

The lattice of arithmetic progressions

MARCEL K. GOH

*Edmonton, Alberta
Canada*

marcel.goh@mail.mcgill.ca

JAD HAMDAN

*Mathematical Institute
University of Oxford
Oxford
U. K.*

jad.hamdan@mail.mcgill.ca

JONAH SAKS

*Department of Mathematics and Statistics
McGill University
Montréal, Québec
Canada*

jonah.saks@mail.mcgill.ca

Abstract

In this paper we investigate properties of the lattice L_n of subsets of $[n] = \{1, \dots, n\}$ that are arithmetic progressions, under the inclusion order. For $n \geq 4$, this poset is not graded and thus not semimodular. We give three independent proofs of the fact that for $n \geq 2$, $\mu_n(L_n) = \mu(n-1)$, where μ_n is the Möbius function of L_n and μ is the classical (number-theoretic) Möbius function. We also show that L_n is comodernistic, which implies that L_n is EL-labelable. Comodernism is then used to prove that the order complex Δ_n of the lattice is either contractible or homotopy equivalent to a sphere.

1 Introduction

The additive structure of certain subsets of additive groups has long been a topic of interest in number theory and combinatorics. A class of sets with a great deal of additive structure is the set of *arithmetic progressions*. These are sets of the form

$$\{a, a + r, \dots, a + (k - 1)r\}$$

where the *base point* a and *step size* (or simply *step*) r are elements of an additive group and the *length* k is an integer. In this paper we take our underlying additive group to be the integers \mathbf{Z} . The business of finding arithmetic progressions in sets of integers goes back to a classical 1927 theorem of van der Waerden [23], which states that any colouring of the integers with finitely many colours gives rise to monochromatic arithmetic progressions of arbitrary length. This was generalised by Szemerédi, who in 1975 proved the existence of arithmetic progressions of arbitrary length in any set of positive upper density [22]. More recently, Green and Tao showed that the same conclusion holds in the primes [14].

Set systems consisting of arithmetic progressions have received some attention in the realm of topology. The topology on \mathbf{Z} generated by (infinite) arithmetic progressions $a + k\mathbf{Z}$ was used by Furstenberg to give an alternative proof of the infinitude of primes [10]. This topology came to be known as Golomb’s topology, after Golomb, who studied its properties more systematically in a 1959 paper [12]. We will restrict ourselves to a finite subset of \mathbf{Z} and study the set of arithmetic progressions itself, rather than the topology it forms a basis of. As with any set of subsets, it is partially ordered by inclusion, and in the present paper we investigate the structure induced by this ordering.

We shall also investigate topological properties of the order complex associated to this lattice. Several other simplicial complexes related to number-theoretic objects have recently appeared in the literature. The simplicial complex of squarefree positive integers less than or equal to n was studied in a 2011 paper by Björner [4], and a 2017 paper [7] of Ehrenborg, Govindaiah, Park and Readdy introduces a simplicial complex called the van der Waerden complex $\text{vdW}(n, k)$, whose facets correspond to arithmetic progressions of length k in $\{1, \dots, n\}$. A subsequent paper of Hooper and Van Tuyl characterised the pairs (n, k) for which $\text{vdW}(n, k)$ is shellable [16]. The simplicial complexes arising from our posets are different in that the vertices are themselves arithmetic progressions.

For brevity, we let $[n]$ denote the set $\{1, 2, \dots, n\}$ and we will also sometimes write sets of integers by concatenating their elements: so, for example, 135 is shorthand for $\{1, 3, 5\}$. For $n \geq 1$ we let L_n denote the partially-ordered set (poset) of all finite integer arithmetic progressions contained in $[n]$ including trivial progressions of length 1 and 2 as well as the empty set \emptyset . When it is convenient, we artificially define $L_0 = \{\emptyset\}$. Small examples are depicted in Figure 1. In each figure, every point represents a progression, progressions with the same cardinality are placed on the same row, and these rows are ordered lexicographically (the reader may find it instructive to spend a minute or two trying to pencil in labels for L_4 and L_5).

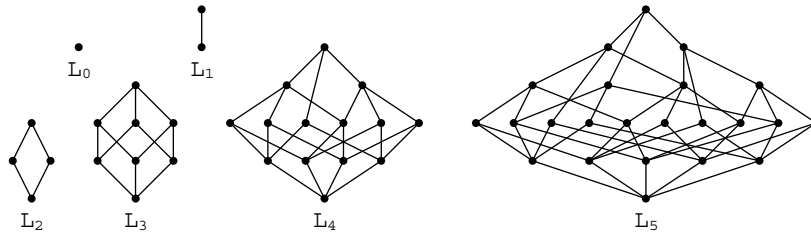


Figure 1: Hasse diagrams of L_n for small values of n .

The notation L_n is motivated by the fact that L_n is a lattice. The meet of two elements is simply the set-theoretic intersection, since the intersection of two integer arithmetic progressions is a (possibly empty) arithmetic progression. By induction, one finds that the meet of any finite number of points is well-defined in L_n , and this as well as the existence of a maximum element $12 \cdots n$ implies the existence of a join of two arbitrary elements $x_1, x_2 \in L_n$.

The poset L_n is not graded for $n \geq 4$. To see this, note that

$$1 < 14 < [4] < [5] < \cdots < [n] \quad \text{and} \quad 1 < 12 < 123 < 1234 < \cdots < [n]$$

are both maximal chains, but the first has length $n - 2$ while the second has length $n - 1$. Since the posets L_n for $n \geq 4$ are not graded, they are also not (upper) semimodular. Indeed, 12 and 14 both cover $12 \wedge 14 = 1$, but $12 \vee 14 = 1234$ does not cover 12.

