Dual Lattices

Luca Notarnicola

Seminar on Lattices and Cryptography

June, 2019

Outline

1. Duality in algebra
2. Dual lattice
3. Properties of dual lattices
4. Transference Theorems
5. q-ary lattices

Dual of a vector space

Dual of a vector space

Let $V \subseteq \mathbb{R}^n$ be an n-dimensional vector space over $\mathbb{R}$ and let $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ the canonical $\mathbb{R}^n$-inner product.

Dual of a vector space

Let $V \subseteq \mathbb{R}^n$ be an n-dimensional vector space over $\mathbb{R}$ and let $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ the canonical $\mathbb{R}^n$-inner product.
We define the **dual vector space** by

$$V^\vee = \{\varphi : V \to \mathbb{R} \text{ linear}\} =: \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$$

Dual of a vector space

Let $V \subseteq \mathbb{R}^n$ be an n-dimensional vector space over $\mathbb{R}$ and let $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ the canonical $\mathbb{R}^n$-inner product.
We define the **dual vector space** by

$$V^\vee = \{\varphi : V \to \mathbb{R} \text{ linear}\} =: \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$$

Any linear function $\varphi : V \to \mathbb{R}$ can be represented as a vector $w \in V$ such that

$$\varphi(x) = \langle w, x \rangle \ , x \in V$$

by choosing the vector

$$w = (\varphi(e_1), \ldots, \varphi(e_n)) \ ,$$

where $e_1, \ldots, e_n$ are the canonical basis of $\mathbb{R}^n$.

Lattices as modules

Lattices as modules

- We know that a lattice is not a vector space because $\mathbb{Z}$ is not a field

Lattices as modules

- We know that a lattice is not a vector space because $\mathbb{Z}$ is not a field
- In Algebra we also say that a lattice is a **free module** over $\mathbb{Z}$ (a module over a ring is essentially the same as a vector space over a field)

$$\mathcal{L} = \sum_{i=1}^{r} \mathbb{Z} b_i \ , b_i \in \mathbb{R}^n$$

Lattices as modules

- We know that a lattice is not a vector space because $\mathbb{Z}$ is not a field
- In Algebra we also say that a lattice is a **free module** over $\mathbb{Z}$ (a module over a ring is essentially the same as a vector space over a field)

$$\mathcal{L} = \sum_{i=1}^{r} \mathbb{Z} b_i \ , b_i \in \mathbb{R}^n$$

- Dual of a module (similarly as for vector spaces previously): Let M be a module over a ring R. The module

$$M^\vee = \{\varphi : M \to R\} = \mathrm{Hom}_R(M, R)$$

is called the **dual module** of M

Dual lattice

Dual lattice

Let $\mathcal{L} \subseteq \mathbb{R}^m$ be a lattice of positive rank $n \leq m$.

Dual lattice

Let $\mathcal{L} \subseteq \mathbb{R}^m$ be a lattice of positive rank $n \leq m$.

Definition

The dual of $\mathcal{L}$ is defined as

$$\mathcal{L}^\vee = \{v \in \text{span}_{\mathbb{R}}(\mathcal{L}) : \langle v, w \rangle \in \mathbb{Z} \text{ for all } w \in \mathcal{L}\}$$

Dual lattice

Let $\mathcal{L} \subseteq \mathbb{R}^m$ be a lattice of positive rank $n \leq m$.

Definition

The dual of $\mathcal{L}$ is defined as

$$\mathcal{L}^\vee = \{v \in \text{span}_{\mathbb{R}}(\mathcal{L}) : \langle v, w \rangle \in \mathbb{Z} \text{ for all } w \in \mathcal{L}\}$$

The definition is equivalent to the abstract definition of duality seen before.

Dual lattice

Let $\mathcal{L} \subseteq \mathbb{R}^m$ be a lattice of positive rank $n \leq m$.

Definition

The dual of $\mathcal{L}$ is defined as

$$\mathcal{L}^\vee = \{v \in \text{span}_{\mathbb{R}}(\mathcal{L}) : \langle v, w \rangle \in \mathbb{Z} \text{ for all } w \in \mathcal{L}\}$$

The definition is equivalent to the abstract definition of duality seen before.

- $\mathcal{L}$ is a $\mathbb{Z}$-module

Dual lattice

Let $\mathcal{L} \subseteq \mathbb{R}^m$ be a lattice of positive rank $n \leq m$.

Definition

The dual of $\mathcal{L}$ is defined as

$$\mathcal{L}^\vee = \{v \in \text{span}_{\mathbb{R}}(\mathcal{L}) : \langle v, w \rangle \in \mathbb{Z} \text{ for all } w \in \mathcal{L}\}$$

The definition is equivalent to the abstract definition of duality seen before.

- $\mathcal{L}$ is a $\mathbb{Z}$-module
- To every $v \in \mathcal{L}^\vee$ we associate the map (a $\mathbb{Z}$-module homomorphism) $\varphi_v(x) = \langle v, x \rangle$ and by assumption we have $\varphi_v(x) \in \mathbb{Z}$. i.e we can identify both notions via

$$\mathcal{L}^\vee \to \text{Hom}_{\mathbb{Z}}(\mathcal{L}, \mathbb{Z}), v \mapsto (\varphi_v : \mathcal{L} \to \mathbb{Z}, x \mapsto \langle x, v \rangle)$$

Basic Examples and natural questions

Basic Examples and natural questions

1. $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$

Basic Examples and natural questions

1. $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$
2. For every real $a > 0$ and every lattice $\mathcal{L}$: $(a\mathcal{L})^\vee = a^{-1}\mathcal{L}^\vee$

Basic Examples and natural questions

1. $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$
2. For every real $a > 0$ and every lattice $\mathcal{L}$: $(a\mathcal{L})^\vee = a^{-1}\mathcal{L}^\vee$
   Pf. If $v \in (a\mathcal{L})^\vee$ then $\langle v, aw\rangle = a\langle v, w\rangle \in \mathbb{Z}$ for all $w \in \mathcal{L}$. Thus $v \in a^{-1}\mathcal{L}^\vee$.
   If $v \in a^{-1}\mathcal{L}^\vee$ then $av \in \mathcal{L}^\vee$, so $\langle av, w\rangle = \langle v, aw\rangle \in \mathbb{Z}$ for all $w \in \mathcal{L}$. Hence $v \in (a\mathcal{L})^\vee$.

