p(\lambda)$ is p to the power of the partition's size: $|\lambda| = \sum x_i\lambda_i$. On the other hand, every minimal system of generators of $G_p(\lambda)$ has $\mathrm{len}(\lambda) = \sum x_i$ elements.[2] Recall that we are interested in groups arising from a quotient of $\mathbb{Z}^r$, which have therefore a system of r generators. This provides the constraint $\mathrm{len}(\lambda) \leq r$ for $\mathcal{L}_r(G_p(\lambda))$ to be nonempty. Indeed, we will find it convenient to add x_{l+1} empty parts to λ, so that $\mathrm{len}(\lambda) + x_{l+1} = r$, as depicted in the figure, using the notation $(\lambda; r) = (\lambda_1^{x_1}, \ldots, \lambda_l^{x_l}, 0^{x_{l+1}})$ for the resulting object.

Cyclic groups (of prime-power order) are associated with one-part partitions. The other degenerate case is constituted by groups where the order of every nonzero element is p (i.e. *elementary abelian groups*), which are associated with one-column partitions (1^x) and can be identified with vector spaces over the field $\mathbb{Z}/p\mathbb{Z}$. For an arbitrary partition λ, setting $G = G_p(\lambda)$, its first column (associated with the group $C_p^{\mathrm{len}(\lambda)}$)

[2]This follows from Burnside Basis Theorem. In the general case of a finite abelian group, there exist minimal systems of generators whose cardinality is any of the numbers in the range $[\max(\mathrm{len}(\lambda)), \sum \mathrm{len}(\lambda)]$, where the maximum and the sum are extended over the partitions associated with the different primary components.

can be thought of as G/pG (the quotient of G by its Frattini subgroup) or as the subgroup consisting of zero and the elements of order p (the group *socle*). In general, G/p^iG is a p-group associated with the partition composed by the first i columns of λ. Analogously, p^iG matches the last $\lambda_1 - i$ columns. The column lengths in the Young diagram constitute the parts of the *conjugate partition* $(\lambda'_1, \ldots, \lambda'_{\lambda_1})$.[3] We have

$$\lambda'_i = \dim_{(\mathbb{Z}/p\mathbb{Z})} \frac{p^{i-1}G_p(\lambda)}{p^iG_p(\lambda)}.$$

(Note that these quotient groups are elementary abelian.) In particular, $\lambda'_1 = \mathrm{len}(\lambda)$. The group $G_p(\mu)$ admits a subgroup of type λ if and only if the partition λ "fits" into μ, i.e. $\lambda \leq \mu$ part-wise. If this is the case, the number of occurring subgroups is (see [3, Lemma 1.4.1])

$$\prod_{j\geq 1} p^{\lambda'_{j+1}(\mu'_j - \lambda'_j)} \begin{bmatrix} \mu'_j - \lambda'_{j+1} \\ \lambda'_j - \lambda'_{j+1} \end{bmatrix}_p . \tag{4}$$

Every quotient of a finite abelian group can be regarded as a subgroup of it. This derives from the identification of G with the (isomorphic) dual group $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$. In this way, a duality is established between subgroups of G, linking S with $\widehat{G/S} = \{\xi \in \widehat{G} \mid \xi(S) = 0\} \subseteq \widehat{G}$ (see [2], [13, II.(1.5)]). The set of subgroups of a finite abelian group is, then, a self-dual poset.

If G is a finite abelian p-group, the *cotype* of a subgroup S is defined as the type of the quotient G/S. For example, in Figure 2, the 4-cyclic subgroup $\langle 2x \rangle$ has cotype $(1, 1)$, whereas the subgroup $\langle 2x+y \rangle$ (4-cyclic as well) is self-dual (its cotype is (2)).

Even though the type of a subgroup does not necessarily determine its cotype, the formula in (4) also counts—by virtue of the duality—subgroups of $G_p(\mu)$ with cotype λ. In Section 5, we see how that formula quickly solves the problem studied in this paper.

4 A lattice lattice

This ill-sounding heading reflects the double meaning in Mathematics of the term *lattice*. Throughout the paper, we are using it to denote

[3] We find it useful to assign different indices to these parts, disregarding whether some of them are equal, in contrast to those of λ, which we have indexed by blocks.

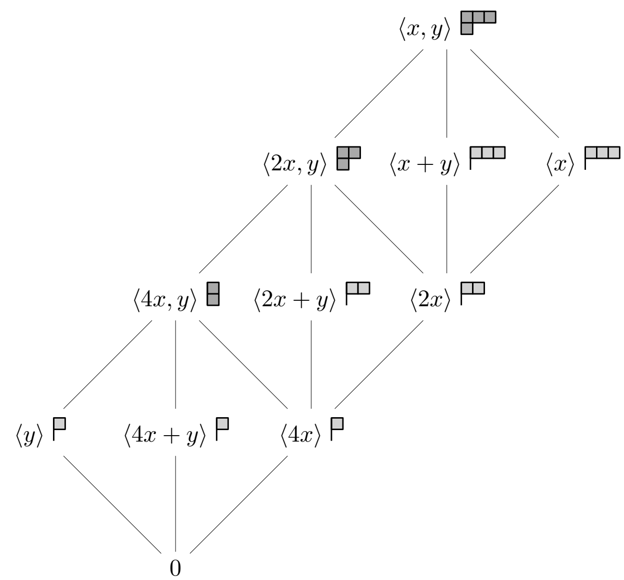


Figure 2: Subgroups of $C_8 \oplus C_2 = \langle x, y \mid 8x = 2y = 0\rangle$

the objects studied by the Geometry of Numbers. However, it more commonly refers to a poset-related concept [18, Sec. 3.3].

In this section, we employ the term in both ways, taking a glance at the interplay between the set of studied lattices and the set of finite abelian groups. This may complete the picture of the proof for the enumeration result given in the following section.

We consider the poset of lattices in dimension r, ordered by reverse inclusion. In general, it will be sufficient to deal with the restriction to lattices with a p-group quotient (see, for instance, Figure 3).