For two elements $x \leq y$ in a poset X , the *interval* $[x, y]$ is the set of all $z \in X$ satisfying $x \leq z \leq y$. If X has a minimum element $\widehat{0}$, then we can define the *principal (order) ideal generated by x* , denoted $\downarrow x$, to be the interval $[\widehat{0}, x]$. A poset is said to be *locally finite* if every interval is finite. The *Möbius function* μ_X of a locally finite poset X is the function from intervals of the poset to the complex field \mathbf{C} given by the formulas $\mu_X(x, x) = 1$ for all $x \in X$ and

$$\mu_X(x, y) = - \sum_{x \leq z < y} \mu_X(x, z) \tag{1.1}$$

for all $x \leq y$ in X , where we have abbreviated $\mu_X([x, y])$ by $\mu_X(x, y)$. If the poset X is a lattice, with minimum element $\widehat{0}$ and maximum element $\widehat{1}$, then $X = [\widehat{0}, \widehat{1}]$ and it makes sense to write $\mu_X(X)$ for $\mu(\widehat{0}, \widehat{1})$. In the case that X is the set of all positive integers, ordered by divisibility, then $\mu_X(m, n) = \mu(n/m)$, where μ is the classical Möbius function. Recall that $\mu(s) = 1$ if $s = 1$ or s is a product of an even number of distinct primes, $\mu(s) = -1$ if s is a product of an odd number of distinct primes, and $\mu(s) = 0$ if s is divisible by a perfect square. We centre our discussion around the following main result.

Theorem 1.1 *Let $\mu_n = \mu_{L_n}$ be the Möbius function of the lattice of arithmetic progressions L_n . We have $\mu_0(L_0) = 1$, $\mu_1(L_1) = -1$, and $\mu_n(L_n) = \mu(n - 1)$ for $n \geq 2$, where μ is the classical Möbius function.*

We now briefly outline the paper. In Section 2, we develop some properties of the number p_{nk} of arithmetic progressions of size k in $[n]$ and show that these quantities arise in a recurrence that proves Theorem 1.1 directly from the definition of the Möbius function. In Section 3, we count chains in L_n in order to gain information about the order complex of L_n and derive the same recurrence in a slightly different manner. We then proceed in Section 4 to study the set of coatoms in L_n in order to give a general formula for μ_n , evaluated at an arbitrary interval of L_n . As a corollary, we obtain a third proof of Theorem 1.1 that is of a rather different nature than the first two proofs. In Section 5, we explicitly compute the homology groups of the order complex Δ_n of L_n . In Section 6, we prove that L_n is comodernistic, a property recently introduced by Schweig and Woodrooffe that in particular implies that Δ_n is shellable for all n [21]. Lastly, in Section 7, we use lemmas proved in previous sections to show that L_n is EL-labelable, that Δ_n is either contractible or has the homotopy type of a sphere, and that L_n is complemented if and only if $n - 1$ is squarefree.

2 The number of arithmetic progressions

Our starting point is the number p_{nk} of arithmetic progressions of length k contained in $[n]$. It was shown in [11] that for $2 \leq k \leq n$,

$$p_{nk} = \sum_{r=1}^{\lfloor (n-1)/(k-1) \rfloor} (n - (k - 1)r) = n \left\lfloor \frac{n - 1}{k - 1} \right\rfloor - \frac{k - 1}{2} \left(\left\lfloor \frac{n - 1}{k - 1} \right\rfloor^2 + \left\lfloor \frac{n - 1}{k - 1} \right\rfloor \right).$$

(We have halved their formula here, because we consider arithmetic progressions as sets and not as ordered sequences.) We also have $p_{n0} = 1$ to count the empty progression as well as $p_{n1} = n$ to count the n singletons. Values of p_{nk} for small values of n and k are collected in Table 1. We first derive a formula for the bivariate generating function of p_{nk} (see, e.g., [8] for an exhaustive reference on generating functions).

Lemma 2.1 *For integers $n, k \geq 0$, let p_{nk} denote the number of arithmetic progressions of size k in the interval $[n]$. We have the formula*

$$f(z, q) = \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} p_{nk} z^n q^k = \frac{1}{(1 - z)^2} \left(1 - z + zq + \sum_{k=2}^{\infty} \frac{(zq)^k}{1 - z^{k-1}} \right)$$

for the bivariate generating function of p_{nk} .

PROOF: The sequences $(p_{n0})_{n \geq 0}$ and $(p_{n1})_{n \geq 0}$ are $(1, 1, 1, \dots)$ and $(0, 1, 2, \dots)$ respectively, so that the coefficient of q^0 in $f(z, q)$ is $1/(1 - z)$ and the coefficient of q is $z/(1 - z)^2$. For $k \geq 2$, there are $n - 1$ possible base points and for each base point a , the number of possible step sizes is $\lfloor (n - a)/(k - 1) \rfloor$. So

$$\sum_{n=2}^{\infty} p_{nk} z^n = \sum_{n=2}^{\infty} \sum_{a=1}^{n-1} \left\lfloor \frac{n - a}{k - 1} \right\rfloor z^n = \sum_{n=0}^{\infty} \sum_{a=1}^{n-1} \left\lfloor \frac{a}{k - 1} \right\rfloor z^n = \frac{1}{1 - z} \sum_{n=0}^{\infty} \left\lfloor \frac{n}{k - 1} \right\rfloor z^n \quad (2.1)$$

n	p_{n0}	p_{n1}	p_{n2}	p_{n3}	p_{n4}	p_{n5}	p_{n6}	p_{n7}	p_{n8}	p_{n9}	$p_{n(10)}$	$p_{n(11)}$
0	1											
1	1	1										
2	1	2	1									
3	1	3	3	1								
4	1	4	6	2	1							
5	1	5	10	4	2	1						
6	1	6	15	6	3	2	1					
7	1	7	21	9	5	3	2	1				
8	1	8	28	12	7	4	3	2	1			
9	1	9	36	16	9	6	4	3	2	1		
10	1	10	45	20	12	8	5	4	3	2	1	
11	1	11	55	25	15	10	7	5	4	3	2	1

Table 1: The number p_{nk} of arithmetic progressions of size k in $\{1, 2, \dots, n\}$

where we have added the empty terms for $n = 0$ and $n = 1$ and reversed the order of summation in the second equality. Note that

$$\begin{aligned}
 \sum_{n=0}^{\infty} \left\lfloor \frac{n}{k-1} \right\rfloor z^n &= \sum_{i=1}^{\infty} \sum_{n=i(k-1)}^{\infty} z^n \\
 &= \sum_{i=1}^{\infty} \frac{z^{i(k-1)}}{1-z} \\
 &= \frac{1}{1-z} \cdot \frac{1-(1-z^k)}{1-z^{k-1}} \\
 &= \frac{z^k}{(1-z^{k-1})(1-z)}.
 \end{aligned}
 \tag{2.2}$$

