# Complexity of lattice problems on cyclic lattices

Xun Sun (Claremont Graduate University)

December 18, 2013

*joint work with L. Fukshansky*

# Rotation shift operator and cyclic lattices



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

$$\mathrm{rot}(x_1, x_2 \ldots, x_{N-1}, x_N) = (x_N, x_1, x_2, \ldots, x_{N-1})$$

for every $(x_1, x_2, \ldots, x_{N-1}, x_N) \in \mathbb{R}^N$. We will write $\mathrm{rot}^k$ for iterated application of rot $k$ times for each $k \in \mathbb{Z}_{>0}$.

**Remark 1**

$\mathrm{rot}^0$ is just the identity map, and $\mathrm{rot}^{N+k} = \mathrm{rot}^k$.

A full-rank sublattice $\Gamma$ of $\mathbb{Z}^N$ is called *cyclic* if $\mathrm{rot}(\Gamma) = \Gamma$, i.e. for every $x \in \Gamma$, $\mathrm{rot}(x) \in \Gamma$.

# 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

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

then for any ideal $I \subseteq \mathbb{Z}[x]/(x^N - 1)$, $\rho(I)$ is a sublatice of $\mathbb{Z}^N$ of full rank. Notice that for every $p(x) \in I$,

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

and so

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

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

# Basic properties of cyclic lattices - 1



## Definition 1

For a vector $a \in \mathbb{Z}^N$, define

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

This is always a cyclic lattice.

The following lemma indicates under which condition $\Lambda(a)$ is full rank.

## Lemma 1

*Let $a \in \mathbb{Z}^N$ and $p_a(x) \in \mathbb{Z}[x]/(x^N - 1)$ be a polynomial with coefficient vector $a$. Then $a, rot(a), \dots, rot^{N-1}(a)$ are linearly dependent if and only if $p_a(x)$ is divisible by some cyclotomic polynomial.*

# Basic properties of cyclic lattices - 2



Let

$$C_R^N = \{x \in \mathbb{R}^N : |x| := \max\{|x_1|, \ldots, |x_N|\} \leq R\}$$

for every $R \in \mathbb{R}_{>0}$, i.e. $C_R^N$ is a cube of side-length $2R$ centered at the origin in $\mathbb{R}^N$.

**Lemma 2**

*Let $R > \frac{N-1}{2}$, then*

$$Prob_{\infty,R}(rk(\Lambda(a)) = N) \geq 1 - \frac{N}{2R+1},$$

*where probability $Prob_{\infty,R}(\cdot)$ is with respect to the uniform distribution among all points $a$ in the set $C_R^N \cap \mathbb{Z}^N$.*

# Lattice Problems

There is a class of algorithmic optimization problems on lattices. We will consider two famous examples.

## Definition 2 (Shortest Vector Problem - SVP)

**Input**: An $N \times N$ basis matrix $A$ for a lattice $\Lambda = A\mathbb{Z}^N \subset \mathbb{R}^N$.
**Output**: A shortest nonzero vector in $\Lambda$, i.e. $x \in \Lambda$ such that

$$\|x\| = \min\{\|y\| : y \in \Lambda \backslash \{0\}\},$$

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

## Remark 2

This is precisely a vector corresponding to $\lambda_1$, the first successive minimum.

# Lattice Problems

**Definition 3 (Shortest Independent Vector Problem - SIVP)**

**Input**: An $N \times N$ basis matrix $A$ for a lattice $\Lambda = A\mathbb{Z}^N \subset \mathbb{R}^N$.
**Output**: A collection of $n$ shortest linearly independent vectors in $\Lambda$, i.e. linearly independent $x_1, \dots, x_N \in \Lambda$ such that

$$\|x_i\| = \lambda_i,$$

the $i$-th successive minimum.

Clearly SIVP should generally be harder than SVP, but how much harder?

# Complexity of lattice problems



SVP and SIVP are both known to be **NP**-hard. In fact, even the problem of finding the first successive minimum $\lambda_1$ of a given lattice is already **NP**-hard.