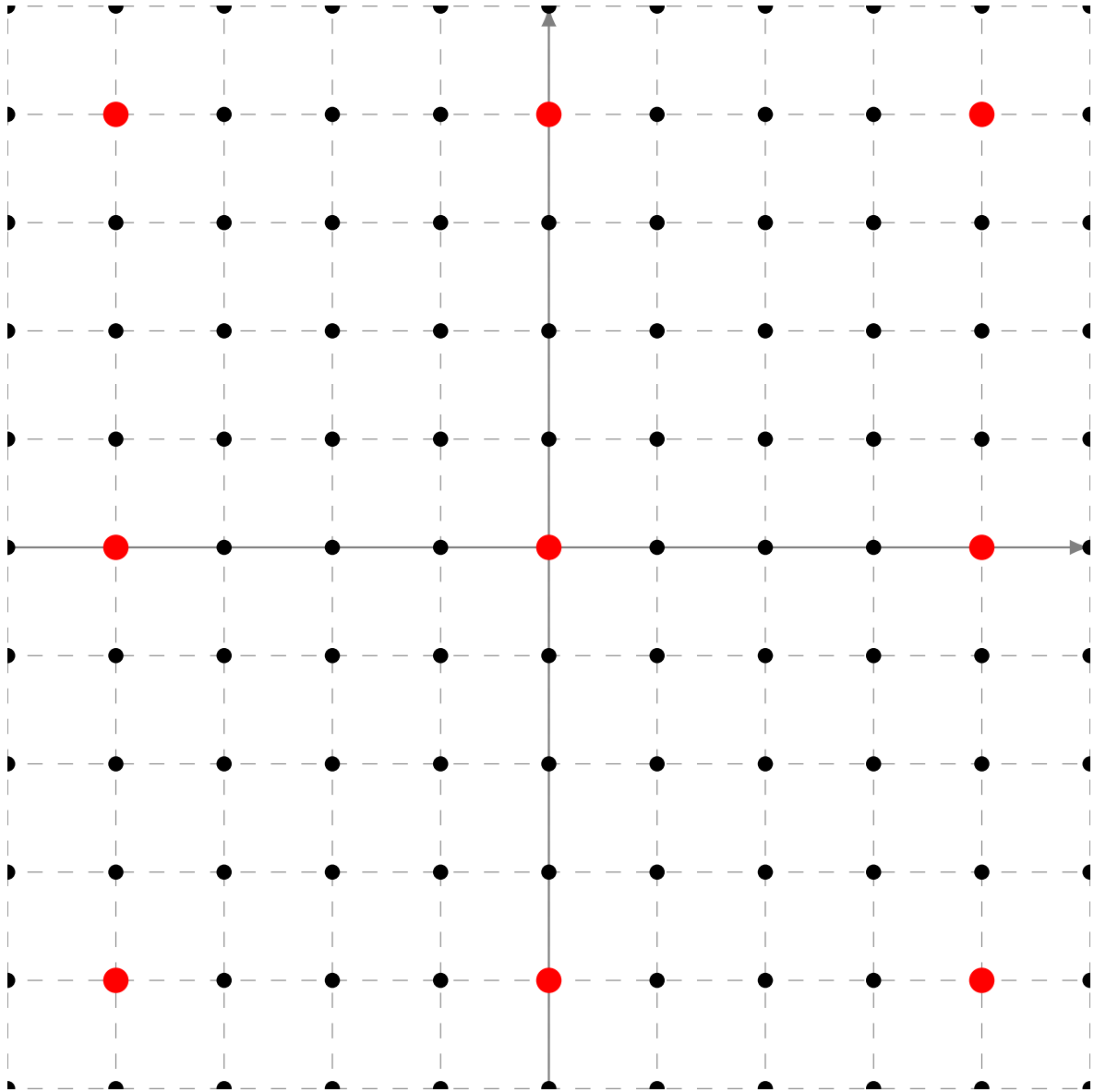
Basic Examples and natural questions

1. $(\mathbb{Z}^n)^\vee = \mathbb{Z}^n$
2. For every real $a > 0$ and every lattice $\mathcal{L}$: $(a\mathcal{L})^\vee = a^{-1}\mathcal{L}^\vee$
   Pf. If $v \in (a\mathcal{L})^\vee$ then $\langle v, aw\rangle = a\langle v, w\rangle \in \mathbb{Z}$ for all $w \in \mathcal{L}$. Thus $v \in a^{-1}\mathcal{L}^\vee$.
   If $v \in a^{-1}\mathcal{L}^\vee$ then $av \in \mathcal{L}^\vee$, so $\langle av, w\rangle = \langle v, aw\rangle \in \mathbb{Z}$ for all $w \in \mathcal{L}$. Hence $v \in (a\mathcal{L})^\vee$.

Some questions

- More generally, can we describe a basis of $\mathcal{L}^\vee$ from a basis of $\mathcal{L}$?
- Can we study the geometry of $\mathcal{L}^\vee$ from the geometry of $\mathcal{L}$?

The lattice $2\mathbb{Z}^2$ and its dual $(1/2)\mathbb{Z}^2$



Dual lattice - back to the definition

Definition

The dual of $\mathcal{L}$ is defined as

$$\mathcal{L}^\vee = \{v \in \text{span}_{\mathbb{R}}(\mathcal{L}) : \langle v, w \rangle \in \mathbb{Z} \text{ for all } w \in \mathcal{L}\}$$

Dual lattice - back to the definition

Definition

The dual of $\mathcal{L}$ is defined as

$$\mathcal{L}^\vee = \{v \in \mathrm{span}_{\mathbb{R}}(\mathcal{L}) : \langle v, w\rangle \in \mathbb{Z} \text{ for all } w \in \mathcal{L}\}$$

For every $v \in \mathcal{L}^\vee$ we obtain a partition of the lattice $\mathcal{L}$ into layers by setting

$$\mathcal{L} = \bigcup_{a\in\mathbb{Z}} \{x \in \mathcal{L} : \varphi_v(x) = \langle v, x\rangle = a\}$$

and we set $\{x \in \mathcal{L} : \langle v, x\rangle = a\} =: \mathcal{L}_a$ for $a \in \mathbb{Z}$. Then we have $\mathcal{L} = \bigcup_a \mathcal{L}_a$.

The dual lattice geometrically speaking

The dual lattice geometrically speaking

Fix a $v \in \mathcal{L}^\vee$.

The dual lattice geometrically speaking

Fix a $v \in \mathcal{L}^\vee$.

- For $a \in \mathbb{Z}$, have $\mathcal{L}_a = \{x \in \mathcal{L} : \langle x, v \rangle = a\}$

The dual lattice geometrically speaking

Fix a $v \in \mathcal{L}^\vee$.

- For $a \in \mathbb{Z}$, have $\mathcal{L}_a = \{x \in \mathcal{L} : \langle x, v \rangle = a\}$

If $v \neq 0$, consider the vector $v' = v/\langle v, v \rangle = v/\|v\|^2$.

The dual lattice geometrically speaking

Fix a $v \in \mathcal{L}^\vee$.

