Basis reduction for layered lattices

Proefschrift

ter verkrijging van de graad van Doctor aan de Universiteit Leiden, op gezag van Rector Magnificus prof. mr. P.F. van der Heijden, volgens besluit van het College voor Promoties te verdedigen op dinsdag 20 December 2011 klokke 16:15 uur.

door

Erwin Lavalliére Torreão Dassen,

geboren te Campina Grande, Brazilië in 1979.

Samenstelling van de promotiecommissie:

Promotor
Prof. Dr. H. W. Lenstra Jr.

Overige leden
Prof. Dr. P. Stevenhagen,
Prof. Dr. J. E. Cremona (University of Warwick),
Prof. Dr. K. Aardal (TU Delft),
Prof. Dr. R. Cramer (Universiteit Leiden, CWI),
Dr. B. de Smit.

Basis reduction for layered lattices

Basis reduction for layered lattices
Erwin L. Torreão Dassen

This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported License. To view a copy of this license, visit *http://creativecommons.org/licenses/by-sa/3.0/* or send a letter to *Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.*

The research leading to this work was supported by Marie-Curie Actions and by NWO.

Typeset in LaTeX.
Printed by Ipskampdrukkers, Enschede.

ISBN/EAN: 978-90-818191-0-7

To my friends and family; to peaceful,
happy, and greedless coexistence.

Contents

1 Introduction **9**
1.1 Main results 9
1.2 Review on ordered sets, and on algebra 14
1.3 Review on complexity theory 16
1.4 Notation 17

2 Ordered vector spaces **21**
2.1 Ordered rings and fields 21
2.2 Ordered vector spaces 23
2.3 Real ordered vector spaces 27
2.4 Symmetric powers 28

3 Layered Euclidean spaces **33**
3.1 Layered forms 33
3.2 Orthogonality 39
3.3 Exterior powers of layered Euclidean spaces 44

4 Layered lattices **49**
4.1 Embedded layered lattices 49
4.2 Layered lattices 51
4.3 Exterior powers of layered lattices 61
4.4 The discriminant 61

5 The layered Gram-Schmidt procedure **63**
5.1 Associated Gram-Schmidt bases 63

5.2 Relation to the discriminant of lattices 71
5.3 A polynomial-time algorithm 72

6 Layered lattice basis reduction 77
6.1 LLL reduction 77
6.2 The layered LLL algorithm 82
6.3 A polynomial-time reduction algorithm 85

A Two algorithms 91

CHAPTER 1

Introduction

1.1 Main results

A *lattice* L is a discrete subgroup of a Euclidean space. As such, it comes equipped with a norm map $q : L \to \mathbb{R}$ and is a free abelian group of finite rank. Lattices were first used in algebraic number theory and since then have been applied in many different areas of mathematics. When one has to do calculations with a lattice, one needs to choose a basis for it. Then, as in linear algebra, certain bases are more suitable than others. For example, bases that are nearly orthogonal and/or whose basis vectors are short, are usually preferred. This leads to the problem of, given an arbitrary basis, finding a "good" one.

In the 1982 paper [8], the authors provide a polynomial time algorithm, now called the LLL algorithm, for solving the above problem. More precisely, they give an algorithm that given a basis $b_1, \ldots, b_m$ of a sublattice of $\mathbb{Z}^m$ such that $\max_i q(b_i) \leqslant B$, computes a *reduced basis* for this sublattice with the number of bit operations bounded by a constant multiple of $n^6(\log B)^3$. A reduced basis in the sense of that paper, for all practical purposes, achieves both conditions stated in the last paragraph. Namely, the computed basis vectors are nearly orthogonal and short; the discovery of this algorithm was a breakthrough in the computational theory of lattices. For instance, in the same paper, the authors used the LLL algorithm to show that factorization of primitive polynomials with rational coefficients is solvable in polynomial time

as well.

Nonetheless, the LLL algorithm has certain shortcomings. The purpose of this work is to extend this algorithm so as to remove one of those shortcomings. The problem in question is exemplified in the following application of the LLL algorithm.

Suppose $f : \mathbb{Z}^m \to \mathbb{Z}^n$ is a group homomorphism and $\mathbf{F}$ is the matrix of f with respect to the canonical bases of $\mathbb{Z}^m$ and $\mathbb{Z}^n$. One wants to compute the *integer kernel* of $\mathbf{F}$, i.e., find a basis for $\ker f$ over $\mathbb{Z}$. To do so we introduce a norm on $\mathbb{Z}^m$ making it into a lattice in such a way that extremely short vectors generate the kernel. Let

$$M > 2^{m-1}(r+1)r^r F^{2r} \tag{1.1}$$

where r is the rank of $\mathbf{F}$ and F is the maximum of the entries of $\mathbf{F}$. Define $q : \mathbb{Z}^m \to \mathbb{R}$ by $q(x) = ||x||^2 + M \cdot ||f(x)||^2$ where $|| \cdot ||$ denotes the usual Euclidean norm. Then applying the LLL algorithm to the canonical basis of $\mathbb{Z}^m$ yields a basis $b_1, \ldots, b_m$ of which the first $m-r$ vectors form a basis for the kernel (see [10, Proposition of section 14, pg. 163] for a proof). Intuitively one sees that as $M \to \infty$ more and more vectors in $\ker f$ will have norm smaller than M and for sufficiently big M the LLL algorithm finds a basis for the kernel among them.

