Mastermath, Spring 2018
Intro to Lattice Algs & Crypto

Lecture 5

Lecturers: D. Dadush, L. Ducas
Scribe: K. de Boer

06/03/18

1 Introduction

This week we continue the analysis of the output of the LLL-algorithm; we examine which particular properties LLL-reduced basis have. Examples include comparing the length of the first basis vector to $\lambda_1(\Lambda)$ and comparing the i-th basis vector to the i-th successive minimum.

After that, the concept of duality will shortly be recalled. We will apply this knowledge to prove that the notion of 'being WeaklyLLL-reduced' is self-dual.

The last treated subject will be the enumeration-algorithm for the shortest- and closest vector problem. As the name indicates, this algorithm will enumerate all vectors close to some target t.

2 Properties of LLL-reduced bases

Before showing the useful properties of LLL-reduced bases, we first need two lemmata that will help us acquiring these properties.

Lemma 1 *For any basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a lattice Λ, we have*

$$\lambda_1(\Lambda) \geq \min_i \|\widetilde{\mathbf{b}}_i\|$$

Proof: **Geometric proof:** As the Babai fundamental domain $\mathcal{F} = \widetilde{\mathbf{B}}[0,1)^n$ is tiling, it contains only one lattice point, which is zero. Verify that therefore $\widetilde{\mathbf{B}}(-1,1)^n \cap \Lambda = \{0\}$. Let $r = \max\{t > 0 \mid t\mathcal{B}_2^n \subseteq \widetilde{\mathbf{B}}(-1,1)^n\}$, then clearly $\lambda_1(\Lambda) \geq r$. It is easy to see that $r = \min_i \|\mathbf{b}_i^*\|$, and the proof is finished.

Algebraic proof: Let $\mathbf{v}$ be a shortest vector in Λ and let $\mathbf{v} = \mathbf{B}\mathbf{x}$, with $\mathbf{x} \in \mathbb{Z}^n$. Let j be the largest index such that $x_j \neq 0$. Gram-Schmidt orthogonalization factorizes $\mathbf{B} = \widetilde{\mathbf{B}}\mu$ with μ upper triangular, and therefore $\mathbf{v} = \widetilde{\mathbf{B}}\mu\mathbf{x}$. Write $\mathbf{y} = \mu\mathbf{x}$, then we can conclude $y_j = \sum_{i \geq j} \mu_{ji} x_i = \mu_{jj} x_j = x_j \in \mathbb{Z} \backslash 0$. Therefore $\|\mathbf{v}\|^2 = \sum_{i=1}^n \|\widetilde{\mathbf{b}}_i\|^2 y_i^2 \geq \|\widetilde{\mathbf{b}}_j\|^2$, as $y_j^2 \geq 1$, which finishes the proof. □

Lemma 2 *For any lattice Λ, one has $\lambda_i(\Lambda_{k:n}) \leq \lambda_{i+k-1}(\Lambda)$.*

Proof: It is enough to prove that $\lambda_i(\Lambda_{k:n}) \leq \lambda_{i+1}(\Lambda_{k-1:n})$ for any $k \in \{2, \ldots, n\}$ and $i \in \{1, \ldots, n-1\}$. Here we will prove this inequality for $k = 2$, and let the reader verify that the exact same proof can easily be amended for general $k \in \{2, \ldots, n\}$. So, our aim is to prove that $\lambda_i(\Lambda_{2:n}) \leq \lambda_{i+1}(\Lambda)$, for all $i \in \{1, \ldots, n-1\}$.

