Well-rounded lattices from algebraic constructions

Lenny Fukshansky
Claremont McKenna College

ANTA Seminar
Aalto University
June 1, 2016

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 $V := \mathrm{span}_{\mathbb{R}} \Lambda$. If $k = n$, i.e. $V = \mathbb{R}^n$, we say that Λ is a lattice of **full rank** in $\mathbb{R}^n$. Hence

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

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

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 $V := \mathrm{span}_{\mathbb{R}} \Lambda$. If $k = n$, i.e. $V = \mathbb{R}^n$, we say that Λ is a lattice of **full rank** in $\mathbb{R}^n$. Hence

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

where $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k \in \mathbb{R}^n$ are $\mathbb{R}$-linearly independent **basis** vectors for Λ and $A = (\boldsymbol{a}_1 \ \ldots \ \boldsymbol{a}_k)$ 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

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

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).

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.

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

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

Lattices: basic notions

Successive minima of Λ are real numbers

$$0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_k,$$

defined by

$$\lambda_i = \min\left\{\lambda \in \mathbb{R}_{>0} : \dim\left(\mathrm{span}_{\mathbb{R}}\left(B_V(\lambda) \cap \Lambda\right)\right) \geq i\right\},$$

where $B_V(\lambda)$ is the unit ball of radius λ centered at $\mathbf{0}$ in V.

Lattices: basic notions

Successive minima of Λ are real numbers

$$0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_k,$$

defined by

$$\lambda_i = \min\left\{\lambda \in \mathbb{R}_{>0} : \dim\left(\mathrm{span}_{\mathbb{R}}\left(B_V(\lambda) \cap \Lambda\right)\right) \geq i\right\},$$

where $B_V(\lambda)$ is the unit ball of radius λ centered at $\mathbf{0}$ in V.

Two lattices $\Lambda, \Omega \subset \mathbb{R}^n$ of rank k are said to be **similar**, written $\Lambda \sim \Omega$, if

$$\Lambda = \alpha U \Omega$$

for some real constant α and orthogonal $k \times k$ matrix U. Then:

$$\lambda_i(\Lambda)/\lambda_{i+1}(\Lambda) = \lambda_i(\Omega)/\lambda_{i+1}(\Omega)$$

for each $1 \leq i \leq k$.

Well-rounded lattices

Minimal norm of a lattice Λ is

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

where $\| \ \|$ is Euclidean norm. This is precisely the first successive minimum λ_1.

Well-rounded lattices

Minimal norm of a lattice Λ is

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

where $\|\ \|$ is Euclidean norm. This is precisely the first successive minimum λ_1.

The set of **minimal vectors** of Λ is

$$S(\Lambda) = \{\boldsymbol{x} \in \Lambda : \|\boldsymbol{x}\| = |\Lambda|\}.$$

Well-rounded lattices

Minimal norm of a lattice Λ is

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

where $\| \ \|$ is Euclidean norm. This is precisely the first successive minimum λ_1.

The set of **minimal vectors** of Λ is

$$S(\Lambda) = \{\boldsymbol{x} \in \Lambda : \|\boldsymbol{x}\| = |\Lambda|\}.$$

A lattice $\Lambda \subset \mathbb{R}^n$ of rank k is called **well-rounded** (abbreviated **WR**) if

$$\lambda_1 = \cdots = \lambda_k.$$

This is equivalent to saying that $V = \operatorname{span}_{\mathbb{R}} S(\Lambda)$.

Well-rounded lattices

Minimal norm of a lattice Λ is

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

where $\| \ \|$ is Euclidean norm. This is precisely the first successive minimum λ_1.

The set of **minimal vectors** of Λ is

$$S(\Lambda) = \{\boldsymbol{x} \in \Lambda : \|\boldsymbol{x}\| = |\Lambda|\}.$$

A lattice $\Lambda \subset \mathbb{R}^n$ of rank k is called **well-rounded** (abbreviated **WR**) if

$$\lambda_1 = \cdots = \lambda_k.$$

This is equivalent to saying that $V = \operatorname{span}_{\mathbb{R}} S(\Lambda)$.

WR lattices are only similar to WR lattices, so we speak of **WR similarity classes**.

Packing density

WR lattices are central to extremal lattice theory, since many classical discrete optimization problems on lattices can be restricted to WR lattices wlog.

Packing density

WR lattices are central to extremal lattice theory, since many classical discrete optimization problems on lattices can be restricted to WR lattices wlog.

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

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

where ω_n is the volume of a unit ball in $\mathbb{R}^n$. It is well known that $\delta(\Lambda)$ can assume its local maxima only on WR lattices.

Counting WR lattices

The set of WR lattices has measure zero in the space of all lattices, however there are still infinitely many similarity classes of WR lattices in every dimension.

Counting WR lattices

The set of WR lattices has measure zero in the space of all lattices, however there are still infinitely many similarity classes of WR lattices in every dimension. In fact, given a lattice Λ of rank n, one can ask for an estimate as $T \to \infty$ on

$$N_{\mathrm{WR}}(\Lambda, T) := \#\{\Omega \subseteq \Lambda : |\Lambda : \Omega| \leq T\}.$$

Counting WR lattices

The set of WR lattices has measure zero in the space of all lattices, however there are still infinitely many similarity classes of WR lattices in every dimension. In fact, given a lattice Λ of rank n, one can ask for an estimate as $T \to \infty$ on

$$N_{\mathrm{WR}}(\Lambda, T) := \#\{\Omega \subseteq \Lambda : |\Lambda : \Omega| \leq T\}.$$

Such estimates are currently only known when $n = 2$:

Theorem 1 (F. (2014))

If $\mathrm{rk}\,\Lambda = 2$ *and* Λ *is similar to an integral lattice (i.e. its Gram matrix has integer entries), then as* $T \to \infty$

$$N_{\mathrm{WR}}(\Lambda, T) = O(T \log T).$$

Counting WR lattices

The set of WR lattices has measure zero in the space of all lattices, however there are still infinitely many similarity classes of WR lattices in every dimension. In fact, given a lattice Λ of rank n, one can ask for an estimate as $T \to \infty$ on

$$N_{\mathrm{WR}}(\Lambda, T) := \#\{\Omega \subseteq \Lambda : |\Lambda : \Omega| \leq T\}.$$

Such estimates are currently only known when $n = 2$:

Theorem 1 (F. (2014))

If $\mathrm{rk}\,\Lambda = 2$ *and* Λ *is similar to an integral lattice (i.e. its Gram matrix has integer entries), then as* $T \to \infty$

$$N_{\mathrm{WR}}(\Lambda, T) = O(T \log T).$$

If $\mathrm{rk}\,\Lambda = 2$ and Λ is not similar to an integral lattice, then $N_{\mathrm{WR}}(\Lambda, T) = 0$ or $O(T)$. *(S. Kühnlein, 2014)*

Algebraic constructions

Many important families of lattices come from algebraic constructions. We consider some well-known instances here:

Algebraic constructions

Many important families of lattices come from algebraic constructions. We consider some well-known instances here:

- Ideal lattices from number fields (Martinet, Bayer-Fluckiger, Nebe, et al.)

Algebraic constructions

Many important families of lattices come from algebraic constructions. We consider some well-known instances here:

- Ideal lattices from number fields (Martinet, Bayer-Fluckiger, Nebe, et al.)
- Ideal lattices from polynomial rings (Lyubashevsky & Micciancio, Peikert & Rosen et al.)

Algebraic constructions

Many important families of lattices come from algebraic constructions. We consider some well-known instances here:

- Ideal lattices from number fields (Martinet, Bayer-Fluckiger, Nebe, et al.)
- Ideal lattices from polynomial rings (Lyubashevsky & Micciancio, Peikert & Rosen et al.)
- Function field lattices from curves over finite fields (Quebbemann, Rosenbloom & Tsfasman, et al.)

Algebraic constructions

Many important families of lattices come from algebraic constructions. We consider some well-known instances here:

- Ideal lattices from number fields (Martinet, Bayer-Fluckiger, Nebe, et al.)
- Ideal lattices from polynomial rings (Lyubashevsky & Micciancio, Peikert & Rosen et al.)
- Function field lattices from curves over finite fields (Quebbemann, Rosenbloom & Tsfasman, et al.)

Lattices from these constructions figure prominently in extremal lattice theory and connected areas, prompting the following question about their geometric properties:

Algebraic constructions

Many important families of lattices come from algebraic constructions. We consider some well-known instances here:

- Ideal lattices from number fields (Martinet, Bayer-Fluckiger, Nebe, et al.)
- Ideal lattices from polynomial rings (Lyubashevsky & Micciancio, Peikert & Rosen et al.)
- Function field lattices from curves over finite fields (Quebbemann, Rosenbloom & Tsfasman, et al.)

Lattices from these constructions figure prominently in extremal lattice theory and connected areas, prompting the following question about their geometric properties:

Question 1

Which lattices coming from the above constructions are WR?

Algebraic constructions

Many important families of lattices come from algebraic constructions. We consider some well-known instances here:

- Ideal lattices from number fields (Martinet, Bayer-Fluckiger, Nebe, et al.)
- Ideal lattices from polynomial rings (Lyubashevsky & Micciancio, Peikert & Rosen et al.)
- Function field lattices from curves over finite fields (Quebbemann, Rosenbloom & Tsfasman, et al.)

Lattices from these constructions figure prominently in extremal lattice theory and connected areas, prompting the following question about their geometric properties:

Question 1

Which lattices coming from the above constructions are WR?

In this talk we give a partial answer to this and related questions, and consider some generalizations.

Ideal lattice construction

We start by fixing some notation:

$K =$ number field of degree n over $\mathbb{Q}$
$\mathcal{O}_K =$ ring of integers of K
$\sigma_1, \ldots, \sigma_{r_1}$ are real embeddings of K
$\tau_1, \overline{\tau}_1, \ldots, \tau_{r_2}, \overline{\tau}_{r_2}$ are pairs of complex conjugate embeddings of K
$n = r_1 + 2r_2$
$\sigma_K = (\sigma_1, \ldots, \sigma_{r_1}, \Re(\tau_1), \Im(\tau_1), \ldots, \Re(\tau_{r_2}), \Im(\tau_{r_2})) : K \to \mathbb{R}^n$ – Minkowski embedding

Ideal lattice construction

We start by fixing some notation:

$K =$ number field of degree n over $\mathbb{Q}$
$\mathcal{O}_K =$ ring of integers of K
$\sigma_1, \ldots, \sigma_{r_1}$ are real embeddings of K
$\tau_1, \overline{\tau}_1, \ldots, \tau_{r_2}, \overline{\tau}_{r_2}$ are pairs of complex conjugate embeddings of K
$n = r_1 + 2r_2$
$\sigma_K = (\sigma_1, \ldots, \sigma_{r_1}, \Re(\tau_1), \Im(\tau_1), \ldots, \Re(\tau_{r_2}), \Im(\tau_{r_2})) : K \to \mathbb{R}^n$ – Minkowski embedding

Let $I \subseteq \mathcal{O}_K$ be an ideal, then $\sigma_K(I)$ is a lattice of full rank in $\mathbb{R}^n$, called an **ideal lattice of trace type** (Bayer-Fluckiger).

