Duality

1 Introduction

In this lecture we introduce the notion of duality for lattice and their basis. One of the role of the dual $L^\vee$ of lattice L is in harmonic analysis: a generalization of Fourier analysis of periodic function over $\mathbb{R}$ to periodic function over $\mathbb{R}^n$. This allows in particular to establish strong "transference" theorems relating the geometry of the primal lattice L to that of its dual. This is also a key tool to prove security of lattice-based cryptosystems. We will not go that far in this course, but the fundamental of harmonic analysis will be considered in the Exercise Sheet 6.

There is also a notion of a dual basis, that will be the main object of this lecture, which interacts very well with Gram-Schmidt Orthogonalization and basis reduction. In particular we will show that WLLL reduction is a self-dual notion, that is a basis is WLLL reduced iff its dual is reduced. We will then consider a stronger notion that is self-dual which will lead to yet another equality on Hermite's constant, namely Mordell's inequality $\gamma_n^{n-2} \leq \gamma_{n-1}^{n-1}$.

2 Duality

2.1 Dual lattice and dual basis

Definition 1 *The dual of a (Euclidean) lattice $L \subset \mathbb{R}^n$ is the set*

$$L^\vee := \{\mathbf{x} \in \mathrm{Span}_{\mathbb{R}}(L) \mid \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \text{ for all } \mathbf{y} \in L\}.$$

The condition "$\langle \mathbf{x}, \mathbf{y} \rangle \subseteq \mathbb{Z}$ for all $\mathbf{y} \in L$" is often shortened to $\langle \mathbf{x}, L \rangle \subseteq \mathbb{Z}$.

Lemma 2 *The dual $L^\vee$ of a lattice L is also a lattice.*

Proof: That $L^\vee$ is a subgroup of $\mathbb{R}^n$ is a consequence of the linearity of $\mathbf{x} \mapsto \langle \mathbf{x}, \mathbf{y} \rangle$. For discreteness, we will show that there exists a minimum distance. The group structure of $L^\vee$ then implies discreteness.

Consider a basis of $\mathbf{b}_1, \dots \mathbf{b}_k$ of L, and for some $\mathbf{y} \in L^\vee \setminus \{\mathbf{0}\}$, consider the inner products $\langle \mathbf{b}_i, \mathbf{y} \rangle$. Each inner product is an integer and at least one of them is non-zero (since otherwise $\mathbf{y} \in \mathrm{Span}_{\mathbb{R}}(L)^\perp$) and therefore not less than 1 in absolute value. By Cauchy-Schwarz we conclude that $\|\mathbf{y}\|_2 \geq 1/\max \|\mathbf{b}_i\|_2$, and therefore that $L^\vee$ is discrete. □

Remark 3 In fact, we have almost established that $\lambda_1(L^\vee) \geq 1/\lambda_n(L)$. To fully prove it, note that we do not need the $\mathbf{b}_i$ to be a basis, but merely a set of independent vectors of L.

Definition 4 *Let $\mathbf{B} \in \mathbb{R}^{n \times k}$ have rank $k \leq n$. The dual basis of $\mathbf{B}$ is defined as $\mathbf{B}^\vee = \mathbf{B}(\mathbf{B}^\top \mathbf{B})^{-1}$.*

Note that in the case of full-rank lattices ($k = n$), the above definition simplifies to the inverse-transpose: $\mathbf{B}^\vee = \mathbf{B}^{-\top}$.

Lemma 5 *$\mathbf{B}^{\vee\top}$ is a pseudo-inverse of $\mathbf{B}$, that is:*

i) $\mathbf{B}^{\vee\top} \cdot \mathbf{B} = \mathbf{I}_k = \mathbf{B}^\top \cdot \mathbf{B}^\vee$

ii) $\mathrm{Span}_{\mathbb{R}}(\mathbf{B}) = \mathrm{Span}_{\mathbb{R}}(\mathbf{B}^\vee)$

iii) $\mathbf{B}^\vee \mathbf{B}^\top \mathbf{y} = \mathbf{y}$ *for all* $\mathbf{y} \in \mathrm{Span}_{\mathbb{R}}(\mathbf{B})$, *i.e.* $\mathbf{B}^\vee \mathbf{B}^\top$ *acts as the identity on* $\mathrm{Span}_{\mathbb{R}}(\mathbf{B})$.