Let $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \Lambda$ attain the successive minima of Λ. Let j be the smallest index such that $\pi_2(v_j) \in \operatorname{span}(\pi_2(v_1), \ldots, \pi_2(v_{j-1}))$. Set

$$\mathbf{w}_i = \begin{cases} \pi_2(v_i) & \text{if} \quad i < j \\ \pi_2(v_i) & \text{if} \quad i > j \end{cases}$$

Note that the $n-1$ vectors $\mathbf{w}_i$ are linearly independent elements of $\Lambda_{2:n}$. Furthermore, we have $\|\mathbf{w}_i\| \leq \max(\|\mathbf{v}_i\|, \|\mathbf{v}_{i+1}\|) \leq \max(\lambda_i, \lambda_{i+1}) \leq \lambda_{i+1}(\Lambda)$. This proves the claim. □

Theorem 3 *Let $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be an ε-LLL reduced basis. Set $\Lambda = \mathcal{L}(\mathbf{B})$ and $\alpha = \gamma_2 + \varepsilon$. Then, we have*

1. $\|\mathbf{b}_1\| \leq \alpha^{\frac{n-1}{2}} \cdot \det(\Lambda)^{1/n}$ *[Root Hermite-factor Bound]*
2. $\|\mathbf{b}_1\| \leq \alpha^{n-1} \cdot \lambda_1(\Lambda)$ *[Approximation factor Bound]*
3. $\|\widetilde{\mathbf{b}}_i\| \leq \alpha^{n-i} \cdot \lambda_i(\Lambda)$.
4. $\|\mathbf{b}_i\| \leq \alpha^{i-1} \cdot \|\widetilde{\mathbf{b}}_i\| \leq \alpha^{n-1} \cdot \lambda_i(\Lambda)$ *[Approximation factor alike Bound]*
5. $\prod_{i=1}^{n} \|\mathbf{b}_i\| \leq \alpha^{\frac{n(n-1)}{2}} \cdot \det(\Lambda)$.

Note that in the following proof, for the inequalities (1.) to (3.) no size-reduction is needed. Thus, those inequalities hold in weakly LLL-reduced bases as well. The last two inequalities, however, do depend on size-reduction.
Proof:

1. The exact same reasoning as in proving the Hermite bound, replacing γ_2 by α, applies here.
2. We have $\|\mathbf{b}_1\| \leq \alpha^{i-1} \cdot \|\widetilde{\mathbf{b}}_i\| \leq \alpha^{n-1} \cdot \min_i \|\widetilde{\mathbf{b}}_i\| \leq \alpha^{n-1} \cdot \lambda_1(\Lambda)$, where the first two inequalities follow from the basis being weakly LLL-reduced and the last inequality uses Lemma 1.
3. Note that $\mathbf{B}$ being Weakly LLL-reduced means that $\mathbf{B}_{i:n}$ is Weakly LLL-reduced, too. Therefore, by part (2.) of this theorem, $\|\widetilde{\mathbf{b}}_i\| \leq \alpha^{n-i} \lambda_1(\Lambda_{i:n}) \leq \alpha^{n-i} \lambda_i(\Lambda)$. The last inequality uses Lemma 2.
4. As the second bound follows from (3.), we only need to prove the first bound. Write $\mathbf{b}_i = \widetilde{\mathbf{b}}_i + \sum_{j<i} c_j \widetilde{\mathbf{b}}_j$. As the basis is both size-reduced and Weakly LLL-reduced, we know that $|c_j| \leq 1/2$ and $\|\widetilde{\mathbf{b}}_j\| \leq \alpha^{i-j} \|\widetilde{\mathbf{b}}_i\|$ for $j < i$. Therefore

$$\|\mathbf{b}_i\|^2 \leq \|\widetilde{\mathbf{b}}_i\|^2 + \frac{1}{4} \sum_{j<i} \|\widetilde{\mathbf{b}}_j\|^2 = \|\widetilde{\mathbf{b}}_i\|^2 \left(1 + \frac{1}{4} \sum_{j<i} \frac{\|\widetilde{\mathbf{b}}_j\|^2}{\|\widetilde{\mathbf{b}}_i\|^2}\right) \leq \|\widetilde{\mathbf{b}}_i\|^2 \left(1 + \frac{1}{4} \sum_{j<i} \alpha^{2(i-j)}\right)$$

$$\leq \|\widetilde{\mathbf{b}}_i\|^2 \left(1 + \frac{1}{4} \sum_{k=1}^{i-1} \alpha^{2k}\right) \leq \alpha^{2(i-1)} \cdot \|\widetilde{\mathbf{b}}_i\|^2.$$