Ideal lattice construction

We start by fixing some notation:

$K =$ number field of degree n over $\mathbb{Q}$
$\mathcal{O}_K =$ ring of integers of K
$\sigma_1, \ldots, \sigma_{r_1}$ are real embeddings of K
$\tau_1, \overline{\tau}_1, \ldots, \tau_{r_2}, \overline{\tau}_{r_2}$ are pairs of complex conjugate embeddings of K
$n = r_1 + 2r_2$
$\sigma_K = (\sigma_1, \ldots, \sigma_{r_1}, \Re(\tau_1), \Im(\tau_1), \ldots, \Re(\tau_{r_2}), \Im(\tau_{r_2})) : K \to \mathbb{R}^n$ – Minkowski embedding

Let $I \subseteq \mathcal{O}_K$ be an ideal, then $\sigma_K(I)$ is a lattice of full rank in $\mathbb{R}^n$, called an **ideal lattice of trace type** (Bayer-Fluckiger).

Some famous lattices were obtained this way, for instance the family of Craig's lattices and their generalizations from cyclotomic fields.

WR ideal lattices

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

Question 2

Which ideals in rings of integers of number fields are WR?

WR ideal lattices

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

Question 2

Which ideals in rings of integers of number fields are WR?

Theorem 2 (F., Petersen (2012))

$\mathcal{O}_K$ 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.

WR ideal lattices

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

Question 2

Which ideals in rings of integers of number fields are WR?

Theorem 2 (F., Petersen (2012))

$\mathcal{O}_K$ 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 under the same Minkowski embedding are always WR.

Proof ingredients for Theorem 2

- Product formula + AM-GM inequality to show that minimal vectors in $\sigma_K(\mathcal{O}_K)$ come only from roots of unity in $\mathcal{O}_K$.

Proof ingredients for Theorem 2

- Product formula + AM-GM inequality to show that minimal vectors in $\sigma_K(\mathcal{O}_K)$ come only from roots of unity in $\mathcal{O}_K$.
- Unique canonical integral bases for ideals in quadratic number fields: $a, b + g\delta$, where:

$$0 \leq b < a,\ 0 < g \leq a,\ g \mid a,\ g \mid b$$

are integers, and

$$\delta = \begin{cases} -\sqrt{D} & \text{if } D \not\equiv 1 (\mathrm{mod}\, 4) \\ \frac{1-\sqrt{D}}{2} & \text{if } D \equiv 1 (\mathrm{mod}\, 4). \end{cases}$$

Proof ingredients for Theorem 2

- Product formula + AM-GM inequality to show that minimal vectors in $\sigma_K(\mathcal{O}_K)$ come only from roots of unity in $\mathcal{O}_K$.
- Unique canonical integral bases for ideals in quadratic number fields: $a, b + g\delta$, where:

$$0 \leq b < a,\ 0 < g \leq a,\ g \mid a,\ g \mid b$$

are integers, and

$$\delta = \begin{cases} -\sqrt{D} & \text{if } D \not\equiv 1 (\mathrm{mod}\, 4) \\ \frac{1-\sqrt{D}}{2} & \text{if } D \equiv 1 (\mathrm{mod}\, 4). \end{cases}$$

- A result of Clary & Fabrykowski (2004) on infinitude of squarefree integers in arithmetic progressions.

WR ideals in quadratic number fields

We can say more in the case of quadratic number fields.

WR ideals in quadratic number fields

We can say more in the case of quadratic number fields.

We say that a positive squarefree integer D satisfies the ν-**nearsquare condition** if it has a divisor d with $\sqrt{\frac{D}{\nu}} \leq d < \sqrt{D}$, where $\nu > 1$ is a real number. We also write K **WR** to indicate that a number field K contains WR ideals.

WR ideals in quadratic number fields

We can say more in the case of quadratic number fields.

We say that a positive squarefree integer D satisfies the ν-**nearsquare condition** if it has a divisor d with $\sqrt{\frac{D}{\nu}} \leq d < \sqrt{D}$, where $\nu > 1$ is a real number. We also write K **WR** to indicate that a number field K contains WR ideals.

Theorem 3 (F., Henshaw, Liao, Prince, Sun, Whitehead, 2013)

If D satisfies the 3-nearsquare condition, then the rings of integers of quadratic number fields $K = \mathbb{Q}(\sqrt{\pm D})$ contain WR ideals; the statement becomes if and only if when $K = \mathbb{Q}(\sqrt{-D})$. This in particular implies that a positive proportion (more than $1/5$) of real and imaginary quadratic number fields contain WR ideals, more specifically

$$\liminf_{N\to\infty} \frac{\left|\left\{\mathbb{Q}(\sqrt{\pm D}) \text{ WR} : 0 < D \leq N\right\}\right|}{\left|\left\{\mathbb{Q}(\sqrt{\pm D}) : 0 < D \leq N\right\}\right|} \geq \frac{\sqrt{3}-1}{2\sqrt{3}}. \qquad (1)$$

WR ideals in imaginary quadratics

Theorem 4 (F., Henshaw, Liao, Prince, Sun, Whitehead, 2013)

For every D satisfying the 3-nearsquare condition the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$ contains only finitely many WR ideals, up to similarity of the corresponding lattices, and this number is

$$\ll \min\left\{2^{\omega(D)-1}, \frac{2^{\omega(D)}}{\sqrt{\omega(D)}}\right\}, \tag{2}$$

where $\omega(D)$ is the number of prime divisors of D.

WR ideals in imaginary quadratics

Theorem 4 (F., Henshaw, Liao, Prince, Sun, Whitehead, 2013)

For every D satisfying the 3-nearsquare condition the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$ contains only finitely many WR ideals, up to similarity of the corresponding lattices, and this number is

$$\ll \min\left\{2^{\omega(D)-1}, \frac{2^{\omega(D)}}{\sqrt{\omega(D)}}\right\}, \tag{2}$$

where $\omega(D)$ is the number of prime divisors of D.

Remark 2

Let $I, J \subseteq \mathcal{O}_K$ be WR ideals, then $\sigma_K(I) \sim \sigma_K(J) \iff I \sim J$, hence their number $\leq h_K \approx O(\sqrt{D})$ as $D \to \infty$ (Siegel), while the bound of (2) is $\approx \frac{(\log D)^{\log 2}}{\sqrt{\log\log D}}$ as $D \to \infty$.

Proof ingredients for Theorems 3 and 4

- Parameterization of similarity classes of integral WR lattices in $\mathbb{R}^2$ by solutions of Pell-type equations $x^2 + Dy^2 = z^2$.

Proof ingredients for Theorems 3 and 4

- Parameterization of similarity classes of integral WR lattices in $\mathbb{R}^2$ by solutions of Pell-type equations $x^2 + Dy^2 = z^2$.
- Unique canonical integral bases for ideals in quadratic number fields, as above.

Proof ingredients for Theorems 3 and 4

- Parameterization of similarity classes of integral WR lattices in $\mathbb{R}^2$ by solutions of Pell-type equations $x^2 + Dy^2 = z^2$.
- Unique canonical integral bases for ideals in quadratic number fields, as above.
- Estimates on the density of squarefree integers with divisors in "floating" intervals around the square-root (this is related to estimates on Hooley's Δ-function).

Proof ingredients for Theorems 3 and 4

- Parameterization of similarity classes of integral WR lattices in $\mathbb{R}^2$ by solutions of Pell-type equations $x^2 + Dy^2 = z^2$.
- Unique canonical integral bases for ideals in quadratic number fields, as above.
- Estimates on the density of squarefree integers with divisors in "floating" intervals around the square-root (this is related to estimates on Hooley's Δ-function).
- Explicit estimates (inequalities) on the prime-counting function (Rosser & Schoenfeld - 1962) and sums of primes (Jakimczuk - 2005).

Principal ideal lattices

As indicated above, in an imaginary quadratic field K, ideals I and J are equivalent if and only if the corresponding ideal lattices $\sigma_K(I)$ and $\sigma_K(J)$ are similar. Hence if I is a principal ideal, then $\sigma_K(I) \sim \sigma_K(\mathcal{O}_K)$, and so

$$\text{principal } I \text{ is WR} \iff K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3}).$$

Principal ideal lattices

As indicated above, in an imaginary quadratic field K, ideals I and J are equivalent if and only if the corresponding ideal lattices $\sigma_K(I)$ and $\sigma_K(J)$ are similar. Hence if I is a principal ideal, then $\sigma_K(I) \sim \sigma_K(\mathcal{O}_K)$, and so

$$\text{principal } I \text{ is WR} \iff K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3}).$$

The situation is different if K is a real quadratic.

Theorem 5 (Gnilke, Hollanti, Karilla, Tran (2016))

There exist infinitely many $K = \mathbb{Q}(\sqrt{D})$ with positive $D \equiv 1 (\mathrm{mod}\, 4)$ and $D \equiv 3 (\mathrm{mod}\, 4)$ such that $\mathcal{O}_K$ contains WR ideals.

Ideal lattices from polynomial rings

Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree $n \geq 1$. Define a map

$$\rho : \mathbb{Z}[x]/f(x) \to \mathbb{Z}^n$$

that takes a polynomial

$$p(x) = \sum_{k=0}^{n-1} a_k x^k \in \mathbb{Z}[x]/f(x)$$

to its coefficient vector:

$$\rho(p(x)) = (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n.$$

Ideal lattices from polynomial rings

Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree $n \geq 1$. Define a map

$$\rho : \mathbb{Z}[x]/f(x) \to \mathbb{Z}^n$$

that takes a polynomial

$$p(x) = \sum_{k=0}^{n-1} a_k x^k \in \mathbb{Z}[x]/f(x)$$

to its coefficient vector:

$$\rho(p(x)) = (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n.$$

Then for any ideal $I \subseteq \mathbb{Z}[x]/f(x)$, $\rho(I)$ is a sublattice of $\mathbb{Z}^n$. Such lattices have been studied in the recent years for their applications in cryptography.

Cyclic lattices from ideals in $\mathbb{Z}[x]/(x^n - 1)$

In the case when

$$f(x) = x^n - 1,$$

such sublattices of $\mathbb{Z}^n$ are called **cyclic**. We will concentrate on this situation.

Cyclic lattices from ideals in $\mathbb{Z}[x]/(x^n - 1)$

In the case when

$$f(x) = x^n - 1,$$

such sublattices of $\mathbb{Z}^n$ are called **cyclic**. We will concentrate on this situation.