The proof of the above consists of expanding Definition 4, and is left to the reader. Below we show that the first two items above are actually a characterization of the dual basis, by unicity.

Lemma 6 *For a basis* $\mathbf{B} \in \mathbb{R}^{n \times k}$ *of rank* k, *there is a unique* $\mathbf{D} \in \mathbb{R}^{n \times k}$ *such that*

$$\mathbf{D}^\top \mathbf{B} = \mathbf{I}_k$$

and

$$\mathrm{Span}_{\mathbb{R}}(\mathbf{B}) = \mathrm{Span}_{\mathbb{R}}(\mathbf{D}).$$

This is the dual basis $\mathbf{B}^\vee$ *of* $\mathbf{B}$.

Proof: Consider two solutions $\mathbf{D}, \mathbf{C}$, and set $\mathbf{E} = \mathbf{D} - \mathbf{C}$. Because $\mathbf{E}^\top \cdot \mathbf{B} = \mathbf{0}$, the columns of $\mathbf{E}$ are orthogonal to $\mathrm{Span}_{\mathbb{R}}(\mathbf{B})$. But we also have that $\mathrm{Span}_{\mathbb{R}}(\mathbf{E}) \subset \mathrm{Span}_{\mathbb{R}}(\mathbf{D}) + \mathrm{Span}_{\mathbb{R}}(\mathbf{C}) = \mathrm{Span}_{\mathbb{R}}(\mathbf{B})$, hence $\mathbf{E} = \mathbf{0}$. □

Lemma 7 *If* $\mathbf{B} \in \mathbb{R}^{n \times k}$ *is a basis of* L, $\mathbf{B}^\vee$ *is a basis of* $L^\vee$.

Proof: We claim that $\mathbf{y} \in \mathrm{Span}_{\mathbb{R}}(L)$ is in $L^\vee$ if and only if $\mathbf{B}^\top \mathbf{y} \in \mathbb{Z}^k$. If $\mathbf{B}^\top \mathbf{y} \in \mathbb{Z}^k$, then $\mathbf{x}^\top \mathbf{y} \in \mathbb{Z}$ for all $\mathbf{x} \in L$ since $\mathbf{x}$ is an integer combination of the columns of $\mathbf{B}$. To see the converse, note that the columns of $\mathbf{B}$ are themselves vectors of L and therefore $\mathbf{B}^\top \mathbf{y} = (\langle \mathbf{b}_1, \mathbf{y} \rangle, \ldots, \langle \mathbf{b}_k, \mathbf{y} \rangle)^\top \in \mathbb{Z}^k$.

The above claim and part i) of Lemma 5 together imply that the columns of $\mathbf{B}^\vee$ belongs to $L^\vee$, since $\mathbf{B}^{\vee\top} \mathbf{B} = \mathbf{I}_k$ is an integer matrix. Hence $\mathbf{B}^\vee \cdot \mathbb{Z}^k \subseteq L^\vee$.

Now consider some $\mathbf{y} \in L^\vee$, and let $\mathbf{x}^\top = \mathbf{y}^\top \mathbf{B}$. By the above claim, $\mathbf{x} \in \mathbb{Z}^k$. We compute $\mathbf{B}^\vee \mathbf{x} = \mathbf{B}^\vee \mathbf{B}^\top \mathbf{y} = \mathbf{y}$, (Lemma 5, part iii)) and deduce that $L^\vee \subseteq \mathbf{B}^\vee \cdot \mathbb{Z}^k$. We conclude that $\mathbf{B}^\vee$ is a basis of $L^\vee$. □

Corollary 8 *Let* L *be a lattice. Then, we have*

i) L *and* $L^\vee$ *have the same* $\mathbb{R}$*-span and in particular the same rank.*

ii) $\det(L) = 1/\det(L^\vee)$.

iii) $L^{\vee\vee} = L$.