Putting everything together, we find that

$$\sum_{n=0}^{\infty} \sum_{k=0}^{\infty} p_{nk} z^n q^k = \frac{1}{1-z} + \frac{z}{(1-z)^2} q + \sum_{k=2}^{\infty} \frac{z^k}{(1-z^{k-1})(1-z)^2} q^k,
 \tag{2.3}$$

which simplifies to the formula we were looking for. □

Because $p_{nk} = 0$ when $k > n$, the horizontal generating functions $f_n(q)$ are polynomials $\sum_{k=0}^n p_{nk} q^k$. For instance, since L_0 through L_3 are just Boolean lattices (consisting of all subsets of a finite ground set), we have $f_n(q) = (1+q)^n$. When $n = 4$, we have $f_4(q) = 1 + 4q + 6q^2 + 2q^3 + q^4$, which is irreducible in $\mathbf{Z}[q]$ by Cohn’s criterion [5], since $f_4(10) = 12641$ is prime. It can also be checked computationally that $f_n(q)$ is irreducible for $5 \leq n \leq 10$, and there is no reason to suspect that this

polynomial has a neat factorisation for any larger values of n . As a corollary of the above lemma, we obtain a nice formula for $f_n(1) = |L_n|$, the number of elements in the lattice. We use the notation $j \mid k$ to indicate that k is an integer multiple of j .

Corollary 2.2 *For $n \in \mathbf{N}$, the poset L_n has*

$$|L_n| = 1 + n + \sum_{a=1}^{n-1} \sum_{r=1}^a \tau(r)$$

elements, where $\tau(r) = \sum_{d \mid r} 1$ is the divisor function.

PROOF: We write

$$|L_n| = f_n(1) = 1 + n + \sum_{a=1}^{n-1} \sum_{r=1}^a \left\lfloor \frac{a}{r} \right\rfloor$$

and then apply the elementary identity $\sum_{k=1}^n \tau(k) = \sum_{k=1}^n \lfloor n/k \rfloor$. □

The sequence $(|L_n| - 1)_{n \geq 1}$ appears in the On-line Encyclopedia of Integer Sequences under the entry A051336. We are almost ready to give the first proof of Theorem 1.1, which expresses the Möbius function of L_n as a recurrence defined in terms of p_{nk} . We start with the following observation.

Lemma 2.3 *Let $n \geq 1$ and let $1 \leq k \leq n$. For any progression $x \in L_n$ of cardinality k , we have $\mu_n(\emptyset, x) = \mu_k(\emptyset, [k])$.*

PROOF: Because $x = \{a, a + r, \dots, a + (k - 1)r\}$ is a progression, one obtains an isomorphism of posets between the ideal $\downarrow x$ and L_k by relabelling the element $a + ir$ with $i + 1$ for $0 \leq i < k$. □

The rest of the proof involves setting up and solving a certain recurrence.

FIRST PROOF OF THEOREM 1.1. Let $M_n = \mu_n(L_n)$ for short. The case $n = 0$ is trivial. For $n \geq 1$, we must subtract $\mu_k(\emptyset, x)$ for every progression $x \in L_n^* = L_n \setminus \{[n]\}$. By Lemma 2.3 and the fact that there are p_{nk} progressions of size k in L_n , we have the recurrence

$$M_n = - \sum_{x \in L_n^*} \mu_n(\emptyset, x) = - \sum_{k=0}^{n-1} M_k p_{nk}. \tag{2.4}$$

We can then compute $M_1 = -1$ and $M_2 = 1 = \mu(1)$. For $n > 2$ we now proceed by strong induction; suppose that $M_k = \mu(k - 1)$ for all $2 \leq k < n$. We expand the

above recurrence to

$$\begin{aligned}
 M_n &= -\left(M_0 p_{n0} + M_1 p_{n1} + \sum_{k=2}^{n-1} M_k p_{nk}\right) \\
 &= -\left(1 - n + \sum_{k=2}^{n-1} \mu(k-1) \sum_{r=1}^{\lfloor (n-1)/(k-1) \rfloor} (n - (k-1)r)\right) \tag{2.5} \\
 &= -\left(1 - n - \mu(n-1) + \sum_{k=1}^{n-1} \mu(k) \sum_{r=1}^{\lfloor (n-1)/k \rfloor} (n - kr)\right)
 \end{aligned}$$

and sum over all possible values of kr by setting $m = kr$ and summing over divisors d of m , for $1 \leq m \leq n - 1$. This gives

$$M_n = -\left(1 - n - \mu(n-1) + \sum_{m=1}^{n-1} \sum_{d|m} \mu(d)(n - m)\right). \tag{2.6}$$

But $\sum_{d|m} \mu(d) = 0$ when $m > 1$ and when $m = 1$, the summation equals $n - 1$. After cancellation, we see that the right-hand side equals $\mu(n - 1)$, which is what we wanted to show. \square

3 Chains and the order complex

An *abstract simplicial complex* is a set system Δ on a vertex set V containing every singleton subset of V and with the property that for every set $F \in \Delta$, all subsets of F also belong to Δ . The elements of Δ are called *faces*, and the *dimension* of a face F is defined to be $|F| - 1$. A face is said to be *maximal* if it is not strictly contained in another face, and the dimension of Δ is the maximum dimension of a (maximal) face in Δ . For our purposes, simplicial complexes will contain the empty set, a face of dimension -1 . We will require various notions from topology in this section. Any definitions that we do not recall here can be found in any introductory textbook, such as [19], for example.

