Friedrich-Alexander-Universität
Naturwissenschaftliche Fakultät

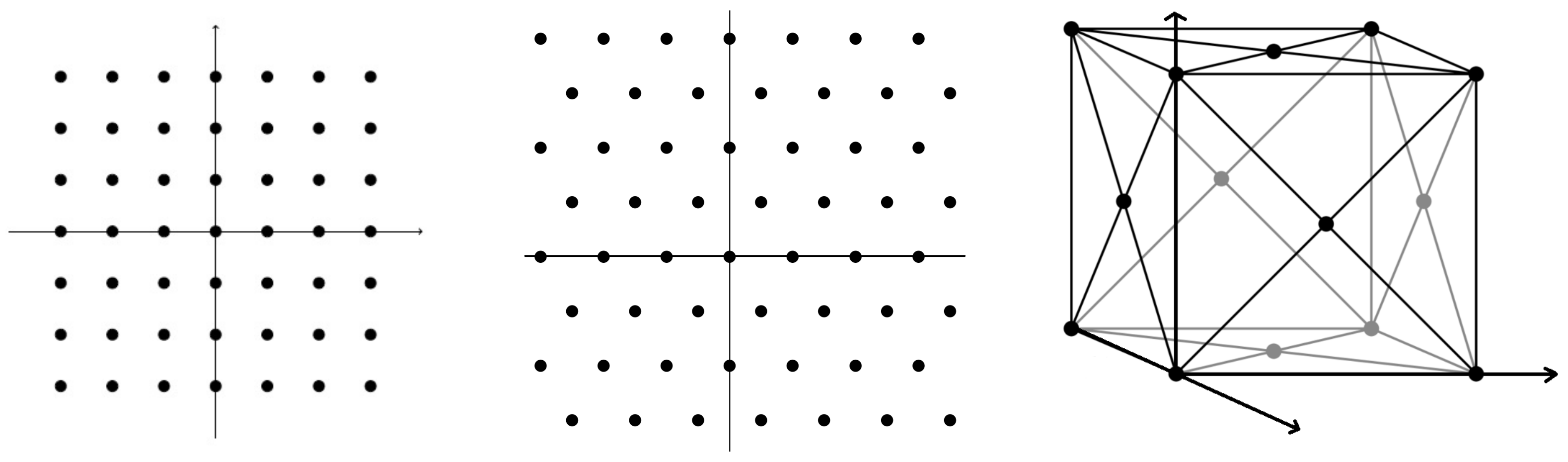
Friedrich-Alexander-Universität
DYNAMICS, CONTROL, MACHINE LEARNING AND NUMERICS

LATTICES FOR RELIABLE AND SECURE COMMUNICATIONS: RECENT ADVANCES AND NEW POSSIBILITIES

Robson Ricardo de Araujo
Professor of Mathematics
Federal Institute of Education, Science and Technology of São Paulo
Catanduva-SP, Brazil

Introduction

Lattices are subsets of $\mathbb{R}^n$ given by all the $\mathbb{Z}$-linear combinations of linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathbb{R}^n$ ($k \leq n$ is the rank of the lattice). These geometric objects have been studied for a long time because they are important in the search for solutions to classical problems in Mathematics, such as the Sphere Packing Problem [1]. In recent decades, lattices have shown to be very useful in communication theory and cryptography, since they have been fundamental in data transmission over Gaussian channels and Rayleigh fading channels [2, 3], and in proposing new cryptographic problems presumably resistant to quantum attacks [4].

