EUCLIDEAN LATTICES: THEORY AND APPLICATIONS

LENNY FUKSHANSKY AND CAMILLA HOLLANTI

Abstract. In this editorial survey we introduce the special issue of the journal Communications in Mathematics on the topic in the title of the article. Our main goal is to briefly outline some of the main aspects of this important area at the intersection of theory and applications, providing the context for the articles showcased in this special issue.

Contents

1. Introduction

A *lattice* L in a Euclidean n-dimensional space $\mathbb{E}_n$ is a discrete subgroup of rank $1 \leq k \leq n$. This is equivalent to saying that there exists a collection of linearly independent elements $\boldsymbol{a}_1, \dots, \boldsymbol{a}_k \in \mathbb{E}_n$ (always written as column vectors) such that

$$L = \left\{ \sum_{i=1}^{k} c_i \boldsymbol{a}_i : c_1, \dots, c_k \in \mathbb{Z} \right\} = A\mathbb{Z}^k,$$

where $\boldsymbol{a}_1, \dots, \boldsymbol{a}_k$ is a basis for L and $A = (\boldsymbol{a}_1 \ \dots \ \boldsymbol{a}_k)$ is the corresponding $n \times k$ basis matrix. If this is the case, then for any $U \in \mathrm{GL}_k(\mathbb{Z})$,

$$L = A\mathbb{Z}^k = (AU)\mathbb{Z}^k,$$

2020 *Mathematics Subject Classification.* 11HXX, 11EXX, 52CXX, 11J25, 11P21, 11T71, 94A60, 94B75.

Key words and phrases. lattices, quadratic forms, geometry of numbers, sphere packing, Diophantine approximations, coding theory, cryptography.

Fukshansky was partially supported by the Simons Foundation grant #519058.

Hollanti was partially supported by the Academy of Finland grant #351271 and by the Finnish Ministry of Defence MATINE grant #2500M-0147.

and so AU is again a basis matrix for L. Identifying $\mathbb{E}_n$ with the real space $\mathbb{R}^n$, we can therefore identify the space of all rank-k lattices in $\mathbb{R}^n$ with the space $\mathrm{GL}_k(\mathbb{R})/\mathrm{GL}_k(\mathbb{Z})$ of all orbits of $\mathrm{GL}_k(\mathbb{R})$ under the action of $\mathrm{GL}_k(\mathbb{Z})$ by right multiplication.

Theory of Euclidean lattices connects number theory to convex and discrete geometry. The study of lattices originally emerged as an important subject in connection with classical discrete optimization problems like sphere packing, covering and kissing number problems, dating as far back as the celebrated 1611 conjecture of Kepler and even earlier; see the classical books of Conway & Sloane [8] and of Martinet [21] for a fairly comprehensive exposition of lattice theory and its many connections, as well as [28] for a popular account of the fascinating history of Kepler's conjecture. Lattices have really come into their own in the context of Minkowski's geometry of numbers (see [23] for Minkowski's original treatise, as well as the standard books [6] by Cassels, [15] by Gruber & Lekkerkerker and [14] by Gruber for more contemporary accounts).

Theory of lattices has seen some very exciting developments and applications over the last century, including Minkowski's proof of the finiteness of class number, major results in arithmetic theory of quadratic forms, advances in discrete and convex geometry and optimization, Diophantine approximations, geometric combinatorics, coding theory, cryptography, and many other areas of mathematics. The recent decades have, in particular, seen such major breakthroughs as the proof of Kepler's conjecture by Hales & Ferguson [16], affirming that the face-centered-cubic lattice provides the densest sphere packing in dimension 3, as well as the spectacular results by Viazovska *et al.* [32], [7] on the optimality of E_8 and the Leech lattice for packing density in dimensions 8 and 24, respectively (Maryna Viazovska received a Fields medal for this work in 2022).

The main goal of our special issue is to collect in one place several of the recent developments and expository surveys on the various aspects of lattice theory and its applications. In the following sections, we will briefly introduce a few different facets of this theory and indicate how different contributions of this special issue fit into the general framework.