Proof: The first item is a direct consequence of Lemma 5. For the second item, simply compute $|\det(\mathbf{B}^{\vee\top} \mathbf{B}^\vee)| = |\det((\mathbf{B}^\top \mathbf{B})^{-\top} \cdot (\mathbf{B}^\top \mathbf{B}) \cdot (\mathbf{B}^\top \mathbf{B})^{-1})| = 1/|\det(\mathbf{B}^\top \mathbf{B})|$. For the third item, unrolling the definition of dual basis twice shows that $\mathbf{B}^{\vee\vee} = \mathbf{B}$. □

2.2 Reversed dual Gram-Schmidt orthogonalization

To simplify the exposition below, we assume that our bases have dimension $n = k$. In this case, the formula for the dual basis simplifies to $\mathbf{B}^\vee = \mathbf{B}^{-\top}$; however, the facts discussed here generalize to the case $k \leq n$ with more bookkeeping effort.

Consider the decomposition of the matrix $\mathbf{B}$:

$$\mathbf{B} = \mathbf{Q}\mathbf{\Delta}\mathbf{T}$$

where $\mathbf{Q} \in \mathcal{O}_n(\mathbb{R})$ is the Gram-Schmidt ortho*normalization* of $\mathbf{B}$, $\mathbf{\Delta}$ is diagonal, and $\mathbf{T}$ is an upper triangular matrix with unit diagonal (the usual orthogonalization is given via $\mathbf{B}^\star = \mathbf{Q} \cdot \mathbf{\Delta}$). Now consider its dual basis, and note that

$$\mathbf{B}^\vee = (\mathbf{Q}\mathbf{\Delta}\mathbf{T})^{-\top} = \mathbf{Q}\mathbf{\Delta}^{-1}\mathbf{T}^{-\top},$$

since $\mathbf{Q}^{-1} = \mathbf{Q}^\top$, and $\mathbf{\Delta}$ is diagonal. This is almost Gram-Schmidt Orthonormalization of $\mathbf{B}^\vee$, the only issue being that $\mathbf{T}^{-\top}$ is *lower* triangular rather than upper triangular. This motivates us to consider the dual basis indexed in reversed order. To do so, consider the *reversal matrix*

$$\mathbf{J}_n = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ & & \iddots & & \\ 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}$$

and note that $\mathbf{J}_n^2 = \mathbf{I}_n$ and $\mathbf{J}_n^\top = \mathbf{J}_n$. When n is clear from context, we will just write $\mathbf{I}$ and $\mathbf{J}$ for $\mathbf{I}_n$ and $\mathbf{J}_n$. The reversed dual basis is defined by $\mathbf{D} = \mathbf{B}^\vee\mathbf{J}$, and we can re-write:

$$\begin{aligned} \mathbf{D} = \mathbf{B}^\vee\mathbf{J} &= \mathbf{Q}\mathbf{\Delta}^{-1}\mathbf{T}^{-\top}\mathbf{J} \\ &= \mathbf{Q}\mathbf{J}^2\mathbf{\Delta}^{-1}\mathbf{J}^2\mathbf{T}^{-\top}\mathbf{J} \\ &= (\mathbf{Q}\mathbf{J}) \cdot (\mathbf{J}\mathbf{\Delta}^{-1}\mathbf{J}) \cdot (\mathbf{J}\mathbf{T}^{-\top}\mathbf{J}). \end{aligned}$$

Note that $\mathbf{Q}\mathbf{J} \in O_n(\mathbb{R})$, while $(\mathbf{J}\mathbf{\Delta}^{-1}\mathbf{J})$ is diagonal, with the same coefficients as $\mathbf{\Delta}^{-1}$ but in reversed order. Finally, $(\mathbf{J}\mathbf{T}^{-\top}\mathbf{J})$ is indeed an upper triangular matrix with unit diagonal.

