On algebraic well-rounded lattices

Lenny Fukshansky
Claremont McKenna College

Quadratic Lattices in Prague 2026
August 17 - 21, 2026

Lattices: basic notions

A **lattice** $\Lambda \subset \mathbb{R}^n$ of rank $1 \leq k \leq n$ is a free $\mathbb{Z}$-module of rank k, which is the same as a discrete co-compact subgroup of $V := \operatorname{span}_{\mathbb{R}} \Lambda$. If $k = n$, i.e. $V = \mathbb{R}^n$, we say that Λ is a lattice of **full rank** in $\mathbb{R}^n$. Hence

$$\Lambda = \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{a}_1, \dots, \boldsymbol{a}_k\} = A\mathbb{Z}^k,$$

where $\boldsymbol{a}_1, \dots, \boldsymbol{a}_k \in \mathbb{R}^n$ are $\mathbb{R}$-linearly independent **basis** vectors for Λ and $A = (\boldsymbol{a}_1 \ \dots \ \boldsymbol{a}_k)$ is the corresponding $n \times k$ basis matrix.

The corresponding $k \times k$ symmetric **Gram** matrix is $A^t A$, which is the matrix of the corresponding quadratic norm form

$$Q_A(\boldsymbol{x}) = Q_A(x_1, \dots, x_k) := \boldsymbol{x}^t A^t A \boldsymbol{x},$$

for $\boldsymbol{x} \in \mathbb{Z}^k$, which gives norm of the vector $A\boldsymbol{x} \in \Lambda$.

Lattices: basic notions

The **determinant** of Λ is

$$\det \Lambda := \sqrt{\det(A^t A)},$$

which is equal to the volume (quotient Lebesgue measure) of V/Λ, i.e. of any fundamental domain of Λ (a measurable minimal complete set of coset representatives of Λ in V).

Let $\mathrm{GL}(\Lambda)$ be the subgroup of $\mathrm{GL}(V)$ that permutes Λ. The **automorphism group** of a lattice $\Lambda \subset \mathbb{R}^n$ is

$$\mathrm{Aut}(\Lambda) := \mathrm{GL}(\Lambda) \cap O(V),$$

where $\mathrm{GL}(\Lambda)$ is discrete and $O(V)$ is the compact group of orthogonal transformations of V onto itself $\Longrightarrow$ $\mathrm{Aut}(\Lambda)$ is finite. For all $n \neq 2, 4, 6, 7, 8, 9, 10$ the largest (with respect to order) automorphism group of a full rank lattice is

$$\mathrm{Aut}(\mathbb{Z}^n) = (\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n.$$

Well-rounded lattices

Minimal norm of a lattice Λ is

$$|\Lambda| = \min\left\{\|\boldsymbol{x}\| : \boldsymbol{x} \in \Lambda \setminus \{\boldsymbol{0}\}\right\},$$

where $\| \ \|$ is Euclidean norm. The set of **minimal vectors** of Λ is

$$S(\Lambda) = \{\boldsymbol{x} \in \Lambda : \|\boldsymbol{x}\| = |\Lambda|\} = \{\pm\boldsymbol{x}_1, \dots, \pm\boldsymbol{x}_k\}.$$

- A lattice Λ is **well-rounded** (WR) if $\operatorname{span}_{\mathbb{R}} \Lambda = \operatorname{span}_{\mathbb{R}} S(\Lambda)$.
- If $\operatorname{rk} \Lambda > 4$, a strictly stronger condition is that Λ is **generated by minimal vectors**, i.e. $\Lambda = \operatorname{span}_{\mathbb{Z}} S(\Lambda)$.
- It has been shown by Conway & Sloane (1995) and Martinet & Schürmann (2011) that there are lattices of rank ≥ 10 generated by minimal vectors which do not contain a **basis of minimal vectors**.

Lattices: eutaxy and perfection

Let $n = \operatorname{rk} \Lambda$ and

$$S(\Lambda) = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{2k}\}$$

be the set of minimal vectors of the lattice Λ.

This lattice is called **eutactic** if there exist positive real numbers $c_1, \ldots, c_{2k}$ such that

$$\|\boldsymbol{v}\|^2 = \sum_{i=1}^{2k} c_i \langle \boldsymbol{v}, \boldsymbol{x}_i \rangle^2$$

for every vector $\boldsymbol{v} \in \operatorname{span}_{\mathbb{R}} \Lambda$. If $c_1 = \cdots = c_{2k}$, we say that Λ is **strongly eutactic**.