The last inequality follows from the following tedious calculations. As $\alpha^2 \geq \gamma_2^2 \geq 4/3$, we have $3\alpha^2 \geq 4$, so $4(\alpha^2 - 1) \geq \alpha^2$ and therefore $1 \geq \frac{\alpha^2}{4(\alpha^2-1)}$.

$$1 + \frac{1}{4} \sum_{k=1}^{i-1} \alpha^{2k} = 1 + \frac{\alpha^2}{4} \sum_{k=0}^{i-2} \alpha^{2k} = 1 + \frac{\alpha^2}{4} \cdot \frac{\alpha^{2(i-1)} - 1}{\alpha^2 - 1} \leq 1 + (\alpha^{2(i-1)} - 1) = \alpha^{2(i-1)}$$

5. This is left as an exercise for the reader.

□

Exercise 1 Prove point (5.) of the last theorem.

3 Duality

3.1 Introduction

The concept of duality is one that occurs in almost all areas of mathematics. Very broadly, duality is a one-to-one operation that takes certain mathematical structures to certain (other) mathematical structures. Often, but not always, this operation is an involution, meaning that taking the dual of the dual of an object returns (an isomorphic image of) the same object.

3.2 The lattice dual

Before defining the lattice dual, we will first recall the dual of a vector space.

Definition 4 *Let V be a finite dimensional vector space over $\mathbb{R}$. Then the dual V^* of V is defined as follows:*

$$V^* := \{f \mid f : V \to \mathbb{R} \textit{ linear maps}\}$$

When V has an inner product (that is, V is a Hilbert space), then there is a canonical isomorphism between V and V^*, namely:

$$\phi : V \to V^*, \; \mathbf{v} \mapsto \langle \cdot, \mathbf{v} \rangle$$

Here $\langle \cdot, \mathbf{v} \rangle$ is the map that takes $\mathbf{w} \in V$ to $\langle \mathbf{w}, \mathbf{v} \rangle \in \mathbb{R}$. Also, V^* can be naturally (canonically) made into a Hilbert space as well, by defining the following inner product on V^*.

$$\langle \langle \cdot, \mathbf{v} \rangle, \langle \cdot, \mathbf{w} \rangle \rangle := \langle \mathbf{v}, \mathbf{w} \rangle$$

Exercise 2 Let V be a finite-dimensional vector space over $\mathbb{R}$ and let V^* be its dual. Prove that there is a one-to-one correspondence between inner products on V and isomorphisms $V \to V^*$.

The definition of the dual of a lattice Λ is in some sense very alike. We will assume that $\mathbb{R}^n$ is enriched with the standard inner product, making $\mathbb{R}^n$ and $(\mathbb{R}^n)^*$ isomorphic via the map $\mathbf{e}_i \mapsto \langle \cdot, \mathbf{e}_i \rangle$.

Definition 5 *For $\Lambda \subseteq \mathbb{R}^n$, we define $\Lambda^* \subseteq (\mathbb{R}^n)^*$ as being the lattice of all linear maps $f : \mathbb{R}^n \to \mathbb{R}$ such that $f(\Lambda) \subseteq \mathbb{Z}$. In mathematical language:*

$$\Lambda^* = \{f \in (\mathbb{R}^n)^* \mid f(\Lambda) \subseteq \mathbb{Z}\} = \{\langle \cdot, v \rangle \in (\mathbb{R}^n)^* \mid \langle \Lambda, v \rangle \subseteq \mathbb{Z}\}$$

Note that the inner product on the lattice Λ^* is inherited from the dual vector space where Λ^* lives in.

Definition 6 *Let $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ be a basis of a lattice Λ. Denote by $\mathbf{b}_i^*$ the unique vector in* $\operatorname{span}(\mathbf{b}_1, \ldots, \mathbf{b}_n)$*, which satisfies*

$$\langle \mathbf{b}_i, \mathbf{b}_j^* \rangle = \begin{cases} 1 & \textit{if} \quad i = j \\ 0 & \textit{if} \quad i \neq j \end{cases}$$

Exercise 3 Convince yourself that such elements $\mathbf{b}_i^*$ exist and that they are linearly independent.

