Well-rounded lattices from algebraic constructions

Lenny Fukshansky
Claremont McKenna College

International Conference on The Algebraic and Arithmetic Theory of Quadratic Forms
Puerto Natales, Patagonia, Chile
December 16-21, 2013

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

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

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 $\lambda_1 = \cdots = \lambda_n$, where

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

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

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 $\lambda_1 = \cdots = \lambda_n$, 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 $\mathbb{R}^n$.
WR lattices are central to extremal lattice theory, since the standard discrete optimization problems on lattices can be restricted to WR lattices wlog.

Algebraic constructions

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

Algebraic constructions

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

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

Algebraic constructions

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

- Ideal lattices from number fields (Martinet, Bayer-Fluckiger, Nebe, et al.)
- Cyclic lattices from polynomial rings (Micciancio, et al.)
- Function field lattices from curves over finite fields (Tsfasman and Vladut, et al.)

Algebraic constructions

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

- Ideal lattices from number fields (Martinet, Bayer-Fluckiger, Nebe, et al.)
- Cyclic lattices from polynomial rings (Micciancio, et al.)
- Function field lattices from curves over finite fields (Tsfasman and Vladut, 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 three well known instances here:

- Ideal lattices from number fields (Martinet, Bayer-Fluckiger, Nebe, et al.)
- Cyclic lattices from polynomial rings (Micciancio, et al.)
- Function field lattices from curves over finite fields (Tsfasman and Vladut, 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 three well known instances here:

- Ideal lattices from number fields (Martinet, Bayer-Fluckiger, Nebe, et al.)
- Cyclic lattices from polynomial rings (Micciancio, et al.)
- Function field lattices from curves over finite fields (Tsfasman and Vladut, 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.

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
$\sigma_1, \dots, \sigma_{r_1}$ 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

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).

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. On the other hand, infinitely many real and imaginary quadratic number fields ($K = \mathbb{Q}(\sqrt{D})$) contain WR ideals.

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

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

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

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

- 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

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

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

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

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

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

Remark 1

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). On the other hand, 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.

Cyclic lattices: definition

Define the **rotational shift operator** on $\mathbb{R}^n$, $n \geq 2$, by

$$\text{rot}(x_1, x_2, \ldots, x_{n-1}, x_n) = (x_n, x_1, x_2, \ldots, x_{n-1})$$

for every $\mathbf{x} = (x_1, x_2, \ldots, x_{n-1}, x_n) \in \mathbb{R}^n$. We will write rot^k for iterated application of rot k times for each $k \in \mathbb{Z}_{>0}$ (then rot^0 is just the identity map, and $\text{rot}^k = \text{rot}^{n+k}$). It is also easy to see that rot (and hence each iteration rot^k) is a linear operator. A lattice Γ is called **cyclic** if $\text{rot}(\Gamma) = \Gamma$, i.e. if for every $\mathbf{x} \in \Gamma$, $\text{rot}(\mathbf{x}) \in \Gamma$. We will be concerned with cyclic sublattices of $\mathbb{Z}^n$; clearly, $\mathbb{Z}^n$ itself is a cyclic lattice.

Cyclic lattices: definition

Define the **rotational shift operator** on $\mathbb{R}^n$, $n \geq 2$, by

$$\operatorname{rot}(x_1, x_2, \ldots, x_{n-1}, x_n) = (x_n, x_1, x_2, \ldots, x_{n-1})$$

for every $\mathbf{x} = (x_1, x_2, \ldots, x_{n-1}, x_n) \in \mathbb{R}^n$. We will write rot^k for iterated application of rot k times for each $k \in \mathbb{Z}_{>0}$ (then rot^0 is just the identity map, and $\operatorname{rot}^k = \operatorname{rot}^{n+k}$). It is also easy to see that rot (and hence each iteration rot^k) is a linear operator. A lattice Γ is called **cyclic** if $\operatorname{rot}(\Gamma) = \Gamma$, i.e. if for every $\mathbf{x} \in \Gamma$, $\operatorname{rot}(\mathbf{x}) \in \Gamma$. We will be concerned with cyclic sublattices of $\mathbb{Z}^n$; clearly, $\mathbb{Z}^n$ itself is a cyclic lattice.

Cyclic lattices were introduced by D. Micciancio in 2002 for cryptographic use.

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

Let

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

Define a map $\rho : \mathbb{Z}[x]/(x^n-1) \to \mathbb{Z}^n$ by

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

then for any ideal $I \subseteq \mathbb{Z}[x]/(x^n-1)$, $\rho(I)$ is a sublattice of $\mathbb{Z}^n$. Notice that 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

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

In other words, $\Gamma \subseteq \mathbb{Z}^n$ is a cyclic lattice if and only if $\Gamma = \rho(I)$ for some ideal $I \subseteq \mathbb{Z}[x]/(x^n-1)$.