- For $a \in \mathbb{Z}$, have $\mathcal{L}_a = \{x \in \mathcal{L} : \langle x, v \rangle = a\}$

If $v \neq 0$, consider the vector $v' = v/\langle v, v \rangle = v/\|v\|^2$.

- Then $\|v'\| = \frac{1}{\|v\|}$

The dual lattice geometrically speaking

Fix a $v \in \mathcal{L}^\vee$.

- For $a \in \mathbb{Z}$, have $\mathcal{L}_a = \{x \in \mathcal{L} : \langle x, v \rangle = a\}$

If $v \neq 0$, consider the vector $v' = v/\langle v, v \rangle = v/\|v\|^2$.

- Then $\|v'\| = \frac{1}{\|v\|}$
- $v'' := v'/\langle v', v' \rangle = v$

The dual lattice geometrically speaking

Fix a $v \in \mathcal{L}^\vee$.

- For $a \in \mathbb{Z}$, have $\mathcal{L}_a = \{x \in \mathcal{L} : \langle x, v \rangle = a\}$

If $v \neq 0$, consider the vector $v' = v/\langle v, v \rangle = v/\|v\|^2$.

- Then $\|v'\| = \frac{1}{\|v\|}$
- $v'' := v'/\langle v', v' \rangle = v$
- We can write

$$\{x \in \mathrm{span}_{\mathbb{R}}(\mathcal{L}) : \langle x, v \rangle \in \mathbb{Z}\} = \mathbb{Z}v' \oplus (\mathbb{R}v)^\perp$$

The dual lattice geometrically speaking

Fix a $v \in \mathcal{L}^\vee$.

- For $a \in \mathbb{Z}$, have $\mathcal{L}_a = \{x \in \mathcal{L} : \langle x, v \rangle = a\}$

If $v \neq 0$, consider the vector $v' = v/\langle v, v \rangle = v/\|v\|^2$.

- Then $\|v'\| = \frac{1}{\|v\|}$
- $v'' := v'/\langle v', v' \rangle = v$
- We can write

$$\{x \in \mathrm{span}_{\mathbb{R}}(\mathcal{L}) : \langle x, v \rangle \in \mathbb{Z}\} = \mathbb{Z}v' \oplus (\mathbb{R}v)^\perp$$

namely we can write: $x = av' + rw$ with $a \in \mathbb{Z}, r \in \mathbb{R}$ and $\langle w, v \rangle = 0$ which gives $\langle x, v \rangle = a$

The dual lattice geometrically speaking

Fix a $v \in \mathcal{L}^\vee$.

- For $a \in \mathbb{Z}$, have $\mathcal{L}_a = \{x \in \mathcal{L} : \langle x, v\rangle = a\}$

If $v \neq 0$, consider the vector $v' = v/\langle v, v\rangle = v/\|v\|^2$.

- Then $\|v'\| = \frac{1}{\|v\|}$
- $v'' := v'/\langle v', v'\rangle = v$
- We can write

$$\{x \in \mathrm{span}_{\mathbb{R}}(\mathcal{L}) : \langle x, v\rangle \in \mathbb{Z}\} = \mathbb{Z}v' \oplus (\mathbb{R}v)^\perp$$

namely we can write: $x = av' + rw$ with $a \in \mathbb{Z}, r \in \mathbb{R}$ and $\langle w, v\rangle = 0$ which gives $\langle x, v\rangle = a$

In conclusion, one has:

$$\begin{aligned} v \in \mathcal{L}^\vee, v \neq 0 \quad &\iff \quad \mathcal{L} \subseteq \{x \in \mathrm{span}_{\mathbb{R}}(\mathcal{L}) : \langle x, v\rangle \in \mathbb{Z}\} \\ &\iff \quad \mathcal{L} \subseteq \mathbb{Z}v' \oplus (\mathbb{R}v)^\perp = \bigcup_{m \in \mathbb{Z}} (mv' + (\mathbb{R}v)^\perp) \end{aligned}$$

Finding a basis for the dual lattice

Finding a basis for the dual lattice

Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a lattice of full rank n, generated by a matrix $B \in GL_n(\mathbb{R})$.

Finding a basis for the dual lattice

Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a lattice of full rank n, generated by a matrix $B \in GL_n(\mathbb{R})$.

Goal.

Can we find a basis for $\mathcal{L}^\vee$?

Finding a basis for the dual lattice

Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a lattice of full rank n, generated by a matrix $B \in GL_n(\mathbb{R})$.

Goal.

Can we find a basis for $\mathcal{L}^\vee$?

We have the equivalences

$$\begin{aligned} v \in \mathcal{L}^\vee &\iff \langle v, x \rangle \in \mathbb{Z}, \forall x \in \mathcal{L} \\ &\iff B^T v \in \mathbb{Z}^n \\ &\iff v \in (B^{-1})^T \mathbb{Z}^n \end{aligned}$$

Finding a basis for the dual lattice

Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a lattice of full rank n, generated by a matrix $B \in GL_n(\mathbb{R})$.

Goal.
Can we find a basis for $\mathcal{L}^\vee$?

We have the equivalences

$$\begin{aligned} v \in \mathcal{L}^\vee &\iff \langle v, x \rangle \in \mathbb{Z}, \forall x \in \mathcal{L} \\ &\iff B^T v \in \mathbb{Z}^n \\ &\iff v \in (B^{-1})^T \mathbb{Z}^n \end{aligned}$$

We have proved that $\mathcal{L}^\vee = (B^{-1})^T \mathbb{Z}^n$ and therefore a basis matrix of $\mathcal{L}^\vee$ is

$$B^\vee := (B^{-1})^T \in GL_n(\mathbb{R})$$

An Example

Consider the lattice $\mathcal{L} \subseteq \mathbb{R}^2$ generated by the columns of the matrix

$$B = \begin{bmatrix} 11 & 5 \\ -7 & 1/2 \end{bmatrix}$$

- $v = (v_1, v_2) \in \mathcal{L}^\vee$ iff $(11v_1 + 5v_2 \in \mathbb{Z}) \wedge (-7v_1 + 1/2v_2 \in \mathbb{Z})$
- Therefore we solve the linear system for $x_1, x_2 \in \mathbb{Z}$:

$$(11v_1 + 5v_2 = x_1) \wedge (-7v_1 + 1/2v_2 = x_2)$$

- which is equivalent to

$$(v_1 = 1/81x_1 - 10/81x_2) \wedge (v_2 = 14/81x_1 + 22/81x_2)$$

A basis matrix for $\mathcal{L}^\vee$ is therefore:

$$B = \begin{bmatrix} 1/81 & -10/81 \\ 14/81 & 22/81 \end{bmatrix} = B^{-1}$$

Finding the dual basis, cont'd

Let's consider general bases $B \in \mathbb{R}^{m \times n}, 0 < n \leq m$.