Lemma 7 *Λ^* is a lattice in $(\mathbb{R}^n)^*$.*

Proof: One way of proving that it is indeed a lattice, is showing that there exists a basis $(f_1, \dots, f_n)$ in $\mathbb{R}^{n*}$ such that any element in Λ^* can be written as an integral linear combination of these basis elements.

Let $f_i = \langle \cdot, \mathbf{b}_i^* \rangle$, for $i \in \{1, \dots, n\}$. Let $f \in \Lambda^*$, i.e., $f : \Lambda \to \mathbb{Z}$. Set $c_i = f(\mathbf{b}_i) \in \mathbb{Z}$. It is easy to prove that $f = \sum_{i=1}^n c_i f_i = \sum_{i=1}^n c_i \langle \cdot, \mathbf{b}_i^* \rangle$. Since the $\mathbf{b}_i^*$ are linearly independent, their dual counterparts $\langle \cdot, \mathbf{b}_i^* \rangle$, are, too. Therefore Λ^* is a lattice. □

Because of the one-to-one relation between $\langle \cdot, \mathbf{b}_i^* \rangle$ and $\mathbf{b}_i^*$, many mathematicians like to identify these two or abuse the notation. Despite the fact that this identification is very natural, the vectors $\mathbf{b}_i^* \in \mathbb{R}^n$ shouldn't be considered as the 'real idea'; that is, when working with the elements $\mathbf{b}_i^*$ in $\text{span}(\Lambda)$, always be conscious of the crude fact that they are just representation of maps $\langle \cdot, \mathbf{b}_i^* \rangle$ from Λ to $\mathbb{Z}$.

Note — for example — that it is possible to add the elements $\mathbf{b}_i^*$ and $\mathbf{b}_i$, as they belong both to $\text{span}(\Lambda)$. But when one is reminded by the fact that $\mathbf{b}_i^*$ actually 'means' $\langle \cdot, \mathbf{b}_i^* \rangle : \Lambda \to \mathbb{Z}$, this addition makes no sense anymore.

For the remainder of this text, we will also identify $\langle \cdot, \mathbf{b}_i^* \rangle$ and $\mathbf{b}_i^*$, and silently hope that it will not cause any confusion.

3.3 The dual basis

Definition 8 *Let* $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ *be a basis of the lattice* Λ*, then* $\mathbf{B}^* = (\mathbf{b}_1^*, \dots, \mathbf{b}_n^*)$ *is called the* dual basis *of* $\mathbf{B}$*.*

The most formal definition of duality requires reversion of the indices, because of the categorical 'swapping of arrows'. Therefore the following notation will be useful.

Notation 9 We denote $\mathbf{b}_{\text{-}i}^* = \mathbf{b}_i^*$.

Definition 10 (Reversed dual basis) *Let* $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ *be a basis of the lattice* Λ*, then* ${}^*\mathbf{B} = (\mathbf{b}_{\text{-}n}^*, \dots, \mathbf{b}_{\text{-}1}^*)$ *is called the* reversed dual basis *of* $\mathbf{B}$*.*

Note that the indices of $\mathbf{b}_i^*$ are going up, from $-n$ to -1.

Notation 11 We denote $\mathbf{B}$ to be the (reversed) dual basis of $\mathbf{D}$ by the following notation: $\mathbf{B} \leftrightarrow \mathbf{D}$

The following lemma is described in human language by the phrase: "Projecting in the primal lattice is sectioning in the dual lattice".