We can now consider the orthonormalization $\mathbf{D}^\star = (\mathbf{Q}\mathbf{J})(\mathbf{J}\mathbf{\Delta}^{-1}\mathbf{J}) = \mathbf{Q}\mathbf{\Delta}^{-1}\mathbf{J} = \mathbf{B}^\star\mathbf{\Delta}^{-2}\mathbf{J}$. We have fully characterized the Gram-Schmidt of the reversed dual basis in term of the Gram-Schmidt of the primal, as summarized below. For convenience, we will use negative indices: for a given matrix $\mathbf{X}$, we use $\mathbf{x}_{-i}$ to denote $\mathbf{x}_{n+1-i}$, i.e. the i-th column vector of $\mathbf{X}\mathbf{J}$.

LEMMA 9 *Let* $\mathbf{B}$ *be a basis and* $\mathbf{D}$ *its reversed-dual basis. Then* $\mathbf{d}_i^\star$ *is given by*

$$\mathbf{d}_i^\star = \mathbf{b}_{-i}^\star / \|\mathbf{b}_{-i}^\star\|_2^2,$$

often called the reciprocal *of* $\mathbf{b}_i^\star$.

2.3 Duality and projected-sublattices

One perhaps surprising consequence of the above is lemma the following: the reciprocal of the last Gram-Schmidt vector of a basis $\mathbf{B}$ of L is a vector of the dual lattice $L^\vee$, since

$$\mathbf{d}_1 = \mathbf{d}_1^\star = \mathbf{b}_n^\star / \|\mathbf{b}_n^\star\|_2^2 \in L^\vee.$$

More generally, we can relate the blocks of the primal to those of the dual.

Let us first recall the notation: $\mathbf{B}_{i:j} := (\pi_i(\mathbf{b}_i), \ldots, \pi_i(\mathbf{b}_j))$, and $\mathbf{B}^\star_{i:j}$ is its GSO (Since $(\mathbf{B}_{i:j})^\star = (\mathbf{b}_i^\star, \ldots, \mathbf{b}_j^\star) = (\mathbf{B}^\star)_{i:j}$, the order doesn't matter). We will also use negative indices with this notation: $\mathbf{B}_{-i:-j} := \mathbf{B}_{n+1-i:n+1-j}$, with n being the number of vectors in B (note that we do not apply $\mathbf{J}$ here).

LEMMA 10 *For any basis $\mathbf{B} \in \mathbb{R}^{n\times k}$, if $\mathbf{D}$ is its reverse dual then $\mathbf{D}^\vee_{i:j} = \mathbf{B}_{-j:-i}\mathbf{J}$ and $\mathbf{D}^\star_{i:j} = \mathbf{B}^\star_{-j:-i}\Delta^{-2}\mathbf{J}$ for any $1 \le i \le j \le n$.*

PROOF: Note that the $a+1$-th column of $\mathbf{D}^\star_{i:j}$ is simply $\mathbf{d}^\star_{i+a}$ and similarly that the column with index $-(a+1)$ of $\mathbf{B}^\star_{-j:-i}$ is $\mathbf{b}^\star_{-i-a}$ (Lecture 4, Fact 14). By Lemma 9 we conclude that $\mathbf{D}^\star_{i:j} = \mathbf{B}^\star_{-j:-i}\Delta^{-2}\mathbf{J}$.

To prove the other equality $\mathbf{D}^\vee_{i:j} = \mathbf{B}_{-j:-i}\mathbf{J}$, consider the Gram Schmidt decomposition in blocks:

$$\mathbf{B} = \mathbf{B}^\star \cdot \mathbf{T} = (\mathbf{B}^\star_{1:-j-1}|\mathbf{B}^\star_{-j:-i}|\mathbf{B}^\star_{-i+1:k}) \cdot \begin{pmatrix} \mathbf{T}_1 & * & * \\ \mathbf{0} & \mathbf{T}_2 & * \\ \mathbf{0} & \mathbf{0} & \mathbf{T}_3 \end{pmatrix} \tag{1}$$