Finding the dual basis, cont'd

Let's consider general bases $B \in \mathbb{R}^{m \times n}, 0 < n \leq m$. We consider the unique matrix $D \in \mathbb{R}^{m \times n}$ such that

1. $\text{span}_{\mathbb{R}}(D) = \text{span}_{\mathbb{R}}(B)$
2. $B^T D = I$

Finding the dual basis, cont'd

Let's consider general bases $B \in \mathbb{R}^{m \times n}, 0 < n \leq m$. We consider the unique matrix $D \in \mathbb{R}^{m \times n}$ such that

1. $\text{span}_{\mathbb{R}}(D) = \text{span}_{\mathbb{R}}(B)$
2. $B^T D = I$

Remark: Condition 2. means that if $(b_i)_i$ and $(d_j)_j$ are the columns of B and D resp., then $\langle b_i, d_j \rangle = \delta_{ij}$ for all i, j.

Finding the dual basis, cont'd

Let's consider general bases $B \in \mathbb{R}^{m \times n}, 0 < n \leq m$. We consider the unique matrix $D \in \mathbb{R}^{m \times n}$ such that

1. $\text{span}_{\mathbb{R}}(D) = \text{span}_{\mathbb{R}}(B)$
2. $B^T D = I$

Remark: Condition 2. means that if $(b_i)_i$ and $(d_j)_j$ are the columns of B and D resp., then $\langle b_i, d_j \rangle = \delta_{ij}$ for all i, j.
We show that the columns of D generate $\mathcal{L}^\vee$.

Finding the dual basis, cont'd

Let's consider general bases $B \in \mathbb{R}^{m\times n}, 0 < n \leq m$. We consider the unique matrix $D \in \mathbb{R}^{m\times n}$ such that

1. $\text{span}_{\mathbb{R}}(D) = \text{span}_{\mathbb{R}}(B)$
2. $B^T D = I$

Remark: Condition 2. means that if $(b_i)_i$ and $(d_j)_j$ are the columns of B and D resp., then $\langle b_i, d_j\rangle = \delta_{ij}$ for all i, j.
We show that the columns of D generate $\mathcal{L}^\vee$.

- $\langle D\rangle \subseteq \mathcal{L}^\vee$: Then for any $x = \sum_{i=1}^n \alpha_i b_i \in \mathcal{L}$ with $\alpha_i \in \mathbb{Z}$ we write for all j: $\langle x, d_j\rangle = \sum_{i=1}^n \alpha_i \langle b_i, d_j\rangle = \alpha_i \in \mathbb{Z}$. Hence every $y = \sum_{j=1}^n \beta_j d_j \in \langle D\rangle$ is in $\mathcal{L}^\vee$.

Finding the dual basis, cont'd

Let's consider general bases $B \in \mathbb{R}^{m \times n}, 0 < n \leq m$. We consider the unique matrix $D \in \mathbb{R}^{m \times n}$ such that

1. $\text{span}_{\mathbb{R}}(D) = \text{span}_{\mathbb{R}}(B)$
2. $B^T D = I$

Remark: Condition 2. means that if $(b_i)_i$ and $(d_j)_j$ are the columns of B and D resp., then $\langle b_i, d_j \rangle = \delta_{ij}$ for all i, j.
We show that the columns of D generate $\mathcal{L}^\vee$.

- $\langle D \rangle \subseteq \mathcal{L}^\vee$: Then for any $x = \sum_{i=1}^n \alpha_i b_i \in \mathcal{L}$ with $\alpha_i \in \mathbb{Z}$ we write for all j: $\langle x, d_j \rangle = \sum_{i=1}^n \alpha_i \langle b_i, d_j \rangle = \alpha_i \in \mathbb{Z}$. Hence every $y = \sum_{j=1}^n \beta_j d_j \in \langle D \rangle$ is in $\mathcal{L}^\vee$.
- $\mathcal{L}^\vee \subseteq \langle D \rangle$: Let $y \in \mathcal{L}^\vee$. In particular $y \in \text{span}_{\mathbb{R}}(B) = \text{span}_{\mathbb{R}}(D)$, so $y = \sum_{i=1}^n \alpha_i d_i$ for $\alpha_i \in \mathbb{R}$. But, $\alpha_j = \sum_i \alpha_i \langle d_i, b_j \rangle = \langle y, b_j \rangle \in \mathbb{Z}$ for all j. This means $y \in \langle D \rangle$.

Finding the dual basis, cont'd

Let's consider general bases $B \in \mathbb{R}^{m \times n}, 0 < n \leq m$. We consider the unique matrix $D \in \mathbb{R}^{m \times n}$ such that

1. $\text{span}_{\mathbb{R}}(D) = \text{span}_{\mathbb{R}}(B)$
2. $B^T D = I$

Remark: Condition 2. means that if $(b_i)_i$ and $(d_j)_j$ are the columns of B and D resp., then $\langle b_i, d_j \rangle = \delta_{ij}$ for all i, j.
We show that the columns of D generate $\mathcal{L}^\vee$.

- $\langle D \rangle \subseteq \mathcal{L}^\vee$: Then for any $x = \sum_{i=1}^n \alpha_i b_i \in \mathcal{L}$ with $\alpha_i \in \mathbb{Z}$ we write for all j: $\langle x, d_j \rangle = \sum_{i=1}^n \alpha_i \langle b_i, d_j \rangle = \alpha_i \in \mathbb{Z}$. Hence every $y = \sum_{j=1}^n \beta_j d_j \in \langle D \rangle$ is in $\mathcal{L}^\vee$.
- $\mathcal{L}^\vee \subseteq \langle D \rangle$: Let $y \in \mathcal{L}^\vee$. In particular $y \in \text{span}_{\mathbb{R}}(B) = \text{span}_{\mathbb{R}}(D)$, so $y = \sum_{i=1}^n \alpha_i d_i$ for $\alpha_i \in \mathbb{R}$. But, $\alpha_j = \sum_i \alpha_i \langle d_i, b_j \rangle = \langle y, b_j \rangle \in \mathbb{Z}$ for all j. This means $y \in \langle D \rangle$.
- We conclue $\langle D \rangle = \mathcal{L}^\vee$.

The dual basis

Theorem

The unique basis $D \in \mathbb{R}^{m \times n}$ (allow $m = n$) satisfying

1. $\text{span}_{\mathbb{R}}(D) = \text{span}_{\mathbb{R}}(B)$
2. $B^T D = I$

is a basis matrix for the dual lattice $\mathcal{L}^{\vee}$.

The dual basis

Theorem

The unique basis $D \in \mathbb{R}^{m \times n}$ (allow $m = n$) satisfying

1. $\text{span}_{\mathbb{R}}(D) = \text{span}_{\mathbb{R}}(B)$
2. $B^T D = I$

is a basis matrix for the dual lattice $\mathcal{L}^\vee$.