2. Geometry of numbers and Diophantine approximations

The first essential invariant of the lattice L as above is its *determinant*, which is defined as

$$\det(L) := \sqrt{\det(A^\top A)}$$

for any choice of a basis matrix A: this is well-defined, since $|\det(U)| = 1$ for any $U \in \mathrm{GL}_k(\mathbb{Z})$. Analytically, this is the volume of a fundamental parallelotope

$$\left\{A\boldsymbol{x} : \boldsymbol{x} \in [0,1)^k\right\},$$

which is a full set of coset representatives for the quotient group V/L, where $V = \mathrm{span}_{\mathbb{R}} L$. In fact, $\det(L)$ is the volume of the closure of any such fundamental domain, including the important *Voronoi cell*

$$\mathcal{V}(L) = \{\boldsymbol{x} \in V : \|\boldsymbol{x}\| \leq \|\boldsymbol{x} - \boldsymbol{y}\| \ \forall\ \boldsymbol{y} \in L\},$$

i.e., the set of all points in V that are no further from the origin than from any other point of the lattice. Our lattice L has full rank in the k-dimensional subspace

V of $\mathbb{R}^n$, which can be identified with the Euclidean space $\mathbb{R}^k$. As such, we will only talk of full rank lattices in $\mathbb{R}^n$ from now on.

We can now define the *sphere packing* and the *sphere covering* associated to L: inscribe a closed ball B_1 in $\mathbb{R}^n$ of maximal possible radius into $\mathcal{V}(L)$ and circumscribe a ball B_2 of minimal possible radius around $\mathcal{V}(L)$, then translating $\mathcal{V}(L)$ by all the points of L we obtain a packing of non-overlapping translates of B_1 in $\mathbb{R}^n$ and a covering of $\mathbb{R}^n$ by translates of B_2. Hence the radius of B_1 is called the *packing radius* $r(L)$ of L and the radius of B_2 the *covering radius* $R(L)$ of L. Now, the *packing density* $\delta(L)$ and the *covering thickness* $\Theta(L)$ are given by the formulas

$$\delta(L) = \frac{\mathrm{Vol}_n(B_1)}{\mathrm{Vol}_n(\mathcal{V}(L))} = \frac{\omega_n r(L)^n}{\det(L)},\ \Theta(L) = \frac{\mathrm{Vol}_n(B_2)}{\mathrm{Vol}_n(\mathcal{V}(L))} = \frac{\omega_n R(L)^n}{\det(L)},$$

where ω_n is the volume of a unit ball $\mathbb{B}_n$ in $\mathbb{R}^n$. In fact, these radii are closely related to another collection of important invariants of the lattice L, called successive minima.

Let K be a closed convex $\mathbf{0}$-symmetric set of positive volume in $\mathbb{R}^n$. The *successive minima* of the lattice L with respect to K,

$$0 < \lambda_1(L,K) \leq \cdots \leq \lambda_n(L,K),$$

are defined as

$$\lambda_i(L,K) = \min\left\{t \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \mathrm{span}_{\mathbb{R}}\, L \cap tK \geq i\right\},$$

i.e., the smallest real number t so that the homogeneous expansion of K by a factor of t contains at least i linearly independent points of L. In the special case when K is the unit ball $\mathbb{B}_n$ centered at the origin in $\mathbb{R}^n$, we refer to $\lambda_i(L,K)$ simply as $\lambda_i(L)$, the successive minima of the lattice. It is then not difficult to see that the packing radius is precisely half the distance from the origin to the shortest nonzero lattice point, i.e.

$$r(L) = \frac{1}{2}\lambda_1(L).$$

The more delicate inequalities of Jarnik (see, e.g., [15, Section 13.2, Theorem 1 and Theorem 4]) also assert that the covering radius satisfies

$$\frac{1}{2}\lambda_n(L) \leq R(L) \leq \frac{1}{2}\sum_{i=1}^{n}\lambda_i(L).$$

Successive minima have been studied extensively by Minkowski himself and by many other mathematicians working in number theory, discrete and convex geometry, and even analysis. In particular, Minkowski's inequalities on successive minima state that

$$\frac{2^n \det(L)}{n!\,\mathrm{Vol}_n(K)} \leq \prod_{i=1}^{n}\lambda_i(L,K) \leq \frac{2^n \det(L)}{\mathrm{Vol}_n(K)}. \tag{1}$$

The survey paper [1] by I. Aliev & M. Henk in this special issue gives an overview of the impact of successive minima on convex and discrete geometry. One significant application of successive minima inequalities that the authors discuss is Siegel's lemma, a vital tool in Diophantine approximations and transcendental number theory, which provides a bound on the size of a "smallest" nonzero solution (or, more generally, a collection of such solutions) to a system of linear forms over a given ring or field of arithmetic interest. The fact that such a solution exists over

a given field is guaranteed by the assumption that these linear forms are linearly dependent over the same field.