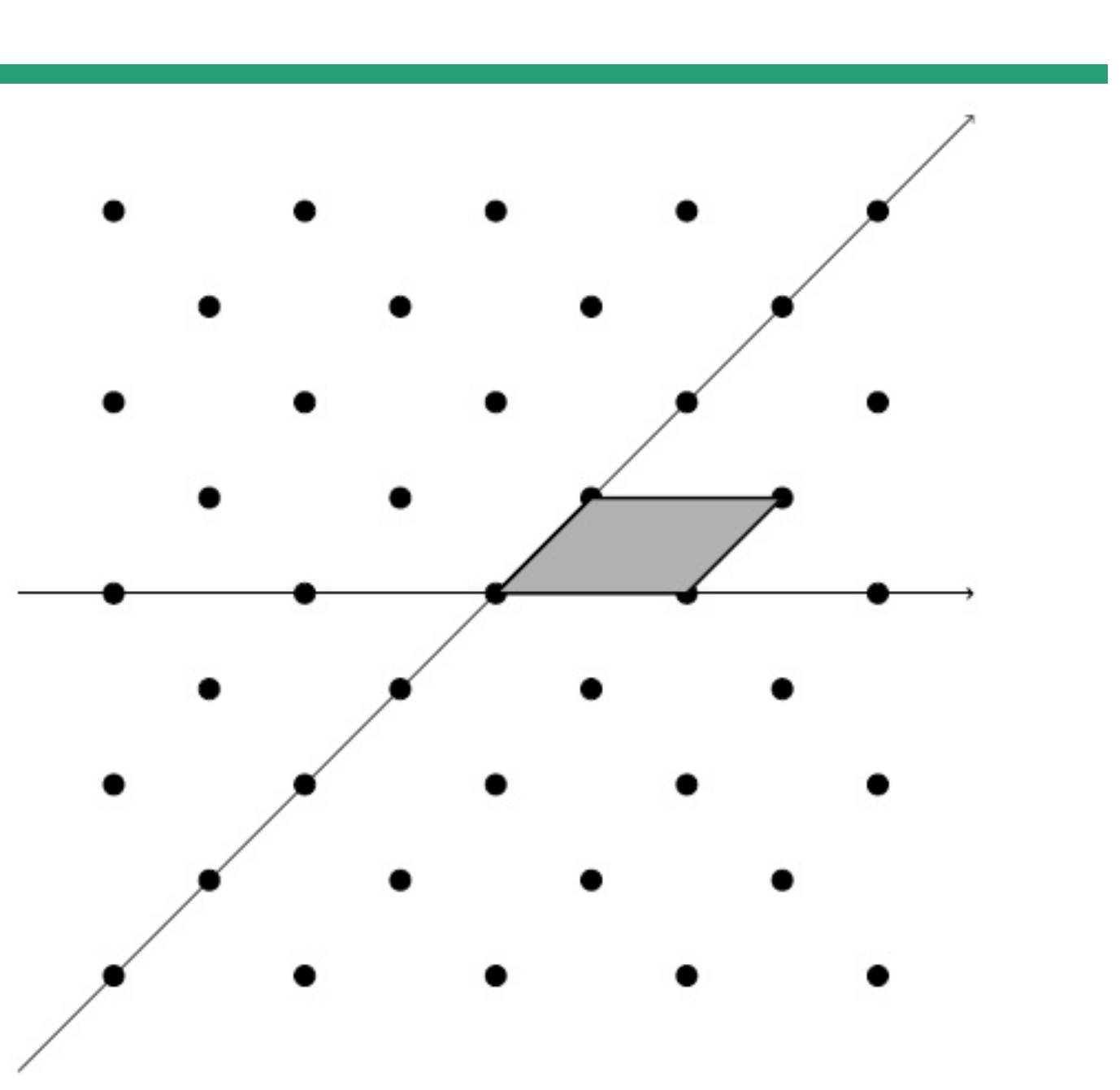


The lattice $\mathbb{Z}^2$, the hexagonal lattice in $\mathbb{R}^2$ and the face-centered cubic (FCC) lattice, respectively.

In this work, we present introductory aspects of lattices and some results on algebraic constructions of the so called well-rounded lattices. Also, we introduce lattice-based cryptography.

Lattices and algebraic lattices

A set $\Lambda \subset \mathbb{R}^n$ is called **lattice** if it is a discrete additive subgroup of $\mathbb{R}^n$. Such set has a **basis** $\mathcal{B}$ with $k \leq n$ elements. If $k = n$, we say that Λ is a **full-rank lattice**. The matrix M whose columns are the vectors of $\mathcal{B}$ is called a **generator matrix** of Λ. The matrix $G = M^T M$ is the **Gram matrix** of G. The **determinant** of Λ is defined to be the determinant of G and is denoted by $\det(\Lambda)$. The **volume** of Λ is given by $\sqrt{\det(\Lambda)}$.
In the figure on the right, the black dots represents a portion of a full lattice in $\mathbb{R}^2$. The area of the parallelogram in the figure is the volume of the lattice.