- We call D the dual basis and we will use the notation

$$D =: B^\vee$$

The dual basis

Theorem

The unique basis $D \in \mathbb{R}^{m \times n}$ (allow $m = n$) satisfying

1. $\text{span}_{\mathbb{R}}(D) = \text{span}_{\mathbb{R}}(B)$
2. $B^T D = I$

is a basis matrix for the dual lattice $\mathcal{L}^\vee$.

- We call D the dual basis and we will use the notation

$$D =: B^\vee$$

- From 2. we can actually set

$$D = B^\vee = B(B^T B)^{-1}$$

The dual basis

Theorem

The unique basis $D \in \mathbb{R}^{m \times n}$ (allow $m = n$) satisfying

1. $\text{span}_{\mathbb{R}}(D) = \text{span}_{\mathbb{R}}(B)$
2. $B^T D = I$

is a basis matrix for the dual lattice $\mathcal{L}^\vee$.

- We call D the dual basis and we will use the notation

$$D =: B^\vee$$

- From 2. we can actually set

$$D = B^\vee = B(B^T B)^{-1}$$

- In particular for the full rank case:

$$B^\vee = B(B^T B)^{-1} = BB^{-1}(B^T)^{-1} = (B^{-1})^T$$

An immediate consequence

Theorem

For any lattice $\mathcal{L}$ one has $(\mathcal{L}^\vee)^\vee = \mathcal{L}$.

An immediate consequence

Theorem

For any lattice $\mathcal{L}$ one has $(\mathcal{L}^\vee)^\vee = \mathcal{L}$.

Proof.

Let B be a basis matrix of $\mathcal{L}$. By the previous theorem a basis of $\mathcal{L}^\vee$ is given by $B^\vee = B(B^T B)^{-1}$. Therefore a basis matrix of $(\mathcal{L}^\vee)^\vee$ is

$$\begin{aligned}(B^\vee)^\vee &= B^\vee((B^\vee)^T B^\vee)^{-1} \\ &= B(B^T B)^{-1}\left((B(B^T B)^{-1})^T B(B^T B)^{-1}\right)^{-1} = B\end{aligned}$$

□

An immediate consequence

Theorem

For any lattice $\mathcal{L}$ one has $(\mathcal{L}^\vee)^\vee = \mathcal{L}$.

Proof.

Let B be a basis matrix of $\mathcal{L}$. By the previous theorem a basis of $\mathcal{L}^\vee$ is given by $B^\vee = B(B^T B)^{-1}$. Therefore a basis matrix of $(\mathcal{L}^\vee)^\vee$ is

$$\begin{aligned}(B^\vee)^\vee &= B^\vee((B^\vee)^T B^\vee)^{-1} \\ &= B(B^T B)^{-1}\left((B(B^T B)^{-1})^T B(B^T B)^{-1}\right)^{-1} = B\end{aligned}$$

□

Conclusion

Let $\mathcal{L}$ be a lattice (primal) and $\mathcal{L}^\vee$ its dual. Then $\mathcal{L}$ is the dual of $\mathcal{L}^\vee$. Hence the pair $(\mathcal{L}, \mathcal{L}^\vee)$ is called a pair of dual lattices.

How are primal and dual related?

Theorem

Let $\mathcal{L}$ be a lattice. The following hold:

1. $\det(\mathcal{L}^\vee) = \det(\mathcal{L})^{-1}$
2. If $\mathcal{L} \subseteq \mathbb{Z}^m$ then $\mathcal{L}^\vee \subseteq \det(\mathcal{L})^{-2}\mathbb{Z}^m$

How are primal and dual related?

Theorem

Let $\mathcal{L}$ be a lattice. The following hold:

1. $\det(\mathcal{L}^\vee) = \det(\mathcal{L})^{-1}$
2. If $\mathcal{L} \subseteq \mathbb{Z}^m$ then $\mathcal{L}^\vee \subseteq \det(\mathcal{L})^{-2}\mathbb{Z}^m$

Proof.

How are primal and dual related?

Theorem

Let $\mathcal{L}$ be a lattice. The following hold:

1. $\det(\mathcal{L}^\vee) = \det(\mathcal{L})^{-1}$
2. If $\mathcal{L} \subseteq \mathbb{Z}^m$ then $\mathcal{L}^\vee \subseteq \det(\mathcal{L})^{-2}\mathbb{Z}^m$

Proof.

1. $\det(\mathcal{L}^\vee) = \sqrt{\det((B^\vee)^T B^\vee)} = \sqrt{\det(B^T B)^{-1}} = \det(\mathcal{L})^{-1}$

How are primal and dual related?

Theorem

Let $\mathcal{L}$ be a lattice. The following hold:

1. $\det(\mathcal{L}^\vee) = \det(\mathcal{L})^{-1}$
2. If $\mathcal{L} \subseteq \mathbb{Z}^m$ then $\mathcal{L}^\vee \subseteq \det(\mathcal{L})^{-2}\mathbb{Z}^m$

Proof.

1. $\det(\mathcal{L}^\vee) = \sqrt{\det((B^\vee)^T B^\vee)} = \sqrt{\det(B^T B)^{-1}} = \det(\mathcal{L})^{-1}$
2. Let $\Delta = \det(\mathcal{L})$. Let $B \in \mathbb{Z}^{m\times n}$ basis matrix for $\mathcal{L}$ with dual basis $B^\vee = BG_B^{-1}$ with $G_B = B^T B$. Since B is integral, it is enough to show that $\langle G_B^{-1}\rangle \subseteq \Delta^{-2}\mathbb{Z}^n$. Since G_B is symmetric we have $G_B^T G_B^{-1} = I$. Moreover, $\mathrm{span}_{\mathbb{R}}(G_B) = \mathrm{span}_{\mathbb{R}}(G_B^{-1})$ (because full rank). Therefore, by Theorem of Dual Basis we have $\langle G_B\rangle^\vee = \langle G_B^{-1}\rangle$. Since $G_B \in \mathbb{Z}^{n\times n}$, it follows $\langle G_B\rangle^\vee \subseteq |\det(G_B)|^{-1}\mathbb{Z}^n = \Delta^{-2}\mathbb{Z}^n$.

