Well-rounded lattices from algebraic constructions

Lenny Fukshansky
Claremont McKenna College

Workshop on "Sphere Packings, Lattices, and Designs"
ESI Programme on
"Minimal Energy Point Sets, Lattices, and Designs"
October 27-31, 2014

Well-rounded lattices

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of full rank. **Minimal norm** of Λ is

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

where $\| \ \|$ is Euclidean norm.

Well-rounded lattices

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of full rank. **Minimal norm** of Λ is

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

where $\| \ \|$ is Euclidean norm.

Λ is called **well-rounded** (abbreviated **WR**) if its set of minimal vectors

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

contains n linearly independent vectors.

Well-rounded lattices

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of full rank. **Minimal norm** of Λ is

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

where $\| \ \|$ is Euclidean norm.
Λ is called **well-rounded** (abbreviated **WR**) if its set of minimal vectors

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

contains n linearly independent vectors.
This is equivalent to saying that Λ has equal successive minima $(|\Lambda| =)\ \lambda_1 = \cdots = \lambda_n$, where

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

where $B_n(\lambda)$ is the unit ball of radius λ centered at $\mathbf{0}$ in $\mathbb{R}^n$.

Well-rounded lattices

Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice of full rank. **Minimal norm** of Λ is

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

where $\|\ \|$ is Euclidean norm.
Λ is called **well-rounded** (abbreviated **WR**) if its set of minimal vectors

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

contains n linearly independent vectors.
This is equivalent to saying that Λ has equal successive minima $(|\Lambda| =)\ \lambda_1 = \cdots = \lambda_n$, where

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

where $B_n(\lambda)$ is the unit ball of radius λ centered at $\mathbf{0}$ in $\mathbb{R}^n$.
WR lattices are central to extremal lattice theory, since many classical discrete optimization problems on lattices can be restricted to WR lattices wlog.

Some more notation

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

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

for some real constant α and orthogonal matrix U.

Some more notation

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

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

for some real constant α and orthogonal matrix U. WR lattices are only similar to WR lattices, so it often makes sense to talk of **WR similarity classes**, or of **WR lattices up to similarity**.

Some more notation

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

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

for some real constant α and orthogonal matrix U. WR lattices are only similar to WR lattices, so it often makes sense to talk of **WR similarity classes**, or of **WR lattices up to similarity**.

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

$$\mathrm{Aut}(\Lambda) := \mathrm{GL}(\Lambda) \cap O(\mathbb{R}^n),$$

where $\mathrm{GL}(\Lambda)$ is discrete and $O(\mathbb{R}^n)$ is the compact group of orthogonal transformations of $\mathbb{R}^n$ onto itself $\implies \mathrm{Aut}(\Lambda)$ is finite.

Some more notation

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

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

for some real constant α and orthogonal matrix U. WR lattices are only similar to WR lattices, so it often makes sense to talk of **WR similarity classes**, or of **WR lattices up to similarity**.

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

$$\mathrm{Aut}(\Lambda) := \mathrm{GL}(\Lambda) \cap O(\mathbb{R}^n),$$

where $\mathrm{GL}(\Lambda)$ is discrete and $O(\mathbb{R}^n)$ is the compact group of orthogonal transformations of $\mathbb{R}^n$ 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) $\mathrm{Aut}(\Lambda)$ is

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

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.)
- 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.)
- Function field lattices from curves over finite fields (Quebbemann, Rosenbloom & Tsfasman, 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.)
- Function field lattices from curves over finite fields (Quebbemann, Rosenbloom & Tsfasman, et al.)
- Ideal lattices from polynomial rings (Lyubashevsky & Micciancio, Peikert & Rosen 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.)
- Function field lattices from curves over finite fields (Quebbemann, Rosenbloom & Tsfasman, et al.)
- Ideal lattices from polynomial rings (Lyubashevsky & Micciancio, Peikert & Rosen 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.)
- Function field lattices from curves over finite fields (Quebbemann, Rosenbloom & Tsfasman, et al.)
- Ideal lattices from polynomial rings (Lyubashevsky & Micciancio, Peikert & Rosen 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 question 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
$\sigma_1, \dots, \sigma_{r_1}$ are real embeddings of K
$\tau_1, \overline{\tau}_1, \dots, \tau_{r_2}, \overline{\tau}_{r_2}$ are pairs of complex conjugate embeddings of K
$n = r_1 + 2r_2$
$\sigma_K = (\sigma_1, \dots, \sigma_{r_1}, \Re(\tau_1), \Im(\tau_1), \dots, \Re(\tau_{r_2}), \Im(\tau_{r_2})) : K \to \mathbb{R}^n$ – 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 1 (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 1 (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 1

- 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 1

- 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

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

Proof ingredients for Theorem 1

- 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

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

- 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 2 (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 3 (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 3 (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

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

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 2 and 3

- 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 2 and 3

- 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 2 and 3

- 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 2 and 3

- 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).