On the other hand, assume that we have a system of linear forms that are linearly independent over $\mathbb{Q}$. Then they will not be simultaneously equal to zero at any nonzero point of the integer lattice. A natural question in Diophantine approximations is how small can such a collection of linear forms in n variables simultaneously be on $\mathbb{Z}^n \setminus \{\mathbf{0}\}$? This question can be made precise by studying the extreme values of certain appropriately defined exponents of approximation, which is done in the paper [13] by O. German in our special issue. His main tool is a lemma of Davenport on successive minima. At the end of this paper, a question about the spectra of these newly introduced Diophantine exponents is formulated.

3. Special classes of lattices

As we remarked above, the analogues of Kepler's conjecture on the densest possible sphere packing in dimension 3 has also been proved in dimensions 8 and 24. In fact, the optimal sphere packing has been obtained earlier in dimension 2 by L. Fejes Tóth [30], who gave the first complete proof of what was previously known as Thue's theorem. These are all the dimensions (besides the trivial dimension 1) in which the optimal sphere packings are known. If, however, we restrict our consideration to lattice packings only, then the optimal results are known in dimensions $1 \leq n \leq 8$ and $n = 24$ (see [8]).

One can then pose a natural question: what properties should a lattice possess to be a potential candidate for maximizing lattice packing density in its dimension? From our discussion above, it is evident that the packing density of a full-rank lattice L in $\mathbb{R}^n$ is given by the formula

$$\delta(L) = \frac{\omega_n \lambda_1(L)^n}{2^n \det(L)}.$$

Let us define an equivalence relation of similarity on lattices in $\mathbb{R}^n$ as follows: two lattices L_1 and L_2 are called *similar* if there exists a positive real constant α and an $n \times n$ real orthogonal matrix U so that $L_2 = \alpha U L_1$. In this case, it is easy to see that $\delta(L_1) = \delta(L_2)$, and so the packing density is constant on a given similarity class. Hence, restricting to unimodular lattices (determinant = 1) we can write

$$\delta(L) = \frac{\omega_n}{2^n} \lambda_1(L)^n,$$

meaning that maximizing packing density is equivalent to maximizing the first successive minimum $\lambda_1(L)$. By Minkowski's inequalities (1), the product of all successive minima in this case is bounded by dimensional constants:

$$\frac{2^n}{n!\,\omega_n} \leq \prod_{i=1}^{n} \lambda_i(L) \leq \frac{2^n}{\omega_n},$$

where $0 < \lambda_1(L) \leq \cdots \leq \lambda_n(L)$. Thus the first step in the direction of maximizing $\lambda_1(L)$ is to take a lattice L with all successive minima equal: lattices like this are called *well-rounded (WR)*. This property is preserved under similarity, so we can talk of WR similarity classes, of which there are infinitely many in any dimension $n \geq 2$. There has been quite a bit of work in the recent years on various explicit

algebraic constructions of WR lattices. Some most notable such constructions come from ideals in algebraic number fields via Minkowski embedding into Euclidean space, the so-called *ideal lattices*. As such, an interesting question remains: under which conditions does an ideal in a number field give rise to WR ideal lattices? A detailed study of WR ideal lattices has been initiated in [12]. While this question has been answered for quadratic number fields and for some special families of number fields of higher degree, in general it is wide open. In article [29] in our special issue, D.T. Tran, N. H. Le and H. T. N. Tran conduct a thorough investigation and establish conditions for the existence of WR ideal lattices coming from cyclic number fields of degree 3 and 4. Their paper starts out with a brief overview of the previous results in this area and also contains a fairly extensive bibliography.

The packing density function is continuous on $\mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z})$, the space of full-rank lattices in $\mathbb{R}^n$, and hence we can talk about its local extrema on this space. While the WR condition is necessary for a local maximum to be achieved, this condition is not sufficient. Define the set *of minimal vectors* of a lattice L as

$$S(L) = \{\boldsymbol{x} \in L : \|\boldsymbol{x}\| = \lambda_1(L)\},$$

and let m be the cardinality of $S(L)$. Notice that m is necessarily even, since minimal vectors come in $\pm$ pairs (more generally, m is divisible by the order of the group of linear automorphisms of L since it acts on $S(L)$ by left multiplication). Further, if L is WR then $m \geq 2n$. Lattice L is called *eutactic* if there exist positive real coefficients $c_1, \ldots, c_m$ such that for any vector $\boldsymbol{v} \in \mathbb{R}^n$,

$$\|\boldsymbol{v}\| = \sum_{i=1}^{m} c_i \left(\boldsymbol{v}^\top \boldsymbol{x}_i\right)^2,$$

where $S(L) = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m\}$. On the other hand, a lattice L is called *perfect* if the space of $n \times n$ real symmetric matrices $\mathrm{Sym}_n(\mathbb{R})$ can be spanned (as a real vector space) by symmetric matrices coming from the minimal vectors of L, i.e.