Let $\mathbb{K}$ be a number field of degree $n = r_1 + 2r_2$, where r_1 is the number of real monomorphisms and $2r_2$ is the number of imaginary monomorphisms from $\mathbb{K}$ to $\mathbb{C}$. Let $\sigma_1, \ldots, \sigma_{r_1}$ be the real monomorphisms and $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ be the imaginary monomorphisms, where $\sigma_{r_1+r_2+i} = \overline{\sigma_{r_1+i}}$ for all $i = 1, 2, \ldots, r_2$. Consider $\mathcal{O}_\mathbb{K}$ the ring of integers of $\mathbb{K}$. The function $\sigma : \mathbb{K} \longrightarrow \mathbb{R}^n$ given by

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re(\sigma_{r_1+1}(x)), \Im(\sigma_{r_1+1}(x)), \ldots, \Re(\sigma_{r_1+r_2}(x)), \Im(\sigma_{r_1+r_2}(x))) \qquad (1)$$

is called the Minkowski embedding of $\mathbb{K}$, where $\Re$ and $\Im$ denote, respectively, the real and the imaginary parts of a complex number. If $\{x_1, x_2, \ldots, x_n\}$ is a $\mathbb{Z}$-basis of a free $\mathbb{Z}$-module M of rank n in $\mathcal{O}_\mathbb{K}$, then $\sigma(M)$ is a full-rank lattice in $\mathbb{R}^n$ with basis $\{\sigma(x_1), \ldots, \sigma(x_n)\}$. This lattice is called an **algebraic lattice**. In particular, M can be taken to be $\mathcal{O}_\mathbb{K}$ or an ideal of it. In the latter case, we can call Λ an **ideal lattice**.

Sphere packing

The **Sphere Packing Problem** in dimension n involves determining how densely a large number of identical spheres can be packed together in $\mathbb{R}^n$. Spheres whose centers are points of a lattice and that the intersection of any two intersecting spheres is just one point provide a *lattice packing*. The hexagonal Λ_2 and FCC lattices are known to be the solutions to the Sphere Packing Problem in dimensions 2 and 3, respectively [1]. Recently, Marina Viazovska was awarded the Fields Medal for confirming that E_8 and Leech lattices solve the Sphere Packing Problem in dimensions 8 and 24, respectively [6].
In some applications in coding theory, it is recommended to use dense lattices. In order to measure the density of a full-rank lattice Λ of rank n, we usually calculate its **center density** $\delta(\Lambda) = \rho^n/vol(\Lambda)$, where ρ is the packing radius of Λ. The higher the value of $\delta(\Lambda)$, the denser the packing provided by Λ.
Considering $\mathbb{K}$ a totally real or a totally imaginary number field of degree n, I a non-zero ideal of $\mathcal{O}_\mathbb{K}$, $d_\mathbb{K}$ the discriminant K, $N(I)$ the norm of the ideal I and $t = \min\{\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\overline{x}) : x \in I, x \neq 0\}$, then