This trick of "weighting" the norm to exploit the LLL algorithm is used in many other circumstances, including the problem of finding a basis out of a generating set of a lattice. We refer the reader to [2] and [12].

The issue we want to address is the choice of the constant M above. As exemplified by (1.1), these numbers are typically huge and, as such, carry severe computational overhead. Except for a lower bound it must satisfy, M is completely arbitrary and this challenges us to find a better solution. The key idea is to indeed let $M \to \infty$ and work with M "as a symbol". Note that this leads to the pleasant fact that, contrary to the case where M is a concrete number, the whole kernel is comprised of "small" vectors (compared to M). On the other hand, the norm is now a vector valued function $q : L \to \mathbb{R} + \mathbb{R} \cdot \infty$ with $\mathbb{R} + \mathbb{R} \cdot \infty$ anti-lexicographically ordered. In a way, the kernel is a "layer" below the other vectors of the lattice. Our discussion so far leads to the concept of a *layered lattice*, which can be defined algebraically as follows.

Definition 1.2. A *layered lattice* is a triple (L, V, q) where L is a finitely generated abelian group, V is a totally ordered, finite-dimensional, real vector space and $q : L \to V$ is a map satisfying the following conditions.

(i) For all $x \in L \setminus \{0\}$ we have $q(x) \neq 0$.

(ii) For all $x, y \in L$ we have $q(x+y) + q(x-y) = 2 \cdot q(x) + 2 \cdot q(y)$.

(iii) The set $q(L) \subset V$ is well-ordered. $\diamondsuit$

The purpose of this work if to develop the ideas above and to describe an algorithm that accomplishes what the LLL algorithm does in the classical case. We develop a theory of layered lattices and their ambient spaces, which we call *layered Euclidean spaces*. In the latter, an important result is the existence of orthogonal bases. We give an algorithm to compute them: the *Gram-Schmidt* procedure.

Definition 1.3. A *layered Euclidean space* is a triple $(E, V, \langle\cdot,\cdot\rangle)$ where E is a finite-dimensional real vector space, V is a totally ordered, finite-dimensional, real vector space, and $\langle\cdot,\cdot\rangle : E \times E \to V$ is a bilinear symmetric map such that the following conditions are satisfied.

(i) For all $x \in E \setminus \{0\}$ we have $\langle x, x\rangle > 0$.

(ii) For all $x, y \in E$ there exists $\lambda \in \mathbb{R}$ such that $\langle x, y\rangle \leqslant \lambda\langle y, y\rangle$.

Given $x, y \in E$, we say that x is *orthogonal* to y if for all $\lambda \in \mathbb{R}$ we have $\lambda\langle x, y\rangle \leqslant \langle y, y\rangle$. We write this condition as $x \perp y$. For a subset $S \subset E$ we write $x \perp S$ if for all $y \in S$ we have $x \perp y$. The set of all $x \in E$ such that $x \perp S$ is denoted by $S^\perp$. $\diamondsuit$

A few words of caution are important here. The notion of orthogonality in layered Euclidean spaces clearly generalizes the usual notion of orthogonality, *but there are important differences*. For example, orthogonality *is not in general a symmetric relation*. In (3.18) we give an example where two vectors x, y in a layered Euclidean space are such that $x \perp y$ but $y \not\perp x$. This subtlety gives rises to new phenomena in the geometry of layered Euclidean spaces. Despite that, this notion of orthogonality turns out to be very useful in our theory. We remark that for any set S, the set $S^\perp$ is a subspace.

Theorem 1.4. *Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space and $b_1, \ldots, b_m$ be an ordered basis of E. Then there exists a unique basis $b_1^*, \ldots, b_m^*$ such that the following holds.*

(a) *For all $i \in \{1, \ldots, m\}$ we have $b_i^* \in (\mathrm{span}\{b_1, \ldots, b_{i-1}\})^\perp$.*
(b) *For all $i \in \{1, \ldots, m\}$ we have $b_i - b_i^* \in \mathrm{span}\{b_1, \ldots, b_{i-1}\}$.*

The basis $\{b_1^*, \ldots, b_m^*\}$ of the theorem above is called the *Gram-Schmidt basis associated to* $\{b_1, \ldots, b_m\}$. For a procedure to compute the Gram-Schmidt basis of $\{b_1, \ldots, b_m\}$ see proposition (5.7). In (5.28) we also give a polynomial-time algorithm to compute such bases.

An *embedded* layered lattice is a subgroup of a layered Euclidean space that is a layered lattice with the norm induced by the inner-product. An important result in the theory, and one which nicely generalizes the classical situation, is that any layered lattice can be embedded in a layered Euclidean space. We

remark that associated to the quadratic norm $q : L \to V$ of a layered lattice there is a bilinear symmetric map $\langle \cdot, \cdot \rangle : L \times L \to V$ such that for all $x \in L$ we have $q(x) = \langle x, x \rangle$.

Theorem 1.5. *Let (L, V, q) be a layered lattice. Then $(\mathbb{R} \otimes_{\mathbb{Z}} L, V, \langle \cdot, \cdot \rangle)$, where the map $\langle \cdot, \cdot \rangle : \mathbb{R} \otimes_{\mathbb{Z}} L \times \mathbb{R} \otimes_{\mathbb{Z}} L \to V$ is given on generators by*

$$\langle \alpha \otimes x, \beta \otimes y \rangle = \alpha\beta \langle x, y \rangle,$$

is a layered Euclidean space. The inclusion map $\iota : L \hookrightarrow \mathbb{R} \otimes_{\mathbb{Z}} L$ given by $x \mapsto 1 \otimes x$ is such that for all $x \in L$ we have $\langle \iota(x), \iota(x) \rangle = q(x)$ and makes $\iota(L)$ into an embedded layered lattice.