$$\mathrm{Sym}_n(\mathbb{R}) = \mathrm{span}_{\mathbb{R}} \left\{\boldsymbol{x}\boldsymbol{x}^\top : \boldsymbol{x} \in S(L)\right\}.$$

Since $\dim_{\mathbb{R}} \mathrm{Sym}_n(\mathbb{R}) = \frac{n(n+1)}{2}$ and for any vector $\boldsymbol{x} \in S(L)$, $\boldsymbol{x}\boldsymbol{x}^\top = (-\boldsymbol{x})(-\boldsymbol{x})^\top$, this perfection condition implies that the cardinality m of $S(L)$ is at least $n(n+1)$. The eutaxy and perfection conditions on lattices are independent (i.e., there are eutactic non-perfect lattices and there are perfect non-eutactic lattices) and they are both preserved under similarity. Furthermore, there are only finitely many eutactic and finitely many perfect similarity classes in any given dimension, although their number grows very fast with the dimension (for instance, for sufficiently large n the number of perfect similarity classes in $\mathbb{R}^n$ is $> e^{n^{1-\varepsilon}}$ for any $\varepsilon > 0$; see [2]). Both, perfect and eutactic lattices are necessarily WR and a famous theorem of Voronoi (1908) asserts that a lattice corresponds to a local maximum of the packing density function in its dimension (called *extreme* lattice) if and only if it is perfect and eutactic (see, e.g., [21]). This observation drives an interest in classification of perfect lattices, a subject of active research often pursued in the language of quadratic forms.

For $L = A\mathbb{Z}^n$, the Euclidean norm of any vector $\boldsymbol{x} = A\boldsymbol{y} \in L$ can be computed as

$$\|\boldsymbol{x}\|^2 = Q_A(\boldsymbol{y}) := \boldsymbol{y}^\top \left(A^\top A\right) \boldsymbol{y},$$

where $Q_A(\boldsymbol{y})$ is a positive definite quadratic form with a symmetric coefficient matrix $A^\top A$. Quadratic forms corresponding to different bases of the same lattice

are called *arithmetically equivalent*: they have the same spectrum of values on $\mathbb{Z}^n$. There is a bijective correspondence between positive definite arithmetic equivalence classes of quadratic forms in n variables and lattices in $\mathbb{R}^n$. The symmetric coefficient matrix of a positive definite quadratic form is then called perfect if the corresponding lattice is perfect. The paper by V. Dannenberg and A. Schürmann [10] in our special issue builds on the classical theory of such perfect matrices to introduce and initiate a study of their generalization, the so-called perfect copositive matrices: a matrix $B \in \mathrm{Sym}_n(\mathbb{R})$ is called *copositive* if

$$\boldsymbol{y}^\top B\boldsymbol{y} \geq \mathbf{0}$$

for all $\boldsymbol{y}$ in the positive orthant $\mathbb{R}^n_{\geq 0}$ (in contrast to the usual positive definite matrices satisfying $\boldsymbol{y}^\top B\boldsymbol{y} \geq \mathbf{0}$ for all nonzero $\boldsymbol{y} \in \mathbb{R}^n$). The authors look at the cone of copositve matrices and study the distribution of perfect matrices in this cone.

4. Arithmetic of quadratic forms

As indicated above, the study of lattices is intrinsically connected to the arithmetic theory of quadratic forms. A key question in that theory is that of representation. A quadratic form $Q(\boldsymbol{y})$ in n variables can always be written in the form

$$Q(\boldsymbol{y}) = \boldsymbol{y}^\top B\boldsymbol{y},$$

where B is a real symmetric coefficient matrix. This form Q is called *integral* if $Q(\boldsymbol{y}) \in \mathbb{Z}$ for every $\boldsymbol{y} \in \mathbb{Z}^n$ and it is called *classically integral* if B is an integer matrix; notice that this second property is stronger than the first. An integral form Q is said to *represent* an integer m if there exists $\boldsymbol{y} \in \mathbb{Z}^n$ such that $Q(\boldsymbol{y}) = m$, and Q is said to be *universal* if it represents every positive integer m. This is equivalent to the corresponding lattice containing vectors of every possible (squared) integer Euclidean norm.