Directions for future work

Question 3

Do there exist real quadratic number fields $\mathbb{Q}(\sqrt{D})$ with positive squarefree D not satisfying the 3-nearsquare condition containing WR ideals?

Directions for future work

Question 3

Do there exist real quadratic number fields $\mathbb{Q}(\sqrt{D})$ with positive squarefree D not satisfying the 3-nearsquare condition containing WR ideals?

Computational evidence suggests that the answer to this question is **no**, however at the moment we only have partial results in this direction.

Directions for future work

Question 3

Do there exist real quadratic number fields $\mathbb{Q}(\sqrt{D})$ with positive squarefree D not satisfying the 3-nearsquare condition containing WR ideals?

Computational evidence suggests that the answer to this question is **no**, however at the moment we only have partial results in this direction.

Problem 1

Study the distribution of WR ideals in number fields of degree ≥ 3.

Function field lattice construction

Let

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

be the well known root lattice. The following construction is due independently to Quebbemann (1989) and Rosenbloom & Tsfasman (1990).

Function field lattice construction

Let

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

be the well known root lattice. The following construction 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 $\mathbb{F}_q$, $K = \mathbb{F}_q(X)$
$X(\mathbb{F}_q) = \{P_1, \dots, P_n\}$ with corresponding valuations $v_1, \dots, v_n$
$\mathcal{O}^*_{X,q} = \{f \in K \setminus \{0\} : \mathrm{Supp}(f) \subseteq X(\mathbb{F}_q)\}$

Function field lattice construction

Let

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

be the well known root lattice. The following construction 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 $\mathbb{F}_q$, $K = \mathbb{F}_q(X)$
$X(\mathbb{F}_q) = \{P_1, \dots, P_n\}$ with corresponding valuations $v_1, \dots, v_n$
$\mathcal{O}^*_{X,q} = \{f \in K \setminus \{0\} : \mathrm{Supp}(f) \subseteq X(\mathbb{F}_q)\}$
For each $f \in \mathcal{O}^*_{X,q}$, the principal divisor

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

Function field lattice construction

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

$$|L_{X,q}| \geq \min\left\{\sqrt{\deg(f)} : f \in \mathcal{O}^*_{X,q} \setminus \mathbb{F}_q\right\},$$

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

Function field lattice construction

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

$$|L_{X,q}| \geq \min\left\{\sqrt{\deg(f)} : f \in \mathcal{O}^*_{X,q} \setminus \mathbb{F}_q\right\},$$

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

This construction in particular leads to some families of asymptotically dense lattices.

Function field lattice construction

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

$$|L_{X,q}| \geq \min\left\{ \sqrt{\deg(f)} : f \in \mathcal{O}^*_{X,q} \setminus \mathbb{F}_q \right\},$$

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

This construction in particular leads to some families of asymptotically dense lattices.

Question 4

Which lattices $L_{X,q}$ as above are WR?

Function field lattice construction

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

$$|L_{X,q}| \geq \min\left\{ \sqrt{\deg(f)} : f \in \mathcal{O}^*_{X,q} \setminus \mathbb{F}_q \right\},$$

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

This construction in particular leads to some families of asymptotically dense lattices.

Question 4

Which lattices $L_{X,q}$ as above are WR?

We provide a partial answer to this question.

WR function field lattices

Theorem 4 (F., Maharaj (2013))

Let $g = 1$ and $n \geq 5$, i.e. X is an elliptic curve with at least 5 points over $\mathbb{F}_q$. Then $L_{X,q}$ is generated by its minimal vectors, so in particular is WR.

WR function field lattices

Theorem 4 (F., Maharaj (2013))

Let $g = 1$ and $n \geq 5$, i.e. X is an elliptic curve with at least 5 points over $\mathbb{F}_q$. Then $L_{X,q}$ is generated by its minimal vectors, so in particular is WR.

Theorem 5 (F., Maharaj (2013))

Let $g = 1$, $n \geq 4$, and let ε be the number of 2-torsion points in $X(\mathbb{F}_q)$. Then

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

A generalization

Question 5

Which of the function field lattices coming from curves of higher genus are WR?

A generalization

Question 5

Which of the function field lattices coming from curves of higher genus are WR?

This question may be hard. In our arguments for the elliptic curve case, we heavily rely on the group structure, which allows a very explicit description of the divisors giving rise to minimal vectors. This leads to a related direction that we recently pursued.