As in the classical case we use Gram-Schmidt bases to introduce the concept of reduced bases of layered lattices.

Definition 1.6. Let $L \subset E$ be a layered lattice of rank m embedded in a layered Euclidean space $(E, V, \langle \cdot, \cdot \rangle)$ of the same dimension (see definition (4.4)). Let $\{b_i\}_{i=1}^m$ be an ordered basis of L and $\{b_i^*\}_{i=1}^m$ be its associated Gram-Schmidt basis. Let $\{\lambda_{i,j}\}_{1 \leqslant j < i \leqslant m}$ be the set of real numbers such that $b_i = b_i^* + \sum_{j<i} \lambda_{i,j} b_j^*$ for all $i \in \{1, \ldots, m\}$ (see proposition (5.7)).

(i) The basis $\{b_i\}_{i=1}^m$ is called *size-reduced* if for all $i \in \{1, \ldots, m\}$ and all $j < i$ we have $|\lambda_{i,j}| \leqslant 1/2$.

(ii) Let $c \in \mathbb{R}, c \geqslant 1$. The basis $\{b_i\}_{i=1}^m$ satisfies the *Lovász condition for c* if for all $\epsilon \in \mathbb{R}_{>0}$ and all $i \in \{2, \ldots, m\}$, we have $q(b_{i-1}^*) \leqslant (c + \epsilon) \cdot q(b_i^*)$.

(iii) A basis satisfying (i) and (ii) above is called *c-reduced.* $\diamondsuit$

One of the main results of this thesis is the theorem below, which is proven in §6.3. For this theorem, a layered lattice is concretely given as

$$(\mathbb{Z}^m, \mathbb{R}^n, \mathbf{B}^1, \ldots, \mathbf{B}^n)$$

where $\mathbb{R}^n$ is anti-lexicographically ordered and the ordered set of *rational* matrices $\mathbf{B}^1, \ldots, \mathbf{B}^n \in \mathrm{M}_m(\mathbb{Q})$ specifies the inner-product by the formula

$$\langle e_i, e_j \rangle = (\mathbf{B}_{i,j}^1, \ldots, \mathbf{B}_{i,j}^n)$$

with $\{e_i\}_{i=1}^m$ denoting the canonical basis of $\mathbb{Z}^m$.

Theorem 1.7. *For each $c \in \mathbb{Q}, c > 4/3$, there is a polynomial-time algorithm that given a layered lattice $(\mathbb{Z}^m, \mathbb{R}^n, \mathbf{B}^1, \ldots, \mathbf{B}^n)$ of rank m, computes a c-reduced basis of this lattice.*

To review some of the definitions on complexity theory including the definition of a polynomial-time algorithm we refer the reader to the last section of this introduction.

We remark that the algorithm of theorem (1.7) is not a direct generalization of the classical LLL algorithm. One might wonder if, and this is highly desirable, performing the steps of the classical LLL algorithm in the layered setting leads to a well-posed, terminating algorithm. We prove this fact in theorem (6.13) of section §6.2. The algorithm one obtains is therefore called the *layered LLL algorithm*. It was not proven that the layered LLL algorithm is polynomial-time, but the author expects it to be the case and we will pursue this line of inquiry in future research.

When $\dim V = 1$ our theory reduces to the classical case of lattices and the LLL algorithm. Therefore, as in that case, not every layered lattice has a c-reduced basis if $c < 4/3$. On the other hand, it is quite easy to show, using the classical theory and some results of this thesis, that every layered lattice admits a 4/3-reduced basis. Our algorithm of theorem (1.7) finds, for a fixed $c > 4/3$ and in polynomial time, a c-reduced basis for an arbitrary layered lattice. No polynomial-time algorithm for computing a 4/3-reduced basis is known even in the classical case.

The rest of this work is divided as follows.

In Chapter 2 we review the necessary background in ordered vector spaces and prove the key result that every finite-dimensional, totally ordered, real vector space is order-isomorphic to $\mathbb{R}^n$ with the anti-lexicographic order.

The theory of *layered Euclidean spaces* is developed in chapter 3. This is the theory concerning itself with the geometry of finite-dimensional real vector spaces endowed with a layered inner-product. Here we define the concept of orthogonality and prove an analogue of the decomposition theorem of Hilbert spaces, i.e., that each subspace of a layered Euclidean space has an orthogonal complement.

Chapter 4 develops the theory of *layered lattices*. For a layered lattice, the discreteness property of a lattice is replaced by the well-ordering of the set of norms of its elements. We prove many results concerning them that are clear analogues of classical results and others that are completely novel.

In chapter 5 we introduce associated Gram-Schmidt bases. As the name suggests there is much in common with the classical Gram-Schmidt orthogonalization procedure although there are some new phenomena, which we will discuss. The chapter ends with the introduction of a polynomial-time algorithm to compute associated Gram-Schmidt bases.

Chapter 6 deals with layered lattice basis reduction. We introduce c-reduced bases of layered lattices and look at some of their properties. In a nutshell, their properties are very similar to the classical c-reduced bases. In fact, one can look at those bases as being "layer-wise" reduced, with the basis vectors

in any one given layer sharing the properties of a classical c-reduced basis (see theorem (6.4) for details).