That poset is a lattice. Indeed, the intersection of two subgroups of $\mathbb{Z}^r$ is their *join* as poset elements, and the lattice sum corresponds to the *meet* operator:

$$\Lambda_1 \vee \Lambda_2 = \Lambda_1 \cap \Lambda_2, \quad \Lambda_1 \wedge \Lambda_2 = \Lambda_1 + \Lambda_2.$$

The poset is infinite and has a zero (namely, $\mathbb{Z}^r$). Note that, for a fixed lattice $\Lambda \subseteq \mathbb{Z}^r$, there is a natural bijection between its superlattices and the subgroups of $\mathbb{Z}^r/\Lambda$. In this way, every principal order ideal (the superlattices of an element) and, more generally, every poset interval corresponds to the lattice of subgroups of a finite abelian group.

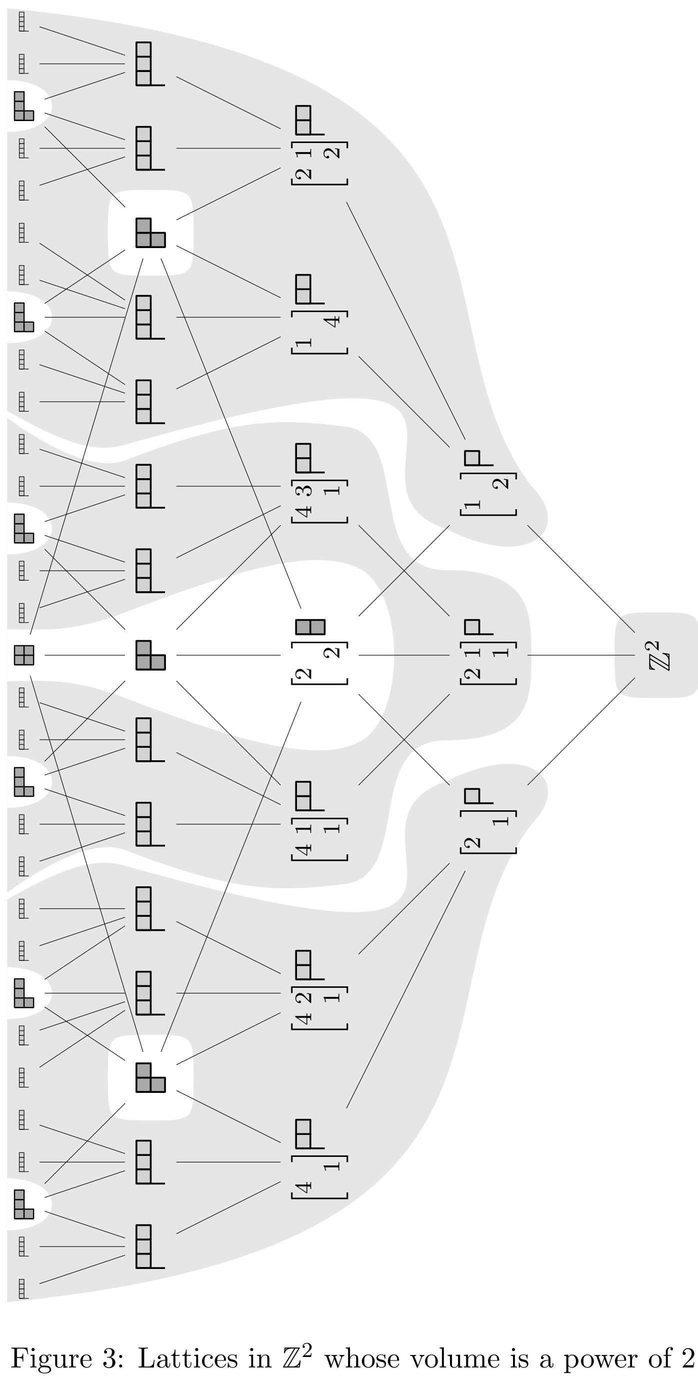


Figure 3: Lattices in $\mathbb{Z}^2$ whose volume is a power of 2

For instance, the lattice of Figure 2 matches six principal ideals from Figure 3. On the other hand, the subposet conformed by the sublattices of an element (a principal filter) is isomorphic to the whole poset.

When restricted to lattices whose volume is a power of a prime p, every element is covered by $[r]_p = 1 + p + \cdots + p^{r-1}$ sublattices. Taking the type of the quotient groups makes our poset collapse onto a subposet of the *Young lattice*, including only partitions with no more than r parts.

In the general case, if two lattices have the same quotient group, they are indistinguishable as poset elements. Indeed, two such lattices admit bases (B_1, B_2) related by a unimodular change of coordinates: $B_1 = PB_2$, with $|\det(P)| = 1$. Note that P is an automorphism of $\mathbb{Z}^r$ and induces an automorphism on the studied poset.

According to next result, a lattice in $\mathbb{Z}^r$ is a characteristic subgroup if and only if it is of the form $n\mathbb{Z}^r$, for a positive integer n.

Lemma 4.1. *Let r be a positive integer. Then, $|\mathcal{L}_r(G)| = 1$ if and only if G is trivial or has r equal invariant factors. In particular, if G is a finite abelian p-group, $|\mathcal{L}_r(G)| = 1$ if and only if G is associated to a partition with r equal (possibly empty) parts.*

Proof. Let n be a positive integer (including the case $n = 1$). If Λ is a lattice in dimension r such that $\mathbb{Z}^r/\Lambda \cong C_n^r$, the order of every integer vector modulo Λ divides n, so that $n\mathbb{Z}^r \subseteq \Lambda$ (and both lattices coincide, since $\mathbb{Z}^r/n\mathbb{Z}^r \cong C_n^r$). Hence, $|\mathcal{L}_r(C_n^r)| = 1$.

Alternatively, if B is a basis for a lattice with quotient group C_n^r, there exist unimodular matrices P and Q such that $PBQ = nI_r \Rightarrow BQ = P^{-1}nI_r = nI_rP^{-1}$, so that the lattice generated by B is $n\mathbb{Z}^r$.

In order to prove the converse, let G be a finite (r or less)-generated abelian group not under the hypothesis. We consider the invariant factor decomposition of G, completed with trivial groups, if necessary, up to r factors:

$$G = C_{d_1} \oplus \cdots \oplus C_{d_r}, \quad d_r \mid \cdots \mid d_1.$$

There must be at least two different factors $d_i \neq d_j$. Then, the lattices spanned by bases $\operatorname{diag}(\ldots, d_i, \ldots, d_j, \ldots)$ and $\operatorname{diag}(\ldots, d_j, \ldots, d_i, \ldots)$ are different and give both G as quotient group. □

5 Enumeration by quotient

Our goal is enumerating $\mathcal{L}_r(G)$, the set of subgroups of $\mathbb{Z}^r$ whose quotient is G, keeping in mind that only finite abelian (r or less)-generated parameters G need to be taken into account.