A *chain* of length k in a poset X is a set $\{x_1, x_2, \dots, x_{k+1}\} \subseteq X$ such that $x_1 < x_2 < \dots < x_{k+1}$; so a chain of length 0 is a singleton set and we will say that an empty chain has length -1 . One can associate a simplicial complex, called the *order complex*, to any lattice (with bottom element $\widehat{0}$ and top element $\widehat{1}$) by taking $L \setminus \{\widehat{0}, \widehat{1}\}$ as the vertex set and letting the faces be chains in this modified poset. Let L'_n denote the poset L_n with the minimum element \emptyset as well as the maximum element $[n]$ removed. Note that chains in L'_n of length $k - 2$ are in bijection with chains of length k in L_n that contain both \emptyset and $[n]$, which we shall count in the next lemma.

n	b_{n1}	b_{n2}	b_{n3}	b_{n4}	b_{n5}	b_{n6}	b_{n7}	b_{n8}	b_{n9}	$b_{n(10)}$	$b_{n(11)}$
1	1										
2	1	2									
3	1	6	6								
4	1	12	24	12							
5	1	21	68	72	24						
6	1	32	144	244	180	48					
7	1	47	283	666	764	432	96				
8	1	64	486	1510	2436	2164	1008	192			
9	1	85	799	3117	6534	8028	5816	2304	384		
10	1	109	1232	5860	15368	24524	24516	15040	5184	768	
11	1	137	1838	10418	33049	65402	84284	70992	37760	11520	1536

Table 2: The number b_{nk} of chains of length $k - 2$ in L'_n

Lemma 3.1 *The number b_{nk} of chains of length k in L_n that contain \emptyset and $[n]$ satisfies the recurrence*

$$b_{nk} = \sum_{i=1}^{n-1} p_{ni} b_{i(k-1)}, \tag{3.1}$$

for $2 \leq k \leq n$, with $b_{n1} = 1$ for all n and $b_{nk} = 0$ whenever $k > n$.

PROOF: The case $k = 1$ is trivial and it is clear that b_{nk} should be zero for $k > n$. In the other cases, we are counting chains $\emptyset \subset x_1 \subset \dots \subset x_k \subset [n]$ (we require strict inclusion here). We split up the cases by the second-greatest element x_k of the chain. It is clear that the subchain $\{\emptyset, x_1, \dots, x_k\}$ is a chain containing both the maximum and minimum element of the ideal $\downarrow x_k$, which, by Lemma 2.3, is isomorphic to L_i , where i is the size of x_k (as a set). Thus the number of such chains is $b_{m(k-1)}$. There were p_{ni} choices for the element of size i , and summing over all possible i gives the recurrence above. \square

For small values of n and k , the values b_{nk} are displayed in Table 2. As a slight digression, note for analogy that if in the recurrence (3.1) we replace p_{nk} with $\binom{n}{k}$, we obtain the array of numbers $k! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$, where $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ is a Stirling number of the second kind (see, e.g., [13]). These numbers count the number of ways to partition n numbers into k nonempty subsets, and for each such partition S_1, S_2, \dots, S_n , we obtain $k!$ chains in the Boolean lattice that contain both \emptyset and $[n]$ (for each permutation σ in \mathfrak{S}_n , we have the chain $\{\emptyset, S_{\sigma(1)}, S_{\sigma(1)} \cup S_{\sigma(2)}, \dots, [n]\}$).

Returning to our numbers b_{nk} , we see that for $-1 \leq k \leq n - 2$, the number of k -dimensional faces of Δ_n is $b_{n(k+2)}$. Hence Δ_n is an $(n - 2)$ -dimensional simplicial complex. Let $\tilde{\chi}(\Delta_n) = \chi(\Delta_n) - 1$ be the reduced Euler characteristic of the order

complex. We have

$$\tilde{\chi}(\Delta_n) = \sum_{k=1}^n (-1)^k b_{nk} \tag{3.2}$$

for $n \geq 1$. Using the fact that the Möbius function of a poset with a maximum and minimum element artificially adjoined equals the reduced Euler characteristic of its order complex, we obtain an alternative proof of Theorem 1.1.

SECOND PROOF OF THEOREM 1.1. Let $M_n = \sum_{k=1}^n (-1)^k b_{nk}$. We compute $M_0 = 1$ and $M_1 = -1$ by hand. To complete the proof, it suffices to show that $\tilde{\chi}(\Delta_n) = M_n = \mu(n-1)$ for all $n \geq 2$. The base case $M_2 = 1$ follows from a direct computation, and for $n > 2$, we have

$$\begin{aligned} M_n &= \sum_{k=1}^n (-1)^k b_{nk} \\ &= -1 + \sum_{k=2}^n (-1)^k \sum_{i=1}^{n-1} p_{ni} b_{i(k-1)} \\ &= -1 + \sum_{i=1}^{n-1} p_{ni} \sum_{k=2}^n (-1)^k b_{i(k-1)}, \end{aligned} \tag{3.3}$$

by Lemma 3.1. We can pull out one of the -1 factors and reindex to obtain

$$M_n = - \left(1 + \sum_{i=1}^{n-1} p_{ni} \sum_{k=1}^i (-1)^k b_{ik} \right). \tag{3.4}$$

Note that the upper index in the inner summation has been changed to i , since $b_{ik} = 0$ when $k > i$. By the induction hypothesis, this inner sum is M_i , so

$$M_n = - \left(1 + \sum_{i=1}^{n-1} p_{ni} M_i \right) = \sum_{i=0}^{n-1} p_{ni} M_i, \tag{3.5}$$

which is the recurrence (2.4) we encountered in the first proof of this theorem. The rest of the proof proceeds exactly as before. \square

4 Coatoms

We now set out to compute $\mu_n(x_1, x_2)$ for arbitrary progressions x_1 and x_2 in L_n . Towards this goal, we will need to study the *coatoms* of L_n , the elements covered by $[n]$. It turns out that we can give an explicit description of the set of coatoms in L_n .

Lemma 4.1 *Let $A_n \subseteq L_n$ be the set of coatoms. We have $A_1 = \{\emptyset\}$, $A_2 = \{1, 2\}$, and $A_3 = \{12, 13, 23\}$. For $n \geq 4$, we have $A_n = B_n \cup C_n$, where $B_n = \{12 \cdots (n-1), 23 \cdots n\}$, and*

$$C_n = \begin{cases} \{1n\}, & \text{if } n-1 \text{ is prime;} \\ \{\{1, 1+p, 1+2p, \dots, n\} : p \text{ prime, } p \mid (n-1)\}, & \text{otherwise.} \end{cases} \tag{4.1}$$

In particular, the size of A_n is $\omega(n - 1) + 2$, where $\omega(n)$ is the number of distinct prime divisors of n .