This lattice is called **perfect** if the set of symmetric matrices

$$\{\boldsymbol{x}_i \boldsymbol{x}_i^\top : \boldsymbol{x}_i \in S(\Lambda)\}$$

spans the space of $n \times n$ symmetric matrices.

Both, perfect and eutactic lattices are WR.

Packing density

WR lattices are central to extremal lattice theory, since many classical discrete optimization problems on lattices can be restricted to WR lattices without loss of generality.

For example, the **lattice sphere packing** problem in $\mathbb{R}^n$ asks for a full rank lattice Λ which maximize the sphere packing density function defined as

$$\delta(\Lambda) = \frac{\omega_n |\Lambda|^n}{2^n \det \Lambda},$$

where ω_n is the volume of a unit ball in $\mathbb{R}^n$.

Geometric properties and packing density of lattices are invariant up to *similarity* (rotation and dilation). There are infinitely many WR similarity classes in each dimension, but only finitely many eutactic similarity classes and perfect similarity classes.

Theorems of Voronoi and Ash

A lattice is called **extremal** if it is a local maximum of the packing density function in its dimension.

Theorem 1 (G. Voronoi – 1908)

A lattice is extremal if and only if it is perfect and eutactic.

Theorem 2 (A. Ash – 1977)

Eutactic lattices are critical points of the packing density function.

Many important families of lattices come from various algebraic constructions. In this talk, we focus on constructions from algebraic number fields.

Further applications

WR lattices also play an important role in cryptography, coding theory, and image compression. There are two additional properties that are often valued in those applications:

- A full-rank WR lattice $\Lambda \subset \mathbb{R}^n$ is called **generic well-rounded (GWR)** if it has precisely $2n$ minimal vectors (Hollanti, Mantilla-Soler, Miller (2025): construction of lattice codes for secure wireless communication).
- A full-rank lattice $\Lambda \subset \mathbb{R}^n$ is called **nearly orthogonal** if it contains a basis $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n$ so that, for any permutation of this basis, each angle θ_k between $\boldsymbol{x}_k$ and the subspace spanned by $\boldsymbol{x}_1, \dots, \boldsymbol{x}_{k-1}$ is in the interval $[\pi/3, 2\pi/3]$, for all $2 \leq k \leq n$ (Neelamani, Dash, Baraniuk (2007): JPEG image compression application).

In this talk, we discuss number field constructions of WR lattices.

Ideal lattice construction

We start by fixing some notation:

K = number field of degree d over $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$. $\sigma_1, \ldots, \sigma_d$ are the embeddings of K into $\mathbb{C}$ with r_1 of them real and r_2 pairs of complex conjugates, thus $d = r_1 + 2r_2$.

The **Minkowski embedding**

$$\Sigma_K = (\sigma_1, \ldots, \sigma_d) : K \hookrightarrow \mathbb{C}^d$$

takes K into the space $K_\mathbb{R} := K \otimes_\mathbb{Q} \mathbb{R}$, which can be viewed as a subspace of

$$\left\{(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : y_{r_2+j} = \bar{y}_j \ \forall \ 1 \leq j \leq r_2\right\} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \subset \mathbb{C}^d,$$

where in the last containment each copy of $\mathbb{R}$ is identified with the real part of the corresponding copy of $\mathbb{C}$.

For any ideal $I \subseteq \mathcal{O}_K$, $\Sigma_K(I) \subset K_\mathbb{R}$ is a lattice of full rank, called an **ideal lattice of trace type**.

WR ideal lattices

For any ideal $I \subseteq \mathcal{O}_K$,

$$\det(\Sigma_K(I)) = \mathbb{N}_K(I)|\Delta_K|^{1/2}.$$

We say that an ideal $I \subseteq \mathcal{O}_K$ is WR if the lattice $\Sigma_K(I)$ is WR.

Theorem 3 (F., Petersen (2012))

Assume $r_1 = 0$ or $r_2 = 0$. Then $\mathcal{O}_K$ is WR if and only if K is cyclotomic, in which case any ideal $I \subseteq \mathcal{O}_K$ is WR. On the other hand, infinitely many real and imaginary quadratic number fields ($K = \mathbb{Q}(\sqrt{D})$) contain WR ideals.