Lemma 12 $(\pi_i(\mathbf{b}_i), \dots, \pi_i(\mathbf{b}_n)) \leftrightarrow (\mathbf{b}_{\text{-}n}^*, \dots, \mathbf{b}_{\text{-}i}^*)$

Proof: It is enough to prove that $\mathbf{b}_{\text{-}n}^*, \dots, \mathbf{b}_{\text{-}i}^* \in \text{span}(\pi_i(\mathbf{b}_i), \dots, \pi_i(\mathbf{b}_n))$ and $\langle \pi_i(\mathbf{b}_j), \mathbf{b}_{\text{-}k}^* \rangle = \delta_{jk}$ (Kronecker delta). The first part can be proven by the fact that $\mathbf{b}_{\text{-}k}^* \in (\mathbf{b}_1, \dots, \mathbf{b}_{i-1})^T = \text{span}(\pi_i(\mathbf{b}_i), \dots, \pi_i(\mathbf{b}_n))$. The last part can be proven by writing out the definition of π_i. □

Note that we can also apply Gram-Schmidt to the dual basis $\mathbf{B}^* = (\mathbf{b}_{\text{-}n}^*, \dots, \mathbf{b}_{\text{-}1}^*)$. We introduce new notation to avoid confusion with π_i on the primal basis.

Notation 13 Denote $\tau_{\text{-}i} = \pi_{(\mathbf{b}_{\text{-}n}^*, \dots, \mathbf{b}_{\text{-}(i+1)}^*)^\perp}$, which are exactly the projections of the Gram-Schmidt procedure applied to $(\mathbf{b}_{\text{-}n}^*, \dots, \mathbf{b}_{\text{-}1}^*)$. Note that these projections are also in negative notation, i.e., starting with $\tau_{\text{-}n} = \text{id}$, $\tau_{\text{-}(n-1)} = \pi_{(\mathbf{b}_{\text{-}n}^*)^\perp}$ and ending with $\tau_1 = \pi_{(\mathbf{b}_{\text{-}n}^*, \dots, \mathbf{b}_{\text{-}2}^*)^\perp}$. Convince yourself that the following equality holds: $\widetilde{\mathbf{b}}_{\text{-}j}^* = \tau_{\text{-}j}(\mathbf{b}_{\text{-}j}^*)$.

LEMMA 14 *For $i \leq j$, $(\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_j)) \leftrightarrow (\tau_{\text{-}j}(\mathbf{b}^*_{\text{-}j}), \ldots, \tau_{\text{-}j}(\mathbf{b}^*_{\text{-}i}))$*

PROOF: According to Lemma 12, we have $(\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_n)) \leftrightarrow (\mathbf{b}^*_{\text{-}n}, \ldots, \mathbf{b}^*_{\text{-}i})$. By the symmetry of duality, we also have $(\mathbf{b}^*_{\text{-}n}, \ldots, \mathbf{b}^*_{\text{-}i}) \leftrightarrow (\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_n))$. Projecting in one argument means, again by Lemma 12, removing basis elements at the end in the second argument, that is,

$$(\tau_{\text{-}j}(\mathbf{b}^*_{\text{-}j}), \ldots, \tau_{\text{-}j}(\mathbf{b}^*_{\text{-}i})) \leftrightarrow (\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_j)).$$

By symmetry, this proves the claim. □

3.4 Self-duality of WeaklyLLL

COROLLARY 15 $(\widetilde{\mathbf{b}}^*_i) = (\tau_i(\mathbf{b}^*_{\text{-}i})) \leftrightarrow (\pi_i(\mathbf{b}_i)) = (\mathbf{b}^*_i)$, *i.e.,* $(\widetilde{\mathbf{b}}^*_{\text{-}i})$ *and* $(\mathbf{b}^*_i)$ *are reversed dual bases.*

In particularly, this means that $\widetilde{\mathbf{b}}^*_{\text{-}i} \in \operatorname{span}(\mathbf{b}^*_i)$ and $\langle \mathbf{b}^*_i, \widetilde{\mathbf{b}}^*_{\text{-}i} \rangle = 1$. Therefore, $\|\mathbf{b}^*_i\| \|\widetilde{\mathbf{b}}^*_{\text{-}i}\| = 1$.