PROOF: The small cases are easily computed explicitly. When $n \geq 4$ there are only two elements of size $n - 1$, and the fact that they are coatoms is obvious. Now any element that does not contain both 1 and n cannot be a coatom, since an element of B_n would contain it. The progressions that contain $1n$ are of the form $x_d = \{1, d + 1, 2d + 1, \dots, n\}$ for divisors d of $n - 1$, but note that if d is composite, then x_d is contained in $x_{d'}$ for any d' dividing d . Hence the remaining coatoms are the progressions with prime steps, implying that C_n is of one of the two forms above. \square

Every non-top element in L_n is contained in some coatom, but when $n \geq 4$, not all elements can be expressed as a meet of coatoms. The next lemma shows that in L_n , if an element can be expressed as a meet of coatoms, then this representation is unique.

Lemma 4.2 *Let L_n be the lattice of arithmetic progressions and let $A_n \subseteq L_n$ be the set of coatoms. If $x \in L_n$ can be expressed as $x = \bigwedge_{s \in S} s$ for some $S \subseteq A_n$, then S is uniquely determined by x .*

PROOF: If $x = \emptyset$, then S must equal A_n , since omitting one of $12 \cdots (n - 1)$ or $23 \cdots n$ would cause one of the elements 1 or n to appear in the meet, and omitting the progression with base point 1, step size p (a prime dividing $n - 1$), and end point n will cause the $p - 1$ elements

$$1 + \frac{n - 1}{p}, 1 + \frac{2(n - 1)}{p}, \dots, n - \frac{n - 1}{p}$$

to appear in the meet. This last observation also shows that if $x = \{1\}$ then we have omitted only $23 \cdots n$ and if $x = \{n\}$, then we have omitted only $12 \cdots (n - 1)$.

Now suppose that x is nonempty and we can write out the elements of $x = \{a, a + r, \dots, a + (k - 1)r\}$. We will consider the possible step sizes r . When $r = 1$, x is either $12 \cdots (n - 1)$, $23 \cdots n$, or $23 \cdots (n - 1)$ and in all three cases it is clear that there is only one representation of x as the meet of coatoms. For $r > 1$, we find that r must be the least common multiple of some primes dividing $n - 1$, and there is only one way to express r as a least common multiple of distinct primes, thus uniquely determining the coatoms with prime step size that are in S . Lastly, note that $12 \cdots (n - 1)$ is in S if and only if $a = 1$ and $23 \cdots n$ is in S if and only if $a + (k - 1)r = n$. \square

These properties of the set of coatoms in L_n imply a general formula for computing $\mu_n(x, [n])$.

Theorem 4.3 *Let $x \neq [n]$ be a progression in L_n .*

$$\mu_n(x, [n]) = \begin{cases} (-1)^k, & \text{if } x \text{ is the meet of } k \text{ coatoms;} \\ 0, & \text{if } x \text{ is not a meet of coatoms.} \end{cases} \tag{4.2}$$

PROOF: We dispense first with the case where x is a coatom, since then it is clear that $\mu_n(x, [n]) = -1$. Otherwise, note that x is the minimum element of the interval $L = [x, [n]]$; the subset $S \subseteq L_n$ of coatoms whose meet equals x is contained in this interval. By the cross-cut theorem [20],

$$\mu_n(x, [n]) = \sum_{k=1}^{|A_n|} (-1)^k N_k, \tag{4.3}$$

where N_k is the number of sets of k coatoms whose meet is x . By Lemma 4.2, $N_{|S|} = 1$ and $N_k = 0$ for all $k \neq |S|$, proving the theorem. \square

It is easy to tell if a given progression x is a meet of coatoms, since such x have a very specific form. In particular, x is a meet of coatoms of L_n if and only if

$$x \cap \{2, \dots, n - 1\} = (1 + d\mathbf{Z}) \cap \{2, \dots, n - 1\}$$

for some divisor d of $n - 1$. One can then work out the number of elements in the meet representation by taking the prime decomposition of d and checking whether 1 or n (or both or neither) are included in x . Let $\omega(n)$ be the number of distinct primes dividing an integer n and let S denote the set of progressions x with $\mu_n(x, [n]) \neq 0$. Lemma 4.1 and Theorem 4.3 together imply that there are exactly $2^{\omega(n-1)+2}$ such elements x in L_n . Since every squarefree divisor of $n - 1$ contributes exactly four progressions to the set S , we can prove the elementary identity $\sum_{d|n} |\mu(d)| = 2^{\omega(n)}$ by counting S in two ways.

Since, by Lemma 2.3, the ideal $\downarrow x \subseteq L_n$ is isomorphic to L_m for any progression x of size m , Theorem 4.3 immediately implies a general method for computing the Möbius function of an arbitrary interval.

Corollary 4.4 *Let x_1 and x_2 be elements of L_n with $x_1 \leq x_2$ and let C be the set of elements covered by x_2 . We have*

$$\mu_n(x_1, x_2) = \begin{cases} (-1)^k, & \text{if } x_1 \text{ is the meet of } k \text{ elements of } C; \\ 0, & \text{if } x_1 \text{ is not a meet of elements of } C. \end{cases} \tag{4.4}$$

This corollary tells us that the Möbius function of L_n takes values in $\{0, \pm 1\}$ no matter the interval at which it is evaluated. Posets with this property are sometimes called *totally unimodular* (see, e.g., [15]). Theorem 4.3 also allows us to give a third proof of Theorem 1.1.