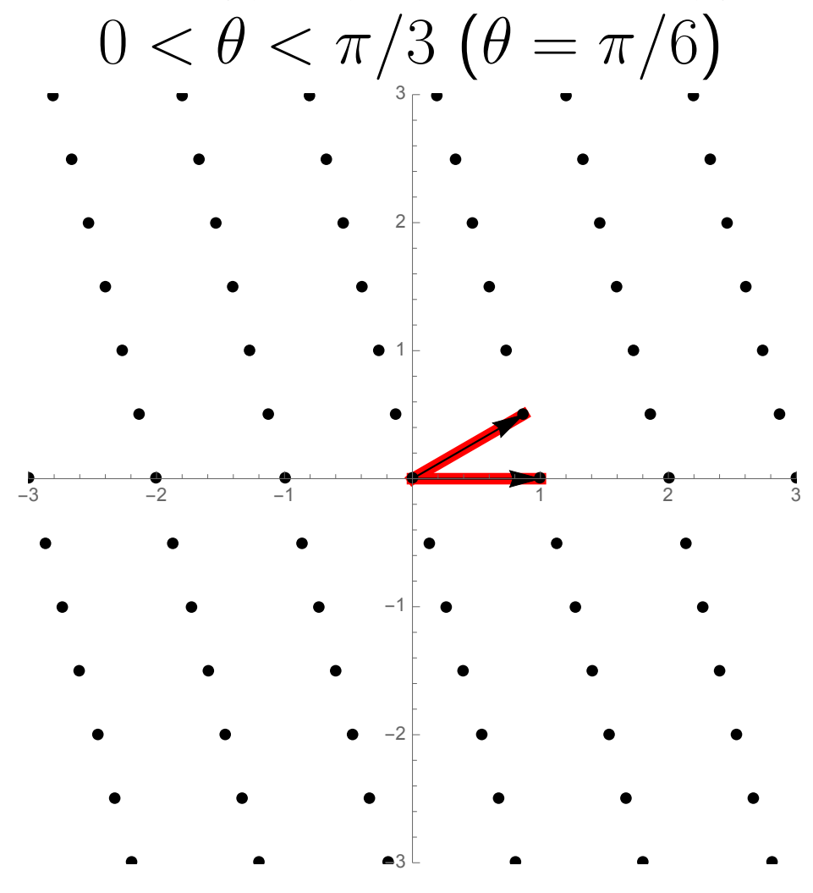
$$\delta(\sigma(I)) = \frac{t^{n/2}}{(2|d_\mathbb{K}|)^{n/2} N(I)}. \qquad (2)$$

Dense lattices can be obtained algebrically as image of $\mathbb{Z}$-modules in ring of integers of algebraic number fields in several dimensions (e.g., in dimensions 2, 3, 4, 5, 6, 7, 8, 12, and 24 [8]). A possibility of study in this area consists of finding new constructions of dense lattices known in other dimensions or even find lattices even denser than those currently known in several dimensions.