LEMMA 16 *Let $\mathbf{B} \leftrightarrow {}^*\mathbf{B}$ be reversed dual bases. Then $\mathbf{B}$ is ε-weakly LLL-reduced if and only if ${}^*\mathbf{B}$ is ε-weakly LLL-reduced.*

PROOF: The basis $\mathbf{B}$ being ε-weakly LLL-reduced means $\frac{\|\mathbf{b}^*_{i+1}\|}{\|\mathbf{b}^*_i\|} \leq \gamma_2 + \varepsilon$. But, by Corollary 15, we have $\frac{\|\mathbf{b}^*_{i+1}\|}{\|\mathbf{b}^*_i\|} = \frac{\|\widetilde{\mathbf{b}}^*_{\text{-}i}\|}{\|\widetilde{\mathbf{b}}^*_{\text{-}(i+1)}\|}$. Noting that the indices are negated in the dual basis, this exactly means that $\mathbf{B}^*$ is ε-weakly LLL-reduced. The reverse statement can be proved similarly. □

4 Enumeration algorithm for SVP and CVP

Algorithm 1: Basic Enumeration algorithm

```
Input  : A basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a lattice $\Lambda$, a target $\mathbf{t} \in \operatorname{span}(\Lambda)$ and a radius
         $r \in \mathbb{R}_{>0}$.
Output: A set of lattice points $\mathcal{E}$ such that $(r\mathcal{B}_2^n + \mathbf{t}) \cap \Lambda \subseteq \mathcal{E}$.

Enum ($\mathbf{B}$,$\mathbf{t}$,$r$):
    $c := \frac{\langle \mathbf{t}, \mathbf{b}^*_n \rangle}{\|\mathbf{b}^*_n\|}$
    $Z := \{z \in \mathbb{Z} \mid (c - z\|\mathbf{b}^*_n\|)^2 \leq r^2\}$
    $\mathcal{E} := \bigcup_{z \in Z} \left( z\mathbf{b}_n + \texttt{Enum}([\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}], \pi_{(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})}(\mathbf{t} - z\mathbf{b}_n), r) \right)$
    return $\mathcal{E}$
```

LEMMA 17 *The basic enumeration algorithm (Algorithm 1) is correct.*

PROOF: It is easy to see that $\mathcal{E}$ indeed consists of lattice points. Suppose that $\mathbf{v} \in (r\mathcal{B}_2^n + \mathbf{t}) \cap \Lambda$. Our aim is to prove that $\mathbf{v} \in \mathcal{E}$.

So, assume $\|\mathbf{v} - \mathbf{t}\| \leq r$ and $\mathbf{v} \in \Lambda$. Decomposing $\mathbf{v} - \mathbf{t} = \sum_{i=1}^n c_i \widetilde{\mathbf{b}}_i$, yields $\sum_{i=1}^n c_i^2 \|\widetilde{\mathbf{b}}_i\|^2 \leq r^2$, and in particular $c_n^2 \|\widetilde{\mathbf{b}}_n\|^2 \leq r^2$. Write $\mathbf{v} = z\mathbf{b}_n + \mathbf{v}'$, where $\mathbf{v}' \in \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}) = \Lambda'$. Then

$$c_n \|\widetilde{\mathbf{b}}_n\|^2 = \langle \mathbf{v} - \mathbf{t}, \widetilde{\mathbf{b}}_n \rangle = \langle z\mathbf{b}_n + \mathbf{v}' - \mathbf{t}, \widetilde{\mathbf{b}}_n \rangle = \langle z\mathbf{b}_n - \mathbf{t}, \widetilde{\mathbf{b}}_n \rangle = z\|\widetilde{\mathbf{b}}_n\|^2 - \langle \mathbf{t}, \widetilde{\mathbf{b}}_n \rangle$$

Dividing by $\|\widetilde{\mathbf{b}}_n\|$ and taking squares yields $\left(z\|\widetilde{\mathbf{b}}_n\| - \frac{\langle \mathbf{t},\widetilde{\mathbf{b}}_n\rangle}{\|\widetilde{\mathbf{b}}_n\|}\right)^2 = c_n^2\|\widetilde{\mathbf{b}}_n\|^2 \leq r^2$. This means that $z \in Z$, where Z is from the third line of Algorithm 1. Note that the proof is complete when we can show that $\mathbf{v}' \in \mathcal{E}' = \texttt{Enum}([\mathbf{b}_1, \ldots, \mathbf{b}_{n-1}], \pi_{(\mathbf{b}_1,\ldots,\mathbf{b}_{n-1})}(\mathbf{t} - z\mathbf{b}_n), r)$. It is enough to prove that $\mathbf{v}' \in (r\mathcal{B}_2^{n-1} + \pi_{(\mathbf{b}_1,\ldots,\mathbf{b}_{n-1})}(\mathbf{t} - z\mathbf{b}_n)) \cap \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$, since this set is in $\mathcal{E}'$ by the induction hypothesis. It is obvious that $\mathbf{v}' \in \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_{n-1})$ holds. For the inclusion in the other part of the intersection, we proceed as follows.