Remark 1

In fact, lattices coming from any fractional ideals in cyclotomic fields are not just WR, but strongly eutactic.

WR ideal lattices

A key observation for lattices $\Sigma_K(\mathcal{O}_K)$ from totally real or totally imaginary number fields is that $\Sigma_K(1)$ is always a minimal vector.

In a recent paper (2025), **C. Alves, J. E. Strapasson and R. R. de Araujo** showed that this is not always the case when K is mixed.

On the other hand, they show that under a modified (weighted) Minkowski embedding the image of 1 is always a minimal vector. Under this modified embedding, they conclude for any K that the image of $\mathcal{O}_K$ is WR if and only if K is cyclotomic.

WR ideals in quadratic number fields

More is known about WR ideals in quadratic number fields.

- **F., Henshaw, Liao, Prince, Sun, Whitehead (2013)** proved existence of a positive proportion of real and imaginary quadratic fields containing WR ideals and classified all imaginary quadratic number fields with WR ideals.
- **Gnilke, Hollanti, Karilla, Tran (2016)** proved that there exist infinitely many $K = \mathbb{Q}(\sqrt{D})$ with positive $D \equiv 1 \pmod 4$ and $D \equiv 3 \pmod 4$ containing WR ideals.
- **Srinivasan (2020)** classified WR ideals in real quadratic number fields.

Additionally, constructions of WR ideals in cyclic cubic and quartic number fields were obtained by **D. T. Tran, Le, H. T. N. Tran (2023)**.

WR lattices from $\mathbb{Z}$-modules in number fields

In addition to ideal lattices, we can also construct *algebraic lattices* coming from more general free $\mathbb{Z}$-modules in rings of algebraic integers of number fields via Minkowski embedding.

In particular, a series of recent papers by **de Araujo, de Andrade, Bastos, Costa, da Nóbrega Neto** produces constructions of WR lattices generated by their minimal vectors coming from certain families of free $\mathbb{Z}$-modules in rings of integers of cyclic number fields of prime degree.

In recent work with my student **Evelyne Knight**, we took a slightly different approach to such constructions in some more generality.

Polynomial construction

Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

be an irreducible polynomial of degree $n \geq 2$ and let

$$\alpha_1, \alpha_2, \ldots, \alpha_n$$

be roots of $f(x)$. Let K be its splitting field and $G(f)$ its Galois group over $\mathbb{Q}$. Then

$$d := [K : \mathbb{Q}] = |G(f)| \leq n!.$$

Define

$$\mathcal{M}_f = \mathrm{span}_{\mathbb{Z}} \{\alpha_1, \ldots, \alpha_n\} \subset \mathcal{O}_K,$$

so $\mathcal{M}_f$ is a $\mathbb{Z}$-module of rank $\leq n$ generated by all the conjugates of α_1. Notice that $\mathcal{M}_f$ is closed under the action of $G(f)$, since automorphisms of the Galois extension $K/\mathbb{Q}$ simply permute the roots of an irreducible polynomial.

Polynomial construction

Define $L_f := \Sigma_K(\mathcal{M}_f)$, which is a Euclidean lattice in $K_{\mathbb{R}}$. Then $G(f) \leq \mathrm{Aut}(L_f)$.

Theorem 4 (F., Knight (2026))

Let $n \geq 3$ be prime. There exist infinitely many polynomials $f(x) \in \mathbb{Z}[x]$ of degree n so that L_f is a GWR nearly orthogonal lattice of rank n in $K_{\mathbb{R}}$, where K is the splitting field of $f(x)$; further, L_f contains a basis consisting of minimal vectors. For example, we can take $f(x) = x^n + a_{n-1}x^{n-1} + a_0$, where

$$|a_0| > \frac{8(n-1)n!}{\sqrt{(n-2)^2 + 16(n-1)} - (n-2)} \tag{1}$$

and $|a_{n-1}| > |a_0| + 1$ are integers.