WR cyclic lattices

Let $\mathcal{C}_n$ be the set of all full rank cyclic sublattices of $\mathbb{Z}^n$.

WR cyclic lattices

Let $\mathcal{C}_n$ be the set of all full rank cyclic sublattices of $\mathbb{Z}^n$.

Question 4

Which lattices in $\mathcal{C}_n$ are WR?

WR cyclic lattices

Let $\mathcal{C}_n$ be the set of all full rank cyclic sublattices of $\mathbb{Z}^n$.

Question 4

Which lattices in $\mathcal{C}_n$ are WR?

Theorem 4 (F., Sun (2013))

For each dimension $n \geq 2$, there exist real constants

$$0 < \alpha_n \leq \beta_n \leq 1,$$

depending only on n, such that

$$\alpha_n \leq \frac{\#\left\{\Gamma \in \mathcal{C}_n : \lambda_n(\Gamma) \leq R,\ \Gamma \text{ is WR}\right\}}{\#\left\{\Gamma \in \mathcal{C}_n : \lambda_n(\Gamma) \leq R\right\}} \leq \beta_n \text{ as } R \to \infty. \tag{3}$$

For instance, one can take $\alpha_2 = 0.261386...$ and $\beta_2 = 0.348652...$, meaning that between 26% and 35% of full rank cyclic sublattices of $\mathbb{Z}^2$ are WR.

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.

Cyclic lattices: basic properties

Definition 1

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

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

Then $\mathrm{rot}(\Lambda(\mathbf{a})) = \Lambda(\mathbf{a})$, 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

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

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 $n - \deg(\Phi)$.

Lemma 5

Let $\mathbf{a} \in \mathbb{R}^n$, then $\operatorname{rk}(\Lambda(\mathbf{a})) < n$ 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 if we pick $\mathbf{a} \in \mathbb{Z}^n$ with large $|\mathbf{a}|$, the probability that

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

is high, 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 if we pick $\mathbf{a} \in \mathbb{Z}^n$ with large $|\mathbf{a}|$, the probability that

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

is high, 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.

Question 5

But 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?*

Cyclic lattices: cryptographic use

Hence if we pick $\mathbf{a} \in \mathbb{Z}^n$ with large $|\mathbf{a}|$, the probability that

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

is high, 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.

Question 5

But 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?*

We do not know, but probably **yes**.

SIVP to SVP on cyclic lattices

On the other hand, there is some indication that SIVP is at least easier on cyclic lattices than on generic lattices.

SIVP to SVP on cyclic lattices

On the other hand, there is some indication that SIVP is at least easier on cyclic lattices than on generic lattices.

Theorem 6 (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 a solution to SVP on Λ, produces an approximate solution to SIVP on Λ within an approximation factor of 2 (compared to $\sqrt{n}$ for generic lattices).*

SIVP to SVP on cyclic lattices

On the other hand, there is some indication that SIVP is at least easier on cyclic lattices than on generic lattices.

Theorem 6 (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 a solution to SVP on Λ, produces an approximate solution to SIVP on Λ within an approximation factor of 2 (compared to $\sqrt{n}$ for generic lattices).*

Our work on WR cyclic lattices leads to further information.

SIVP to SVP on cyclic lattices

On the other hand, there is some indication that SIVP is at least easier on cyclic lattices than on generic lattices.

Theorem 6 (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 a solution to SVP on Λ, produces an approximate solution to SIVP on Λ within an approximation factor of 2 (compared to $\sqrt{n}$ for generic lattices).*

Our work on WR cyclic lattices leads to further information.

Corollary 7 (F., Sun (2013))

In **every** *dimension $n \geq 2$, SIVP and SVP are equivalent on a positive proportion of cyclic lattices.*

Proof ingredients for Theorem 4

- Reduction to the set of cyclic lattices in $\mathbb{R}^n$ with a basis of vectors corresponding to successive minima, the so-called Minkowskian lattices. Let $\mathcal{G}_n$ be the set of Minkowskian sublattices of $\mathbb{Z}^n$ with this property.

Proof ingredients for Theorem 4

- Reduction to the set of cyclic lattices in $\mathbb{R}^n$ with a basis of vectors corresponding to successive minima, the so-called Minkowskian lattices. Let $\mathcal{G}_n$ be the set of Minkowskian sublattices of $\mathbb{Z}^n$ with this property.
- Representation of Minkowskian cyclic lattices in the form $\bigoplus \Lambda(\mathbf{a}_i)$ with $\mathbf{a}_i$'s corresponding to successive minima.