The problem is trivial in dimension 1: the quotient group of $\mathbb{Z}$ by the only lattice of volume n (i.e. $n\mathbb{Z}$) is cyclic. For dimension 2, there is a neat solution as well (the picture provided by Rutherford [16] is correct in dimension 2). On the one hand, for a cyclic quotient, $|\mathcal{L}_2(C_n)| = \psi(n)$, the Dedekind ψ function [14, A001615], i.e. the sum of the divisors of n whose codivisor is squarefree. Indeed, the Smith Normal Form of a basis in (1) is the diagonal $(n, 1)$ if and only if $\gcd(d, b, n/d) = 1$, so that $|\mathcal{L}_2(C_n)|$ equals the cardinality of the set A below. Those matrices can be classified according to the squarefree kernel of n/d. We recall that the squarefree kernel, written $\mathrm{rad}(m)$, of a positive integer m is the largest squarefree integer dividing m. It is also the product of all the different prime divisors of m. The following map is a bijection from A to a set readily enumerated by $\psi(n)$.

$$A = \left\{ \begin{pmatrix} d & b \\ 0 & n/d \end{pmatrix} \ : \ d \mid n, \quad 0 \le b < d, \quad \gcd(d, b, n/d) = 1 \right\}$$

$$B = \left\{ \begin{pmatrix} d & b \\ 0 & n/d \end{pmatrix} \ : \ d \mid n, \quad 0 \le b < d, \quad n/d \text{ squarefree} \right\}$$

$$\begin{array}{ccc} A & \longrightarrow & B \\ \begin{pmatrix} d & b \\ 0 & n/d \end{pmatrix} & \mapsto & \begin{pmatrix} \frac{n}{\mathrm{rad}(n/d)} & \frac{b \cdot n/d}{\mathrm{rad}(n/d)} \\ 0 & \mathrm{rad}(n/d) \end{pmatrix} \end{array}$$

On the other hand, if $d \mid n$, we have $|\mathcal{L}_2(C_n \oplus C_d)| = |\mathcal{L}_2(C_{n/d})| = \psi(n/d)$, after the bijection that maps a lattice $\Lambda \in \mathcal{L}_2(C_n \oplus C_d)$ to $\frac{1}{d}\Lambda$. This reduction to the cyclic case cannot be extended to higher dimensions, apart from the full-column removal considered in Section 9.

Before proceeding to arbitrary dimension, we notice that, as announced, the problem can be reduced to p-groups. The enumeration by volume studied in Section 2 is solved by a multiplicative function ($a_r(uv) = a_r(u)a_r(v)$, for coprime u and v). As for the enumeration by quotient, we can rely on the following property (cf. [11, Thm. 2.7]).

Lemma 5.1. *Let G_1, G_2 be two finite abelian groups with coprime orders. Then,*

$$|\mathcal{L}_r(G_1 \oplus G_2)| = |\mathcal{L}_r(G_1)| \cdot |\mathcal{L}_r(G_2)|.$$

Proof. We draw on the bijection between superlattices of a lattice Λ and subgroups of $\mathbb{Z}^r/\Lambda$. Among the subgroups of $G_1 \oplus G_2$, there are unique copies of G_1 and G_2.

As a consequence, every element of $\mathcal{L}_r(G_1 \oplus G_2)$ can be expressed in exactly one way as the intersection of a pair of lattices in $\mathcal{L}_r(G_1) \times \mathcal{L}_r(G_2)$; conversely, every such intersection has quotient $G_1 \oplus G_2$. $\square$

With this result in mind, in order to enumerate lattices by quotient in arbitrary dimension, we restate a result proved by Kwak, Chun, and Lee [11, Thm. 3.4] (see also [12, Thm. 13]) under a different language.

Theorem 5.2. *Let p be a prime number, r a positive integer, and λ a partition with no more than r parts. Let $x_1, \ldots, x_l$ be the part multiplicities, so that $len(\lambda) = \sum x_i$, and $x_{l+1} = r - len(\lambda)$. Then, the number of lattices in $\mathbb{Z}^r$ whose quotient is a p-group of type λ is*

$$|\mathcal{L}_r(G_p(\lambda))| = p^{c(\lambda;r)} \begin{bmatrix} r \\ x_1, \ldots, x_l, x_{l+1} \end{bmatrix}_p,$$

where, writing $(\lambda'_1, \ldots, \lambda'_{\lambda_1})$ for the conjugate partition (the columns in the associated Young diagram), $c(\lambda; r)$ equals $\sum_{i=1}^{\lambda_1 - 1} (r - \lambda'_i)\lambda'_{i+1}$.

Writing $\lambda^{(i)}$ for the partition obtained from the first $x_1 + \cdots + x_i$ parts of λ, with λ_{i+1} units removed from each (see Figure 4), the exponent above can also be expressed as $c(\lambda; r) = \sum_{i=1}^{l} x_{i+1}(|\lambda^{(i)}| - \text{len}(\lambda^{(i)}))$.

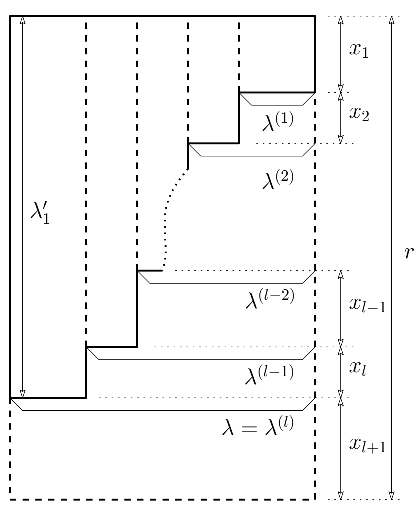


Figure 4: Partition $(\lambda; r) = (\lambda_1^{x_1}, \ldots, \lambda_l^{x_l}, 0^{x_{l+1}})$

In the following three sections, we set our focus into a proof which provides a natural interpretation for the theorem formula. Below, we show instead how the result can be considered a particular case of Equation (4). In this way, the theorem is handily proved, after paying the toll of turning to that enumeration result.