Sketch of proof

For each $1 \leq i \leq n$, write $\boldsymbol{\alpha}_i = \Sigma_K(\alpha_i)$. Then

$$L_f = \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_n\}.$$

Define the **coherence** of a pair of vectors $\boldsymbol{\alpha}_i, \boldsymbol{\alpha}_j$ to be

$$c(\boldsymbol{\alpha}_i, \boldsymbol{\alpha}_j) = \frac{\langle \boldsymbol{\alpha}_i, \boldsymbol{\alpha}_j \rangle}{\|\boldsymbol{\alpha}_i\| \|\boldsymbol{\alpha}_j\|}$$

under trace-induced Euclidean inner product and norm. In other words, coherence is cosine of the angle between these two vectors. It follows from a theorem of **F., Kogan (2020)** that if $\operatorname{rk} L_f = n$ and

$$\max_{i \neq j} |c(\boldsymbol{\alpha}_i, \boldsymbol{\alpha}_j)| \leq \frac{\sqrt{(n-2)^2 + 16(n-1)} - (n-2)}{8(n-1)}, \qquad (2)$$

then L_f is a GWR nearly orthogonal lattice with the minimal vectors $\pm\boldsymbol{\alpha}_1, \dots, \pm\boldsymbol{\alpha}_n$.

Sketch of proof

The upper bound

$$c_n := \frac{\sqrt{(n-2)^2 + 16(n-1)} - (n-2)}{8(n-1)}$$

in (2) is asymptotically optimal to ensure that the lattice is GWR.

Indeed, notice that

$$\lim_{n\to\infty} (c_n/(1/n)) = 1,$$

where

$$\max\{|c(\boldsymbol{x}, \boldsymbol{y})| : \boldsymbol{x}, \boldsymbol{y} \in S(A_n^*)\} = 1/n$$

with A_n^* being the dual of the root lattice A_n. The lattice A_n^* is certainly well-rounded (and even strongly eutactic), but it has rank n and $2(n+1)$ minimal vectors; thus it is not GWR.

Sketch of proof

Thus, we want to find families of irreducible polynomials $f(x)$ with small coherence between the roots.

By **Strong Approximation Theorem**, there exist algebraic integers α_1 in any number field so that $|\alpha_1|$ is large while $|\alpha_i|$ is small for all of its conjugates.

In particular, each number field with at least one real embedding contains infinitely many **Pisot numbers**, i.e., real algebraic integers > 1 with all of its conjugates ≤ 1 in absolute value.

The minimal polynomial of a Pisot number is called a **Pisot polynomial**. Let $f(x) = x^n + \sum_{k=0}^{n-1} a_k x^k \in \mathbb{Z}[x]$ be such that

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|.$$

Then **Perron's irreducibility criterion (1907)** implies that $f(x)$ is a Pisot polynomial, and

$$|\alpha_1| \geq \prod_{i=1}^{n} |\alpha_i| = |a_0|.$$

Sketch of proof

Finally, we want to choose $f(x)$ so that rank of L_f equal to n, which is achieved by $\alpha_1, \ldots, \alpha_n$ being $\mathbb{Q}$-linearly independent.

Since

$$\alpha_1 + \cdots + \alpha_n = -a_{n-1}, \tag{3}$$

we have $a_{n-1} \neq 0$ is a necessary condition.

It follows from a theorem of **Kurbatov (1977)** that this condition is also sufficient if n is prime. This completes our proof.

Corollary 5 (Bonini, F. (2026))

Let $n \geq 3$, not necessarily prime, and let the rest of the notation be as in Theorem 4. There exist infinitely many trinomials $f(x) = x^n + a_{n-1}x^{n-1} + a_0$ satisfying conditions (1) and $|a_{n-1}| > |a_0| + 1$ as in Theorem 4 such that L_f is GWR nearly orthogonal with a basis of minimal vectors.

Sketch of proof

Notice that the only way in which our argument above relies on n being prime is to establish linear independence of the roots of $f(x)$ via Kurbatov's theorem.

A theorem of **C. Smyth (1986)** asserts that if the necessary trace condition (3) is satisfied and additionally $G(f) = S_n$, then the roots $\alpha_1, \dots, \alpha_n$ are $\mathbb{Q}$-linearly independent, for any n.