THIRD PROOF OF THEOREM 1.1. We take $n \geq 4$; smaller cases can easily be worked out explicitly. First suppose that $n - 1$ is squarefree, equalling the product of distinct primes p_1, p_2, \dots, p_k , so that $\mu(n - 1) = (-1)^k$. The claim is that for any nonempty progression $x \in L_n$, there is some coatom that does not contain x . If x contains either 1 or n , then one of the two progressions in L_n of size $n - 1$ does not contain x . Otherwise, x contains some integer $1 + m$ for $1 \leq m \leq n - 2$. Since $m < n - 1 = \text{lcm}(p_1, p_2, \dots, p_k)$, there is some prime p_i that does not divide m , hence $1 + m$ is not contained in the coatom of step size p_i . There are $k + 2$ coatoms in L_n , so Theorem 4.3 can be applied to give $\mu_n(L_n) = (-1)^{k+2} = (-1)^k = \mu(n - 1)$.

Now assume that $n - 1$ is divisible by p^2 for some prime p . Since the integer $(n - 1)/p$ is divisible by every prime dividing $n - 1$, the element $1 + (n - 1)/p$ belongs to every coatom of L_n . So \emptyset cannot be expressed as a meet of coatoms and $\mu_n(L_n) = 0$. □

5 Homology groups of the order complex

Although less direct than the first two proofs we supplied, the proof of Theorem 1.1 given in the previous section reveals much of the internal structure of L_n . We now show that it can be reinterpreted to give a complete characterisation of the homology groups of Δ_n , a strictly stronger result than Theorem 1.1. A simplicial complex Δ , as we have defined it, is simply a set system, but Δ can be embedded in Euclidean space to give rise to a topological space $|\Delta|$ called its *geometric realisation*. We will sometimes abuse notation and ascribe topological properties of $|\Delta|$ to Δ . The reduced Euler characteristic of an n -dimensional simplicial complex Δ can also be expressed as the alternating sum

$$\tilde{\chi}(\Delta) = \tilde{\chi}(|\Delta|) = \sum_{i=0}^n (-1)^i \text{rank } \tilde{H}_i(|\Delta|, \mathbf{Z}), \tag{5.1}$$

where $\tilde{H}_i(|\Delta|, \mathbf{Z})$ is the i th reduced homology group of the topological space $|\Delta|$ (whenever we refer to a homology group, we shall understand reduced homology group).

To derive the homology groups of L_n , we will require the notion of cross-cuts. A *cross-cut* C of a lattice L (with maximum $\hat{1}$ and minimum $\hat{0}$) is a subset of L not containing either of $\hat{1}$ and $\hat{0}$ such that no two elements of C are comparable and every maximal chain in the lattice contains some element of C . A subset S of L is said to be *spanning* if the join of all its elements is $\hat{1}$ and the meet of all its elements is $\hat{0}$. For a cross-cut C of a lattice L , we can define a simplicial complex $\Delta(C)$ whose vertices are the elements of C and whose faces are given by subsets of C that are *not* spanning. A paper of Folkman [9] showed that $\tilde{H}_i(\Delta(C), \mathbf{Z}) \cong \tilde{H}_i(\Delta, \mathbf{Z})$ for all i , where Δ is the order complex of L . We use this to derive the homology groups of Δ_n .

Lemma 5.1 *For $n \geq 4$, let L_n be the lattice of arithmetic progressions and let Δ_n be the order complex of $L'_n = L_n \setminus \{\emptyset, [n]\}$. Let $H_i(\Delta_n, \mathbf{Z})$ be the i th reduced homology group of Δ_n . If $n - 1$ is squarefree and equal to the product of k distinct primes, then*

$$\tilde{H}_i(\Delta_n, \mathbf{Z}) = \begin{cases} \mathbf{Z}, & \text{if } i = k; \\ 0, & \text{otherwise.} \end{cases}$$

If $n - 1$ is not squarefree, then all the homology groups of Δ_n are trivial.

PROOF: Let C be the set of coatoms of L_n , whose explicit construction was given by Lemma 4.1. Let $k = \omega(n - 1)$, so that $|C| = k + 2$. If $n - 1$ is squarefree, then as we saw earlier in the third proof of Theorem 1.1, we can express \emptyset as a meet of elements of C , so C is a spanning set. However, any proper subset C' of C is not spanning, since if c_i is the element of C that is not in C' , then we can build a chain $\emptyset \subset \dots \subset c_i \subset [n]$ that does not contain an element of C' . So every subset of C with cardinality $k + 1$ is an element of the abstract simplicial complex $\Delta(C)$, i.e., $\Delta(C)$ is the boundary of a $(k + 1)$ -dimensional simplex, whose k th homology group is \mathbf{Z} and whose other reduced homology groups are all trivial.

When $n - 1$ is not squarefree, the construction we gave in the third proof of Theorem 1.1 shows that \emptyset is not the meet of the elements of C , which means that C itself does not span. Hence $\Delta(C)$ is the $(k + 1)$ -dimensional simplex, including its interior, all of whose reduced homology groups are trivial. \square

We will use Lemma 5.1 later on to prove the stronger fact that Δ_n has the homotopy type of a sphere when $n - 1$ is squarefree.

6 Left-modularity and comodernism

An element m in a lattice L is *left-modular in L* if for all $x < y \in L$, $(x \vee m) \wedge y = x \vee (m \wedge y)$. A lattice L is *comodernistic* if every interval $[x, y] \subseteq L$ has a coatom which is left-modular in $[x, y]$. The aim of this section is to show that L_n is comodernistic. To do so, we will make use of two of the lemmas in the paper of Schweig and Woodroffe that introduced the definition of comodernism.

Lemma A ([21], Lemma 2.12) *Let m be a coatom of the lattice L . Then m is left-modular in L if and only if for every $y \in L$ with $y \not\leq m$, y covers $m \wedge y$.*

Lemma B ([21], Lemma 4.1) *Let L' be a sublattice of a lattice L . If $m \in L'$ is a left-modular coatom in L , then m is also left-modular in L' .*

Note that we have modified these lemmas slightly to suit our notation and usage; in particular, the original version of Lemma B requires only that L' be a meet subsemilattice. We begin with a small lemma.