and note that $\mathbf{B}_{-j:-i} = \mathbf{B}^\star_{-j:-i} \cdot \mathbf{T}_2$. Also recall that the Gram-Schmidt decomposition of the reverse dual basis is given by $\mathbf{D} = \mathbf{D}^\star \cdot (\mathbf{J}\mathbf{T}^{-\top}\mathbf{J})$. Because $\mathbf{T}$ is triangular with unit diagonal, it's inverse $\mathbf{T}^{-1}$ has the form

$$\mathbf{T}^{-1} = \begin{pmatrix} \mathbf{T}_1^{-1} & * & * \\ \mathbf{0} & \mathbf{T}_2^{-1} & * \\ \mathbf{0} & \mathbf{0} & \mathbf{T}_3^{-1} \end{pmatrix}$$

which leads to:

$$\mathbf{J}\mathbf{T}^{-\top}\mathbf{J} = \begin{pmatrix} \mathbf{J}\mathbf{T}_3^{-\top}\mathbf{J} & * & * \\ \mathbf{0} & \mathbf{J}\mathbf{T}_2^{-\top}\mathbf{J} & * \\ \mathbf{0} & \mathbf{0} & \mathbf{J}\mathbf{T}_1^{-\top}\mathbf{J} \end{pmatrix}.$$

Hence, $\mathbf{D}_{i:j} = \mathbf{D}^\star_{i:j} \cdot (\mathbf{J}\mathbf{T}_2^{-\top}\mathbf{J})$. It remains to check that $\mathbf{B}_{-j:-i}\mathbf{J}$ and $\mathbf{D}_{i:j}$ satisfy the characterization of the dual basis from Lemma 6, by checking that $(\mathbf{B}_{-i:-j}\mathbf{J})^\top\mathbf{D}_{i:j} = \mathbf{I}_{j-i}$ and that they have the same span. The latter follows from the fact that $\mathbf{D}^\star_{i:j}$ and $\mathbf{B}^\star_{-j:-i}$ have the same span, since right multiplication by invertible matrices does not affect span. Finally, we compute

$$\begin{aligned}(\mathbf{B}_{-j:-i}\mathbf{J})^\top\mathbf{D}_{i:j} &= (\mathbf{B}^\star_{-j:-i}\mathbf{T}_2\mathbf{J})^\top \cdot (\mathbf{D}^\star_{i:j}\mathbf{J}\mathbf{T}_2^{-\top}\mathbf{J}) \\ &= \mathbf{J}\mathbf{T}_2^\top{\mathbf{B}^\star_{-j:-i}}^\top \cdot \mathbf{B}^\star_{-j:-i}\boldsymbol{\Delta}^{-2}\mathbf{J}\mathbf{J}\mathbf{T}_2^{-\top}\mathbf{J} \\ &= \mathbf{I}_{j-i},\end{aligned}$$

□

One may make a more geometric interpretation of the above claim by looking at the case when $i = 1$: informally, sectioning in the primal corresponds to projecting in the dual. More formally, we have the below Lemma.

LEMMA 11 *Let L be a lattice, and $S \subseteq \mathrm{Span}_R(L)$ be a real subvector space such that $\dim(S) = \dim(S \cap L)$. Then, $(S \cap L)^\vee = \pi_S(L^\vee)$ where π_S is the orthogonal projection onto S.*

The proof is left as exercise.

3 Dual Reduction

3.1 Dual profile

Recall that the general objective of of basis reduction was to make the profile $\ell_i(\mathbf{B}) = \log\|\mathbf{b}_i^\star\|_2$ as flat as possible. Now, note that if $\mathbf{D}$ is the reversed dual basis of $\mathbf{B}$, then

$$\ell_i(\mathbf{D}) = -\ell_{n-i+1}(\mathbf{B}),$$

so the plot of $i \mapsto \ell_i(\mathbf{D})$ is simply the plot of $i \mapsto \ell_i(\mathbf{B})$ rotated by 180° around the point $((n+1)/2, 0)$, as depicted in Figure 1.