Write $\pi = \pi_{(\mathbf{b}_1,\ldots,\mathbf{b}_{n-1})}$. Again, decompose $\mathbf{v}' - \pi(\mathbf{t} - z\mathbf{b}_n) = \sum_{i=1}^{n-1} d_i \widetilde{\mathbf{b}}_i$. Note that the index i goes up to $n-1$, instead of n. We will show that $d_i = c_i$ for all $i \in \{1, \ldots, n-1\}$, where c_i are the coefficients in the decomposition of $\mathbf{v} - \mathbf{t}$. We compute

$$\langle \mathbf{v}' - \pi(\mathbf{t} - z\mathbf{b}_n), \widetilde{\mathbf{b}}_i\rangle = \langle \mathbf{v} - z\mathbf{b}_n, \widetilde{\mathbf{b}}_i\rangle + \langle \pi(z\mathbf{b}_n - \mathbf{t}), \widetilde{\mathbf{b}}_i\rangle = \langle \mathbf{v} - z\mathbf{b}_n, \widetilde{\mathbf{b}}_i\rangle + \langle z\mathbf{b}_n - \mathbf{t}, \widetilde{\mathbf{b}}_i\rangle = \langle \mathbf{v} - \mathbf{t}, \widetilde{\mathbf{b}}_i\rangle.$$

Therefore $\|\mathbf{v}' - \pi(\mathbf{t} - z\mathbf{b}_n)\| = \sum_{i=1}^{n-1} c_i^2 \|\widetilde{\mathbf{b}}_i\|^2 \leq \sum_{i=1}^{n} c_i^2 \|\widetilde{\mathbf{b}}_i\|^2 = \|\mathbf{v} - \mathbf{t}\| \leq r$, which proves the claim.□

Lemma 18 *The running time of the basic enumeration algorithm is* $O(\frac{2^n \cdot r^n}{\det(\Lambda)})$.

Proof: The cardinality of the set Z is at most $\frac{2r}{\|\widetilde{\mathbf{b}}_n\|}$. Therefore the number of recursive calls is bounded by $\prod_{i=1}^n \frac{2r}{\|\widetilde{\mathbf{b}}_n\|} = \frac{2^n r^n}{\det \Lambda}$. □

Algorithm 2: An Enumeration algorithm solving SVP

```
Input  : A basis $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of a lattice $\Lambda$.
Output: A shortest vector $v \in \Lambda \backslash \{0\}$.

Enum ($\mathbf{B}$):
    LLL-reduce the basis $\mathbf{B}$
    $\mathcal{E} := \texttt{Enum}(\mathbf{B}, 0, \|\mathbf{b}_1\|)$
    Find $\mathbf{v} \in \mathcal{E} \backslash \{0\}$ with $\|v\|$ minimal
    return $\mathbf{v}$
```

Exercise 4 Prove that Algorithm 2 indeed returns the shortest vector.

Lemma 19 *The running time of the enumeration algorithm solving SVP is* $2^{O(n^2)}$.

Proof: According to Lemma 18, the running time is $O(\frac{2^n r^n}{\det \Lambda})$. In the algorithm, $r = \|\mathbf{b}_1\|$. By the fact that the basis $\mathbf{B}$ is LLL-reduced, we know $\frac{\|\mathbf{b}_1\|^n}{\det(\Lambda)} \leq \alpha^{n(n-1)/2}$. Therefore, the running time is $O(2^n \alpha^{n(n-1)/2}) = 2^{O(n^2)}$. □