Perhaps the starting point of the theory of universal quadratic forms is the famous classical theorem of Lagrange (1770) stating that the positive definite integral quadratic form given by the sum of four squares is universal (see, for instance, [33] for details). On the other hand, no positive definite integral form in fewer than four variables can be universal. The major results on universal forms from the past thirty years include the impressive necessary and sufficient universality criteria for integral and classically integral quadratic forms in any number of variables, known as theorems 290 and 15, respectively.

The survey article by V. Kala [17] (based on the author's lectures on this subject) in this special issue gives an overview of the theory of universal quadratic forms, including these celebrated theorems, but placing the main focus on the recent developments for quadratic lattices over ring of integers $\mathcal{O}_K$ in a totally real number field K. The key tool emphasized by the author is the notion of an indecomposable element in $\mathcal{O}_K$: a totally positive element in $\mathcal{O}_K$ is called *indecomposable* if it cannot be written as a sum of two other totally positive elements in the same ring. The significance of indecomposables in the context of quadratic forms is that they essentially appear as coefficients of diagonal universal forms over $\mathcal{O}_K$ and hence the number of their square classes gives a lower bound on the number of variables in

which such forms can exist. The author carefully develops the theory of indecomposables in this context, showing also some interesting connections, including one to continued fractions.

5. Geometric combinatorics and integer geometry

Another important facet of the theory has to do with counting lattice points in compact domains in $\mathbb{R}^n$. More specifically, let us start with a full rank lattice L and a compact measurable set $K \subset \mathbb{R}^n$ of positive volume. Let $r \in \mathbb{R}_{>0}$ and define the counting function

$$f_{L,K}(r) = |L \cap rK| .$$

One can ask how does $f_{L,K}(r)$ grow as $r \to \infty$? The first observation is that each point $\boldsymbol{x} \in L$ is contained in its unique translate of the Voronoi cell $\boldsymbol{x} + \mathcal{V}(L)$, hence counting lattice points can be replaced by counting translates of the Voronoi cell. As r becomes large, the number of such translates that are fully contained in rK gives the main term of the asymptotic formula for $f_{L,K}(r)$, whereas the error term comes from the number of such translates intersecting tie boundary of rK whose corresponding lattice points are in rK. Hence the main term can be approximated simply by the quotient of the volume of rK by the volume of the Voronoi cell, $\det(L)$. Under appropriate smooth conditions on the boundary of K, such as Lipschitz parametrizability, the error term can be controlled and the following asymptotic holds (see, e.g., [19], Chapter VI, §2, Theorem 2):

$$f_{L,K}(r) = \frac{\mathrm{Vol}_n(K)}{\det(L)}\ r^n + O(r^{n-1}).$$

A considerably more delicate problem is to give tight (and as explicit as possible) estimates on the error term

$$\left| f_{L,K}(r) - \frac{\mathrm{Vol}_n(K)}{\det(L)}\ r^n \right| .$$

There is a vast amount of literature on different versions of this counting problem. In fact, this problem is not fully resolved even in a seemingly simple case of $L = \mathbb{Z}^2$ and K being the unit circle S^1 – this is the famous Gauss circle problem, where the standing conjecture is that

$$\left| f_{\mathbb{Z}^2,S^1}(r) - \pi r^2 \right| = O(r^{1/2+\varepsilon})$$

for any $\varepsilon > 0$.

A variation of this counting problem is treated in a paper of J. D. Vaaler [31] in this special issue: given an $n \times m$ real matrix A, $m \le n$, obtain an estimate on the error term

$$\left| f_{A\mathbb{Z}^m, rB(\boldsymbol{x})} - \mathrm{Vol}_m(B(\boldsymbol{x}))\ r^m \right|$$

for the number of points of the lattice $A\mathbb{Z}^m$ in the ball $rB(\boldsymbol{x})$ of radius r centered at an arbitrary point $\boldsymbol{x}$ in the subspace $A\mathbb{R}^m \subseteq \mathbb{R}^n$ spanned by this lattice, as $r \to \infty$. While a number of estimates on such quantities have been previously obtained (see [31] for some bibliography), the author's estimate is explicit and uniform over all matrices A with norm bounded by an explicit constant. Further, his inequality takes a particularly simple form for dimension $m = 3$. The author's method uses careful analysis of extremal functions; as such, Bessel functions naturally occur in the estimates.