A generalization

Question 5

Which of the function field lattices coming from curves of higher genus are WR?

This question may be hard. In our arguments for the elliptic curve case, we heavily rely on the group structure, which allows a very explicit description of the divisors giving rise to minimal vectors. This leads to a related direction that we recently pursued.

Let

$$G = \{P_0, P_1, \ldots, P_{n-1}\}$$

be an abelian group of order n with P_0 the identity. A relation in the multiplication table of G can be written as

$$\sum_{i=1}^{n-1} a_i P_i = P_0,$$

where $a_i \in \mathbb{Z}$ for all $1 \leq i \leq n-1$.

Lattices from abelian groups

Hence every relation in G can be identified with the vector

$$\left(a_1, \dots, a_{n-1}, -\sum_{i=1}^{n-1} a_i \right) \in \mathbb{Z}^n,$$

and the set of all such vectors forms a finite index sublattice of the root lattice A_{n-1}, call it L_G.

Lattices from abelian groups

Hence every relation in G can be identified with the vector

$$\left(a_1, \dots, a_{n-1}, -\sum_{i=1}^{n-1} a_i \right) \in \mathbb{Z}^n,$$

and the set of all such vectors forms a finite index sublattice of the root lattice A_{n-1}, call it L_G.

This is a direct generalization of the lattice $L_{X,q}$ described above when X is an elliptic curve. However, lattices L_G are more general, since not every abelian group can be realized as the group of points on an elliptic curve over a finite field.

Lattices from abelian groups

Hence every relation in G can be identified with the vector

$$\left(a_1, \dots, a_{n-1}, -\sum_{i=1}^{n-1} a_i\right) \in \mathbb{Z}^n,$$

and the set of all such vectors forms a finite index sublattice of the root lattice A_{n-1}, call it L_G.

This is a direct generalization of the lattice $L_{X,q}$ described above when X is an elliptic curve. However, lattices L_G are more general, since not every abelian group can be realized as the group of points on an elliptic curve over a finite field.

Question 6

For which groups G are the lattices L_G WR?

Three conditions

A lattice Λ is WR if and only if

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

Three conditions

A lattice Λ is WR if and only if

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

For lattices of rank > 4, a strictly stronger condition is that Λ is spanned by its set of minimal vectors, i.e.

$$\Lambda = \operatorname{span}_{\mathbb{Z}} S(\Lambda). \tag{3}$$

Three conditions

A lattice Λ is WR if and only if

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

For lattices of rank > 4, a strictly stronger condition is that Λ is spanned by its set of minimal vectors, i.e.

$$\Lambda = \operatorname{span}_{\mathbb{Z}} S(\Lambda). \tag{3}$$

It has been shown by Conway & Sloane (1995) and Martinet & Schürmann (2011) that for lattices of rank ≥ 10 condition (3) is strictly weaker than containing a basis of minimal vectors.

Lattices from abelian groups

Theorem 6 (Böttcher, F., Garcia, Maharaj (2014))

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

Lattices from abelian groups

Theorem 6 (Böttcher, F., Garcia, Maharaj (2014))

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

Lattices from abelian groups

Theorem 6 (Böttcher, F., Garcia, Maharaj (2014))

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.*

Lattices from abelian groups

Theorem 6 (Böttcher, F., Garcia, Maharaj (2014))

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.*

Lattices from abelian groups

Theorem 6 (Böttcher, F., Garcia, Maharaj (2014))

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. *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 6 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 6 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:

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

Proof outline for Theorem 6

Part 1. Define an additive group homomorphism

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

by

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

Then φ is surjective and

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

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 6

Parts 2–4. We explicitly construct bases of minimal vectors.

Proof outline for Theorem 6

Parts 2–4. We explicitly construct bases of minimal vectors. Let $n \geq 5$ and consider the cyclic group

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

Proof outline for Theorem 6

Parts 2–4. We explicitly construct bases of minimal vectors. Let $n \geq 5$ and consider the cyclic group

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

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 6

Parts 2–4. We explicitly construct bases of minimal vectors. Let $n \geq 5$ and consider the cyclic group

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

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 6

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

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

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 6

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

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

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. This completes the proof.

Proof outline for Theorem 6

Part 5. If

$$G = \{P_0, P_1, \dots, P_{n-1}\},$$

with P_0 the identity, as above, then any automorphism of G fixes P_0 and permutes $P_1, \dots, P_{n-1}$. Hence $\mathrm{Aut}(G)$ can be identified with some subgroup H of S_{n-1}.