For every $p(x) \in I$,

$$xp(x) = a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2} x^{n-1} \in I,$$

and so

$$\rho(xp(x)) = (a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in \rho(I).$$

Rotational shift operator

In other words, cyclic lattices are sublattices of $\mathbb{Z}^n$ closed under the **rotational shift operator** on $\mathbb{R}^n$, $n \geq 2$:

$$\mathrm{rot}(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_n, a_1, a_2, \ldots, a_{n-1})$$

for every $\boldsymbol{a} = (a_1, a_2, \ldots, a_{n-1}, a_n) \in \mathbb{R}^n$.

Rotational shift operator

In other words, cyclic lattices are sublattices of $\mathbb{Z}^n$ closed under the **rotational shift operator** on $\mathbb{R}^n$, $n \geq 2$:

$$\mathrm{rot}(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_n, a_1, a_2, \ldots, a_{n-1})$$

for every $\boldsymbol{a} = (a_1, a_2, \ldots, a_{n-1}, a_n) \in \mathbb{R}^n$.
Let σ_n be the standard n-cycle $(1\ 2 \ldots\ n)$ in the symmetric group S_n. For any $\tau \in S_n$, define

$$\tau(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_{\tau(1)}, a_{\tau(2)}, \ldots, a_{\tau(n)}).$$

Rotational shift operator

In other words, cyclic lattices are sublattices of $\mathbb{Z}^n$ closed under the **rotational shift operator** on $\mathbb{R}^n$, $n \geq 2$:

$$\mathrm{rot}(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_n, a_1, a_2, \ldots, a_{n-1})$$

for every $\boldsymbol{a} = (a_1, a_2, \ldots, a_{n-1}, a_n) \in \mathbb{R}^n$.
Let σ_n be the standard n-cycle $(1\ 2 \ldots\ n)$ in the symmetric group S_n. For any $\tau \in S_n$, define

$$\tau(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_{\tau(1)}, a_{\tau(2)}, \ldots, a_{\tau(n)}).$$

Then $\mathrm{rot}(\boldsymbol{a}) = \sigma_n^{-1}(\boldsymbol{a})$, and hence the set of cyclic lattices is

$$\{\rho(I) \subseteq \mathbb{Z}^n : I \subseteq \mathbb{Z}[x]/(x^n - 1)\}$$

Rotational shift operator

In other words, cyclic lattices are sublattices of $\mathbb{Z}^n$ closed under the **rotational shift operator** on $\mathbb{R}^n$, $n \geq 2$:

$$\mathrm{rot}(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_n, a_1, a_2, \ldots, a_{n-1})$$

for every $\boldsymbol{a} = (a_1, a_2, \ldots, a_{n-1}, a_n) \in \mathbb{R}^n$.
Let σ_n be the standard n-cycle $(1\ 2 \ldots\ n)$ in the symmetric group S_n. For any $\tau \in S_n$, define

$$\tau(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_{\tau(1)}, a_{\tau(2)}, \ldots, a_{\tau(n)}).$$

Then $\mathrm{rot}(\boldsymbol{a}) = \sigma_n^{-1}(\boldsymbol{a})$, and hence the set of cyclic lattices is

$$\begin{aligned} & \{\rho(I) \subseteq \mathbb{Z}^n : I \subseteq \mathbb{Z}[x]/(x^n - 1)\} \\ = \quad & \{\Gamma \subseteq \mathbb{Z}^n : \mathrm{rot}(\Gamma) = \Gamma\} \end{aligned}$$

Rotational shift operator

In other words, cyclic lattices are sublattices of $\mathbb{Z}^n$ closed under the **rotational shift operator** on $\mathbb{R}^n$, $n \geq 2$:

$$\mathrm{rot}(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_n, a_1, a_2, \ldots, a_{n-1})$$

for every $\boldsymbol{a} = (a_1, a_2, \ldots, a_{n-1}, a_n) \in \mathbb{R}^n$.
Let σ_n be the standard n-cycle $(1\ 2 \ldots\ n)$ in the symmetric group S_n. For any $\tau \in S_n$, define

$$\tau(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_{\tau(1)}, a_{\tau(2)}, \ldots, a_{\tau(n)}).$$

Then $\mathrm{rot}(\boldsymbol{a}) = \sigma_n^{-1}(\boldsymbol{a})$, and hence the set of cyclic lattices is

$$\begin{aligned} & \{\rho(I) \subseteq \mathbb{Z}^n : I \subseteq \mathbb{Z}[x]/(x^n - 1)\} \\ = \ & \{\Gamma \subseteq \mathbb{Z}^n : \mathrm{rot}(\Gamma) = \Gamma\} \\ = \ & \{\Gamma \subseteq \mathbb{Z}^n : \langle \sigma_n \rangle \leq \mathrm{Aut}(\Gamma)\}. \end{aligned}$$

Cyclic lattices: basic properties

Definition 1

For a vector $\boldsymbol{a} \in \mathbb{R}^n$, define a lattice

$$\Lambda(\boldsymbol{a}) = \mathrm{span}_{\mathbb{Z}} \left\{ \boldsymbol{a}, \mathrm{rot}(\boldsymbol{a}), \ldots, \mathrm{rot}^{n-1}(\boldsymbol{a}) \right\}.$$

Then $\mathrm{rot}(\Lambda(\boldsymbol{a})) = \Lambda(\boldsymbol{a})$, and if $\boldsymbol{a} \in \mathbb{Z}^n$ then $\Lambda(\boldsymbol{a})$ is a cyclic lattice.

Cyclic lattices: basic properties

Definition 1

For a vector $\boldsymbol{a} \in \mathbb{R}^n$, define a lattice

$$\Lambda(\boldsymbol{a}) = \mathrm{span}_{\mathbb{Z}} \left\{ \boldsymbol{a}, \mathrm{rot}(\boldsymbol{a}), \ldots, \mathrm{rot}^{n-1}(\boldsymbol{a}) \right\}.$$

Then $\mathrm{rot}(\Lambda(\boldsymbol{a})) = \Lambda(\boldsymbol{a})$, and if $\boldsymbol{a} \in \mathbb{Z}^n$ then $\Lambda(\boldsymbol{a})$ is a cyclic lattice.

Let $\Phi(x) \mid x^n - 1$ be a cyclotomic polynomial, then

$$H_\Phi = \left\{ \boldsymbol{a} \in \mathbb{R}^n : \Phi(x) \mid p_{\boldsymbol{a}}(x) := \sum_{k=1}^{n} a_k x^{k-1} \right\} \subseteq \mathbb{R}^n$$

is a subspace of dimension $n - \deg(\Phi)$.

Cyclic lattices: basic properties

Definition 1

For a vector $\boldsymbol{a} \in \mathbb{R}^n$, define a lattice

$$\Lambda(\boldsymbol{a}) = \mathrm{span}_{\mathbb{Z}} \left\{ \boldsymbol{a}, \mathrm{rot}(\boldsymbol{a}), \ldots, \mathrm{rot}^{n-1}(\boldsymbol{a}) \right\}.$$

Then $\mathrm{rot}(\Lambda(\boldsymbol{a})) = \Lambda(\boldsymbol{a})$, and if $\boldsymbol{a} \in \mathbb{Z}^n$ then $\Lambda(\boldsymbol{a})$ is a cyclic lattice.

Let $\Phi(x) \mid x^n - 1$ be a cyclotomic polynomial, then

$$H_\Phi = \left\{ \boldsymbol{a} \in \mathbb{R}^n : \Phi(x) \mid p_{\boldsymbol{a}}(x) := \sum_{k=1}^{n} a_k x^{k-1} \right\} \subseteq \mathbb{R}^n$$

is a subspace of dimension $n - \deg(\Phi)$.

Lemma 6

Let $\boldsymbol{a} \in \mathbb{R}^n$, then $\mathrm{rk}(\Lambda(\boldsymbol{a})) < n$ if and only if $p_{\boldsymbol{a}}(x) \in H_\Phi$ for some cyclotomic polynomial $\Phi(x) \mid x^n - 1$.

Cyclic lattices: cryptographic use

Hence for a generic vector $\boldsymbol{a} \in \mathbb{Z}^n$,

$$\mathrm{rk}(\Lambda(\boldsymbol{a})) = n, \tag{3}$$

i.e., the probability that (3) holds tends to 1 as $\|\boldsymbol{a}\| \to \infty$, and the size of the input data necessary to describe this lattice is only n (instead of n^2 for generic lattices). This observation makes cyclic lattices very attractive for cryptographic purposes.

Cyclic lattices: cryptographic use

Hence for a generic vector $\boldsymbol{a} \in \mathbb{Z}^n$,

$$\mathrm{rk}(\Lambda(\boldsymbol{a})) = n, \tag{3}$$

i.e., the probability that (3) holds tends to 1 as $\|\boldsymbol{a}\| \to \infty$, and the size of the input data necessary to describe this lattice is only n (instead of n^2 for generic lattices). This observation makes cyclic lattices very attractive for cryptographic purposes.

Cyclic lattices were used in the NTRU crypto system by J. Hoffstein, J. Pipher, and J. H. Silverman (1996), and then systematically studied in cryptographic context by D. Micciancio (2002).

Cyclic lattices: cryptographic use

Hence for a generic vector $\boldsymbol{a} \in \mathbb{Z}^n$,

$$\mathrm{rk}(\Lambda(\boldsymbol{a})) = n, \tag{3}$$

i.e., the probability that (3) holds tends to 1 as $\|\boldsymbol{a}\| \to \infty$, and the size of the input data necessary to describe this lattice is only n (instead of n^2 for generic lattices). This observation makes cyclic lattices very attractive for cryptographic purposes.

Cyclic lattices were used in the NTRU crypto system by J. Hoffstein, J. Pipher, and J. H. Silverman (1996), and then systematically studied in cryptographic context by D. Micciancio (2002).

Question 3 (Open Question)

Are cyclic lattices hard enough? For instance, are the Shortest Vector Problem (SVP) and the Shortest Independent Vector Problem (SIVP) still **NP***-hard on cyclic lattices?*

SIVP to SVP on cyclic lattices

There is some indication that SIVP is at least easier on cyclic lattices than on generic lattices.

SIVP to SVP on cyclic lattices

There is some indication that SIVP is at least easier on cyclic lattices than on generic lattices.

Theorem 7 (Peikert, Rosen (2005))

Let n be a **prime** *and let $\Lambda \subset \mathbb{R}^n$ be a cyclic lattice of rank n. There exists a polynomial time algorithm that, given an oracle for SVP, produces an approximate solution to SIVP on Λ within an approximation factor of 2 (compared to $\sqrt{n}$ for generic lattices) with only one call to the oracle.*

SIVP to SVP on cyclic lattices

There is some indication that SIVP is at least easier on cyclic lattices than on generic lattices.