We recall again the bijection between superlattices of $\Lambda \subseteq \mathbb{Z}^r$ and subgroups of $\mathbb{Z}^r/\Lambda$. Among the latter, those with a certain type (or cotype) are enumerated through Equation (4), but we are not interested (in principle) in counting superlattices of a fixed lattice. However, in our setting (counting lattices with a fixed quotient), it turns out that there is a sublattice common to every sought lattice and it presents a simple quotient group.

Proof of Theorem 5.2. Partition λ is "contained" into (λ_1^r), so $C^r_{p^{\lambda_1}}$ has a subgroup isomorphic to $G_p(\lambda)$. Therefore, there exists $\Lambda \in \mathcal{L}_r(G_p(\lambda))$ such that $p^{\lambda_1}\mathbb{Z}^r \subseteq \Lambda \subseteq \mathbb{Z}^r$.

As pointed out in the previous section, elements with the same quotient group play an identical role in the poset of lattices. Any other element $\Lambda' \in \mathcal{L}_r(G_p(\lambda))$ must then contain a sublattice with quotient group $C^r_{p^{\lambda_1}}$. After Lemma 4.1, that lattice is unique, so $p^{\lambda_1}\mathbb{Z}^r$ is a sublattice common to every element of $\mathcal{L}_r(G_p(\lambda))$. In other words, the searched for lattices are all superlattices $\Lambda \supseteq p^{\lambda_1}\mathbb{Z}^r$ with $\mathbb{Z}^r/\Lambda \cong G_p(\lambda)$. Setting $\mu'_j = r$ for $j = 1, \ldots, \lambda_1$, Equation (4) proves the result. $\square$

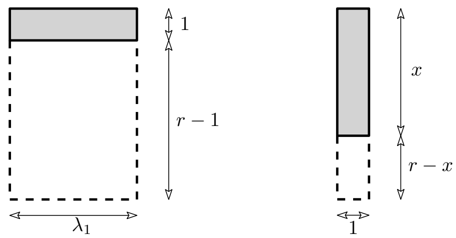
Notice that the common sublattice used in the prove above is just the join of the elements in $\mathcal{L}_r(G_p(\lambda))$—a finite set, since $a_r(p^{|\lambda|})$ is finite—, i.e. their intersection. We have seen that $p^{\lambda_1}\mathbb{Z}^r \subseteq \bigcap\{\Lambda \in \mathcal{L}_r(G_p(\lambda))\}$. Conversely, that intersection must be the only lattice with its quotient group (if there were another, this would be contained in every element of $\mathcal{L}_r(G_p(\lambda))$ as well). Then, after Lemma 4.1, the intersection's quotient group is associated to a partition with r equal parts.

6 Elementary abelian case

Let us consider the specialization of Theorem 5.2 in degenerate cases of the partition λ. Firstly, when the quotient group is cyclic—i.e. one-row partitions—we get [14, A263950]

$$c(\lambda_1, 0^{r-1}) = (r-1)(\lambda_1 - 1), \quad |\mathcal{L}_r(C_{p^{\lambda_1}})| = p^{(r-1)(\lambda_1-1)}[r]_p. \tag{5}$$

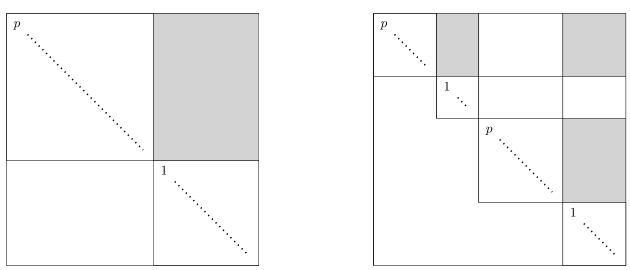
Note that, in dimension 2, $|\mathcal{L}_2(C_{p^{\lambda_1}})| = p^{\lambda_1-1}(1+p) = \psi(p^{\lambda_1})$.



The case of a one-column partition is of particular interest, since it constitutes the basis for the inductive proof presented in Section 7. We have $c(1^x, 0^{r-x}) = 0$, so that Theorem 5.2 is reduced to $|\mathcal{L}_r(C_p^x)| = \begin{bmatrix} r \\ x \end{bmatrix}_p$, a coefficient which is known to enumerate subspaces of $(\mathbb{Z}/p\mathbb{Z})^r$ with dimension x (as well as those with dimension $r - x$).

The componentwise projection from $\mathbb{Z}^r$ onto $(\mathbb{Z}/p\mathbb{Z})^r$, to which we come back in the next section, yields a bijection between subspaces of $(\mathbb{Z}/p\mathbb{Z})^r$ and lattices with a p-elementary quotient.

Let us characterize normalized bases of such lattices. The diagonal is a permutation σ of the multiset $\{1^{r-x}, p^x\}$ and an entry above the diagonal is zero if its row's diagonal element is 1 or if its column's diagonal element is p. In other case (shadowed regions in the figure below), the entry can take any value from 0 to $p - 1$.



The number of nondiagonal entries that can take nonzero values is the number of inversions of σ. Hence, these matrices add up to

$$\sum_{\sigma \in \mathfrak{S}(\{1^{r-x}, p^x\})} p^{\mathrm{inv}(\sigma)} = \begin{bmatrix} r \\ x \end{bmatrix}_p,$$

after Carlitz summation formula [4], [18, Prop. 1.3.17]. Incidentally, note the following identity, which we fail to top off with a suitable bijection:

$$|\mathcal{L}_r(C_p^x)| = a_{r-x+1}(p^x) = a_{x+1}(p^{r-x}).$$

7 Subspace chain liftings

In this article, we intend to stress the combinatorial interpretation presented below for the formula of Theorem 5.2, providing thus an alternative proof. That formula involves two parts: a p-multinomial coefficient and a power of p. The former can be factorized as

$$\begin{bmatrix} r \\ x_1, \dots, x_{l+1} \end{bmatrix}_p = \begin{bmatrix} x_l + x_{l+1} \\ x_{l+1} \end{bmatrix}_p \cdots \begin{bmatrix} r - \operatorname{len}(\lambda^{(i-1)}) \\ r - \operatorname{len}(\lambda^{(i)}) \end{bmatrix}_p \cdots \begin{bmatrix} r \\ r - x_1 \end{bmatrix}_p,$$

showing that it enumerates subspace chains of the form

$$V_l \lneq \cdots \lneq V_1 \lneq V_0 = (\mathbb{Z}/p\mathbb{Z})^r, \quad \dim(V_i) = r - \operatorname{len}(\lambda^{(i)}). \tag{6}$$

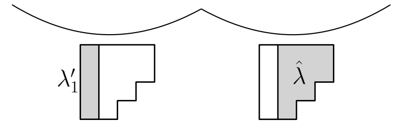
The componentwise projection $\pi : \mathbb{Z}^r \longrightarrow (\mathbb{Z}/p\mathbb{Z})^r$ relates lattices and vector spaces by means of a monotone Galois connection. As we have already pointed out, it induces a bijection between $(\mathbb{Z}/p\mathbb{Z})$-spaces of codimension x and lattices with an elementary abelian quotient C_p^x (joins of x atoms in the poset of Figure 3). Any $(\mathbb{Z}/p\mathbb{Z})$-vector space V satisfies $V = \pi(\pi^{-1}(V))$.