The short Appendix gives two "implementations" of algorithms presented in the text; one for a layered Gram-Schmidt procedure, another for the layered LLL algorithm.

1.2 Review on ordered sets, and on algebra

A *partially ordered set* is a pair $(S, \leqslant)$ where S is a set and $\leqslant$ is a binary relation on S that is reflexive, transitive and anti-symmetric. By anti-symmetric we mean that if $a, b \in S$ are elements such that $a \leqslant b$ and $b \leqslant a$ then $a = b$. A partially ordered set is also called a *poset*. When the relation is clear from the context we will adopt the custom of denoting the poset $(S, \leqslant)$ by S. If $(S, \leqslant)$ is a poset, we denote the dual relation on S by $\geqslant$. This relation is defined by the condition that $a \geqslant b$ if and only if $b \leqslant a$. Given $a, b \in S$ we write $a < b$ to denote the condition $a \leqslant b$ with $a \neq b$.

A *morphism* of posets $f : S \to T$ is a morphism of the underlying sets with the property that if $a, b \in S$ are such that $a \leqslant b$ then $f(a) \leqslant f(b)$. A *maximal element* of a poset S is an element $m \in S$ such that if $a \in S$ and $m \leqslant a$ then $m = a$. Such an element need not to be unique or exist. There is a corresponding notion of *minimal element* of a poset; it is a maximal element with respect to the dual relation.

A *totally ordered set* is a poset $(S, \leqslant)$ where the relation is total, i.e. for any $a, b \in S$ we have $a \leqslant b$ or $b \leqslant a$. From now on whenever we write ordered set we implicitly mean a totally ordered set. In case we deal with only a partial order we will explicitly say so. For any $n \in \mathbb{Z}_{\geqslant 0}$ we denote by $\underline{n}$ the ordered set $\{1, 2, \ldots, n\}$ and by $\underline{n}_0$ the ordered set $\{0, 1, \ldots, n\}$.

A *well-ordered set* is an ordered set in which any non-empty subset has a minimal element. This element is unique for this subset. Such an order is called a *well-order* on S. If S is a non-empty subset of a well-ordered set we denote its minimum element by $\min S$. For any $s \in S$, the *successor* of s, denoted by $s + 1$, is the element $\min\{t \in S : s < t\} \in S$ in case this set is non-empty (so that its minimum exists). If S is a *finite* ordered set then it is automatically well-ordered. In this case, and only in this case, the dual order on S is also a well-order. The successor of an element $s \in S$ in the dual order is called the *predecessor* of s and denoted by $s - 1$.

Let $\{S_k\}_{k \in K}$ be a family of posets indexed by an ordered set K. Their co-product as sets, i.e., their disjoint union, denoted by $\coprod_{k \in K} S_k$, can be ordered as follows. Let $\pi : \coprod_{k \in K} S_k \to K$ be the map given by $s \mapsto k$ where k is the unique element of K such that $s \in S_k$. Given two elements $s, t \in \coprod_{k \in K} S_k$ we let $s \leqslant t$ if either $\pi(s) < \pi(t)$ or both $\pi(s) = \pi(t)$ and $s \leqslant t$ in $S_{\pi(s)}$. This is

a partial order in $\coprod_{k\in K} S_k$ and is a total order in case all the S_k are totally ordered. In this case, we call this order the *anti-lexicographic* order on the coproduct of the $\{S_k\}_{k\in K}$ *with respect to* K.

Given a finite family of posets $\{S_k\}_{k\in\underline{n}}$, indexed by the ordered set $\underline{n}$, their *product* denoted by $\prod_{k\in\underline{n}} S_k$ is their product as sets with the order given as follows. For $s = (s_k)_{k\in\underline{n}}, t = (t_k)_{k\in\underline{n}} \in \prod_{k\in\underline{n}} S_k$ we set $s \leqslant t$ if either $s = t$ or both $s \neq t$ and $s_l < t_l$ for $l = \max\{k : s_k \neq t_k\}$. This order is called the *anti-lexicographic* order on $\prod_{k\in\underline{n}} S_k$.

Let I be a set and G a group. The I-fold *direct product* of G, denoted by G^I, is the set of maps $I \to G$; it is a group with the operation given component-wise. The I-fold *direct sum* of G is then the subgroup $G^{(I)} \subset G^I$ of functions which take the identity value almost everywhere, i.e., except for a finite subset of I.

In the present work all rings are assumed commutative with unity. Let R be a ring. We denote by $R^\times$ the group of invertible elements of R under multiplication. If I is a set then the group $R^{(I)}$ is an R-module and there is a canonical map $I \to R^{(I)}$ given by mapping $i \in I$ to its *characteristic function* e_i, i.e., the function such that $e_i(i) = 1$ and $e_i(j) = 0$ for $j \neq i$. If M is an R-module then given any map $I \to M$ there is a unique R-linear map $R^{(I)} \to M$ factoring $I \to M$ through the canonical map $I \to R^{(I)}$, i.e., such that the composition $I \to R^{(I)} \to M$ equals $I \to M$. We say that $I \to M$ is *linearly independent* if this induced map is injective and that it *generates* M if this map is surjective. If it both generates M and is linearly independent, we say it is a *basis* for M. A module M is *free* if there exists a basis $I \to M$ for M. If M is a free R-module and $I \to M$ is a basis then the *rank* of M is the cardinal $\#I$ and this is well defined if $R \neq \{0\}$. If $I \to M$ is a basis (or just linearly independent) and $R \neq \{0\}$ then $I \to M$ is injective and, therefore, I can be identified with its image. In such a case, we may represent the basis $I \to M$ by its image $\{m_i\}_{i\in I} \subset M$. By abuse of notation we call $\{m_i\}_{i\in I}$ a basis as well. An *ordered basis* is a basis for which I is ordered.