Theorem 7 (Peikert, Rosen (2005))

Let n be a **prime** *and let $\Lambda \subset \mathbb{R}^n$ be a cyclic lattice of rank n. There exists a polynomial time algorithm that, given an oracle for SVP, produces an approximate solution to SIVP on Λ within an approximation factor of 2 (compared to $\sqrt{n}$ for generic lattices) with only one call to the oracle.*

Our work on WR cyclic lattices leads to some additional information.

WR cyclic lattices

Let

$$\mathcal{C}_n = \{\Gamma \subseteq \mathbb{Z}^n : \Gamma = \Lambda(\boldsymbol{a}) \text{ for some } \boldsymbol{a} \in \mathbb{Z}^n,\ \mathrm{rk}(\Lambda(\boldsymbol{a})) = n\},$$

and let $\mathcal{C}'_n = \{\Gamma \in \mathcal{C}_n : \Gamma \text{ contains a basis of minimal vectors}\}$.

WR cyclic lattices

Let

$$\mathcal{C}_n = \{\Gamma \subseteq \mathbb{Z}^n : \Gamma = \Lambda(\boldsymbol{a}) \text{ for some } \boldsymbol{a} \in \mathbb{Z}^n,\ \mathrm{rk}(\Lambda(\boldsymbol{a})) = n\},$$

and let $\mathcal{C}'_n = \{\Gamma \in \mathcal{C}_n : \Gamma \text{ contains a basis of minimal vectors}\}$.

Theorem 8 (F., Sun (2013))

For each dimension $n \geq 2$, there exists a real constant $\alpha_n > 0$, depending only on n, such that

$$\#\left\{\Gamma \in \mathcal{C}'_n : \lambda_n(\Gamma) \leq R\right\} \geq \alpha_n R^n \text{ as } R \to \infty. \tag{4}$$

WR cyclic lattices

Let

$$\mathcal{C}_n = \{\Gamma \subseteq \mathbb{Z}^n : \Gamma = \Lambda(\boldsymbol{a}) \text{ for some } \boldsymbol{a} \in \mathbb{Z}^n,\ \mathrm{rk}(\Lambda(\boldsymbol{a})) = n\},$$

and let $\mathcal{C}'_n = \{\Gamma \in \mathcal{C}_n : \Gamma \text{ contains a basis of minimal vectors}\}$.

Theorem 8 (F., Sun (2013))

For each dimension $n \geq 2$, there exists a real constant $\alpha_n > 0$, depending only on n, such that

$$\#\left\{\Gamma \in \mathcal{C}'_n : \lambda_n(\Gamma) \leq R\right\} \geq \alpha_n R^n \text{ as } R \to \infty. \tag{4}$$

Remark 3

This is the same asymptotic order as for the number of *all* ideal lattices from rings of integers of number fields or from polynomial quotient rings $\mathbb{Z}[x]/(f(x))$, where $f(x) \in \mathbb{Z}[x]$ is monic irreducible.

SVP - SIVP equivalence

In particular, one can explicitly construct families of cyclic lattices with bases of minimal vectors on which SVP and SIVP are equivalent.

SVP - SIVP equivalence

In particular, one can explicitly construct families of cyclic lattices with bases of minimal vectors on which SVP and SIVP are equivalent.

Corollary 9 (F., Sun (2013))

Let $k_1, \ldots, k_{n-1} \in \mathbb{Z}$ *be nonzero integers,* $m = \mathrm{lcm}(k_1, \ldots, k_{n-1})$, *and*

$$\boldsymbol{a} = \left(m, \frac{m}{k_1}, \ldots, \frac{m}{k_{n-1}} \right)^t \in \mathbb{Z}^n.$$

There exists an integer l, *depending only on* n, *such that whenever* $|k_1|, \ldots, |k_{n-1}| \geq l$, *we have:*

SVP - SIVP equivalence

In particular, one can explicitly construct families of cyclic lattices with bases of minimal vectors on which SVP and SIVP are equivalent.

Corollary 9 (F., Sun (2013))

Let $k_1, \ldots, k_{n-1} \in \mathbb{Z}$ *be nonzero integers,* $m = \mathrm{lcm}(k_1, \ldots, k_{n-1})$, *and*

$$\boldsymbol{a} = \left(m, \frac{m}{k_1}, \ldots, \frac{m}{k_{n-1}} \right)^t \in \mathbb{Z}^n.$$

There exists an integer l, *depending only on* n, *such that whenever* $|k_1|, \ldots, |k_{n-1}| \geq l$, *we have:*

- $|\Lambda(\boldsymbol{a})| = \|\boldsymbol{a}\|$

SVP - SIVP equivalence

In particular, one can explicitly construct families of cyclic lattices with bases of minimal vectors on which SVP and SIVP are equivalent.

Corollary 9 (F., Sun (2013))

Let $k_1, \ldots, k_{n-1} \in \mathbb{Z}$ *be nonzero integers,* $m = \mathrm{lcm}(k_1, \ldots, k_{n-1})$, *and*

$$\boldsymbol{a} = \left(m, \frac{m}{k_1}, \ldots, \frac{m}{k_{n-1}} \right)^t \in \mathbb{Z}^n.$$

There exists an integer l, *depending only on* n, *such that whenever* $|k_1|, \ldots, |k_{n-1}| \geq l$, *we have:*

- $|\Lambda(\boldsymbol{a})| = \|\boldsymbol{a}\|$
- $\mathrm{rk}(\Lambda(\boldsymbol{a})) = n$

SVP - SIVP equivalence

In particular, one can explicitly construct families of cyclic lattices with bases of minimal vectors on which SVP and SIVP are equivalent.

Corollary 9 (F., Sun (2013))

Let $k_1, \ldots, k_{n-1} \in \mathbb{Z}$ *be nonzero integers,* $m = \mathrm{lcm}(k_1, \ldots, k_{n-1})$, *and*

$$\boldsymbol{a} = \left(m, \frac{m}{k_1}, \ldots, \frac{m}{k_{n-1}} \right)^t \in \mathbb{Z}^n.$$

There exists an integer l, *depending only on* n, *such that whenever* $|k_1|, \ldots, |k_{n-1}| \geq l$, *we have:*

- $|\Lambda(\boldsymbol{a})| = \|\boldsymbol{a}\|$
- $\mathrm{rk}(\Lambda(\boldsymbol{a})) = n$
- *SVP* $\equiv$ *SIVP on* $\Lambda(\boldsymbol{a})$.

General permutation invariant lattices

More generally, let $\tau \in S_n$ be an element of order ν, such that

$$\tau = c_1 \cdots c_\ell$$

is a product of $\ell \geq 1$ disjoint cycles of orders $k_1, \ldots, k_\ell$, respectively. Consider the set of τ-**invariant** lattices

$$\mathcal{C}_n(\tau) = \{\Gamma \subset \mathbb{R}^n : \mathrm{rk}(\Gamma) = n,\ \langle\tau\rangle \leq \mathrm{Aut}(\Gamma)\}\,.$$

General permutation invariant lattices

More generally, let $\tau \in S_n$ be an element of order ν, such that

$$\tau = c_1 \cdots c_\ell$$

is a product of $\ell \geq 1$ disjoint cycles of orders $k_1, \ldots, k_\ell$, respectively. Consider the set of τ-**invariant** lattices

$$\mathcal{C}_n(\tau) = \{\Gamma \subset \mathbb{R}^n : \mathrm{rk}(\Gamma) = n,\ \langle\tau\rangle \leq \mathrm{Aut}(\Gamma)\}\,.$$

Definition 2

For a vector $\boldsymbol{a} \in \mathbb{R}^n$, define a lattice

$$\Lambda_\tau(\boldsymbol{a}) = \mathrm{span}_{\mathbb{Z}}\left\{\boldsymbol{a}, \tau(\boldsymbol{a}), \ldots, \tau^{\nu-1}(\boldsymbol{a})\right\},$$

which is τ-invariant.

General permutation invariant lattices

Define

$$\mathsf{o}_\tau := n - \sum_{\substack{d \mid \gcd(k_i, k_j) \\ i<j}} \varphi(d),$$

where φ is the Euler totient function and the sum above is understood as 0 if $\ell = 1$.

General permutation invariant lattices

Define

$$\mathsf{o}_\tau := n - \sum_{\substack{d \mid \gcd(k_i,k_j) \\ i<j}} \varphi(d),$$

where φ is the Euler totient function and the sum above is understood as 0 if $\ell = 1$.

Theorem 10 (F., Garcia, Sun (2014))

For any $\boldsymbol{a} \in \mathbb{R}^n$, $\mathrm{rk}(\Lambda_\tau(\boldsymbol{a})) \leq \mathsf{o}_\tau$ and the equality is achieved on generic vectors, i.e., with probability tending to 1 as $\|\boldsymbol{a}\| \to \infty$. This implies that the set

$$\mathcal{W}_n(\tau) = \{\Gamma \in \mathcal{C}_n(\tau) : \Gamma \text{ is well-rounded } \}$$

has co-dimension $\geq \left\lceil \frac{n}{\mathsf{o}_\tau} \right\rceil - 1$ in $\mathcal{C}_n(\tau)$.

Function field lattices

Let

$$A_{n-1} = \left\{ \boldsymbol{a} \in \mathbb{Z}^n : \sum_{i=1}^{n} a_i = 0 \right\}$$

be the well-known root lattice. The following construction of sublattices of A_{n-1} is due independently to Quebbemann (1989) and Rosenbloom & Tsfasman (1990).