□

Transference Theorems related to successive minima

Transference Theorems related to successive minima

Recall (Successive minima)

For a lattice $\mathcal{L}$ in $\mathbb{R}^m$ of rank $0 < n \leq m$, the ith $(1 \leq i \leq n)$ successive minimum is defined as

$$\lambda_i(\mathcal{L}) = \inf\{\rho > 0 : \dim_{\mathbb{R}}(\mathrm{span}_{\mathbb{R}}(\mathcal{L}) \cap B_m(0, \rho)) \geq i\}$$

i.e. the smallest positive radius of an m-dimensional ball containing i linearly independent vectors of $\mathcal{L}$

Transference Theorems related to successive minima

Recall (Successive minima)

For a lattice $\mathcal{L}$ in $\mathbb{R}^m$ of rank $0 < n \leq m$, the ith $(1 \leq i \leq n)$ successive minimum is defined as

$$\lambda_i(\mathcal{L}) = \inf\{\rho > 0 : \dim_{\mathbb{R}}(\mathrm{span}_{\mathbb{R}}(\mathcal{L}) \cap B_m(0, \rho)) \geq i\}$$

i.e. the smallest positive radius of an m-dimensional ball containing i linearly independent vectors of $\mathcal{L}$

Goal question

Consider $\mathcal{L}$ (rank n in $\mathbb{R}^m$) with successive minima $(\lambda_1, \ldots, \lambda_n)$ and $\mathcal{L}^\vee$ with successive minima $(\lambda_1^\vee, \ldots, \lambda_n^\vee)$. Can we 'transfer' knowledge from $(\lambda_1, \ldots, \lambda_n)$ to $(\lambda_1^\vee, \ldots, \lambda_n^\vee)$?

What can we say about λ_1?

What can we say about λ_1?

By Minkowski's Theorem we know that

What can we say about λ_1?

By Minkowski's Theorem we know that

$$\lambda_1 \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$$

What can we say about λ_1?

By Minkowski's Theorem we know that

$$\lambda_1 \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$$

$$\lambda_1^{\vee} \leq \sqrt{n} \cdot \det(\mathcal{L}^{\vee})^{1/n} = \sqrt{n} \cdot \det(\mathcal{L})^{-1/n}$$

What can we say about λ_1?

By Minkowski's Theorem we know that

$$\lambda_1 \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$$

$$\lambda_1^{\vee} \leq \sqrt{n} \cdot \det(\mathcal{L}^{\vee})^{1/n} = \sqrt{n} \cdot \det(\mathcal{L})^{-1/n}$$

Therefore we deduce

$$\lambda_1 \cdot \lambda_1^{\vee} \leq n$$

What can we say about λ_1?

By Minkowski's Theorem we know that

$$\lambda_1 \leq \sqrt{n} \cdot \det(\mathcal{L})^{1/n}$$

$$\lambda_1^\vee \leq \sqrt{n} \cdot \det(\mathcal{L}^\vee)^{1/n} = \sqrt{n} \cdot \det(\mathcal{L})^{-1/n}$$

Therefore we deduce

$$\lambda_1 \cdot \lambda_1^\vee \leq n$$

Remark. In fact a stronger version of Minkowski's Theorem is true: $\lambda_1 \leq \sqrt{\gamma_n} \det(\mathcal{L})^{1/n}$ where γ_n is Hermite's constant in dimension n. Therefore the stronger inequality holds, namely $\lambda_1 \lambda_1^\vee \leq \gamma_n$.

Consequences of $\lambda_1 \cdot \lambda_1^\vee \leq n$

Consequences of $\lambda_1 \cdot \lambda_1^\vee \leq n$

- If λ_1 is large, say $\lambda_1 > N$ for some large $N > 0$. Then

$$\lambda_1^\vee \leq \frac{n}{\lambda_1} \leq \frac{n}{N}$$

  is small.

Consequences of $\lambda_1 \cdot \lambda_1^\vee \leq n$

- If λ_1 is large, say $\lambda_1 > N$ for some large $N > 0$. Then

$$\lambda_1^\vee \leq \frac{n}{\lambda_1} \leq \frac{n}{N}$$

  is small.

Example

Consider $\mathcal{L} = 10^6 \cdot \mathbb{Z}^5$.

Consequences of $\lambda_1 \cdot \lambda_1^\vee \leq n$

- If λ_1 is large, say $\lambda_1 > N$ for some large $N > 0$. Then

$$\lambda_1^\vee \leq \frac{n}{\lambda_1} \leq \frac{n}{N}$$

  is small.

Example

Consider $\mathcal{L} = 10^6 \cdot \mathbb{Z}^5$. We know that $\mathcal{L}^\vee = 10^{-6}\mathbb{Z}^5$. Then $\lambda_1 = 10^6$ and $\lambda_1^\vee = 10^{-6}$.

Another transference result on successive minima

Another transference result on successive minima

We show that

$$\lambda_1 \cdot \lambda_n^{\vee} \geq 1.$$

Another transference result on successive minima

We show that

$$\lambda_1 \cdot \lambda_n^{\vee} \geq 1.$$

- Let $v \in \mathcal{L}$ with $\|v\| = \lambda_1$

Another transference result on successive minima

We show that

$$\lambda_1 \cdot \lambda_n^{\vee} \geq 1.$$

- Let $v \in \mathcal{L}$ with $\|v\| = \lambda_1$
- let $x_1, \ldots, x_n \in \mathcal{L}^{\vee}$ linearly independent such that $\|x_n\| = \lambda_n^{\vee}$ and $\|x_i\| \leq \|x_n\|$ for all $1 \leq i \leq n-1$

Another transference result on successive minima

We show that

$$\lambda_1 \cdot \lambda_n^\vee \geq 1.$$

- Let $v \in \mathcal{L}$ with $\|v\| = \lambda_1$
- let $x_1, \ldots, x_n \in \mathcal{L}^\vee$ linearly independent such that $\|x_n\| = \lambda_n^\vee$ and $\|x_i\| \leq \|x_n\|$ for all $1 \leq i \leq n-1$
- Not all of x_j are orthogonal to v, otherwise there would be n linearly independent vectors in the $n-1$ dimensional space $(\mathbb{R}v)^\perp$

Another transference result on successive minima

We show that

$$\lambda_1 \cdot \lambda_n^{\vee} \geq 1.$$

- Let $v \in \mathcal{L}$ with $\|v\| = \lambda_1$
- let $x_1, \ldots, x_n \in \mathcal{L}^{\vee}$ linearly independent such that $\|x_n\| = \lambda_n^{\vee}$ and $\|x_i\| \leq \|x_n\|$ for all $1 \leq i \leq n-1$
- Not all of x_j are orthogonal to v, otherwise there would be n linearly independent vectors in the $n-1$ dimensional space $(\mathbb{R}v)^{\perp}$
- Therefore, and by definition of duality, there exists $1 \leq j \leq n$ s.t.:

$$\langle v, x_j \rangle \in \mathbb{Z} \backslash \{0\}$$

Another transference result on successive minima

We show that

$$\lambda_1 \cdot \lambda_n^\vee \geq 1.$$

- Let $v \in \mathcal{L}$ with $\|v\| = \lambda_1$
- let $x_1, \ldots, x_n \in \mathcal{L}^\vee$ linearly independent such that $\|x_n\| = \lambda_n^\vee$ and $\|x_i\| \leq \|x_n\|$ for all $1 \leq i \leq n-1$
- Not all of x_j are orthogonal to v, otherwise there would be n linearly independent vectors in the $n-1$ dimensional space $(\mathbb{R}v)^\perp$
- Therefore, and by definition of duality, there exists $1 \leq j \leq n$ s.t.:

$$\langle v, x_j \rangle \in \mathbb{Z} \backslash \{0\}$$

- It follows:

$$1 \leq |\langle v, x_j \rangle| \leq \|v\| \cdot \|x_j\| \leq \lambda_1 \cdot \lambda_n^\vee$$