**Theorem 3 (SIVP to SVP reduction by D. Micciancio (2002))**

*For lattices of rank $N$, there exists a polynomial time reduction algorithm from a solution to SVP to an approximate solution to SIVP within an approximation factor of $\sqrt{N}$ - that is, a collection of linearly independent vectors $a_1, a_2, \dots, a_N \in \Lambda$ with*

$$\|a_1\| \leq \|a_2\| \leq \cdots \leq \|a_N\| \leq \sqrt{N}\lambda_N.$$

# Complexity of lattice problems on cyclic lattices



Xun Sun (Claremont Graduate University)



How hard are SVP and SIVP on cyclic lattices? This is an open question, however there is some indication that SIVP to SVP reduction is easier.

**Theorem 4 (Peikert, Rosen (2005))**

*Let $N$ be* **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 $\Lambda$, produces an approximate solution to SIVP on $\Lambda$ within an approximation factor of 2. Specifically, given an oracle for SVP we can find a collection of linearly independent vectors $a_1, a_2, \dots, a_N \in \Lambda$ with*

$$\|a_1\| \leq \|a_2\| \leq \cdots \leq \|a_N\| \leq 2\lambda_N$$

*in polynomial time. Furthermore, only one call to the oracle is needed.*

# Well-rounded lattices



Xun Sun (Claremont Graduate University)



More generally, we can show in **every** dimension $N$, SIVP is equivalent to SVP on a positive proportion of cyclic lattices.

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

$$\lambda_1(\Gamma) = \lambda_2(\Gamma) = \ldots = \lambda_N(\Gamma).$$

Notice that for a WR lattice, finding $\lambda_1$ is equivalent to finding all successive minima.

# Our results: any dimension

Let $\mathcal{C}_N$ be the set of all cyclic sublattices of $\mathbb{Z}^N$.

**Theorem 5 (Fukshansky, S. (2013))**

*For each dimension $N \geq 2$, there exists a positive constant $\alpha_N \leq 1$, depending only on $N$, such that*

$$\frac{\#\{\Gamma \in \mathcal{C}_N : \lambda_N(\Gamma) \leq R,\ \Gamma \text{ is } WR\}}{\#\{\Gamma \in \mathcal{C}_N : \lambda_N(\Gamma) \leq R\}} \geq \alpha_N \text{ as } R \to \infty. \qquad (1)$$

*Furthermore, SIVP and SVP are equivalent on a positive proportion of WR cyclic lattices, meaning that*

$$\frac{\#\{\Gamma \in \mathcal{C}_N : \lambda_N(\Gamma) \leq R,\ \Gamma \text{ is } WR,\ SIVP = SVP\}}{\#\{\Gamma \in \mathcal{C}_N : \lambda_N(\Gamma) \leq R,\ \Gamma \text{ is } WR\}} \geq \beta_N \qquad (2)$$

*as $R \to \infty$ for some $0 < \beta_N \leq 1$.*

# Our results: $N = 2$



**Theorem 6 (Fukshansky, S. (2013))**

*Let notation be as in Theorem 5 above, and let $N = 2$. Then $\beta_2 = 1$, meaning that SIVP is equivalent to SVP on all WR cyclic lattices in $\mathbb{R}^2$, and*

$$0.261386... \leq \alpha_2 \leq 0.348652...,$$

*meaning that between 26% and 35% of cyclic lattices in $\mathbb{R}^2$ are WR.*

# Permutation invariant lattices



Xun Sun (Claremont Graduate University)



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

$$\langle (1 \ \dots N) \rangle \leq S_N.$$

**Question 1**

*What can be said about the proportion of WR lattices (and, respectively, relation between SVP and SIVP) among sublattices of $\mathbb{Z}^N$ closed under the action of an arbitrary subgroup $H \leq S_N$?*

This is currently work in progress.

Xun Sun (Claremont Graduate University)