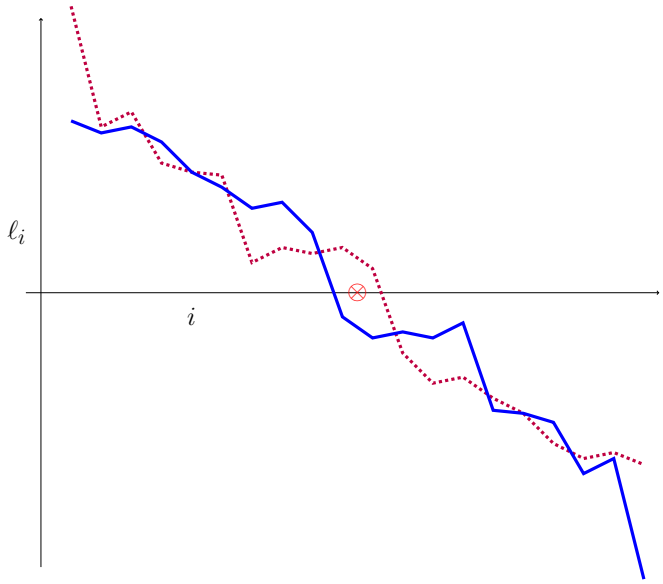

Figure 1: The profile of a basis in dimension 20 (dashed) and of its reversed dual (plain)

Hence, the general goal of flattening the profile is self-dual, in the sense that flattening the profile of the lattice will also flatten the profile of the reverse dual. More specific reduction notions may not be self-dual in this sense. For example, a WLLL reduced lattice has a WLLL reduced reversed dual, but the same is not true for LLL reduction. The dual of an LLL reduced basis will still of course be WLLL reduced, but may no longer be size-reduced.

LEMMA 12 *A basis* $\mathbf{B}$ *of a* 2*-dimensional lattice* L *is Lagrange-reduced if and only if its reverse dual basis* $\mathbf{D} = \mathbf{B}^\vee\mathbf{J}$ *is.*

PROOF: Because of the lattice invariant $\|\mathbf{b}_1\|_2 \cdot \|\mathbf{b}_2^\star\|_2 = \det(L)$, minimizing $\mathbf{b}_1$ is equivalent to maximizing $\mathbf{b}_2^\star$, which is equivalent to minimizing $\|\mathbf{d}_1\|_2$.

Regarding the second property (size-reduction) of Lagrange-reduced basis $|\langle \mathbf{b}_1, \mathbf{b}_2\rangle| \leq 1/2\|\mathbf{b}_1\|_2^2$, note that this is equivalent to stating that the off diagonal cofficient $\mathbf{T}_{1,2}$ of $\mathbf{T}$ in the GSO decomposition $\mathbf{B} = \mathbf{B}^\star \cdot \mathbf{T}_\mathbf{B}$ is less than $1/2$ in absolute value. Above, we have seen that $\mathbf{T}_\mathbf{D} = \mathbf{J}\mathbf{T}_\mathbf{B}^{-\top}\mathbf{J}$. Let us write $\mathbf{T}_\mathbf{B} = \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$, and note that $\mathbf{T}_\mathbf{B}^{-1} = \left(\begin{smallmatrix} 1 & -x \\ 0 & 1 \end{smallmatrix}\right)$, therefore $\mathbf{T}_\mathbf{D} = \left(\begin{smallmatrix} 1 & -x \\ 0 & 1 \end{smallmatrix}\right)$. Hence, $\mathbf{B}$ is size-reduced if and only if $\mathbf{D}$ is also size-reduced. □

This, together with the block duality property (Lemma 10) directly lead to the self duality of weak-LLL reduction.

COROLLARY 13 *A basis* $\mathbf{B}$ *WLLL-reduced if and only if its reverse dual basis* $\mathbf{D} = \mathbf{B}^\vee \cdot \mathbf{J}$ *is.*

REMARK 14 The LLL reduction is however not self-dual (that is, WLLL and size-reduced), because size reduction for basis of rank $n > 2$ is not self dual. Indeed, size reduction is a constraint on the off diagonal elements of $\mathbf{T}$ being less than $1/2$ in absolute value, which is not preserved by duality. In fact, the coefficients of $\mathbf{T}^{-1}$ can be as large as exponential in n when those of $\mathbf{T}$ are bounded by $1/2$.