Banaszczyk's Transference Theorem

More generally, it holds (partial summary)

Banaszczyk's Transference Theorem

More generally, it holds (partial summary)

Theorem

Let $\mathcal{L}$ be a lattice of full rank n. Then

1. $\lambda_1 \cdot \lambda_1^\vee \leq n$
2. $\lambda_1 \cdot \lambda_n^\vee \geq 1$
3. More generally, for all $1 \leq k \leq n$: $1 \leq \lambda_k \cdot \lambda_{n-k+1}^\vee \leq n$

Banaszczyk's Transference Theorem

More generally, it holds (partial summary)

Theorem

Let $\mathcal{L}$ be a lattice of full rank n. Then

1. $\lambda_1 \cdot \lambda_1^\vee \leq n$
2. $\lambda_1 \cdot \lambda_n^\vee \geq 1$
3. More generally, for all $1 \leq k \leq n$: $1 \leq \lambda_k \cdot \lambda_{n-k+1}^\vee \leq n$

Remark.

Banaszczyk's Transference Theorem

More generally, it holds (partial summary)

Theorem

Let $\mathcal{L}$ be a lattice of full rank n. Then

1. $\lambda_1 \cdot \lambda_1^\vee \leq n$
2. $\lambda_1 \cdot \lambda_n^\vee \geq 1$
3. More generally, for all $1 \leq k \leq n$: $1 \leq \lambda_k \cdot \lambda_{n-k+1}^\vee \leq n$

Remark. 1. The last statement is often referred to as Banaszczyk's Transference Theorem. We will skip the proof.

Banaszczyk's Transference Theorem

More generally, it holds (partial summary)

Theorem

Let $\mathcal{L}$ be a lattice of full rank n. Then

1. $\lambda_1 \cdot \lambda_1^\vee \leq n$
2. $\lambda_1 \cdot \lambda_n^\vee \geq 1$
3. More generally, for all $1 \leq k \leq n$: $1 \leq \lambda_k \cdot \lambda_{n-k+1}^\vee \leq n$

Remark. 1. The last statement is often referred to as Banaszczyk's Transference Theorem. We will skip the proof.
2. Improved bounds can be found in the literature.

q-ary lattices

q-ary lattices

Definition

Let $q \in \mathbb{Z}_{\geq 3}$ be an odd prime number, $m \in \mathbb{Z}_{\geq 1}$. A lattice $\mathcal{L} \subseteq \mathbb{Z}^m$ is called q-**ary** if

$$q\mathbb{Z}^m \subseteq \mathcal{L} \subseteq \mathbb{Z}^m$$

q-ary lattices

Definition

Let $q \in \mathbb{Z}_{\geq 3}$ be an odd prime number, $m \in \mathbb{Z}_{\geq 1}$. A lattice $\mathcal{L} \subseteq \mathbb{Z}^m$ is called q-**ary** if

$$q\mathbb{Z}^m \subseteq \mathcal{L} \subseteq \mathbb{Z}^m$$

- $\mathcal{L}$ has full rank m

q-ary lattices

Definition

Let $q \in \mathbb{Z}_{\geq 3}$ be an odd prime number, $m \in \mathbb{Z}_{\geq 1}$. A lattice $\mathcal{L} \subseteq \mathbb{Z}^m$ is called q-**ary** if

$$q\mathbb{Z}^m \subseteq \mathcal{L} \subseteq \mathbb{Z}^m$$

- $\mathcal{L}$ has full rank m
- q-ary lattices are important for many cryptographic lattice-based schemes/problems, i.e. LWE, SIS, etc.

Typical examples

Let q be an odd prime. Denote $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$ the finite field with q elements. Let $A \in (\mathbb{F}_q)^{m \times n}$ be a matrix, $m \geq n$.

Typical examples

Let q be an odd prime. Denote $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$ the finite field with q elements. Let $A \in (\mathbb{F}_q)^{m \times n}$ be a matrix, $m \geq n$.

Definition

$$\Lambda_q(A) = \{y \in \mathbb{Z}^m : y = Ax \pmod{q} \text{ for some } x \in \mathbb{Z}^n\}$$

$$\Lambda_q^{\perp}(A) = \{y \in \mathbb{Z}^m : A^T y \equiv 0 \pmod{q}\}$$

Typical examples

Let q be an odd prime. Denote $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$ the finite field with q elements. Let $A \in (\mathbb{F}_q)^{m \times n}$ be a matrix, $m \geq n$.

Definition

$$\Lambda_q(A) = \{y \in \mathbb{Z}^m : y = Ax \pmod{q} \text{ for some } x \in \mathbb{Z}^n\}$$

$$\Lambda_q^{\perp}(A) = \{y \in \mathbb{Z}^m : A^T y \equiv 0 \pmod{q}\}$$

The lattices $\Lambda_q(A)$ and $\Lambda_q^{\perp}(A)$ are q-ary.

Typical examples

Let q be an odd prime. Denote $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$ the finite field with q elements. Let $A \in (\mathbb{F}_q)^{m \times n}$ be a matrix, $m \geq n$.