Function field lattices

Let

$$A_{n-1} = \left\{ \boldsymbol{a} \in \mathbb{Z}^n : \sum_{i=1}^{n} a_i = 0 \right\}$$

be the well-known root lattice. The following construction of sublattices of A_{n-1} is due independently to Quebbemann (1989) and Rosenbloom & Tsfasman (1990).

p is prime, q is a power of p, $\mathbb{F}_q$ is the field with q elements
X a smooth curve of genus g over $\mathbb{F}_q$, $K = \mathbb{F}_q(X)$
$X(\mathbb{F}_q) = \{P_1, \ldots, P_n\}$ with corresponding valuations $v_1, \ldots, v_n$
$\mathcal{O}^*_{X,q} = \{f \in K \setminus \{0\} : \mathrm{Supp}(f) \subseteq X(\mathbb{F}_q)\}$

Function field lattices

Let

$$A_{n-1} = \left\{ \boldsymbol{a} \in \mathbb{Z}^n : \sum_{i=1}^{n} a_i = 0 \right\}$$

be the well-known root lattice. The following construction of sublattices of A_{n-1} is due independently to Quebbemann (1989) and Rosenbloom & Tsfasman (1990).

p is prime, q is a power of p, $\mathbb{F}_q$ is the field with q elements
X a smooth curve of genus g over $\mathbb{F}_q$, $K = \mathbb{F}_q(X)$
$X(\mathbb{F}_q) = \{P_1, \ldots, P_n\}$ with corresponding valuations $v_1, \ldots, v_n$
$\mathcal{O}^*_{X,q} = \{f \in K \setminus \{0\} : \mathrm{Supp}(f) \subseteq X(\mathbb{F}_q)\}$

For each $f \in \mathcal{O}^*_{X,q}$, we have the principal divisor

$$(f) = \sum_{i=1}^{n} v_i(f) P_i, \ \sum_{i=1} v_i(f) = 0, \ \deg(f) := \sum_{i=1} |v_i(f)|.$$

Function field lattices

Define the map $\phi : \mathcal{O}^*_{X,q} \to \mathbb{Z}^n$ given by $\phi(f) = (v_1(f), \ldots, v_n(f))$, then $L_{X,q} := \phi(\mathcal{O}^*_{X,q}) \subseteq A_{n-1}$ is a sublattice of finite index with

$$\begin{aligned} |L_{X,q}| &:= \min\{\|\boldsymbol{x}\| : \boldsymbol{x} \in L_{X,q} \setminus \{\mathbf{0}\}\} \\ &\geq \min\left\{\sqrt{\deg(f)} : f \in \mathcal{O}^*_{X,q} \setminus \mathbb{F}_q\right\}, \end{aligned}$$

where $\| \ \|$ is Euclidean norm, and

$$\det(L_{X,q}) \leq \sqrt{n}\left(1 + q + \frac{n-q-1}{g}\right)^g.$$

Function field lattices

Define the map $\phi : \mathcal{O}^*_{X,q} \to \mathbb{Z}^n$ given by $\phi(f) = (v_1(f), \ldots, v_n(f))$, then $L_{X,q} := \phi(\mathcal{O}^*_{X,q}) \subseteq A_{n-1}$ is a sublattice of finite index with

$$\begin{aligned} |L_{X,q}| &:= \min\{\|\boldsymbol{x}\| : \boldsymbol{x} \in L_{X,q} \setminus \{\mathbf{0}\}\} \\ &\geq \min\left\{\sqrt{\deg(f)} : f \in \mathcal{O}^*_{X,q} \setminus \mathbb{F}_q\right\}, \end{aligned}$$

where $\| \ \|$ is Euclidean norm, and

$$\det(L_{X,q}) \leq \sqrt{n}\left(1 + q + \frac{n-q-1}{g}\right)^g.$$

This construction famously led to some families of asymptotically dense lattices.

Abelian group lattices

We discuss an algebraic construction of lattices which generalizes the function field lattices. Given a finite Abelian group G and a subset

$$S = \{g_0 := 0, g_1, \ldots, g_{n-1}\}$$

of G, we define the sublattice $L_G(S)$ of A_{n-1} by

$$L_G(S) = \left\{ \boldsymbol{x} = (x_0, \ldots, x_{n-1}) \in A_{n-1} : \sum_{j=1}^{n-1} x_j g_j = 0 \right\}.$$

Abelian group lattices

We discuss an algebraic construction of lattices which generalizes the function field lattices. Given a finite Abelian group G and a subset

$$S = \{g_0 := 0, g_1, \ldots, g_{n-1}\}$$

of G, we define the sublattice $L_G(S)$ of A_{n-1} by

$$L_G(S) = \left\{ \boldsymbol{x} = (x_0, \ldots, x_{n-1}) \in A_{n-1} : \sum_{j=1}^{n-1} x_j g_j = 0 \right\}.$$

In case G is the subgroup of the degree zero divisor class group $\mathrm{Cl}^0(K)$ of $K = \mathbb{F}_q(X)$ generated by a set of divisor classes

$$S = \{[P_i - P_1] : P_i \in X(\mathbb{F}_q), 1 \leq i \leq n\}$$

we have

$$L_G(S) = L_{X,q}.$$

In other words, our Abelian group lattices are a generalization of function field lattices.

Some questions

Due to the importance of function field lattices, we decided to systematically investigate geometric properties of the more general Abelian group lattices, guided by the following questions:

Some questions

Due to the importance of function field lattices, we decided to systematically investigate geometric properties of the more general Abelian group lattices, guided by the following questions:

- What are their minimal norms and determinants?

Some questions

Due to the importance of function field lattices, we decided to systematically investigate geometric properties of the more general Abelian group lattices, guided by the following questions:

- What are their minimal norms and determinants?
- What are their covering radii?

Some questions

Due to the importance of function field lattices, we decided to systematically investigate geometric properties of the more general Abelian group lattices, guided by the following questions:

- What are their minimal norms and determinants?
- What are their covering radii?
- How many minimal vectors do these lattices have?

Some questions

Due to the importance of function field lattices, we decided to systematically investigate geometric properties of the more general Abelian group lattices, guided by the following questions:

- What are their minimal norms and determinants?
- What are their covering radii?
- How many minimal vectors do these lattices have?
- Are they well-rounded?

Some questions

Due to the importance of function field lattices, we decided to systematically investigate geometric properties of the more general Abelian group lattices, guided by the following questions:

- What are their minimal norms and determinants?
- What are their covering radii?
- How many minimal vectors do these lattices have?
- Are they well-rounded? Generated by their minimal vectors?

Some questions

Due to the importance of function field lattices, we decided to systematically investigate geometric properties of the more general Abelian group lattices, guided by the following questions:

- What are their minimal norms and determinants?
- What are their covering radii?
- How many minimal vectors do these lattices have?
- Are they well-rounded? Generated by their minimal vectors? Have bases of minimal vectors?

Some questions

Due to the importance of function field lattices, we decided to systematically investigate geometric properties of the more general Abelian group lattices, guided by the following questions:

- What are their minimal norms and determinants?
- What are their covering radii?
- How many minimal vectors do these lattices have?
- Are they well-rounded? Generated by their minimal vectors? Have bases of minimal vectors?
- What can be said about their automorphism groups?

Some questions

Due to the importance of function field lattices, we decided to systematically investigate geometric properties of the more general Abelian group lattices, guided by the following questions:

- What are their minimal norms and determinants?
- What are their covering radii?
- How many minimal vectors do these lattices have?
- Are they well-rounded? Generated by their minimal vectors? Have bases of minimal vectors?
- What can be said about their automorphism groups?
- Do these lattices give rise to spherical designs?

Some questions

Due to the importance of function field lattices, we decided to systematically investigate geometric properties of the more general Abelian group lattices, guided by the following questions:

- What are their minimal norms and determinants?
- What are their covering radii?
- How many minimal vectors do these lattices have?
- Are they well-rounded? Generated by their minimal vectors? Have bases of minimal vectors?
- What can be said about their automorphism groups?
- Do these lattices give rise to spherical designs?

The answers to these questions certainly depend on the group G and the set S. In this talk we present some results we have obtained thus far.

Some results

Specifically, we have addressed the questions raised above in several situations:

- Function field lattices from elliptic curves over a finite field, in which case $G = S$ and the groups that can appear this way are always of the form $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ (with further restrictions on the pairs (m_1, m_2)) as characterized by H.-G. Rück in 1987.

Some results

Specifically, we have addressed the questions raised above in several situations:

- Function field lattices from elliptic curves over a finite field, in which case $G = S$ and the groups that can appear this way are always of the form $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ (with further restrictions on the pairs (m_1, m_2)) as characterized by H.-G. Rück in 1987.
- The Abelian group G is arbitrary, but the set S coincides with all of G; this is a generalization of function field lattices from elliptic curves.

Some results

Specifically, we have addressed the questions raised above in several situations:

- Function field lattices from elliptic curves over a finite field, in which case $G = S$ and the groups that can appear this way are always of the form $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ (with further restrictions on the pairs (m_1, m_2)) as characterized by H.-G. Rück in 1987.
- The Abelian group G is arbitrary, but the set S coincides with all of G; this is a generalization of function field lattices from elliptic curves.
- Function field lattices from Hermitian curves over finite fields, in which case the generating set S is a proper subset of the group G.

Three conditions on lattices

We first recall some more notation. For a lattice $L \subseteq \mathbb{R}^n$ we write $S(L)$ for its set of minimal vectors, as before.

Three conditions on lattices

We first recall some more notation. For a lattice $L \subseteq \mathbb{R}^n$ we write $S(L)$ for its set of minimal vectors, as before.

- A lattice L is **well-rounded** (WR) if

$$\operatorname{span}_{\mathbb{R}} L = \operatorname{span}_{\mathbb{R}} S(L).$$

Three conditions on lattices

We first recall some more notation. For a lattice $L \subseteq \mathbb{R}^n$ we write $S(L)$ for its set of minimal vectors, as before.

- A lattice L is **well-rounded** (WR) if

$$\operatorname{span}_{\mathbb{R}} L = \operatorname{span}_{\mathbb{R}} S(L).$$

- If $\operatorname{rk} L > 4$, a strictly stronger condition is that L is **generated by minimal vectors**, i.e.

$$L = \operatorname{span}_{\mathbb{Z}} S(L).$$

Three conditions on lattices

We first recall some more notation. For a lattice $L \subseteq \mathbb{R}^n$ we write $S(L)$ for its set of minimal vectors, as before.

- A lattice L is **well-rounded** (WR) if

$$\operatorname{span}_{\mathbb{R}} L = \operatorname{span}_{\mathbb{R}} S(L).$$

- If $\operatorname{rk} L > 4$, a strictly stronger condition is that L is **generated by minimal vectors**, i.e.

$$L = \operatorname{span}_{\mathbb{Z}} S(L).$$

- 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**.