3.2 Mordell reduction

DEFINITION 15 (SVP-REDUCTION A DUAL-SVP-REDUCTION) *A basis* $\mathbf{B}$ *is said to be SVP-reduced if* $\mathbf{b}_1$ *is a shortest vector of the lattice generated by* $\mathbf{B}$*. It is said dual-SVP-reduced if its reverse dual basis* $\mathbf{D}$ *is SVP-reduced.*

In other terms, SVP-reduction requires $\ell_1(\mathbf{B})$ to be minimized, while dual-SVP-reduction requires $\ell_n(\mathbf{B})$ to be maximized. The definition of Hermite's constant gives, for an SVP-reduced basis,

$$\|\mathbf{b}_1\|_2 \leq \gamma_n^{1/2} \cdot \det(L)^{1/n}.$$

Applying it in the dual gives us

$$\|\mathbf{b}_n^\star\|_2 \geq \gamma_n^{-1/2} \cdot \det(L)^{1/n}.$$

An important point is that (dual-)SVP-reduced basis indeed exists, because the shortest non-zero vector is always primitive, and can therefore be completed into a basis of the same lattice. A slightly less straightforward fact is that this can be done efficiently given a shortest vector. The following lemma is stated for primitive vectors, and therefore holds for shortest vectors.

LEMMA 16 *There exists a polynomial time algorithm that, given a basis* $\mathbf{B}$ *of a lattice* L *and a primitive vector* $\mathbf{v} \in L$*, outputs a basis* $\mathbf{C}$ *of* L *such that* $\mathbf{c}_1 = \mathbf{v}$*.*

The proof requires Hermite Normal Form which has not been treated in this course, and will therefore be left to the curious reader. The bottom line for our purpose is that the hard part of SVP-reduction really is finding the shortest vector; reconstructing the rest of the basis is algorithmically efficient.

We are now ready to state Mordell's reduction, its associated algorithm, and associated bound. It is another example of a self-dual reduction notion.

DEFINITION 17 *A basis* $\mathbf{B}$ *of rank* n *is said to be* Mordell reduced *if* $\mathbf{B}_{1:n-1}$ *is SVP-reduced and* $\mathbf{B}_{2:n}$ *is dual-SVP-reduced.*

This notion of reduction will lead to the bound in Theorem 18. The proof will follow the same pattern as that of Hermite's bound. First we show that Mordell reduced bases exist via an algorithmic proof, where correctness is by construction but termination requires an argument. Then, we show that this reduction notion implies an upper bound on the first basis vector, leading to the existence of a short vector in the lattice.

THEOREM 18 (MORDELL'S BOUND)

$$\gamma_n^{n-2} \leq \gamma_{n-1}^{n-1}.$$

Algorithm 1: Mordell reduction's algorithm

Input : A basis $\mathbf{B}$ of a lattice L of rank n. An SVP-reduction oracle $\mathcal{O}$ for lattices of dimension $n-1$

Output: A Mordell reduced basis of $\mathbf{B}$

repeat
  SVP-reduce $\mathbf{B}_{1:n-1}$ using $\mathcal{O}$
  dual-SVP-reduce $\mathbf{B}_{2:n}$ using $\mathcal{O}$
until $\mathbf{B}_{1:n-1}$ *is SVP-reduced (test using* $\mathcal{O}$*)*
return B

LEMMA 19 *Mordell's reduction algorithm terminates and is correct.*

PROOF: By the terminating condition of the **repeat-until** loop, the outputted basis $\mathbf{B}$ satisfies that $\mathbf{B}_{1:n-1}$ is SVP-reduced. The last modification of $\mathbf{B}$ was to dual-SVP-reduce $\mathbf{B}_{2:n}$, so the output $\mathbf{B}$ is Mordell's reduced.