The situation with counting integer lattice points becomes more manageable when the compact set K is a convex lattice polytope. Indeed, assume K is a convex polytope in $\mathbb{R}^n$ with positive volume and vertices at points of the integer lattice $\mathbb{Z}^n$. Consider the counting function $f_{\mathbb{Z}^n,K}(r)$ for integer values of the homogeneous expansion parameter r. A classical theorem of Ehrhart (1962) states that $f_{\mathbb{Z}^n,K}(r)$ is a polynomial in r of degree n with integer coefficients, where the leading coefficient is $\mathrm{Vol}_n(K)$ (see [3] as well as Chapter 12 of [22] for a nice introduction to Ehrhart theory). This polynomial is called *Ehrhart polynomial* of the polytope K. More generally, let us define the *integer point transform* of the polytope rK by

$$\sigma_{rK}(\boldsymbol{\xi}) = \sum_{\boldsymbol{v}\in\mathbb{Z}^n\cap rK} e^{2\pi i(\boldsymbol{v}^\top\boldsymbol{\xi})},$$

for all $\boldsymbol{\xi}\in\mathbb{R}^n$. In particular, notice that

$$\sigma_{rK}(\mathbf{0}) = \sum_{\boldsymbol{v}\in\mathbb{Z}^n\cap rK} 1 = f_{\mathbb{Z}^n,K}(r),$$

and hence the integer point transform of a polytope is a certain generalization of Ehrhart polynomial. In his paper [26] in this special issue, S. Robins proves that the integer point transform is a complete invariant of the polytope in the following sense: two lattice polytopes K_1 and K_2 are equal to each other if and only if $\sigma_{K_1}(\boldsymbol{\xi}^*) = \sigma_{K_2}(\boldsymbol{\xi}^*)$ for

$$\boldsymbol{\xi}^* = \frac{1}{\pi}(\sqrt{p_1},\dots,\sqrt{p_n})^\top,$$

where $p_1,\dots,p_n$ are the first n primes. In fact, the author first uses the Lindemann–Weierstrass theorem from transcendental number theory to prove the analogous property for equality of arbitrary finite sets of integer lattice points instead of sets contained in polytopes, and then passes to polytopes. Further, he proves the complete invariant property also for Fourier transforms of general rational polyhedra. Additionally, he discusses lattice spanning properties of polytopes and the integer point transform of finite abelian groups.

Ehrhart's theorem is often seen as a higher-dimensional generalization of the famous Pick's theorem (1899; see, e.g., [3] and Chapter 2 of [18]): if S is the area of an integer polygon in the plane, I is the number of integer lattice points in its interior and E is the number of integer lattice points on its boundary, then

$$S = I + \frac{E}{2} - 1.$$

The essential feature of this theorem is that it connects a combinatorial notion (the number of integer lattice points in a polygon) with an analytic notion (the area of this polygon). This is the main idea of integer geometry: introducing "discrete" ways of measuring some traditionally "continuous" objects, as alluded to in the title of Beck & Robins's book [3]. A good introduction to integer geometry and its connections to continued fractions is given in Karpenkov's book [18]. In their paper [4] in this special issue, J. Blackman, J. Dolan and O. Karpenkov take this exploration a step further and introduce the theory of multidimensional integer trigonometry. The integer length and integer area are defined in terms of indices of sublattices in the integer lattice generated by lattice points on a given line segment or in a given triangle (which then generalizes to arbitrary polygons via sums over triangulations). Integer area can then be used to define integer trigonometric functions in the plane,

which are also closely connected to continued fractions. After giving a careful exposition of planar integer trigonometry, the authors of [4] present a generalization of this theory to higher dimensions via integer volume of appropriate simplices. They prove a variety of different properties of integer trigonometric functions in arbitrary dimensions and discuss an algorithmic approach to constructions of rational polyhedra via given collections of rational cones. They also discuss approximations of simplicial cones, which generalize classical approximation by continued fractions.

6. Applications to coding theory and cryptography

Arithmetic lattices have also made their way into many applications, perhaps most notably within coding theory and cryptography.

6.1. **Lattices from error-correcting codes.** The association of lattices with error-correcting codes is natural and, in order to reduce the decoding complexity, a possible direction is the construction of multilevel lattices from a family of nested codes, allowing for *multistage decoding*. Several different constructions have been used to derive lattices from codes [8]. To provide one explicit example, let $\rho : \mathbb{Z}_q \to \mathbb{Z}$ be the standard inclusion map, which can be naturally extended to vectors and matrices. Then, the q-ary Construction A lattice associated to the linear code $C \subseteq \mathbb{Z}_q^n$ can be defined as

$$L_A(C) = \rho(C) + q\mathbb{Z}^n.$$

In the article [11] in this special issue, F. do Carmo Silva, A. P. de Souza, E. Strey, and S. I. R. Costa consider Constructions D, D$'$, and A from nested q-ary linear codes over $\mathbb{Z}_q$. They study the volume, L_P-minimum distance ($1 \leq P \leq \infty$), and lower bounds for the coding gain of these constructions. Further, the aforementioned multistage decoding method is extended with re-encoding to Construction D$'$ from q-ary linear codes under specific conditions. The definitions of Constructions D and D$'$ are somewhat more involved, and we refer the reader to the article for more details.