If I is finite then $R^{(I)} = R^I$ and if I is also ordered then I is order-isomorphic to $\underline{n}$ for $n = \#I$. In this case we write $R^{\underline{n}}$ for this direct sum. For $n \in \mathbb{Z}_{\geqslant 0}$, the *determinant* is the unique n-multilinear, alternating function

$$\det : R^n \times \cdots \times R^n \to R$$

such that $\det(e_1, \ldots, e_n) = 1$. If the elements of R^n are written as "column vectors" we may view the determinant as a function on the set $\mathrm{M}_n(R)$ of n by n matrices over R.

Let M be an R-module. A *filtration* $\mathcal{F}$ of M is a totally ordered subset of the poset $\mathrm{Sub}(M)$ comprised of all submodules of M partially ordered by inclusion. A filtration $\mathcal{G}$ of M is a *refinement* of $\mathcal{F}$ if $\mathcal{F} \subset \mathcal{G}$.

Now let R be a field or the ring of integers $\mathbb{Z}$ and M be a free R-module. A *flag* of M is a filtration $\mathcal{F}$ satisfying two conditions. First, the elements of $\mathcal{F}$ are *pure* submodules, i.e., for all $N \in \mathcal{F}$ the quotient M/N is free. Second, the filtration is *maximal* among the filtrations by pure submodules, i.e., satisfying the first condition. If M is finitely generated and $n = \operatorname{rank} M$ then a flag of M is nothing but a set $M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_n$ of pure submodules where $\operatorname{rank} M_i = i$ for all $i \in \underline{n}_0$. Given an ordered basis $\{m_k\}_{k \in \underline{n}}$ of M, there is a canonical filtration associated to this basis. Namely, for each $k \in \underline{n}_0$ one sets $M_k = \operatorname{span}\{m_l : l \leqslant k\}$. We denote this flag by $\mathcal{F}(I \to M)$ or $\mathcal{F}(\{m_k\}_{k \in \underline{n}})$.

1.3 Review on complexity theory

It is important, especially for chapters 5 and 6, to give a quick review of some results from complexity theory. Words like *input*, *output*, *arithmetical complexity*, *binary complexity* and *polynomial-time* should be well-known to anyone working with algorithms on a theoretical level. To precisely define these terms here would take us too far afield so we refer the reader to [13, Chapter 2] where all of this can be found; we contend ourselves with some general remarks.

For us, an algorithm can be thought as a procedure that can be given to a computer, a Turing machine for example, and that "implements" a function $f : \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0}$, i.e., given $n \in \mathbb{Z}_{\geqslant 0}$, this algorithm computes $f(n)$. A good example of an algorithm is the Euclidean algorithm, which on input $p, q \in \mathbb{Z}$ computes the greatest common divisor of the pair (p, q), i.e., the unique number $r \in \mathbb{Z}_{\geqslant 0}$ such that we have $\mathbb{Z}r = \mathbb{Z}p + \mathbb{Z}q$. One might argue that, phrased in this way, the input of the Euclidean algorithm is not really a positive integer n but this is immaterial (for the purpose of what an algorithm *is*) since one can "encode" the input in terms of positive integers, i.e., find a way of representing a pair (p, q) by an integer $n > 0$.

Of course in the realm of algorithms we have special interest in finding efficient ones. The word "efficient" here already entails some discussion (now, for example, even the encoding referred to in the last paragraph is of importance as it has to be efficient as well) but the concept of a *polynomial-time* algorithm seems to have stood the test of time.

Definition 1.8. (i) Let $f, g : \mathbb{Z}_{\geqslant 0} \to \mathbb{R}$ be two functions. We say that f is *big-O of* g, denoted by $f \in O(g)$, if there exists $M \in \mathbb{R}_{>0}$ such that for all $n \in \mathbb{Z}_{\geqslant 0}$ we have $|f(n)| \leqslant M|g(n)|$.

(ii) Let F be a field. By an *arithmetical operation* in F we mean one instantiation of an algorithm that performs the sum, subtraction, multiplication or division of two elements of F (the first by the second in the case of subtraction and division).

(iii) By a *binary operation* we mean an arithmetic operation in the field $\mathbb{F}_2$ of two elements.

The importance of this definition is that a binary operation, *for all practical purposes*, is the atomic unit in which algorithms are evaluated qua efficiency. To elaborate, since computers are universal Turing machines working almost exclusively with bits or a fixed-sized string of bits, an algorithm implemented on a computer will, for any given input $n \in \mathbb{Z}_{\geqslant 0}$, perform a series of binary operations. One counts how many of these the algorithm takes to compute the output associated to this given input, and this number is a measure of the efficiency of the algorithm. In practice, one gives bounds for the number of binary operations in terms of the binary length of the input ($\log_2 n$ in our notation).