Results on lattices from full Abelian group

Theorem 11 (Böttcher, F., Garcia, Maharaj (2014))

Let $n = |G|$ and write L_G for the lattice $L_G(G)$. Then:

Results on lattices from full Abelian group

Theorem 11 (Böttcher, F., Garcia, Maharaj (2014))

Let $n = |G|$ and write L_G for the lattice $L_G(G)$. Then:

1. *For any G, $\det L_G = n^{3/2}$.*

Results on lattices from full Abelian group

Theorem 11 (Böttcher, F., Garcia, Maharaj (2014))

Let $n = |G|$ and write L_G for the lattice $L_G(G)$. Then:

1. *For any G,* $\det L_G = n^{3/2}$.
2. $$|L_G| = \begin{cases} \sqrt{8} & \text{if } G = \mathbb{Z}/2\mathbb{Z}, \\ \sqrt{6} & \text{if } G = \mathbb{Z}/3\mathbb{Z}, \\ 2 & \text{for any other } G. \end{cases}$$

Results on lattices from full Abelian group

Theorem 11 (Böttcher, F., Garcia, Maharaj (2014))

Let $n = |G|$ and write L_G for the lattice $L_G(G)$. Then:

1. *For any G, $\det L_G = n^{3/2}$.*
2. $|L_G| = \begin{cases} \sqrt{8} & \text{if } G = \mathbb{Z}/2\mathbb{Z}, \\ \sqrt{6} & \text{if } G = \mathbb{Z}/3\mathbb{Z}, \\ 2 & \text{for any other } G. \end{cases}$
3. *For $G = \mathbb{Z}/4\mathbb{Z}$, the lattice L_G is not WR.*

Results on lattices from full Abelian group

Theorem 11 (Böttcher, F., Garcia, Maharaj (2014))

Let $n = |G|$ and write L_G for the lattice $L_G(G)$. Then:

1. *For any G, $\det L_G = n^{3/2}$.*
2. $|L_G| = \begin{cases} \sqrt{8} & \text{if } G = \mathbb{Z}/2\mathbb{Z}, \\ \sqrt{6} & \text{if } G = \mathbb{Z}/3\mathbb{Z}, \\ 2 & \text{for any other } G. \end{cases}$
3. *For $G = \mathbb{Z}/4\mathbb{Z}$, the lattice L_G is not WR.*
4. *For any $G \neq \mathbb{Z}/4\mathbb{Z}$, the lattice L_G has a basis of minimal vectors.*

Results on lattices from full Abelian group

Theorem 11 (Böttcher, F., Garcia, Maharaj (2014))

Let $n = |G|$ and write L_G for the lattice $L_G(G)$. Then:

1. *For any G, $\det L_G = n^{3/2}$.*
2. $$|L_G| = \begin{cases} \sqrt{8} & \text{if } G = \mathbb{Z}/2\mathbb{Z}, \\ \sqrt{6} & \text{if } G = \mathbb{Z}/3\mathbb{Z}, \\ 2 & \text{for any other } G. \end{cases}$$
3. *For $G = \mathbb{Z}/4\mathbb{Z}$, the lattice L_G is not WR.*
4. *For any $G \neq \mathbb{Z}/4\mathbb{Z}$, the lattice L_G has a basis of minimal vectors.*
5. *Let $\varepsilon = |\{g \in G : 2g = 0\}|$, then*

$$|S(L_G)| = \frac{n}{4\varepsilon}\left((n-\varepsilon)(n-\varepsilon-2) + n(n-2)(\varepsilon-1)\right).$$

Results on lattices from full Abelian group

Theorem 11 (Böttcher, F., Garcia, Maharaj (2014))

Let $n = |G|$ and write L_G for the lattice $L_G(G)$. Then:

1. *For any G, $\det L_G = n^{3/2}$.*
2. $|L_G| = \begin{cases} \sqrt{8} & \text{if } G = \mathbb{Z}/2\mathbb{Z}, \\ \sqrt{6} & \text{if } G = \mathbb{Z}/3\mathbb{Z}, \\ 2 & \text{for any other } G. \end{cases}$
3. *For $G = \mathbb{Z}/4\mathbb{Z}$, the lattice L_G is not WR.*
4. *For any $G \neq \mathbb{Z}/4\mathbb{Z}$, the lattice L_G has a basis of minimal vectors.*
5. *Let $\varepsilon = |\{g \in G : 2g = 0\}|$, then*

$$|S(L_G)| = \frac{n}{4\varepsilon}\left((n-\varepsilon)(n-\varepsilon-2) + n(n-2)(\varepsilon-1)\right).$$

6. *For any G, $\mathrm{Aut}(L_G) \cap S_{n-1} \cong \mathrm{Aut}(G)$.*

Remarks

If X is an elliptic curve over $\mathbb{F}_q$, a result of H.-G. Rück (1987) states that

$$X(\mathbb{F}_q) \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$$

for some $m_1 \mid m_2, q-1$.

Remarks

If X is an elliptic curve over $\mathbb{F}_q$, a result of H.-G. Rück (1987) states that

$$X(\mathbb{F}_q) \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$$

for some $m_1 \mid m_2, q-1$.

In the special case when G is a subgroup of some $X(\mathbb{F}_q)$, parts 1 – 4 of Theorem 11 were also independently established by Min Sha (2014).

Remarks

If X is an elliptic curve over $\mathbb{F}_q$, a result of H.-G. Rück (1987) states that

$$X(\mathbb{F}_q) \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$$

for some $m_1 \mid m_2, q-1$.

In the special case when G is a subgroup of some $X(\mathbb{F}_q)$, parts 1 – 4 of Theorem 11 were also independently established by Min Sha (2014).

In the special case when G is a cyclic group, the lattices L_G recover the well known family of Barnes lattices:

$$\mathcal{B}_{n-1} = \left\{ \boldsymbol{a} \in A_{n-1} : \sum_{i=1}^{n} i x_i \equiv 0 \pmod{n} \right\}.$$

Proof outline for Theorem 11

Part 1. Define an additive group homomorphism

$$\varphi : A_{n-1} \to G$$

by

$$\varphi\left(x_1, \ldots, x_{n-1}, -\sum_{i=1}^{n-1} x_i\right) = \sum_{i=1}^{n-1} x_i P_i.$$

Then φ is surjective and

$$\mathrm{Ker}(\varphi) = L_G.$$

Hence $G \cong A_{n-1}/L_G$, and so

$$n = |G| = |A_{n-1}/L_G| = \det L_G / \det A_{n-1} = \det L_G / \sqrt{n}.$$

Proof outline for Theorem 11

Parts 2–5. We explicitly construct bases of minimal vectors.

Proof outline for Theorem 11

Parts 2–5. We explicitly construct bases of minimal vectors. Let $n \geq 5$ and consider the cyclic group

$$G := \mathbb{Z}/n\mathbb{Z} = \{\mathbf{0}, \mathbf{1}, \ldots, \boldsymbol{n-1}\}.$$

Proof outline for Theorem 11

Parts 2–5. We explicitly construct bases of minimal vectors. Let $n \geq 5$ and consider the cyclic group

$$G := \mathbb{Z}/n\mathbb{Z} = \{\mathbf{0}, \mathbf{1}, \ldots, \boldsymbol{n-1}\}.$$

Then G has relations :

$$(-1)\mathbf{1} + (-1)\mathbf{2} + (1)\mathbf{3} = \mathbf{0},$$

$$(1)\mathbf{1} + (-1)\mathbf{2} + (-1)\mathbf{3} + (1)\mathbf{4} = \mathbf{0},$$

$$(-1)\mathbf{1} + (-1)\mathbf{3} + (1)\mathbf{4} = \mathbf{0},$$

$$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$$

Proof outline for Theorem 11

Parts 2–5. We explicitly construct bases of minimal vectors. Let $n \geq 5$ and consider the cyclic group

$$G := \mathbb{Z}/n\mathbb{Z} = \{\mathbf{0}, \mathbf{1}, \ldots, \boldsymbol{n-1}\}.$$

Then G has relations :

$$(-1)\mathbf{1} + (-1)\mathbf{2} + (1)\mathbf{3} = \mathbf{0},$$

$$(1)\mathbf{1} + (-1)\mathbf{2} + (-1)\mathbf{3} + (1)\mathbf{4} = \mathbf{0},$$

$$(-1)\mathbf{1} + (-1)\mathbf{3} + (1)\mathbf{4} = \mathbf{0},$$

$$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$$

In other words, the corresponding lattice L_G has n linearly independent vectors with 4 nonzero coordinates, all equal to ± 1. These are minimal vectors in L_G, and hence $|L_G| = 2$.

Proof outline for Theorem 11

Let A be the matrix whose columns are these minimal vectors. Then $A^t A$ is a certain (cornered) Toeplitz matrix. Using Cauchy-Binet formula, we show that

$$\left|\det(A^t A)\right| = n^3 = (\det L_G)^2$$

which means that A is a basis matrix for L_G. This establishes parts 2–4 of the theorem for cyclic groups of order ≥ 5. Small cyclic groups are treated separately.

Proof outline for Theorem 11

Let A be the matrix whose columns are these minimal vectors. Then $A^t A$ is a certain (cornered) Toeplitz matrix. Using Cauchy-Binet formula, we show that

$$\left|\det(A^t A)\right| = n^3 = (\det L_G)^2$$

which means that A is a basis matrix for L_G. This establishes parts 2–4 of the theorem for cyclic groups of order ≥ 5. Small cyclic groups are treated separately.

A general abelian group G can be presented as a direct product of cyclic groups. We show that a minimal basis matrix can be constructed as an upper block-triangular matrix with blocks corresponding to minimal basis matrices of lattices coming from the cyclic group factors.

Proof outline for Theorem 11

Let A be the matrix whose columns are these minimal vectors. Then $A^t A$ is a certain (cornered) Toeplitz matrix. Using Cauchy-Binet formula, we show that

$$\left|\det(A^t A)\right| = n^3 = (\det L_G)^2$$

which means that A is a basis matrix for L_G. This establishes parts 2–4 of the theorem for cyclic groups of order ≥ 5. Small cyclic groups are treated separately.

A general abelian group G can be presented as a direct product of cyclic groups. We show that a minimal basis matrix can be constructed as an upper block-triangular matrix with blocks corresponding to minimal basis matrices of lattices coming from the cyclic group factors.

Finally, since we can explicitly construct minimal vectors, we can also directly count them. This completes the proof.

Proof outline for Theorem 11

Part 6. If

$$G = \{g_0, g_1, \ldots, g_{n-1}\},$$

with g_0 the identity, as above, then any automorphism of G fixes g_0 and permutes $g_1, \ldots, g_{n-1}$. Hence $\mathrm{Aut}(G)$ can be identified with some subgroup H of S_{n-1}.

Proof outline for Theorem 11

Part 6. If

$$G = \{g_0, g_1, \ldots, g_{n-1}\},$$

with g_0 the identity, as above, then any automorphism of G fixes g_0 and permutes $g_1, \ldots, g_{n-1}$. Hence $\mathrm{Aut}(G)$ can be identified with some subgroup H of S_{n-1}.

We explicitly construct a map

$$\Phi : H \to \mathrm{Aut}(L_G) \cap S_{n-1},$$

given by $\Phi(\sigma) = \tau$ for every $\sigma \in H$, where

$$\tau\left(x_1, \ldots, x_{n-1}, -\sum_{i=1}^{n-1} x_i\right) = \left(x_{\sigma(1)}, \ldots, x_{\sigma(n-1)}, -\sum_{i=1}^{n-1} x_{\sigma(i)}\right).$$

Proof outline for Theorem 11

Part 6. If

$$G = \{g_0, g_1, \ldots, g_{n-1}\},$$

with g_0 the identity, as above, then any automorphism of G fixes g_0 and permutes $g_1, \ldots, g_{n-1}$. Hence $\mathrm{Aut}(G)$ can be identified with some subgroup H of S_{n-1}.