Now, the Galois group of a Pisot polynomial "most frequently" is S_n, especially with a strongly dominant root. In particular, the fact that there exist infinitely many trinomials $x^n + a_{n-1}x^{n-1} + a_0$ satisfying conditions of Theorem 4 with Galois group equal to S_n follows from a theorem of **H. Osada (1987)**.

Of course, this means that L_f is a lattice of rank n in $n!$-dimensional space $K_{\mathbb{R}}$. This being said, we can obtain an isometric copy of L_f in $\mathbb{R}^n$ by computing its Gram matrix.

Determinant computation

We can compute the determinant of our lattice L_f in many cases. First observation is that if $G(f) = \mathbb{Z}/n\mathbb{Z}$, then

$$\det(L_f) = \prod_{j=1}^{n-1}\left(\sum_{i=1}^{n}\alpha_i\zeta_n^{j(i-1)}\right),$$

where $\zeta_n = e^{2pi/n}$ is n-th primitive root of unity.

Theorem 6 (F. Knight (2026))

Let $A = \sum_{i\leq n}\alpha_i^2$ and $B = \sum_{i<j}\alpha_i\alpha_j$. If $G(f) = S_n$, then

$$\det(L_f) = \left\{((n-2)!)^n(n-1)(A+2B)\left((n-1)A-2B\right)^{n-1}\right\}^{1/2}.$$

If $G(f) = A_n$, then

$$\det(L_f) = \left\{((n-2)!)^n(n-1)(A+B)\left((n-1)A-B\right)^{n-1}\right\}^{1/2}.$$

Some cubic examples

Let $f(x) = x^3 + ax^2 + bx + c$. For the following values of a, b, c, this is a Pisot polynomial as in our Theorem 4, and hence the corresponding lattice L_f is GWR nearly orthogonal of rank 3.

a, b, c	Galois Group
$\pm 42, 0, \mp 24$	$\mathbb{Z}/3\mathbb{Z}$
$32, 0, -28$	S_3
$49, 0, 47$	S_3
$-47, 0, 28$	S_3

The Galois group of the polynomial is $\mathbb{Z}/3\mathbb{Z}$ if and only if the discriminant $-4a^3b - 27b^2$ of $f(x)$ is a square. Further, all the roots need to be real, which implies that $ab \leq 0$.

Two-dimensional case

Theorem 7 (F., Knight (2026))

Let $f(x) = x^2 + a_1 x + a_0 \in \mathbb{Z}[x]$ *be an irreducible quadratic polynomial with discriminant* $D = a_1^2 - 4a_0$ *and the corresponding algebraic lattice*

$$L_f = \begin{pmatrix} \frac{-a_1+\sqrt{D}}{2} & \frac{-a_1-\sqrt{D}}{2} \\ \frac{-a_1-\sqrt{D}}{2} & \frac{-a_1+\sqrt{D}}{2} \end{pmatrix} \mathbb{Z}^2.$$

If for some nonzero integer k, $f(x)$ *is one of*

$$x^2 + 2kx - 2k^2,\ x^2 + kx + k^2,\ x^2 + 6kx + 6k^2,\ x^2 + 3k + 3k^2,$$

then L_f *is similar to the hexagonal lattice.*

Two-dimensional case

Continuation of Theorem 7 (F., Knight (2026))

Otherwise, L_f *is well-rounded if and only if* $a_1^2 > 2\max\{3a_0, -a_0\}$. *If this is the case,*

$$S(L_f) = \left\{ \pm \begin{pmatrix} \frac{-a_1+\sqrt{D}}{2} \\ \frac{-a_1-\sqrt{D}}{2} \end{pmatrix}, \pm \begin{pmatrix} \frac{-a_1-\sqrt{D}}{2} \\ \frac{-a_1+\sqrt{D}}{2} \end{pmatrix} \right\}$$

and $\mathrm{Aut}(L_f) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *with one of the isomorphic copies of* $\mathbb{Z}/2\mathbb{Z}$ *coming from the Galois action and the other from the* $\pm$ *signs.*

References

L. Fukshansky, E. Knight, *On lattices generated by algebraic conjugates of prime degree*, Illinois Journal of Mathematics, vol. 70 no.1 (2026), pg. 193—211

This and other papers of mine mentioned above are available at:

`www1.cmc.edu/pages/faculty/lenny/research.html`

Děkuji vám za pozornost!

And thanks a lot to the organizers for an excellent conference!