Definition 1.9. An algorithm is called *polynomial-time* if there exists a polynomial $f \in \mathbb{Q}[x]$ such that for any given input $n \in \mathbb{Z}_{\geqslant 0}$, the number of binary operations performed by the algorithm to compute the associated output is bounded by $f(\log_2 n)$. $\diamondsuit$

If c denotes the *cost* function of the algorithm, i.e., for any $n \in \mathbb{Z}_{\geqslant 0}$, the number of binary operations performed by the algorithm on input n is $c(n)$, then the algorithm is polynomial-time if there exists $f \in \mathbb{Q}[x]$ such that $c \in O(f \circ \log_2)$.

1.4 Notation

To facilitate the reading of this work we give a list of the more "non-standard" notations used together with a reference to where the respective definition can be found.

Notation	**Description**	**Reference**
$A \subset B$	The set A is a subset of the set B with, possibly, an equality of sets.	
$A \subsetneqq B$	The set A is a *proper* subset of the set B, i.e., $A \subset B$ and $A \neq B$ hold.	
$\underline{m}$	For $m \in \mathbb{Z}_{\geqslant 0}$ denotes the ordered set $\{1, 2, \ldots, m\}$.	Section 1.1
$\underline{m}_0$	For $m \in \mathbb{Z}_{\geqslant 0}$ denotes the ordered set $\{0, 1, \ldots, m\}$.	Section 1.1

Notation	Description	Reference
$I^{\underline{m}}$	For $m \in \mathbb{Z}_{\geqslant 0}$ and I an ordered set, denotes the m-fold product of I anti-lexicographically ordered with respect to $\underline{m}$.	Section 1.1
$R_{\geqslant 0}$, $R_{>0}$	For an ordered ring R, respectively, denotes the subset of non-negative elements and the subset of positive elements.	
$R^{\times}$	For a ring R, denotes its group of units, i.e., the group of invertible elements of R.	
$R^{\underline{n}}$	For an ordered ring R denotes the n-fold direct sum of R ordered anti-lexicographically.	Section 1.1
$\mathrm{M}_m(R)$, $\mathrm{M}_{m\times n}(R)$	Respectively, the sets of m by m and m by n matrices over the ring R.	
$\mathrm{GL}_m(R)$	The group $M_m(R)^{\times}$ of invertible m by m matrices over the ring R.	
$\mathcal{F}(\{m_i\}_{i\in I})$, $\mathcal{F}(I \to M)$	The flag associated to a basis of a vector space or of a lattice.	Section 1.1
$\diamondsuit$	Signals the end of a definition.	
$\square$	Signals the end of a proof.	
$\mathcal{C}(V)$	The filtration of convex susbspaces of an ordered vector space V.	(2.16)
$\mathcal{C}^*(V)$	$\mathcal{C}(V) \setminus \{\{0\}\}$.	
$\mathcal{C}(u)$	The convex subspace spanned by u.	(2.16)
$u \preccurlyeq v$	Reads: u is "dominated" by v, i.e., $\mathcal{C}(u) \subset \mathcal{C}(v)$.	(2.16)
$u \ll v$	Reads: u is "infinitesimal" with respect to v, i.e., $\mathcal{C}(u) \subsetneqq \mathcal{C}(v)$ or $u = 0$.	(2.16)
$u \sim v$	Reads: u is "comparable" to v, i.e., $\mathcal{C}(u) = \mathcal{C}(v)$.	(2.16)
$u \simeq v$	Reads: u is "infinitely close" to v, i.e., $u - v \ll v$.	(2.16)
$S(V)$, $S^m(V)$	The (graded) symmetric algebra of a vector space V and its m-th homogeneous subspace.	(2.26)

Notation	**Description**	**Reference**
E_U	The U-th layer of a layered Euclidean space E.	(3.3)
L_U	The U-th layer of a layered lattice L.	(4.18)
$\mathcal{L}(E), \mathcal{L}(L)$	The ordered set of layers of a layered Euclidean space E or of a layered lattice L.	(3.3) and (4.18)
$\mathcal{L}(x)$	The layer of x; equals $E_{\mathcal{C}(q(x))}$.	(3.3)
$(\cdot, x)$	For each x in a layered Euclidean space this denotes a special kind of functional associated to x.	(5.5)
$f \in O(g)$	Reads: f is big-O of g and means that $\lvert f \rvert$ is bounded by a constant multiple of $\lvert g \rvert$.	(1.8)

CHAPTER 2

Ordered vector spaces

In this chapter we review some results on ordered algebraic structures, specifically, ordered vector spaces. We prove that in the case the field in question is the field of real numbers there is essentially only one type of totally ordered vector space of dimension n for each $n \in \mathbb{Z}_{\geqslant 0}$. A generalization of this result can be found in [6] but, for completeness, we give this special case here in full detail.

2.1 Ordered rings and fields

Definition 2.1. An *ordered ring* is an ordered set $(R, \leqslant)$ where R is a ring and $\leqslant$ satisfies the following conditions.

(i) For all $a, b, c \in R$ such that $a \leqslant b$ we have $a + c \leqslant b + c$.

(ii) For all $a, b \in R$ such that $0 < a$ and $0 < b$ we have $0 < ab$.