Lemma 6.1 *For $n \geq 1$, the elements $12 \cdots (n - 1)$ and $23 \cdots n$ are left-modular in L_n .*

PROOF: Without loss of generality, let $m = 12 \cdots (n - 1)$; the case where $m = 23 \cdots n$ is symmetric. Let $y \in L_n$ be such that $y \not\leq m$, so it must be that $n \in y$; hence $m \wedge y = y \setminus \{n\}$ which is covered by y . By Lemma A, this shows that m is left-modular. \square

We are now able to show that L_n is comoderistic for all n . For brevity of notation, in the following proof we let $\uparrow_k x$ denote the *principal filter* of $x \in L_k$; that is, $\uparrow_k x = \{y \in L_k : x \leq y\}$.

Theorem 6.2 *For all $n \geq 0$, the lattice L_n is comoderistic.*

PROOF: Let $[x, y]$ be an interval in L_n . We once again employ Lemma 2.3, which says that $\downarrow y$ is isomorphic to L_k where $k = |y|$. This isomorphism sends $[x, y]$ to the interval $\uparrow_k x \subseteq L_k$, so it suffices to show that, for all $k \geq 1$ and $x \in L_k$, the principal filter $\uparrow_k x$ contains a coatom which is left-modular (in the filter). Let $A_k = B_k \cup C_k$ be the coatoms of L_k , with B_k and C_k defined as in Theorem 4.1. Clearly, the coatoms of $\uparrow_k x$ are a subset of A_k . If $\uparrow_k x \cap B_k \neq \emptyset$, then by Lemma 6.1, $\uparrow_k x$ contains a coatom which is left-modular in all of L_k , and by Lemma B it is also a left-modular coatom $\uparrow_k x$. If $\uparrow_k x \cap B_k$ is empty, then the progression x must contain both 1 and k , so $\uparrow_k x \subseteq \uparrow_k 1k$ and in particular, every coatom of $\uparrow_k x$ is also a coatom of $\uparrow_k 1k$. By another application of Lemma B, we may reduce our proof to showing that every coatom of $\uparrow_k 1k$ is left-modular in this filter.

The coatoms of $\uparrow_k 1k$ are precisely the elements in C_k . If $k - 1$ is prime, Lemma 4.1 tells us that $1k$ is a coatom, so $\uparrow_k 1k$ contains only the two elements $1k$ and $[k]$, the former of which is trivially left-modular in this interval. On the other hand, let $k - 1$ be composite and let m be a coatom of $\uparrow_k 1k$; by Lemma 4.1, m is of the form $\{1, 1 + p, \dots, k\}$ for some p dividing $k - 1$. If $y \in \uparrow_k 1k$ satisfies $y \not\leq m$, then $y = \{1, 1 + r, \dots, k\}$ where r divides $k - 1$ and p does not divide r . So $m \wedge y = \{1, 1 + s, \dots, k\}$ where $s = \text{lcm}(r, p) = rp$, hence $m \wedge y$ is covered by y and we conclude that m is left-modular by Lemma A. \square

7 EL-labelability, homotopy type, and complements

We now use the lemmas of the previous sections to demonstrate further properties of L_n . Here we show that L_n is EL-labelable, that Δ_n is either homotopy equivalent to a point or a sphere, and that L_n is complemented if and only if $n - 1$ is squarefree.

7.1 EL-labelability

Given a lattice L , let $E(L)$ be the set of all $(x, y) \in L$ such that y covers x ; thus $E(L)$ is the edge set of the Hasse diagram of L . We say that a function $\lambda : E(L) \rightarrow \mathbf{Z}$ is an

ER-labeling (or *edge-rising labeling*) if for every interval $[x, y] \subseteq L$, there is a unique maximal chain $x = x_0 < x_1 < \dots < x_s = y$ with increasing labels, that is, with

$$\lambda(x_0, x_1) < \lambda(x_1, x_2) < \dots < \lambda(x_{s-1}, x_s).$$

Let \mathbf{Z}^* denote the set of all finite sequences of integers. One defines a lexicographic partial order \preceq on \mathbf{Z}^* by declaring $(a_1, \dots, a_m) \preceq (b_1, \dots, b_n)$ if either $a_i = b_i$ for $1 \leq i \leq m$ and $m \leq n$ or else $a_i < b_i$ for the smallest i with $a_i \neq b_i$. Note that the function λ defines a map $\bar{\lambda}$ from chains in L to tuples of positive integers; namely if c is the chain formed by $x_0 < x_1 < \dots < x_s$, then

$$\bar{\lambda}(c) = (\lambda(x_0, x_1), \lambda(x_1, x_2), \dots, \lambda(x_{s-1}, x_s)).$$

Let λ be an ER-labeling with the further property that for all $[x, y]$, the unique increasing maximal chain m has $\bar{\lambda}(m) \preceq \bar{\lambda}(m')$ for all other maximal chains m' in $[x, y]$. Such an ER-labeling is called an *EL-labeling* (or *edge-lexicographic labeling*). A lattice that admits an ER-labeling is said to be *ER-labelable* and one that admits an EL-labeling is *EL-labelable*.

A paper of Li showed that comodernistic lattices are EL-labelable [18], so in particular we find that for all $n \geq 0$, L_n is EL-labelable. The looser property of ER-labelability is useful in certain enumerative problems. For example, it has been shown that the zeta and Möbius transforms for ER-labelable posets P can be computed in at most $|E(P)|$ elementary arithmetic operations [17].

7.2 Homotopy type

A simplicial complex Δ is *nonpure shellable* if its facets can be given an order C_1, C_2, \dots, C_m such that for all $2 \leq k \leq m$, the facets in the complex $(\bigcup_{i=1}^{k-1} C_i) \cap C_k$ all have dimension $\dim C_k - 1$. The earliest treatment of nonpure shellable complexes was carried out by Björner and Wachs in [2] and [3]; Corollary 13.3 of the latter asserts that a nonpure shellable complex is homotopy equivalent to a wedge of spheres. Proposition 2.3 of an earlier paper by the same authors [1] states that EL-labelable posets are nonpure shellable, so Δ_n is homotopy equivalent to a wedge of spheres. In fact, Δ_n is either contractible or homotopy equivalent to a single sphere, as the following strengthening of Lemma 5.1 shows.