Proof outline for Theorem 6

Part 5. If

$$G = \{P_0, P_1, \dots, P_{n-1}\},$$

with P_0 the identity, as above, then any automorphism of G fixes P_0 and permutes $P_1, \dots, P_{n-1}$. 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

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

Proof outline for Theorem 6

Part 5. If

$$G = \{P_0, P_1, \dots, P_{n-1}\},$$

with P_0 the identity, as above, then any automorphism of G fixes P_0 and permutes $P_1, \dots, P_{n-1}$. 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

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

We then show that Φ is a group isomorphism.

Covering radius

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

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

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

Covering radius

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

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

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

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

$$\mu(L_G) \leq \frac{1}{2}\sqrt{n} + \sqrt{2}. \tag{4}$$

Covering radius

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

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

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

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

$$\mu(L_G) \leq \frac{1}{2}\sqrt{n} + \sqrt{2}. \tag{4}$$

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

$$\mu(L_G) \leq \frac{1}{2}\sqrt{n + 4\log(n-2) + 6 - 4\log 2 + 10/(n-1)}. \tag{5}$$

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 (5)	Bound (4)
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

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:

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

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

Rotational shift operator

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

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

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

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

Rotational shift operator

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

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

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

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

Then $\operatorname{rot}(\mathbf{a}) = \sigma_n^{-1}(\mathbf{a})$, 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 $\mathbb{R}^n$, $n \geq 2$:

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

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

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

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

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

Rotational shift operator

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

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

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

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

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

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

Cyclic lattices: basic properties

Definition 1

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

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

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

Cyclic lattices: basic properties

Definition 1

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

$$\Lambda(\mathbf{a}) = \operatorname{span}_{\mathbb{Z}} \left\{ \mathbf{a}, \operatorname{rot}(\mathbf{a}), \dots, \operatorname{rot}^{n-1}(\mathbf{a}) \right\}.$$

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

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

$$H_\Phi = \{\mathbf{a} \in \mathbb{R}^n : \Phi(x) \mid p_{\mathbf{a}}(x)\} \subseteq \mathbb{R}^n$$

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

Cyclic lattices: basic properties

Definition 1

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

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

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

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

$$H_\Phi = \{\mathbf{a} \in \mathbb{R}^n : \Phi(x) \mid p_{\mathbf{a}}(x)\} \subseteq \mathbb{R}^n$$

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

Lemma 7

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

Cyclic lattices: cryptographic use

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

$$\operatorname{rk}(\Lambda(\mathbf{a})) = n, \tag{6}$$

i.e., the probability that (6) holds tends to 1 as $\|\mathbf{a}\| \to \infty$, 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 $\mathbf{a} \in \mathbb{Z}^n$,

$$\mathrm{rk}(\Lambda(\mathbf{a})) = n, \tag{6}$$

i.e., the probability that (6) holds tends to 1 as $\|\mathbf{a}\| \to \infty$, 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 $\mathbf{a} \in \mathbb{Z}^n$,

$$\mathrm{rk}(\Lambda(\mathbf{a})) = n, \tag{6}$$

i.e., the probability that (6) holds tends to 1 as $\|\mathbf{a}\| \to \infty$, 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 7 (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 8 (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 8 (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

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

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

WR cyclic lattices

Let

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

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

Theorem 9 (F., Sun (2013))

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

$$\# \left\{\Gamma \in \mathcal{C}'_n : \lambda_n(\Gamma) \leq R\right\} \geq \alpha_n R^n \text{ as } R \to \infty. \tag{7}$$

WR cyclic lattices

Let

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

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

Theorem 9 (F., Sun (2013))

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

$$\#\left\{\Gamma \in \mathcal{C}'_n : \lambda_n(\Gamma) \leq R\right\} \geq \alpha_n R^n \text{ as } R \to \infty. \tag{7}$$

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 10 (F., Sun (2013))

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

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

There exists an integer l, *depending only on* n, *such that whenever* $|k_1|, \dots, |k_{n-1}| \geq l$, *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 10 (F., Sun (2013))

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

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

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

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

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 10 (F., Sun (2013))

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

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

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

- $|\Lambda(\mathbf{a})| = \|\mathbf{a}\|$
- $\operatorname{rk}(\Lambda(\mathbf{a})) = n$

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 10 (F., Sun (2013))

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

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

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

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

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 $k_1, \dots, k_\ell$, respectively. Consider the set of τ-**invariant** lattices

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

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 $k_1, \dots, k_\ell$, 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 $\mathbf{a} \in \mathbb{R}^n$, define a lattice

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

which is τ-invariant.

General permutation invariant lattices

Define

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

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

General permutation invariant lattices

Define

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

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

Theorem 11 (F., Garcia, Sun (2014))

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

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

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

Thank you!