Proof ingredients for Theorem 4

- Reduction to the set of cyclic lattices in $\mathbb{R}^n$ with a basis of vectors corresponding to successive minima, the so-called Minkowskian lattices. Let $\mathcal{G}_n$ be the set of Minkowskian sublattices of $\mathbb{Z}^n$ with this property.
- Representation of Minkowskian cyclic lattices in the form $\bigoplus \Lambda(\mathbf{a}_i)$ with $\mathbf{a}_i$'s corresponding to successive minima.
- Parameterization of Minkowskian lattices of the form $\Lambda(\mathbf{a})$ by points in a certain convex polyhedral cone of positive volume with lattices in $\mathcal{G}_n$ corresponding to integer lattice points.

Proof ingredients for Theorem 4

- Reduction to the set of cyclic lattices in $\mathbb{R}^n$ with a basis of vectors corresponding to successive minima, the so-called Minkowskian lattices. Let $\mathcal{G}_n$ be the set of Minkowskian sublattices of $\mathbb{Z}^n$ with this property.
- Representation of Minkowskian cyclic lattices in the form $\bigoplus \Lambda(\mathbf{a}_i)$ with $\mathbf{a}_i$'s corresponding to successive minima.
- Parameterization of Minkowskian lattices of the form $\Lambda(\mathbf{a})$ by points in a certain convex polyhedral cone of positive volume with lattices in $\mathcal{G}_n$ corresponding to integer lattice points.
- Bounding the cone, applying lattice point counting estimates, and factoring in restrictions to cyclotomic subspaces in the cases of not full rank.

Further work

The symmetric group S_n has a natural action on $\mathbb{R}^n$ by permutation of the coordinates. Cyclic lattices are precisely the sublattices of $\mathbb{Z}^n$ closed under the action of the cyclic subgroup

$$\langle (1 \ \ldots n) \rangle \leq S_n.$$

Further work

The symmetric group S_n has a natural action on $\mathbb{R}^n$ by permutation of the coordinates. Cyclic lattices are precisely the sublattices of $\mathbb{Z}^n$ closed under the action of the cyclic subgroup

$$\langle(1 \ \ldots n)\rangle \leq S_n.$$

What happens if we consider lattices with automorphism groups containing a different subgroup of S_n?

Further work

The symmetric group S_n has a natural action on $\mathbb{R}^n$ by permutation of the coordinates. Cyclic lattices are precisely the sublattices of $\mathbb{Z}^n$ closed under the action of the cyclic subgroup

$$\langle (1 \ \dots n) \rangle \leq S_n.$$

What happens if we consider lattices with automorphism groups containing a different subgroup of S_n?

Conjecture / Theorem 8 (F., Sun (2013/2014))

The proportion of WR lattices among sublattices of $\mathbb{Z}^n$ closed under the action of a subgroup $H \leq S_n$ is positive if and only if $H = \langle \tau \rangle$, where τ is an n-cycle.

Function field lattice construction

This construction is due to Tsfasman and Vladut:

p is prime, q is a power of p, $\mathbb{F}_q$ is the field with q elements
X a 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 $v_1, \dots, v_n$
$\mathcal{O}^*_{X,q} = \{f \in K : \mathrm{Supp}(f) \subseteq X(\mathbb{F}_q)\}$

Function field lattice construction

This construction is due to Tsfasman and Vladut:

p is prime, q is a power of p, $\mathbb{F}_q$ is the field with q elements
X a 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 $v_1, \dots, v_n$
$\mathcal{O}^*_{X,q} = \{f \in K : \mathrm{Supp}(f) \subseteq X(\mathbb{F}_q)\}$
For each $f \in \mathcal{O}^*_{X,q}$, the principal divisor

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

Function field lattice construction

This construction is due to Tsfasman and Vladut:

p is prime, q is a power of p, $\mathbb{F}_q$ is the field with q elements
X a 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 $v_1, \dots, v_n$
$\mathcal{O}^*_{X,q} = \{f \in K : \mathrm{Supp}(f) \subseteq X(\mathbb{F}_q)\}$
For each $f \in \mathcal{O}^*_{X,q}$, the principal divisor

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

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

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

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

WR function field lattices

Question 6

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

WR function field lattices

Question 6

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

We provide a partial answer to this question:

Theorem 9 (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

Question 6

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

We provide a partial answer to this question:

Theorem 9 (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 10 (F., Maharaj (2013))

Let $g = 1$, $n \geq 4$, and let ε be the number of 2-torsion points on X. Then

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

Directions for future work

Question 7

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

Directions for future work

Question 7

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 another direction that we are currently pursuing.

Directions for future work

Question 7

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 another direction that we are currently pursuing.

Let

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

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 $1 \leq i \leq n-1$.

Directions for future work

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 A_{n-1}, call it L_G.

Directions for future work

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 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.

Directions for future work

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 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 8

For which groups G are the lattices L_G WR?

Directions for future work

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 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 8

For which groups G are the lattices L_G WR?

This is currently work in progress.

Thank you!