For a lattice Λ, we have $\Lambda \subseteq \pi^{-1}(\pi(\Lambda))$. The latter is a lattice with a p-elementary quotient; moreover, it is contained in every lattice that contains Λ and has a p-elementary quotient.

Therefore, if $\Lambda_1 \subseteq \Lambda_2$ are two lattices whose volume is a power of p and their respective quotients are associated to partitions λ_1 and λ_2, we have $\pi(\Lambda_1) = \pi(\Lambda_2)$ if and only if $\operatorname{len}(\lambda_1) = \operatorname{len}(\lambda_2)$. Hence, that projection is a vector space of dimension $r - \operatorname{len}(\lambda)$. In Figure 3, lattices are divided into five classes, according to which of the five vector subspaces of $(\mathbb{Z}/2\mathbb{Z})^2$ they project onto.

For $\Lambda \in \mathcal{L}_r(G_p(\lambda))$, let us build a lattice chain projecting to the vector spaces in (6). As a first step, we set up a superlattice whose quotient group is $pG_p(\lambda) \cong G_p(\hat{\lambda})$, where $\hat{\lambda}$ is the partition obtained by removing the leftmost column from λ.

$$\Lambda \subseteq \underset{\displaystyle p^{-1}\Lambda \cap \mathbb{Z}^r}{\overset{\|}{\{\mathbf{x} \in \mathbb{Z}^r : p\mathbf{x} \in \Lambda\}}} \subseteq \mathbb{Z}^r$$



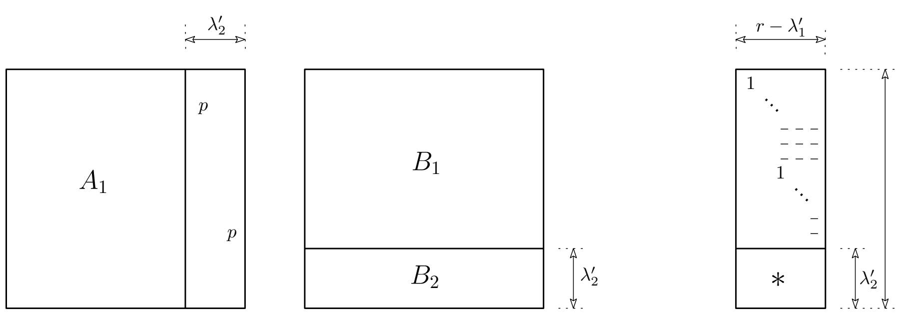
That is achieved by appending to Λ those integer vectors whose order in the quotient group is p. Iterating the process, the following chain is reached (refer to (8) for a couple of examples):

$$\Lambda \subsetneq p^{-1}\Lambda \cap \mathbb{Z}^r \subsetneq p^{-2}\Lambda \cap \mathbb{Z}^r \subsetneq \cdots \subsetneq p^{1-\lambda_1}\Lambda \cap \mathbb{Z}^r \subsetneq \mathbb{Z}^r. \tag{7}$$

This recursive technique of trimming partition columns from the left, building on the simple case of elementary abelian groups, is common in relevant literature. The following result, inspired by a memoir of Butler [3], adapts to our problem the concept of fibre count per subspace chain and provides, in this manner, a natural interpretation of Theorem 5.2.

Proposition 7.1. *Let p be a prime number, r a positive integer, and λ a partition with no more than r parts. For every subspace chain as in (6), there are exactly $p^{c(\lambda;r)}$ lattices Λ with a p-power volume such that, for $i = 0, 1, \ldots, \lambda_1$, $\pi(p^{-i}\Lambda \cap \mathbb{Z}^r) = V_j$, where $j \leq l$ is the maximum index satisfying $i < \lambda_j$ (and $j = 0$, if $i = \lambda_1$). The quotient of $\mathbb{Z}^r$ by each of these lattices is $G_p(\lambda)$.*

Proof. We use induction on λ_1. If λ is empty, the subspace chain is reduced to $V_0 = (\mathbb{Z}/p\mathbb{Z})^r$, and the only lattice with a p-power volume that projects onto it is $\mathbb{Z}^r$. In other case, the induction hypothesis shows that there are $p^{c(\hat{\lambda};r)}$ possibilities for $\hat{\Lambda} = p^{-1}\Lambda \cap \mathbb{Z}^r$. For each of these, $\mathbb{Z}^r/\hat{\Lambda} \cong G_p(\hat{\lambda})$. Now, candidates for Λ are sublattices of $\hat{\Lambda}$ such that $\mathbb{Z}^r/\Lambda$ is a p-group whose type is $\hat{\lambda}$ plus a column attached on the left. The condition $\pi(\Lambda) = V_l$ implies $\hat{\Lambda}/\Lambda \cong C_p^{\lambda'_1}$, and is enough to guarantee $\Lambda \in \mathcal{L}_r(G_p(\lambda))$.



If A is a basis for $\hat{\Lambda}$, any basis of any sublattice takes the form AB, for a certain square matrix B. Basis A can be taken with its last

$\lambda'_2 = \mathrm{len}(\hat{\lambda})$ columns in $p\mathbb{Z}$, the first ones describing a $(\mathbb{Z}/p\mathbb{Z})$-basis of $\pi(\hat{\Lambda})$. Then, with the notation from the figure, $\pi(AB\mathbb{Z}^r)$ is spanned by the columns of A_1B_1.