We explicitly construct a map

$$\Phi : H \to \mathrm{Aut}(L_G) \cap S_{n-1},$$

given by $\Phi(\sigma) = \tau$ for every $\sigma \in H$, where

$$\tau\left(x_1, \ldots, x_{n-1}, -\sum_{i=1}^{n-1} x_i\right) = \left(x_{\sigma(1)}, \ldots, x_{\sigma(n-1)}, -\sum_{i=1}^{n-1} x_{\sigma(i)}\right).$$

We then show that Φ is a group isomorphism.

Covering radius

An important invariant of a lattice L is its covering radius:

$$\mu(L) = \inf \{\mu \in \mathbb{R}_{>0} : B(\mu) + L = \mathrm{span}_{\mathbb{R}} L\},$$

where $B(\mu)$ is the ball of radius μ centered at the origin in $\mathrm{span}_{\mathbb{R}} L$.

Covering radius

An important invariant of a lattice L is its covering radius:

$$\mu(L) = \inf \{\mu \in \mathbb{R}_{>0} : B(\mu) + L = \mathrm{span}_{\mathbb{R}} L\},$$

where $B(\mu)$ is the ball of radius μ centered at the origin in $\mathrm{span}_{\mathbb{R}} L$.

In 2013, we produced a bound on the covering radius of lattices L_G, which was then improved by Min Sha (2014): if $|G| = n$, then

$$\mu(L_G) \leq \frac{1}{2}\sqrt{n} + \sqrt{2}. \tag{5}$$

Covering radius

An important invariant of a lattice L is its covering radius:

$$\mu(L) = \inf \{\mu \in \mathbb{R}_{>0} : B(\mu) + L = \operatorname{span}_{\mathbb{R}} L\},$$

where $B(\mu)$ is the ball of radius μ centered at the origin in $\operatorname{span}_{\mathbb{R}} L$.

In 2013, we produced a bound on the covering radius of lattices L_G, which was then improved by Min Sha (2014): if $|G| = n$, then

$$\mu(L_G) \leq \frac{1}{2}\sqrt{n} + \sqrt{2}. \tag{5}$$

In fact, if $G = \mathbb{Z}/n\mathbb{Z}$ for $n \geq 2$, we can do a little better (2014):

$$\mu(L_G) \leq \frac{1}{2}\sqrt{n + 4\log(n-2) + 6 - 4\log 2 + 10/(n-1)}. \tag{6}$$

Covering radius: some data

Here is data (chopped after the fourth digit after the decimal point) for $\mu(L_G)$ of several cyclic groups $G = \mathbb{Z}/n\mathbb{Z}$:

n	Bound (6)	Bound (5)
4	1.8257	2.4142
5	1.9443	2.5097
6	2.0477	2.6390
7	2.1408	2.7235
21	3.0210	3.7029
51	4.1831	4.9842
101	5.5387	6.4389
1 001	16.0613	17.2335
10 001	50.1026	51.4167
100 001	158.1536	159.5289
1 000 001	500.0149	501.4145

Spherical designs

Let $n \geq 2$. A collection of points $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$ on the unit sphere Σ_{n-2} in $\mathbb{R}^{n-1}$ is called a **spherical t-design** for an integer $t \geq 1$ if

$$\int_{\Sigma_{n-2}} f(\boldsymbol{X})\, d\nu(\boldsymbol{X}) = \frac{1}{m} \sum_{k=1}^{m} f(\boldsymbol{y}_k)$$

for every polynomial $f(\boldsymbol{X}) = f(X_1, \ldots, X_{n-1})$ with real coefficients of degree $\leq t$, where ν is the surface measure so that $\nu(\Sigma_{n-2}) = 1$.

Spherical designs

Let $n \geq 2$. A collection of points $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$ on the unit sphere Σ_{n-2} in $\mathbb{R}^{n-1}$ is called a **spherical t-design** for an integer $t \geq 1$ if

$$\int_{\Sigma_{n-2}} f(\boldsymbol{X})\, d\nu(\boldsymbol{X}) = \frac{1}{m} \sum_{k=1}^{m} f(\boldsymbol{y}_k)$$

for every polynomial $f(\boldsymbol{X}) = f(X_1, \ldots, X_{n-1})$ with real coefficients of degree $\leq t$, where ν is the surface measure so that $\nu(\Sigma_{n-2}) = 1$. A full-rank lattice in $\mathbb{R}^{n-1}$ is called **strongly eutactic** if its set of minimal vectors (normalized to lie on the unit sphere) forms a spherical 2-design. The Abelian group lattices L_G can be viewed as full-rank lattices in $\mathbb{R}^{n-1}$.

Spherical designs

Let $n \geq 2$. A collection of points $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m$ on the unit sphere Σ_{n-2} in $\mathbb{R}^{n-1}$ is called a **spherical t-design** for an integer $t \geq 1$ if

$$\int_{\Sigma_{n-2}} f(\boldsymbol{X})\, d\nu(\boldsymbol{X}) = \frac{1}{m} \sum_{k=1}^{m} f(\boldsymbol{y}_k)$$

for every polynomial $f(\boldsymbol{X}) = f(X_1, \ldots, X_{n-1})$ with real coefficients of degree $\leq t$, where ν is the surface measure so that $\nu(\Sigma_{n-2}) = 1$. A full-rank lattice in $\mathbb{R}^{n-1}$ is called **strongly eutactic** if its set of minimal vectors (normalized to lie on the unit sphere) forms a spherical 2-design. The Abelian group lattices L_G can be viewed as full-rank lattices in $\mathbb{R}^{n-1}$.

Theorem 12 (Böttcher, F., Garcia, Maharaj (2015))

The lattice L_G is strongly eutactic if and only if the Abelian group G has odd order or $G = (\mathbb{Z}/2\mathbb{Z})^k$ for some $k \geq 1$.

Perfection and packing density

A full-rank lattice $L \subset \mathbb{R}^n$ is called **perfect** if the set

$$\{\boldsymbol{x}\boldsymbol{x}^t : \boldsymbol{x} \in S(L)\}$$

spans the space of real symmetric $n \times n$ matrices as a real vector space.

Perfection and packing density

A full-rank lattice $L \subset \mathbb{R}^n$ is called **perfect** if the set

$$\{\boldsymbol{x}\boldsymbol{x}^t : \boldsymbol{x} \in S(L)\}$$

spans the space of real symmetric $n \times n$ matrices as a real vector space.

A classical result of Voronoi (1908) guarantees that perfect eutactic lattices are local maxima of the sphere packing density function on the space of lattices in a given dimension.

Perfection and packing density

A full-rank lattice $L \subset \mathbb{R}^n$ is called **perfect** if the set

$$\{\boldsymbol{x}\boldsymbol{x}^t : \boldsymbol{x} \in S(L)\}$$

spans the space of real symmetric $n \times n$ matrices as a real vector space.

A classical result of Voronoi (1908) guarantees that perfect eutactic lattices are local maxima of the sphere packing density function on the space of lattices in a given dimension.

Roland Bacher (2015) proved that if $|G| \geq 9$, the corresponding lattice L_G is perfect.

Perfection and packing density

A full-rank lattice $L \subset \mathbb{R}^n$ is called **perfect** if the set

$$\{\boldsymbol{x}\boldsymbol{x}^t : \boldsymbol{x} \in S(L)\}$$

spans the space of real symmetric $n \times n$ matrices as a real vector space.

A classical result of Voronoi (1908) guarantees that perfect eutactic lattices are local maxima of the sphere packing density function on the space of lattices in a given dimension.

Roland Bacher (2015) proved that if $|G| \geq 9$, the corresponding lattice L_G is perfect.

Hence, combining Bacher's result with ours, we obtain:

Corollary 13

If $|G| \geq 9$ is odd or $G = (\mathbb{Z}/2\mathbb{Z})^k$ for some $k \geq 4$, then L_G is a local maximum of the sphere packing density function on the space of lattices in its dimension.

General subsets of an Abelian group

Let $S \subseteq G$ contain the identity, $|G| = n \geq |S| = m$. Define

$$\mathrm{Aut}(G, S) := \{\sigma \in \mathrm{Aut}(G) \ : \ \sigma(g) \in S \ \forall g \in S\},$$

$$\mathrm{Aut}(G, S)^* := \{\sigma|_S : S \to S \ : \ \sigma \in \mathrm{Aut}(G, S)\}.$$

General subsets of an Abelian group

Let $S \subseteq G$ contain the identity, $|G| = n \geq |S| = m$. Define

$$\mathrm{Aut}(G, S) := \{\sigma \in \mathrm{Aut}(G) \ : \ \sigma(g) \in S \ \forall g \in S\},$$

$$\mathrm{Aut}(G, S)^* := \{\sigma|_S : S \to S \ : \ \sigma \in \mathrm{Aut}(G, S)\}.$$

Theorem 14 (Böttcher, F., Garcia, Maharaj (2015))

With notation as above:

General subsets of an Abelian group

Let $S \subseteq G$ contain the identity, $|G| = n \geq |S| = m$. Define

$$\mathrm{Aut}(G, S) := \{\sigma \in \mathrm{Aut}(G) \ : \ \sigma(g) \in S \ \forall g \in S\},$$

$$\mathrm{Aut}(G, S)^* := \{\sigma|_S : S \to S \ : \ \sigma \in \mathrm{Aut}(G, S)\}.$$

Theorem 14 (Böttcher, F., Garcia, Maharaj (2015))

With notation as above:

1. $|L_G(S)| = 2$ *if* $m(m-1) \geq 2(n+1)$

General subsets of an Abelian group

Let $S \subseteq G$ contain the identity, $|G| = n \geq |S| = m$. Define

$$\mathrm{Aut}(G, S) := \{\sigma \in \mathrm{Aut}(G) \ : \ \sigma(g) \in S \ \forall g \in S\},$$

$$\mathrm{Aut}(G, S)^* := \{\sigma|_S : S \to S \ : \ \sigma \in \mathrm{Aut}(G, S)\}.$$

Theorem 14 (Böttcher, F., Garcia, Maharaj (2015))

With notation as above:

1. $|L_G(S)| = 2$ *if* $m(m-1) \geq 2(n+1)$
2. $|L_G(S)| \leq \sqrt{6}$ *if* $m(m-1)(m-2) \geq 6(n+1)$

General subsets of an Abelian group

Let $S \subseteq G$ contain the identity, $|G| = n \geq |S| = m$. Define

$$\mathrm{Aut}(G,S) := \{\sigma \in \mathrm{Aut}(G) \ : \ \sigma(g) \in S \ \forall g \in S\},$$

$$\mathrm{Aut}(G,S)^* := \{\sigma|_S : S \to S \ : \ \sigma \in \mathrm{Aut}(G,S)\}.$$

Theorem 14 (Böttcher, F., Garcia, Maharaj (2015))

With notation as above:

1. $|L_G(S)| = 2$ *if* $m(m-1) \geq 2(n+1)$
2. $|L_G(S)| \leq \sqrt{6}$ *if* $m(m-1)(m-2) \geq 6(n+1)$
3. $\mathrm{Aut}(G,S)^*$ *is isomorphic to a subgroup of* $\mathrm{Aut}(L_G(S)) \cap S_{m-1}$. *If* S *is a generating set for* G, *then*

$$\mathrm{Aut}(G,S)^* \cong \mathrm{Aut}(L_G(S)) \cap S_{m-1}.$$

Lattices from Hermitian curves

When the lattice $L_G(S)$ comes from a Hermitian curve X:

$$y^q + y = x^{q+1}$$

over a finite field $\mathbb{F}_{q^2}$, q is a prime power, we have further results.