6.2. **Lattice-based cryptography.** One of the most promising paradigms for post-quantum security is *lattice-based cryptography*, often based on different variants of the so-called *learning with errors (LWE)* problem [25]. The hardness of such cryptosystems can be proved by providing a reduction from a known hard lattice problem, e.g., the approximate shortest vector problem.

To give an example, let us consider the ring $R_q = \mathbb{F}_q[x]/(f(x))$, where q is prime and $f(x) \in \mathbb{Z}[x]$ is monic and irreducible. The polynomial learning with errors (PLWE) [27] decision problem asks to distinguish, with a non-negligible advantage, a sample $(a, b = as+e) \in R_q^2$, where s and e are drawn from an appropriate discrete Gaussian distribution, from a uniformly random sample $(a, b) \in R_q^2$. In article [5] in our special issue, I. Blanco-Chacón, R. Durán-Diáz, R. Njah Nchiwo, and B. Barbero-Lucas study a decisional attack against a version of the PLWE problem in which the samples are taken from a certain proper subring of large dimension of the cyclotomic ring $\mathbb{F}_q[x]/(\Phi_{p^k}(x))$ for $k > 1$, Φ not totally split, and $q \equiv 1 \pmod{p}$. The attack exploits the fact that the roots of Φ have zero trace over suitable sub-extensions. This allows for a good attack success probability as a function of input samples. The paper points out a nice open question regarding the existence of rings with the related distribution-respecting reduction map. We refer to the

article for more details as well as for an exposition on the ring and polynomial LWE problems.

6.3. **Lattice codes for secure wireless communications.** Yet another interesting application of arithmetic lattices appears in the context of *physical layer security*. Namely, lattice coset codes can be utilized for communication over the wireless medium, where eavesdroppers may receive the transmitted signals in addition to the legitimate receiver [24]. The security of such physical layer communications can be measured in many different ways, including the *eavesdropper's correct decision probability* or the *information leakage*. It has been shown that both of these quantities are bounded from above by the so-called *flatness factor* [20], yielding a natural criterion for the flatness factor of the lattice to be minimized. Essentially, the flatness factor $\epsilon_L(\sigma)$ measures the deviation of the lattice Gaussian distribution from the uniform distribution on a Voronoi cell, and it is closely related to the lattice theta series $\Theta_L(q) = \sum_{x \in L} q^{||x||^2}$ as follows:

$$\epsilon_L(\sigma) = \frac{\mathrm{Vol}(L)}{(\sqrt{2}\pi\sigma)^n}\Theta_L(e^{-\frac{1}{2\sigma^2}}) - 1 = \Theta_{L^*}(e^{-2\pi\sigma^2}) - 1,$$

where L^* denotes the dual lattice.

For a "flat" lattice, it is harder to distinguish the received message from a uniformly random sample. In order to minimize the flatness factor, well-rounded lattices have been proposed as a coding solution [9]. This motivates the search for good well-rounded lattices in small and moderate dimensions, in addition to the purely theoretical interest. In this special issue, well-rounded ideal lattices from cyclic cubic and quartic fields are studied in article [29], as already mentioned in Section 3.

Acknowledgement: We wish to thank the referees for the thorough read and helpful comments.

References

[1] I. Aliev and M. Henk. Minkowski's successive minima in convex and discrete geometry. *Commun. Math.*, 31(2), 2023.
[2] R. Bacher. On the number of perfect lattices. *J. Théor. Nombres Bordeaux*, 30(3):917–945, 2018.
[3] M. Beck and S. Robins. *Computing the continuous discretely. Integer-point enumeration in polyhedra. 2nd edition.* Undergraduate Texts in Mathematics. Springer, New York, 2015.
[4] J. Blackman, J. Dolan, and O. Karpenkov. Multidimensional integer trigonometry. *Commun. Math.*, 31(2), 2023.
[5] I. Blanco-Chacón, B. Barbero-Lucas, R. Durán-Dıaz, and R. Y. Njah Nchiwo. Trace-based cryptanalysis of cyclotomic $R_{q,0} \times R_q$-PLWE for the non-split case. *Commun. Math.*, 31(2), 2023.
[6] J. W. S. Cassels. *An Introduction to the Geometry of Numbers*. Springer-Verlag, 1959.
[7] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko, and M. S. Viazovska. The sphere packing problem in dimension 24. *Ann. of Math. (2)*, 185(3):1017–1033, 2017.
[8] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices, and Groups*. Springer-Verlag, Third edition, 1999.
[9] M. T. Damir, A. Karrila, L. Amorós, O. W. Gnilke, D. Karpuk, and C. Hollanti. Well-rounded lattices: Towards optimal coset codes for Gaussian and fading wiretap channels. *IEEE Transactions on Information Theory*, 67(6):3645–3663, 2021.
[10] V. Dannenberg and A. Schürmann. Perfect copositive matrices. *Commun. Math.*, 31(2), 2023.