The condition on $\hat{\Lambda}/\Lambda$ is equivalent to $B\mathbb{Z}^r \in \mathcal{L}_r(C_p^{\lambda'_1})$. In this way, projection π identifies the choices for $B\mathbb{Z}^r$ with $(r-\lambda'_1)$-dimensional subspaces of $(\mathbb{Z}/p\mathbb{Z})^r$. The projection of B_1 is determined by V_l. Therefore, the sought sublattices are in bijection with vector spaces of dimension $r-\lambda'_1$ with the projection onto the first $r-\lambda'_2$ components fixed. They are in number $p^{(r-\lambda'_1)\lambda'_2}$, then. Finally, note that $c(\lambda;p) = c(\hat{\lambda};p) + (r-\lambda'_1)\lambda'_2$. $\square$

8 Examples

Let $r=3$, $p=2$, and $\lambda=(2,1)$. The number of subspace chains of dimensions 1 and 2 in $(\mathbb{Z}/p\mathbb{Z})^3$ is $[3]_2[2]_2 = 21$. For each of these, there are two lattices (since $c(2,1,0)=1$) in $\mathbb{Z}^3$ with quotient group $C_4 \oplus C_2$, bases for which share a cell in Table 1. For instance, for the last two lattices listed, the superlattice sequences described in (7) are

(8)
$$\begin{pmatrix} 4 & 2 & 1 \\ & 2 & 1 \\ & & 1 \end{pmatrix} \mathbb{Z}^3 \subsetneq \begin{pmatrix} 2 & 1 & \\ & 1 & \\ & & 1 \end{pmatrix} \mathbb{Z}^3, \qquad \begin{pmatrix} 4 & 2 & 3 \\ & 2 & 1 \\ & & 1 \end{pmatrix} \mathbb{Z}^3 \subsetneq \begin{pmatrix} 2 & 1 & \\ & 1 & \\ & & 1 \end{pmatrix} \mathbb{Z}^3.$$

Those are the two lattices projecting to the subspace chain

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} (\mathbb{Z}/2\mathbb{Z}) \lneq \begin{pmatrix} 1 & \\ 1 & \\ & 1 \end{pmatrix} (\mathbb{Z}/2\mathbb{Z})^2.$$

Recovering the poset of Figure 3, let us count the sublattices of $\mathbb{Z}^2$ whose quotient is C_8. In this case, the vector chain of (6) is simply

$$V_1 \lneq (\mathbb{Z}/2\mathbb{Z})^2, \qquad \dim(V_1) = 1.$$

There are therefore three options, as shown in the figure. Each suitable lattice determines a chain

$$\Lambda \subsetneq 2^{-1}\Lambda \cap \mathbb{Z}^2 \subsetneq 2^{-2}\Lambda \cap \mathbb{Z}^2 \subsetneq \mathbb{Z}^2,$$

where the first three elements project onto V_1. These chains can be determined from right to left. Once V_1 is fixed, there is only one choice

$\begin{pmatrix}1&&\\&2&\\&&4\end{pmatrix}\begin{pmatrix}2&&1\\&2&\\&&2\end{pmatrix}$	$\begin{pmatrix}1&&\\&4&\\&&2\end{pmatrix}\begin{pmatrix}2&1&\\&2&\\&&2\end{pmatrix}$	$\begin{pmatrix}1&&\\&4&2\\&&2\end{pmatrix}\begin{pmatrix}2&1&1\\&2&\\&&2\end{pmatrix}$
$\begin{pmatrix}2&&\\&1&\\&&4\end{pmatrix}\begin{pmatrix}2&&\\&2&1\\&&2\end{pmatrix}$	$\begin{pmatrix}4&&\\&1&\\&&2\end{pmatrix}\begin{pmatrix}4&2&\\&1&\\&&2\end{pmatrix}$	$\begin{pmatrix}4&&2\\&1&\\&&2\end{pmatrix}\begin{pmatrix}4&2&2\\&1&\\&&2\end{pmatrix}$
$\begin{pmatrix}2&1&\\&1&\\&&4\end{pmatrix}\begin{pmatrix}2&&1\\&2&1\\&&2\end{pmatrix}$	$\begin{pmatrix}4&1&\\&1&\\&&2\end{pmatrix}\begin{pmatrix}4&3&\\&1&\\&&2\end{pmatrix}$	$\begin{pmatrix}4&1&2\\&1&\\&&2\end{pmatrix}\begin{pmatrix}4&3&2\\&1&\\&&2\end{pmatrix}$
$\begin{pmatrix}2&&\\&4&\\&&1\end{pmatrix}\begin{pmatrix}2&&\\&4&2\\&&1\end{pmatrix}$	$\begin{pmatrix}4&&\\&2&\\&&1\end{pmatrix}\begin{pmatrix}4&&2\\&2&\\&&1\end{pmatrix}$	$\begin{pmatrix}4&2&\\&2&\\&&1\end{pmatrix}\begin{pmatrix}4&2&2\\&2&\\&&1\end{pmatrix}$
$\begin{pmatrix}2&&1\\&4&\\&&1\end{pmatrix}\begin{pmatrix}2&&1\\&4&2\\&&1\end{pmatrix}$	$\begin{pmatrix}4&&1\\&2&\\&&1\end{pmatrix}\begin{pmatrix}4&&3\\&2&\\&&1\end{pmatrix}$	$\begin{pmatrix}4&2&1\\&2&\\&&1\end{pmatrix}\begin{pmatrix}4&2&3\\&2&\\&&1\end{pmatrix}$
$\begin{pmatrix}2&&\\&4&1\\&&1\end{pmatrix}\begin{pmatrix}2&&\\&4&3\\&&1\end{pmatrix}$	$\begin{pmatrix}4&&\\&2&1\\&&1\end{pmatrix}\begin{pmatrix}4&&2\\&2&1\\&&1\end{pmatrix}$	$\begin{pmatrix}4&2&\\&2&1\\&&1\end{pmatrix}\begin{pmatrix}4&2&2\\&2&1\\&&1\end{pmatrix}$
$\begin{pmatrix}2&&1\\&4&1\\&&1\end{pmatrix}\begin{pmatrix}2&&1\\&4&3\\&&1\end{pmatrix}$	$\begin{pmatrix}4&&1\\&2&1\\&&1\end{pmatrix}\begin{pmatrix}4&&3\\&2&1\\&&1\end{pmatrix}$	$\begin{pmatrix}4&2&1\\&2&1\\&&1\end{pmatrix}\begin{pmatrix}4&2&3\\&2&1\\&&1\end{pmatrix}$

Table 1: $|\mathcal{L}_3(G_2(\boxplus))| = |\mathcal{L}_3(C_4 \oplus C_2)| = 42$

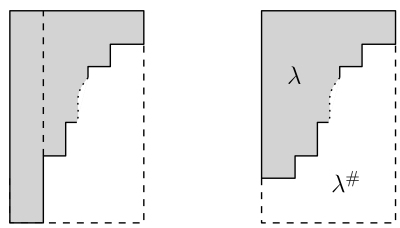
for $2^{-2}\Lambda \cap \mathbb{Z}^2$ and $2 = 2^{c(2,0)}$ choices for $2^{-1}\Lambda \cap \mathbb{Z}^2$. For each of these, there are two choices for Λ. In total, there are $4 = 2^{c(3,0)}$ lattices projecting to a fixed vector space chain.