An element $a \in R$ such that $0 < a$ is called *positive*. An *ordered field* is an ordered ring which is also a field. $\diamondsuit$

Remark 2.2. (a) It is easy to see that in an ordered ring R we have $0 \leqslant 1$. Thus, by repeatedly using (i) above, if $1 \neq 0$ in R then $n \cdot 1$ is positive for all $n \in \mathbb{Z}_{\geqslant 0} \setminus \{0\}$. Hence, if $R \neq \{0\}$ then R has characteristic zero. In particular, if F is an *ordered field* then F is an extension of $\mathbb{Q}$.

(b) It is an easy consequence of (i) and (ii) above that if $a, b, c \in R$ with $a \leqslant b$ and $0 \leqslant c$ then $ac \leqslant bc$.

Proposition 2.3. *Let $(R, \leqslant)$ be an ordered ring with $R \neq \{0\}$. Then R is a domain. The quotient field of R is an ordered field under the relation*

$$\frac{a}{b} \leqslant \frac{c}{d} \iff ad \leqslant bc$$

where b and d are taken positive.

Proof. That R is a domain follows immediately from axiom (ii) above. Let $a/b, c/d, e/f \in F$ with b, d, f positive, $a/b \leqslant c/d$ and $c/d \leqslant e/f$. We have

$$ad \leqslant bc, \quad cf \leqslant de.$$

Multiplying the first of these inequalities by f and the second by b we obtain

$$adf \leqslant bcf \leqslant edb.$$

Using that d is positive and the contrapositive of item (b) of remark (2.2) we obtain $af \leqslant eb$, that is to say, $a/b \leqslant e/f$. From the above argument it not only follows that $\leqslant$ is transitive but also that $\leqslant$ is well-defined for if $a/b = c/d$ and $c/d \leqslant e/f$ then $a/b \leqslant e/f$ too. Finally, the relation is clearly reflexive and anti-symmetric, thus, an order on F. It is straight-forward to check that $(F, \leqslant)$ is an ordered field. □

Proposition 2.4. *Let F be an ordered field. Then the set of positive elements of F is a subgroup of $F^\times$ of index 2.*

Proof. Follows from results in [1, Chapter 6, § 2]. □

Proposition 2.5. *Let $\leqslant$ be an order on $\mathbb{Q}$ such that $(\mathbb{Q}, \leqslant)$ is an ordered field. Then $\leqslant$ is the usual order.*

Proof. See [1, Chapter 6, § 2]. □

Definition 2.6. Let F be an ordered field. We say F is *Archimedean* if for each positive $a \in F$ there exists $n \in \mathbb{Z}_{\geqslant 0}$ such that $a < n \cdot 1$. ♢

The following result is an easy consequence of the uniqueness of the field of real numbers as a complete, Archimedean ordered field.

Proposition 2.7. *Let F be an Archimedean ordered field. Then F embeds into $\mathbb{R}$ as an ordered field, i.e., F is order isomorphic to a subfield of $\mathbb{R}$.*

Proof. See [4, Propositions 6.1.1 and 6.3.1]. □

2.2 Ordered vector spaces

Definition 2.8. Let F be an ordered field. An *ordered F-vector space* is an ordered set $(V, \leqslant)$ where V is an F-vector space and $\leqslant$ satisfies the following conditions.

(i) For all $u, v, w \in V$ such that $u \leqslant v$ we have $u + w \leqslant v + w$.

(ii) For all $u \in V$ and all $\lambda \in F$ such that $0 \leqslant u$ and $0 \leqslant \lambda$ we have $0 \leqslant \lambda u$.

An element $u \in V$ such that $0 < u$ is called *positive* and the set $P = \{u \in V : 0 < u\}$ is called the *positive cone* of V. A *morphism* of ordered vector spaces $V \to W$ is a morphism of the underlying posets which is also a morphism of vector spaces, i.e., F-linear. $\diamondsuit$

In the remainder of this chapter F will denote an ordered field.

Lemma 2.9. *Let V be a one-dimensional, ordered F-vector space. For any positive $\lambda \in F$ the map $x \mapsto \lambda x$ is an order automorphism of V. Conversely every order automorphism is of this form for some $\lambda \in F$ positive. The dual order on V is the only other relation making V into an ordered F-vector space.*

Proof. An automorphism of V is of the form $x \mapsto \lambda x$ for $\lambda \in F$. If $\lambda < 0$ then clearly it reverses the order and is, thus, not an order isomorphism. Let $\leqslant'$ be another order on V. If $v \in V$ is a non-zero vector with $0 < v$ then either $0 <' v$ in which case $\leqslant$ and $\leqslant'$ are the same or $v' < 0$ in which case $\leqslant'$ is the order dual to $\leqslant$. $\square$

Example 2.10. Let K be an ordered set and $\{V_k\}_{k \in K}$ be a sequence of ordered F-vector spaces. Let $V = \bigoplus_{k \in K} V_k$ and $u = (u_k)_{k \in K}, v = (v_k)_{k \in K}$ be elements of V. We define $u \leqslant v$ if either $u = v$, or $u \neq v$ and $u_l \leqslant v_l$ for $l = \max\{k \in K : u_k \neq v_k\}$. Note that such l exists since u and v have finite support. We obtain an order on V, which we call the anti-lexicographic order. With this order, V is an ordered vector space.

Definition 2.11. Let K be an ordered set and $\{V_k\}_{k \in K}$ be a sequence of ordered F-vector spaces. The ordered vector space $V = \bigoplus_{k \in K} V_k$ with the order described in example (2.10) is called the *anti-lexicographic sum* of $\{V_k\}_{k \in K}$. $\diamondsuit$

Throughout our work, whenever we consider $F^{(K)}$ as an ordered vector space we implicitly assume the order to be the anti-lexicographic order, i.e., we set $V_k = F$ for all $k \in K$ in the construction above.