[11] F. do Carmo Silva, A. P. de Souza, E. Strey, and S. I. R. Costa. On lattice constructions D and D' from q-ary linear codes. *Commun. Math.*, 31(2), 2023.
[12] L. Fukshansky and K. Petersen. On well-rounded ideal lattices. *Int. J. Number Theory*, 8(1):189–206, 2012.
[13] O. German. On triviality of uniform diophantine exponents of lattices. *Commun. Math.*, 31(2), 2023.
[14] P. M. Gruber. *Convex and Discrete Geometry*. Grundlehren der mathematischen Wissenschaften 336. Springer, Berlin, 2007.
[15] P. M. Gruber and C. G. Lekkerkerker. *Geometry of Numbers*. North-Holland Publishing Co., 1987.
[16] T. Hales and S. Ferguson. *The Kepler conjecture. The Hales-Ferguson proof. Including papers reprinted from Discrete Comput. Geom. 36 (2006), no. 1. Edited by Jeffrey C. Lagarias.* Springer, New York, 2011.
[17] V. Kala. Universal quadratic forms and indecomposables in number fields: a survey. *Commun. Math.*, 31(2), 2023.
[18] O. Karpenkov. *Geometry of continued fractions*. Algorithms and Computation in Mathematics, 26. Springer-Verlag, Berlin, 2013.
[19] S. Lang. *Algebraic Number Theory, 2nd edition*. Springer, New York, 1994.
[20] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé. Semantically secure lattice codes for the Gaussian wiretap channel. *IEEE Transactions on Information Theory*, 60(10):6399–6416, 2014.
[21] J. Martinet. *Perfect Lattices in Euclidean Spaces*. Springer-Verlag, 2003.
[22] E. Miller and B. Sturmfels. *Combinatorial commutative algebra*. Graduate Texts in Mathematics, 227. Springer-Verlag, New York, 2005.
[23] H. Minkowski. *Geometrie der Zahlen*. Teubner, Leipzig (reprint, Chelsea, New York, 1953), 1896/1910.
[24] F. Oggier, P. Solé, and J.-C. Belfiore. Lattice codes for the wiretap Gaussian channel: Construction and analysis. *IEEE Transactions on Information Theory*, 62(10):5690–5708, 2016.
[25] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC'05)*, pages 84–93, 2005.
[26] S. Robins. The integer point transform as a complete invariant. *Commun. Math.*, 31(2), 2023.
[27] M. Rosca, D.Stehlé, and A.Wallet. On the ring-LWE and polynomial-LWE problems. In *Advances in Cryptology – EUROCRYPT 2018*, pages 146–173, 2018.
[28] G. G. Szpiro. *Kepler's Conjecture: How Some of the Greatest Minds in History Helped Solve One of the Oldest Math Problems in the World*. Wiley, First edition, 2003.
[29] D. T. Tan, N. H. Le, and H. T. N. Tran. Well-rounded ideal lattices of cyclic cubic and quartic fields. *Commun. Math.*, 31(2), 2023.
[30] L. Fejes Tóth. Über die dichteste Kugellagerung. *Math. Z.*, 48:676–684, 1943.
[31] J. D. Vaaler. On the number of lattice points in a ball. *Commun. Math.*, 31(2), 2023.
[32] M. S. Viazovska. The sphere packing problem in dimension 8. *Ann. of Math. (2)*, 185(3):991–1015, 2017.
[33] A. Weil. *Number theory. An approach through history. From Hammurapi to Legendre*. Birkhäuser Boston, Inc., Boston, MA, 1984.

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711, USA
Email address: lenny@cmc.edu

Department of Mathematics and Systems Analysis, Aalto University, P.O. Box 11100, FI-00076 Aalto, Finland
Email address: camilla.hollanti@aalto.fi