In contrast, if $\mathbb{Z}^2/\Lambda \cong C_4 \oplus C_2$, we have $\pi(\Lambda) = 0$ and $\dim(\pi(2^{-1}\Lambda \cap \mathbb{Z}^2)) = 1$. For every line in $(\mathbb{Z}/2\mathbb{Z})^2$, there is a single ($c(2,1) = 0$) lattice in $\mathcal{L}_2(C_4 \oplus C_2)$.

9 Conservative transformations

We remark in this section a couple of partition transformations that keep the amount of associated lattices unchanged, as is apparent from Theorem 5.2.

We have seen at the beginning of Section 5 how, in dimension 2, the enumeration of lattices with a cyclic quotient solves the general case. The transformation that removes (or appends) full columns (as long as the dimension r) from a partition can be thought of as a generalization to arbitrary dimension of the reduction from the group $C_n \oplus C_d$ to $C_{n/d}$, valid in dimension 2.



That removal does not affect the part multiplicities $x_1, \ldots, x_{l+1}$, nor the exponent $c(\lambda; r)$, so that the number of associated lattices remains the same.

An explicit bijection is given by $\Lambda \mapsto p^{-\lambda_l}\Lambda$. Notice that, in a lattice whose quotient is associated to a partition with λ_l full columns, the entries of every element are multiples of p^{λ_l}.

It is not that simple to describe the effect on the number of associated lattices produced by the removal of trailing empty rows (i.e. reducing the dimension). This, combined with the previous remark, would lead to another inductive technique to solve the enumeration considered in this paper.

Another conservative partition transformation consists of taking the complement to a box with r rows and (at least) λ_1 columns. In this case, a bijection can be achieved by $\Lambda \mapsto p^{\lambda_1}\Lambda^{\#}$, where $\Lambda^{\#}$ is the *dual lattice*, defined as

$$\Lambda^{\#} = \{\mathbf{x} \in \mathbb{Q}^r \ : \ \langle \mathbf{x}, \mathbf{v} \rangle \in \mathbb{Z}, \ \forall \mathbf{v} \in \Lambda\}.$$

Note that this is not necessarily an integer lattice. Indeed, $\mathbb{Z}^r$ is the only integer lattice whose dual is also integer. The dual $\Lambda^{\#}$ is spanned by the transpose inverse of any basis of Λ. From the computational point of view, this object is an important tool to deal with lattice intersections. Since we have algorithms to compute the dual of a lattice (just given) and a lattice sum (reducing the juxtaposition of summand bases), the intersection can be obtained through the following formula:

$$\Lambda_1 \cap \Lambda_2 = (\Lambda_1^{\#} + \Lambda_2^{\#})^{\#}.$$

In particular, the elements in the lattice chain (7) can be computed as

$$(p^i \Lambda^{\#} + \mathbb{Z}^r)^{\#}.$$

10 Epimorphism count

The enumeration result studied in this article has been proved (see Section 5) relying on Equation (4). As pointed out by Butler [3], the count of subgroups with a given type appeared in three different papers published in the same year. From the exposition of Delsarte [5, §2.(4),(20)], the following expression for that count can be extracted:

$$\frac{|\mathrm{Epi}(G_p(\mu), G_p(\lambda))|}{|\mathrm{Aut}(G_p(\lambda))|}.$$

The approach followed by Kwak, Chun, and Lee relies instead on a technique due to Hall [8, Thm. 1.4], who enumerates subgroups of an arbitrary group (not necessarily abelian) with a prescribed quotient, focusing on subgroups of free groups. Applying that method to our problem, we get (see [11, Thm. 2.6], [12, Thm. 10])

$$|\mathcal{L}_r(G)| = \frac{|\mathrm{Epi}(\mathbb{Z}^r, G)|}{|\mathrm{Aut}(G)|}.$$

Notice the coincidence of numerators in both approaches when μ is set to (λ_1^r), as is done in Section 5. Both fractions above admit a simple interpretation as the orbit count relative to the free action by composition of the automorphism group on the set of epimorphisms [10].

In the second case, the epimorphism enumeration can be directly derived [11, Lemma 3.3]. Setting (for the rest of the section) $x = \mathrm{len}(\lambda)$,

$$\begin{aligned} |\mathrm{Epi}(\mathbb{Z}^r, G_p(\lambda))| = & p^{r(|\lambda|-x)} |\mathrm{Epi}(\mathbb{Z}^r, C_p^x)| = \\ & p^{r(|\lambda|-x)} (p^r - 1)(p^r - p) \cdots (p^r - p^{x-1}) = \\ & p^{r(|\lambda|-x)} p^{\frac{x(x-1)}{2}} (p-1)^x \frac{[r]_p!}{[x_{l+1}]_p!}. \end{aligned} \tag{9}$$

This, combined with the automorphism count below (which follows [5, §2.(18)], cf. [13, II.(1.6)], [9, Thm. 4.1], [11, Lemma 3.3]), proves Theorem 5.2.

$$|\mathrm{Aut}(G_p(\lambda))| = p^{\frac{x(x-1)}{2} + \sum \lambda_i' \lambda_{i+1}'} (p-1)^x [x_1]_p! \cdots [x_l]_p!$$

Epimorphism enumeration is a natural application of the extended Möbius principle [15]. Indeed, the sources of both approaches above [5, 8] constitute two among the first antecedents to Rota's formalization of the concept, using the poset of subgroups of a finite group.