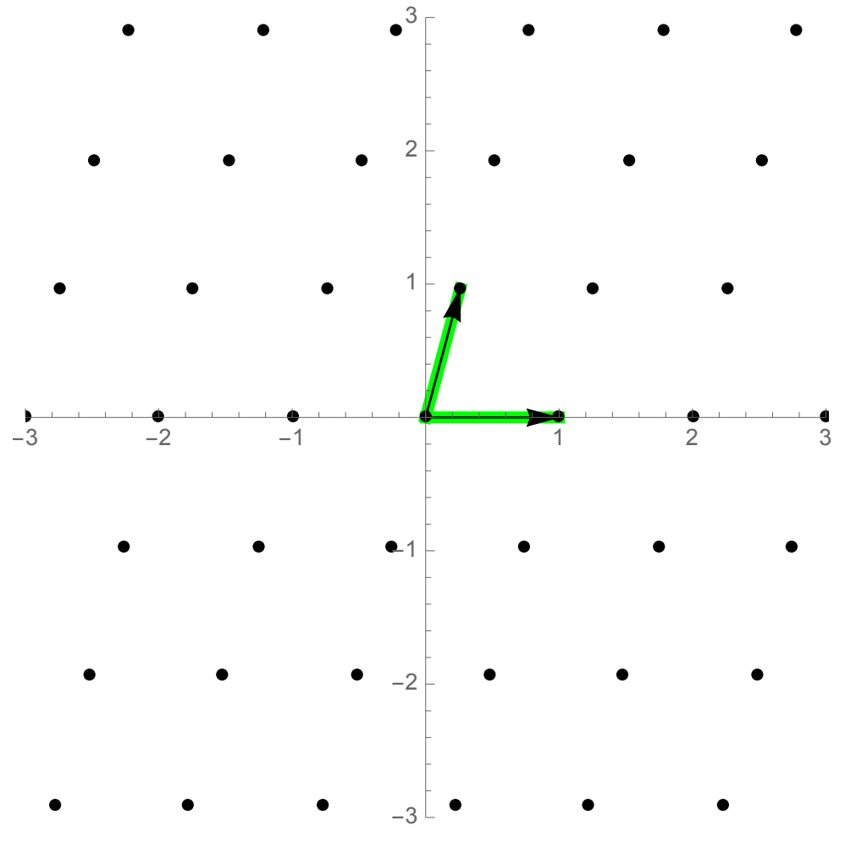
Well-rounded lattices

Let $\Lambda \subseteq \mathbb{R}^n$ be a full-rank lattice. The **minimum norm** λ_1 of Λ is defined to be the minimum of $\|\mathbf{v}\|$, for all $\mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}$, where $\|.\|$ denotes the usual Euclidean norm. The packing radius of Λ is given by $\lambda_1/2$. The set of minimum vectors of Λ is so given by $S(\Lambda) := \{\mathbf{v} \in \Lambda \ : \ \|\mathbf{v}\| = \lambda_1\}$. Recently, more attention has been paid to **well-rounded lattices**, which are those Λ such that $S(\Lambda)$ generates $\mathbb{R}^n$. This means that Λ is well-rounded if $S(\Lambda)$ contains n linearly independent vectors. In dimension 2, it is a well-known result that a full-rank lattice Λ is well-rounded if and only if the number of minimum vectors is 4 or 6 [5].

Example of a non well-rounded lattice
$\mathcal{B} = \{(1,0), (\cos\theta, \sin\theta)\}$
$0 < \theta < \pi/3$ $(\theta = \pi/6)$



Example of a well-rounded lattice
$\mathcal{B} = \{(1,0), (\cos\theta, \sin\theta)\}$
$\pi/3 \leq \theta \leq \pi/2$ $(\theta = 5\pi/12)$



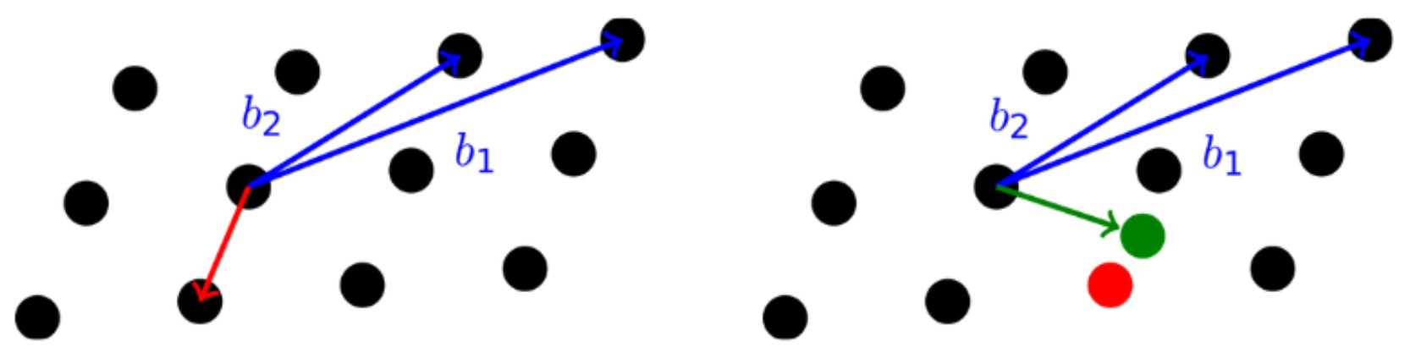
In [5] it is shown that, if $\mathbb{K}$ is a Galois number field, the lattice $\sigma(\mathcal{O}_\mathbb{K})$ is well-rounded if and only if $\mathbb{K}$ is a cyclotomic field. Despite this, we are interested in investigate whether it is possible to create well-rounded algebraic lattices coming from $\mathbb{Z}$-modules inside non-cyclotomic number fields.
Let $p > 2$ be a prime number and $m > 0$ be an integer number such that $m \equiv 1 \pmod{p}$ and $\sqrt{q/(p+1)} \leq m \leq \sqrt{q(p+1)}$. Let $\mathbb{K}$ be a number field of degree p, θ be a generator of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ and q be a prime number such that $q \equiv 1 \pmod{p}$. In [7], we show that $\sigma(M_m)$ is a full-rank well-rounded lattice in $\mathbb{R}^p$, where M_m is the $\mathbb{Z}$-module

$$M_m = \left\{ \sum_{i=0}^{p-1} a_i \theta^i \left(\mathrm{Tr}_{\mathbb{Q}(\zeta_q)/\mathbb{K}}(\zeta_q) \right) \in \mathcal{O}_\mathbb{K} \ : \ \sum_{i=0}^{p-1} a_i \equiv 0 \pmod{m} \right\}.$$

Consequently, there exist infinitely many non-equivalent well-rounded algebraic lattices in $\mathbb{R}^p$, for each prime number $p > 2$. This opens up new questions and new possibilities for study: given any (Galois) number field, is there always a well-rounded algebraic lattice obtained as an image of some $\mathbb{Z}$-module within its ring of integers? How can we obtain well-rounded lattices using algebraic or other methods?