For termination, we only need to note that the dual reduction step does not modify $\mathbf{b}_1$, while the primal reduction step can only cause $\|\mathbf{b}_1\|$ to decrease. If it does not decrease after the primal reduction step, then the algorithm terminates. By discreteness of L, $\|\mathbf{b}_1\|$ can only decrease finitely many times before it reaches a minimum, and so the algorithm terminates in finitely many steps. □

Note that, as for Hermite's algorithm the number of iterations of the **repeat-until** loop might be extremely large to start with. However, if one first pre-processes the basis with LLL, and relaxes the termination condition to "$\mathbf{B}_{1:n-1}$ is $(1+\varepsilon)$-SVP-reduced", the algorithm can be shown to terminate in $O(n/\varepsilon)$ loops. Though, a simpler approach is to make the primal SVP call in full dimension n, a single iteration is required.

COROLLARY 20 *Every lattice admits a Mordell reduced basis.*

LEMMA 21 *If* $\mathbf{B}$ *is a Mordell reduced basis of a lattice* L *of rank* $n > 2$*, then*

$$\|\mathbf{b}_1\|_2^2 \leq \gamma_{n-1}^{\frac{n-1}{n-2}} \cdot \det(L)^{1/n}.$$

PROOF: Let us define the log-volume of the block $\mathbf{B}_{i:j}$ as

$$\ell_{i:j} = \log \det(L_{i:j})$$

and note that it relates to the profile ℓ_i of $\mathbf{B}$ via $\ell_{i:j} = \sum_{k=i}^{j} \ell_i$. Let us also define $g_n = \log \sqrt{\gamma_n}$, the half-logarithm of the Hermite constant for n dimensions. The condition that $\mathbf{B}_{1:n-1}$ is SVP reduced guarantees that

$$\ell_1 \leq g_{n-1} + \frac{1}{n-1}\ell_{1:n-1}, \tag{2}$$

while the fact that $\mathbf{B}_{2:n}$ is dual SVP-reduced guarantees that

$$\ell_n \geq -g_{n-1} + \frac{1}{n-1}\ell_{2:n}. \tag{3}$$

We start from inequality (2), and put it in terms of only g_{n-1}, ℓ_1 and $\ell_{1:n}$.

$$\begin{aligned}
\ell_1 &\leq g_{n-1} + \frac{1}{n-1}\left(\ell_{1:n} - \ell_n\right) && \text{[decompose } \ell_{1:n}\text{]} \\
&\leq g_{n-1} + \frac{1}{n-1}\left(\ell_{1:n} + g_{n-1} - \frac{1}{n-1}\ell_{2:n}\right) && \text{[apply lower bound on } \ell_n\text{]} \\
&\leq g_{n-1} + \frac{1}{n-1}\left(\ell_{1:n} + g_{n-1} - \frac{1}{n-1}\left(\ell_{1:n} - \ell_1\right)\right) && \text{[decompose } \ell_{2:n}\text{]}
\end{aligned}$$

We collect similar terms and simplify their coefficients:

$$\begin{aligned}
\left(1 - \frac{1}{(n-1)^2}\right) \cdot \ell_1 &\leq \left(1 + \frac{1}{n-1}\right) \cdot g_{n-1} + \frac{1}{n-1}\left(1 - \frac{1}{n-1}\right) \cdot \ell_{1:n} \\
\frac{(n-2)\cdot n}{(n-1)^2} \cdot \ell_1 &\leq \frac{n}{n-1} \cdot g_{n-1} + \frac{n-2}{(n-1)^2} \cdot \ell_{1:n}.
\end{aligned}$$

we finally rescale and obtain $\ell_1 \leq \frac{n-1}{n-2} \cdot g_{n-1} + \frac{1}{n} \cdot \ell_{1:n}$; taking the exponential, we conclude. □

Combining Corollary 20 and Lemma 21 directly leads to Theorem 18: Mordell-reduced basis exists, and such basis contains a vector of the prescribed norm.