Definition

$$\Lambda_q(A) = \{y \in \mathbb{Z}^m : y = Ax \pmod{q} \text{ for some } x \in \mathbb{Z}^n\}$$

$$\Lambda_q^{\perp}(A) = \{y \in \mathbb{Z}^m : A^T y \equiv 0 \pmod{q}\}$$

The lattices $\Lambda_q(A)$ and $\Lambda_q^{\perp}(A)$ are q-ary. Even stronger:

Theorem

The following are equivalent:

1. $\mathcal{L}$ is q-ary
2. $\mathcal{L} = \Lambda_q(A)$ for some A
3. $\mathcal{L} = \Lambda_q^{\perp}(A')$ for some A'

An example for $\Lambda_q(A)$ and $\Lambda_q^{\perp}(A)$

Let $q = 131101$ prime, $m = 3, n = 2$ Let

$$A = \begin{pmatrix} 66612 & 77907 \\ 64603 & 16912 \\ 10733 & 125395 \end{pmatrix}$$

Then $\Lambda_q(A)$ and $\Lambda_q^{\perp}(A)$ are

An example for $\Lambda_q(A)$ and $\Lambda_q^{\perp}(A)$

Let $q = 131101$ prime, $m = 3, n = 2$ Let

$$A = \begin{pmatrix} 66612 & 77907 \\ 64603 & 16912 \\ 10733 & 125395 \end{pmatrix}$$

Then $\Lambda_q(A)$ and $\Lambda_q^{\perp}(A)$ are

1. Elements $v \in \Lambda_q(A)$ satisfy:

$$v \equiv \alpha_1 \begin{pmatrix} 66612 \\ 64603 \\ 10733 \end{pmatrix} + \alpha_2 \begin{pmatrix} 77907 \\ 16912 \\ 125395 \end{pmatrix} \pmod{131101}$$

An example for $\Lambda_q(A)$ and $\Lambda_q^{\perp}(A)$

Let $q = 131101$ prime, $m = 3, n = 2$ Let

$$A = \begin{pmatrix} 66612 & 77907 \\ 64603 & 16912 \\ 10733 & 125395 \end{pmatrix}$$

Then $\Lambda_q(A)$ and $\Lambda_q^{\perp}(A)$ are

1. Elements $v \in \Lambda_q(A)$ satisfy:
$$v \equiv \alpha_1 \begin{pmatrix} 66612 \\ 64603 \\ 10733 \end{pmatrix} + \alpha_2 \begin{pmatrix} 77907 \\ 16912 \\ 125395 \end{pmatrix} \pmod{131101}$$
2. Elements $w = (w_1, w_2, w_3) \in \Lambda_q^{\perp}(A)$ satisfy:
$66612w_1 + 64603w_2 + 10733w_3 \equiv 0 \pmod{131101}$
$77907w_1 + 16912w_2 + 125395w_3 \equiv 0 \pmod{131101}$

Properties of $\Lambda_q(A)$ and $\Lambda_q^{\perp}(A)$

Properties of $\Lambda_q(A)$ and $\Lambda_q^{\perp}(A)$

Proposition

1. $\det(\Lambda_q^{\perp}(A)) \leq q^n$ with equality iff $rk_{\mathbb{F}_q}(A) = n$
2. $\det(\Lambda_q(A)) \geq q^{m-n}$ with equality iff $rk_{\mathbb{F}_q}(A) = n$

Moreover the following is true:

Properties of $\Lambda_q(A)$ and $\Lambda_q^\perp(A)$

Proposition

1. $\det(\Lambda_q^\perp(A)) \leq q^n$ with equality iff $rk_{\mathbb{F}_q}(A) = n$
2. $\det(\Lambda_q(A)) \geq q^{m-n}$ with equality iff $rk_{\mathbb{F}_q}(A) = n$

Moreover the following is true:

Proposition

$$\Lambda_q^\perp(A) = q(\Lambda_q(A))^\vee$$

and

$$\Lambda_q(A) = q((\Lambda_q^\perp(A))^\vee) \ .$$

Moreover, $\det(\Lambda_q^\perp(A)) \cdot \det(\Lambda_q(A)) = q^m$

$\Lambda_q^{\perp}(A) = q(\Lambda_q(A))^{\vee}$ (proof)

$\Lambda_q^{\perp}(A) = q(\Lambda_q(A))^{\vee}$ (proof)

1. We first show that $\Lambda_q^{\perp}(A) \subseteq q(\Lambda_q(A))^{\vee}$
   - Let $y \in \Lambda_q^{\perp}(A)$. Thus $A^T y \equiv 0 \pmod{q}$ i.e. $A^T y = qz$ for some $z \in \mathbb{Z}^m$.
   - Let $y' \in \Lambda_q(A)^{\vee}$. Thus $y' = Ax + qz'$ for some vectors $x \in \mathbb{Z}^n, z' \in \mathbb{Z}^m$.
   - Now write

$$\begin{aligned} \langle y, y' \rangle &= \langle y, Ax \rangle + q\langle y, z' \rangle = \langle A^T y, x \rangle + q\langle y, z' \rangle \\ &= q\langle z, x \rangle + q\langle y, z' \rangle \end{aligned}$$

   - This implies $\langle (1/q)y, y' \rangle \in \mathbb{Z}$, so $(1/q)y \in (\Lambda_q(A))^{\vee}$

$\Lambda_q^{\perp}(A) = q(\Lambda_q(A))^{\vee}$ (proof)

1. We first show that $\Lambda_q^{\perp}(A) \subseteq q(\Lambda_q(A))^{\vee}$
   - Let $y \in \Lambda_q^{\perp}(A)$. Thus $A^T y \equiv 0 \pmod{q}$ i.e. $A^T y = qz$ for some $z \in \mathbb{Z}^m$.
   - Let $y' \in \Lambda_q(A)^{\vee}$. Thus $y' = Ax + qz'$ for some vectors $x \in \mathbb{Z}^n, z' \in \mathbb{Z}^m$.
   - Now write

$$\begin{aligned} \langle y, y' \rangle &= \langle y, Ax \rangle + q\langle y, z' \rangle = \langle A^T y, x \rangle + q\langle y, z' \rangle \\ &= q\langle z, x \rangle + q\langle y, z' \rangle \end{aligned}$$

   - This implies $\langle (1/q)y, y' \rangle \in \mathbb{Z}$, so $(1/q)y \in (\Lambda_q(A))^{\vee}$
2. Now we show that $\Lambda_q^{\perp}(A) \supseteq q(\Lambda_q(A))^{\vee}$
   - Let $qy \in q(\Lambda_q(A))^{\vee}$. This implies $\langle y, y' \rangle \in \mathbb{Z}$ for all $y' \in \Lambda_q(A)$.
   - In particular this holds for the basis vectors: $\Lambda_q(A)$ being generated by columns of A and vectors $qe_1, \ldots, qe_n$ we have: $A^T y \in \mathbb{Z}^n$ and $qy \in \mathbb{Z}^m$.
   - So: $A^T(qy) = q(A^T y) \equiv 0 \pmod{q}$.

Conclusion

Conclusion

- The knowledge of the geometry in $\mathcal{L}$ gives insight in the geometry of $\mathcal{L}^\vee$.

Conclusion

- The knowledge of the geometry in $\mathcal{L}$ gives insight in the geometry of $\mathcal{L}^\vee$.
- Dual bases can be explicitely described from primal bases.

Conclusion

- The knowledge of the geometry in $\mathcal{L}$ gives insight in the geometry of $\mathcal{L}^\vee$.
- Dual bases can be explicitely described from primal bases.
- Duality in Crypto: Many applications using q-ary lattices, applications to LWE, SIS, CVP, etc.

Many thanks for your attention.