Classifying homomorphisms with respect to their image, we get the expression

$$|\mathrm{Hom}(\mathbb{Z}^r, G)| = \sum_{S \le G} |\mathrm{Epi}(\mathbb{Z}^r, S)|,$$

where the sum is extended over the subgroups of G. As the computation of homomorphisms is easily done (for abelian G, $|\mathrm{Hom}(\mathbb{Z}^r, G)| = |G|^r$), it is useful to invert previous expression:

$$|\mathrm{Epi}(\mathbb{Z}^r, G)| = \sum_{S \le G} \mu([S, G])|S|^r = \sum_{S \le G} \mu([0, S])|G/S|^r.$$

When $G = C_n$ is cyclic, the Möbius function on the poset of subgroups coincides with the classic number-theoretic Möbius function on the divisors of n. This gives

$$|\mathcal{L}_r(C_n)| = \frac{1}{\varphi(n)} \sum_{d|n} \mu\left(\frac{n}{d}\right) d^r = \frac{J_r(n)}{\varphi(n)},$$

where φ denotes Euler's totient function and J_r is the r-th Jordan function. This expression recovers the one given in (5), when the group order is a prime power.

Going back to the general case, in any finite (poset) lattice, the Möbius function $\mu([0, a])$ is zero for every poset element a, except possibly for joins of atoms [8, Thm. 2.3 and 2.4], [15, Sec. 5, Cor. to Prop. 2], [18, Cor. 3.9.5]. In the lattice of subgroups of $G_p(\lambda)$, atoms are the several copies of C_p, and their joins correspond to elementary abelian subgroups. For these, $\mu\left([0, C_p^k]\right) = (-1)^k p^{\frac{k(k-1)}{2}}$ [5, p. 603], [15, Sec. 5, Ex. 2], [18, Ex. 3.10.2]. Moreover, the amount of subgroups of the form C_p^k in $G_p(\lambda)$ is $\left[\begin{smallmatrix} x \\ k \end{smallmatrix}\right]_p$. Then,

$$|\mathrm{Epi}(\mathbb{Z}^r, G_p(\lambda))| = \sum_{k=0}^{x} \begin{bmatrix} x \\ k \end{bmatrix}_p (-1)^k p^{\frac{k(k-1)}{2}} p^{r(|\lambda|-k)} =$$
$$p^{r(|\lambda|-x)} \sum_{k=0}^{x} \begin{bmatrix} x \\ k \end{bmatrix}_p (-1)^k p^{\frac{k(k-1)}{2}} p^{r(x-k)}.$$

Developing the Gaussian polynomial with Carlitz formula, the sum above equals

$$\sum_{k=0}^{x} (-1)^k p^{\frac{k(k-1)}{2}} p^{r(x-k)} \sum_{\sigma \in \mathfrak{S}(\{1^k, 0^{x-k}\})} p^{\mathrm{inv}(\sigma)}, \tag{10}$$

where $\mathrm{inv}(\sigma)$ is the number of inversions of a permutation of the multiset $\{1^k, 0^{x-k}\}$. These permutations correspond to subsets of $\{0, 1, \ldots, x-1\}$ with k elements. Moreover, the sum of the elements in such a subset is $0 + 1 + \cdots + (k-1)$ plus the number of inversions of the associated permutation. This turns (10) into

$$\sum_{k=0}^{x} (-1)^k p^{r(x-k)} \sum_{\substack{I \subseteq \{0,\ldots,x-1\} \\ |I|=k}} p^{\sum_{i \in I} i},$$

which equals $(p^r - 1) \cdots (p^r - p^{x-1})$, recovering (9).

Álvar Ibeas Martín
ibeas@gmx.com

References

[1] Michael Baake, *Solution of the coincidence problem in dimensions $d \leq 4$*, arXiv:math/0605222 [math.MG] (2006).

[2] Reinhold Baer, *Dualism in abelian groups*, Bull. Amer. Math. Soc., **43** no. 2 (1937), 121–124.

[3] Lynne Butler, Subgroup Lattices and Symmetric Functions, Mem. Amer. Math. Soc., **112** no. 539 (1994).

[4] L. Carlitz, *Sequences and inversions*, Duke Math. J., **37** (1970), 193–198.

[5] S. Delsarte, *Fonctions de Möbius sur les groupes abeliens finis*, Annals of Math., **49** (1948), 600–609.

[6] P. E. Dyubyuk, *On the number of subgroups of an abelian p-group*, Izv. Akad. Nauk. Ser. Mat., **12** no. 4 (1948), 351–378 (in Russian).

[7] B. Gruber, *Alternative formulae for the number of sublattices*, Acta Cryst., **A53** (1997), 807–808.

[8] P. Hall, *The Euclidean functions of a group*, Quat. J. Math., **7** (1936), 134–151.

[9] Christopher J. Hillar, Darren L. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly., **114** no. 10 (2007), 917–923.

[10] Gareth. A. Jones, *Counting subgroups of non-Euclidean crystallographic groups*, Math. Scand., **84** (1999), 23–29.

[11] Jin Ho Kwak, Jang-Ho Chun, Jaeun Lee, *Enumeration of regular graph coverings having finite abelian covering transformation groups*, SIAM J. Discrete Math., **11** no. 2 (1998), 273–285.

[12] Jin Ho Kwak, Jaeun Lee, *Enumeration of graph coverings, surface branched coverings and related group theory*, in Combinatorial and Computational Mathematics, edited by S. Hong et al., World Scientific, Singapore (2001), 97–161.

[13] I. G. Macdonald, Symmetric Functions and Hall Polynomials, Oxford University Press (1998).

[14] OEIS Foundation Inc. (2011), The On-Line Encyclopedia of Integer Sequences, *http://oeis.org*

[15] Gian-Carlo Rota, *On the foundations of combinatorial theory I. Theory of Möbius functions*, Z. Wahrscheinlichkeitstheorie, **2** (1964), 340–368.

[16] John S. Rutherford, *The enumeration and symmetry-significant properties of derivative lattices. II. Classification by colour lattice group*, Acta Cryst., **A49** (1993), 293–300.

[17] Günter Scheja, Uwe Storch, Lehrbuch der Algebra, Teil 2, BG Teubner, Stuttgart (1988).

[18] Richard P. Stanley, Enumerative Combinatorics, Wadsworth Publ. Co., Belmont, CA (1986).

[19] Yenchien Yeh, *On prime power abelian groups*, Bull. Amer. Math. Soc., **54** no. 4 (1948), 323–327.

[20] Yi Ming Zou, *Gaussian binomials and the number of sublattices*, Acta Cryst., **A62** (2006), 409–410.