Lattices from Hermitian curves

When the lattice $L_G(S)$ comes from a Hermitian curve X:

$$y^q + y = x^{q+1}$$

over a finite field $\mathbb{F}_{q^2}$, q is a prime power, we have further results.

Theorem 15 (Böttcher, F., Garcia, Maharaj (2015))

Let $L_G(S)$ come from a Hermitian curve X over $\mathbb{F}_{q^2}$, i.e.

$$S = \{[P_i - P_1] : P_i \in X(\mathbb{F}_{q^2}), 1 \leq i \leq m\} \subset \mathrm{Cl}^0(\mathbb{F}_{q^2}(X))$$

and $G \leq \mathrm{Cl}^0(\mathbb{F}_{q^2}(X))$ is generated by S. Then:

Lattices from Hermitian curves

When the lattice $L_G(S)$ comes from a Hermitian curve X:

$$y^q + y = x^{q+1}$$

over a finite field $\mathbb{F}_{q^2}$, q is a prime power, we have further results.

Theorem 15 (Böttcher, F., Garcia, Maharaj (2015))

Let $L_G(S)$ come from a Hermitian curve X over $\mathbb{F}_{q^2}$, i.e.

$$S = \{[P_i - P_1] : P_i \in X(\mathbb{F}_{q^2}), 1 \leq i \leq m\} \subset \mathrm{Cl}^0(\mathbb{F}_{q^2}(X))$$

and $G \leq \mathrm{Cl}^0(\mathbb{F}_{q^2}(X))$ is generated by S. Then:

1. $|L_G(S)| = \sqrt{2q}$ *and* $\det L_G(S) = \sqrt{q^3+1}(q+1)^{q^2-q}$.

Lattices from Hermitian curves

When the lattice $L_G(S)$ comes from a Hermitian curve X:

$$y^q + y = x^{q+1}$$

over a finite field $\mathbb{F}_{q^2}$, q is a prime power, we have further results.

Theorem 15 (Böttcher, F., Garcia, Maharaj (2015))

Let $L_G(S)$ come from a Hermitian curve X over $\mathbb{F}_{q^2}$, i.e.

$$S = \{[P_i - P_1] : P_i \in X(\mathbb{F}_{q^2}), 1 \leq i \leq m\} \subset \mathrm{Cl}^0(\mathbb{F}_{q^2}(X))$$

and $G \leq \mathrm{Cl}^0(\mathbb{F}_{q^2}(X))$ is generated by S. Then:

1. $|L_G(S)| = \sqrt{2q}$ *and* $\det L_G(S) = \sqrt{q^3+1}(q+1)^{q^2-q}$.
2. $L_G(S)$ *is generated by minimal vectors.*

Lattices from Hermitian curves

When the lattice $L_G(S)$ comes from a Hermitian curve X:

$$y^q + y = x^{q+1}$$

over a finite field $\mathbb{F}_{q^2}$, q is a prime power, we have further results.

Theorem 15 (Böttcher, F., Garcia, Maharaj (2015))

Let $L_G(S)$ come from a Hermitian curve X over $\mathbb{F}_{q^2}$, i.e.

$$S = \{[P_i - P_1] : P_i \in X(\mathbb{F}_{q^2}), 1 \leq i \leq m\} \subset \mathrm{Cl}^0(\mathbb{F}_{q^2}(X))$$

and $G \leq \mathrm{Cl}^0(\mathbb{F}_{q^2}(X))$ is generated by S. Then:

1. $|L_G(S)| = \sqrt{2q}$ *and* $\det L_G(S) = \sqrt{q^3+1}(q+1)^{q^2-q}$.
2. $L_G(S)$ *is generated by minimal vectors.*
3. $L_G(S)$ *contains at least* $q^7 - q^5 + q^4 - q^2$ *minimal vectors.*

Lattices from Hermitian curves

When the lattice $L_G(S)$ comes from a Hermitian curve X:

$$y^q + y = x^{q+1}$$

over a finite field $\mathbb{F}_{q^2}$, q is a prime power, we have further results.

Theorem 15 (Böttcher, F., Garcia, Maharaj (2015))

Let $L_G(S)$ come from a Hermitian curve X over $\mathbb{F}_{q^2}$, i.e.

$$S = \{[P_i - P_1] : P_i \in X(\mathbb{F}_{q^2}), 1 \leq i \leq m\} \subset \mathrm{Cl}^0(\mathbb{F}_{q^2}(X))$$

and $G \leq \mathrm{Cl}^0(\mathbb{F}_{q^2}(X))$ is generated by S. Then:

1. $|L_G(S)| = \sqrt{2q}$ *and* $\det L_G(S) = \sqrt{q^3+1}(q+1)^{q^2-q}$.
2. $L_G(S)$ *is generated by minimal vectors.*
3. $L_G(S)$ *contains at least* $q^7 - q^5 + q^4 - q^2$ *minimal vectors.*
4. $\mathrm{Aut}(\mathbb{F}_{q^2}(X)) \cong$ *to a subgroup of* $\mathrm{Aut}(L_G(S)) \cap S_{m-1}$.

Idea of proof

- We first characterize divisors of all lines in the Hermitian function field $K = \mathbb{F}_{q^2}(X)$, that is functions of the form $ax + by + c$ ($a, b, c \in \mathbb{F}_{q^2}$ with a, b not both zero).

Idea of proof

- We first characterize divisors of all lines in the Hermitian function field $K = \mathbb{F}_{q^2}(X)$, that is functions of the form $ax + by + c$ ($a, b, c \in \mathbb{F}_{q^2}$ with a, b not both zero).
- We show that minimal vectors in the lattice $L_G(S)$ come precisely from divisors of functions of the form (f_1/f_2), where f_1 and f_2 are two distinct lines satisfying some additional conditions, which we explicitly describe and count. We use this description to compute the minimal norm of the lattice.

Idea of proof

- We first characterize divisors of all lines in the Hermitian function field $K = \mathbb{F}_{q^2}(X)$, that is functions of the form $ax + by + c$ ($a, b, c \in \mathbb{F}_{q^2}$ with a, b not both zero).
- We show that minimal vectors in the lattice $L_G(S)$ come precisely from divisors of functions of the form (f_1/f_2), where f_1 and f_2 are two distinct lines satisfying some additional conditions, which we explicitly describe and count. We use this description to compute the minimal norm of the lattice.
- G. Hiss (2004) showed that every function in $\mathcal{O}^*_{X,q^2}$ (in case $X/\mathbb{F}_{q^2}$ is a Hermitian curve) is the product of functions of the form $ax + by + c$ and their inverses. We use Hiss's result, along with our above description of minimal vectors, to prove that the lattice $L_G(S)$ is generated by minimal vectors.

Idea of proof

- We first characterize divisors of all lines in the Hermitian function field $K = \mathbb{F}_{q^2}(X)$, that is functions of the form $ax + by + c$ ($a, b, c \in \mathbb{F}_{q^2}$ with a, b not both zero).
- We show that minimal vectors in the lattice $L_G(S)$ come precisely from divisors of functions of the form (f_1/f_2), where f_1 and f_2 are two distinct lines satisfying some additional conditions, which we explicitly describe and count. We use this description to compute the minimal norm of the lattice.
- G. Hiss (2004) showed that every function in $\mathcal{O}^*_{X,q^2}$ (in case $X/\mathbb{F}_{q^2}$ is a Hermitian curve) is the product of functions of the form $ax + by + c$ and their inverses. We use Hiss's result, along with our above description of minimal vectors, to prove that the lattice $L_G(S)$ is generated by minimal vectors.
- In the Hermitian case, $A_{n-1}/L_G(S) \cong \mathrm{Cl}^0(K)$, and so determinant of $L_G(S)$ can be related to the class number of K, which is well-known.

Remarks

- In general, lattices of the form $L_G(S)$ may be WR and non-WR. For example, if $G = \mathbb{Z}/7\mathbb{Z}$ and S runs over all non-trivial subsets of G containing 0, then out of the 62 resulting lattices of the form $L_G(S)$, 26 are WR and 36 are not. Interestingly, the group $\mathrm{Aut}(G, S)^*$ can be non-trivial even when $L_G(S)$ is not WR.

Remarks

- In general, lattices of the form $L_G(S)$ may be WR and non-WR. For example, if $G = \mathbb{Z}/7\mathbb{Z}$ and S runs over all non-trivial subsets of G containing 0, then out of the 62 resulting lattices of the form $L_G(S)$, 26 are WR and 36 are not. Interestingly, the group $\mathrm{Aut}(G, S)^*$ can be non-trivial even when $L_G(S)$ is not WR.
- The function field lattice corresponding to the Klein curve

$$(x + y + 1)^4 + (xy + x + y)^2 + xy(x + y + 1) = 0$$

over $\mathbb{F}_4$ has rank 13 in $\mathbb{R}^{14}$ and 168 minimal vectors, which generate a sublattice of index 2: it is WR, but not generated by its minimal vectors.

Remarks

- In general, lattices of the form $L_G(S)$ may be WR and non-WR. For example, if $G = \mathbb{Z}/7\mathbb{Z}$ and S runs over all non-trivial subsets of G containing 0, then out of the 62 resulting lattices of the form $L_G(S)$, 26 are WR and 36 are not. Interestingly, the group $\mathrm{Aut}(G, S)^*$ can be non-trivial even when $L_G(S)$ is not WR.
- The function field lattice corresponding to the Klein curve

$$(x + y + 1)^4 + (xy + x + y)^2 + xy(x + y + 1) = 0$$

over $\mathbb{F}_4$ has rank 13 in $\mathbb{R}^{14}$ and 168 minimal vectors, which generate a sublattice of index 2: it is WR, but not generated by its minimal vectors.

- In recent work, L. Ates and H. Stichtenoth (2015) obtained many examples of function field lattices from hyperelliptic curves over finite fields which are not WR.

The papers that I talked about are available at:

`http://math.cmc.edu/lenny/research.html`

The papers that I talked about are available at:

`http://math.cmc.edu/lenny/research.html`

Thank you!