Lattice-based cryptography

In 1994, the mathematician Peter Shor showed that currently used cryptographic algorithms, as RSA or those based on elliptic curves, will not resist quantum computers. Since then, much effort has been made to obtain cryptographic systems resistant to quantum attacks. Lattice-based cryptosystems are a great promise for post-quantum cryptography, as was seen in the North American agency NIST's competition for the standardization of post-quantum cryptography finished in 2022. Lattice-based cryptosystems are those based on the presumed hardness of lattice problems, as the Shortest Vector Problem (SVP), the Closest Vector Problem (CVP), the Bounded Distance Decoding Problem (BDD), among others.



Respectively, ilustrations of the SVP and the CVP problems. Figure by Sebastian Schmittner, taken from `https://en.wikipedia.org/wiki/Lattice_problem`

There are several proposed methods to obtain public key encryption schemes based on the hardness of lattice problems. Among them, we can highlight the cryptosystems GGH (1997), NTRU (1996), Ajtai-Dwork (1997) and, mainly, the Learning With Errors (LWE, 2005) and their structured (algebraic) versions (Ring-LWE, Module-LWE and Twisted-Ring-LWE). For instance, the security proof of the LWE problem is based on the hardness of the approximate SVP problem. Recently, the **Lattice Isomorphism Problem (LIP)** has been proposed for lattice-based cryptography - it was used to construct the scheme Hawk, currently in evaluation for digital post-quantum signature. Two lattices L_1 and L_2 are said isomorphic if $L_1 = O \cdot L_2$ for some orthogonal transformation O. So, the search version of LIP consists of finding a linear isometry mapping two lattices L_1 and L_2 which are known to be isomorphic. Recently, the Module-LIP, an algebraic version of LIP, was defined and studied in [9]. In [9], an algorithm solving Module-LIP was proposed for modules of rank 2 over totally real number fields. A research line on this topic consists to investigate the Module-LIP for other classes of number fields. Furthermore, an open question related to this is the following: can the algebraic structure of Module-LIP be used to provide more efficient algorithms for solving it than those known for solving LIP?

References

[1] J.H. Conway, N.J.A. Sloane. *Sphere packings, lattices and groups*. New York: Spring-Verlag, 1998.

[2] J. J. Boutros, E. Viterbo, C. Rastello, and J.-C. Belfiore. *Good lattice constellations for both Rayleigh fading and Gaussian channels*. IEEE Transactions on Information Theory **42** (1996), 502—518.

[3] S. I. R. Costa, F. Oggier, A. Campello, J.-C. Belfiore, E. Viterbo. *Lattices Applied to Coding for Reliable and Secure Communications*. Cham: Springer, 2017.

[4] C. Peikert, O. Regev, N. Stephens-Davidowitz. *Pseudorandomness of ring-LWE for Any Ring and Modulus*, Proc. 49th ACM SIGACT - STOC 2017, Montreal, ACM, 2017, 461-–473.

[5] L. Fukshansky, K. Petersen. *On well-rounded ideal lattices*. Int. J. Numb. Th. 8(1) (2012), 189–206.

[6] M. Viazovska. *Almost impossible E8 and Leech lattices*. Eur. Math. Soc. Mag. **121** (2021), 4—8.

[7] R. R. de Araujo, S. I. R. Costa. *Well-rounded algebraic lattices in odd prime dimension*, Arch. Math. **112** (2019), 138-–148.

[8] G. C. Jorge, A. A. Andrade, S. I. R. Costa, J. E. Strapasson. *Algebraic constructions of densest lattices*. Journal of Algebra **429** (2015), 218-–235.

[9] G. Mureau, A. Pellet-Mary, H. Pliatsok, A. Wallet. *Cryptanalysis of rank-2 module-LIP in Totally Real Number Fields*. Advances in Cryptology – EUROCRYPT 2024.

Unterstützt von / Supported by
Department MATHEMATIK
Alexander von Humboldt Stiftung/Foundation
FAPESP SÃO PAULO RESEARCH FOUNDATION