Theorem 7.1 *Let Δ_n be the order complex of the lattice of arithmetic progressions L_n . If $n - 1$ is not squarefree, then Δ_n is contractible. Otherwise, Δ_n has the homotopy type of S^k , where k is the number of distinct primes dividing $n - 1$.*

PROOF: We already know, from the above discussion, that Δ_n is homotopy equivalent to a wedge of spheres. If the wedge product consisted of more than one sphere, then the sum over the ranks of the reduced homology groups of Δ_n would be greater than 1. But by Lemma 5.1, this sum equals 0 when $n - 1$ is not squarefree, in which case Δ_n must have the homotopy type of a point, and when $n - 1$ is squarefree it equals 1, meaning that there is exactly one sphere in the wedge product. \square

7.3 Complements

We finish with a miscellaneous result about complements in L_n . A lattice L with maximum element $\widehat{1}$ and minimum element $\widehat{0}$ is said to be *complemented* if for all $x \in L$, there exists $y \in L$ such that $x \vee y = \widehat{1}$ and $x \wedge y = \widehat{0}$. The elements x and y are called *complements* of one another, and if we remove the condition that $x \wedge y = \widehat{0}$, then x and y are said to be *upper semicomplements*. The next theorem gives a necessary and sufficient condition for L_n to be complemented.

Theorem 7.2 *Let $n \geq 2$. The lattice L_n is complemented if and only if $n - 1$ is squarefree. In particular, if $n - 1$ is not squarefree, there exists an element $x \notin \{\emptyset, [n]\}$ of L_n whose only upper semicomplement is $[n]$.*

PROOF: For the “if” direction, we note that when $n - 1$ is squarefree, we have $\mu_n(L_n) \neq 0$, which, by a result of Crapo (namely, the corollary to Theorem 3 in [6]), implies that L_n is complemented. For the converse, suppose that $n - 1$ is divisible by p^2 for some prime p . Consider the progression

$$x = \left\{ 1 + \frac{n-1}{p}, 1 + \frac{2(n-1)}{p}, \dots, n - \frac{n-1}{p} \right\},$$

which has length $p - 1$ and is thus not empty. Note that any $x' \in L$ satisfying $x' \vee x = [n]$ must contain both 1 and n and the step size r must be coprime to $(n - 1)/p$. We also know that r must divide $n - 1$. But the only such integer r is 1, in which case we see that x must be $[n]$. \square

Acknowledgements

The bulk of this paper was written when all three authors were students at McGill University and the first and third authors were supported by the Natural Sciences and Engineering Research Council of Canada. We would like to thank Andrew Granville for helpful conversations and for giving us the key idea in solving the recurrence that appears in the first two proofs of Theorem 1.1. We thank Daniel Wise for enjoyable conversations and for his advice on the topological section in particular. We are grateful also to Jukka Kohonen for answering a question of the first author on MathOverflow and for the enlightening discussions that followed via email. Lastly, we thank our comrades Amanda Gu and Rosie Zhao for technical feedback on a preliminary draft.

References

- [1] A. Björner and M. L. Wachs, On lexicographically shellable posets, *Trans. Amer. Math. Soc.* **277** (1983), 323–341.
- [2] A. Björner and M. L. Wachs, Shellable nonpure complexes and posets I, *Trans. Amer. Math. Soc.* **348** (1996), 1299–1327.
- [3] A. Björner and M. L. Wachs, Shellable nonpure complexes and posets II, *Trans. Amer. Math. Soc.* **349** (1997), 3945–3975.
- [4] A. Björner, A cell complex in number theory, *Adv. Appl. Math.* **46** (2011), 71–85.
- [5] J. Brillhart, M. Filaseta and A. Odlyzko, On an irreducibility theorem of A. Cohn, *Canad. J. Math.* **33**, 1055–1059.
- [6] H. H. Crapo, The Möbius function of a lattice, *J. Combin. Theory* **1** (1966), 126–131.
- [7] R. Ehrenborg, L. Govindaiah, P. S. Park and M. Readdy, The van der Waerden complex, *J. Number Theory* **172** (2017), 287–300.
- [8] P. Flajolet and R. Sedgewick, *Analytic Combinatorics* New York: Cambridge University Press, 2009.
- [9] J. Folkman, The homology groups of a lattice, *J. Math. Mech.* **15** (1966), 631–636.
- [10] H. Furstenberg, On the infinitude of primes, *Amer. Math. Monthly* **62** (1955), 353.
- [11] M. K. Goh and R. Y. Zhao, Arithmetic subsequences in a random ordering of an additive set, *Integers: Electron. J. Combin. Number Theory* **21** (2021), art. A89.
- [12] S. W. Golomb, A connected topology for the integers, *Amer. Math. Monthly* **66** (1959), 663–665.
- [13] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, Reading: Addison-Wesley, 1989.
- [14] B. Green and T. Tao, The primes contain arbitrarily long arithmetic progressions, *Ann. Math.* **167** (2008), 481–547.
- [15] C. Greene, A class of lattices with Möbius function $\pm 1, 0$, *European J. Combin.* **9** (1988), 225–240.
- [16] B. Hooper and A. Van Tuyl, A note on the van der Waerden complex, *Math. Scand.* **124** (2019), 179–187.

- [17] P. Kaski, J. Kohonen and T. Westerböck, Fast Möbius inversion in semimodular lattices and ER-labelable posets, *Elec. J. Combin.* **23** (3) (2016), #P3.26.
- [18] T. Li, EL-shelling on comodernistic lattices, *J. Combin. Theory Ser. A* **177** (2021), Paper No. 105334, 8pp.
- [19] J. Munkres, *Topology*, 2nd edition, Upper Saddle River: Prentice Hall, 2000.
- [20] G.-C. Rota, On the foundations of combinatorial theory I, Theory of Möbius Functions, *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete* **2** (1964), 340–368.
- [21] J. Schweig and R. Woodrooffe, A broad class of shellable lattices, *Adv. Math.* **313** (2017), 537–563.
- [22] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arith.* **27** (1975), 199–245.
- [23] B. L. van der Waerden, Beweis einer Baudetschen Vermutung, *Nieuw Arch. Wiskd.* **15** (1927), 212–216.

(Received 8 Jan 2022; revised 24 Aug 2022)