Definition 2.12. Let V be an ordered F-vector space. We say the order on V is *anti-lexicographic* or that V is *anti-lexicographically ordered* if there exists

an ordered basis $K \to V$ such that the resulting isomorphism $F^{(K)} \simeq V$ is an isomorphism of ordered vector spaces. Any such basis is called an *anti-lexicographic basis.* ♢

Definition 2.13. Let V be an ordered F-vector space and P its positive cone. We define the function $|\cdot| : V \to P \cup \{0\}$, called the *absolute value* function, by the formula

$$|v| = \begin{cases} v, \text{ if } v \in P \text{ or } v = 0 \\ -v, \text{ otherwise.} \end{cases}$$

♢

Definition 2.14. Let V be an ordered F-vector space. A subset $U \subset V$ is *convex* if for all $v \in V$ such that there exists $u \in U$ satisfying $|v| \leqslant |u|$ we have $v \in U$. The set of convex subspaces of V we denote by $\mathcal{C}(V)$. ♢

Proposition 2.15. *Let V be an ordered F-vector space.*

(a) *The set of convex subspaces of V is totally ordered by inclusion.*

(b) *Let $\{U_k\}_{k\in K}$ be a family of convex subspaces. Then $\bigcap_{k\in K} U_k$ and $\bigcup_{k\in K} U_k$ are convex subspaces.*

Proof. (a) Let U and W be convex subspaces and $u \in U, w \in W$. If $|u| \leqslant |w|$ then by the convexity of W we have $u \in W$. This means that if $U \setminus W \neq \varnothing$ and $u \in U \setminus W$ then we have $|u| > |w|$. Then by the convexity of U we have $w \in U$. Since w is arbitrary in this argument we conclude that $W \subset U$. Similarly, if $W \setminus U \neq \varnothing$ one obtains $U \subset W$. Supposing that $U \neq W$, one of those conditions must hold. This shows that $\mathcal{C}(V)$ is totally ordered by inclusion.

(b) Let $u \in \bigcap_{k\in K} U_k$ and $v \in V$ with $0 \leqslant |v| \leqslant |u|$. By the convexity of U_k we have $v \in U_k$ for all k thus $v \in \bigcap_{k\in K} U_k$. A very similar argument shows that $\bigcup_{k\in K} U_k$ is convex since it is a subspace by (a) above. □

Definition 2.16. Let V be an ordered F-vector space. The ordered set $\mathcal{C}(V)$ of convex subspaces of V is called the *convex filtration* of V. The *convex subspace generated by* $v \in V$, denoted by $\mathcal{C}(v)$, is the element $\bigcap\{U \in \mathcal{C}(V) : v \in U\}$ of $\mathcal{C}(V)$. We define the following binary relations on V:

$$\begin{aligned} u \preccurlyeq v &\iff \mathcal{C}(u) \subset \mathcal{C}(v) \\ u \ll v &\iff \mathcal{C}(u) \subsetneqq \mathcal{C}(v) \text{ or } u = 0 \\ u \sim v &\iff \mathcal{C}(u) = \mathcal{C}(v) \\ u \simeq v &\iff u - v \ll v \end{aligned}$$

♢

Remark 2.17. Note that the convex filtration is a filtration in the sense we defined in the review section of the introduction. Also, it is obvious that if $u \ll 0$ then $u = 0$ and, thus, if $u \simeq 0$ then $u = 0$ and similarly, if $0 \simeq v$ then $v = 0$. It is an easy exercise to show that if $u \simeq v$ then $u \sim v$. Hence, the relation $\simeq$ is actually symmetric. Since it is also reflexive and transitive, it is an equivalence relation on V.

Notation. For an ordered vector space V we denote the subset $\mathcal{C}(V) \setminus \{\{0\}\}$ of $\mathcal{C}(V)$ by $\mathcal{C}^*(V)$.

Lemma 2.18. *Let V be an ordered F-vector space and $v \in V$. Then we have*

$$\mathcal{C}(v) = \{u \in V : \exists \lambda \in F : |u| \leqslant \lambda v\}.$$

Proof. Denote the righthand side of the equation above by U. By using that $|v + v'| \leqslant |v| + |v'|$ for all $v, v' \in V$, it is easy to show that U is a subspace. If $w \in V$ is such that there exists $u \in U$ with $|w| \leqslant |u|$ then by the definition of U there is also a $\lambda \in F$ such that $|u| \leqslant \lambda|v|$. By transitivity we have $|w| \leqslant \lambda|v|$ and thus $w \in U$. This shows that U is convex. By the definition of $\mathcal{C}(v)$ we have $\mathcal{C}(v) \subset U$.

For the other inclusion, let $u \in U$. Then we have $|u| \leqslant \lambda|v|$ for some $\lambda \in F$. Since $\lambda|v| \in \mathcal{C}(v)$, by the convexity of the latter is follows that $u \in \mathcal{C}(v)$. Thus we have $U \subset \mathcal{C}(v)$. □

The following examples illustrate the connection between convex subspaces and anti-lexicographic orders. This relation is formalized in the next proposition and, intuitively, it is the fact that every finite-dimensional ordered vector space can be decomposed, in a canonical way, into an anti-lexicographic sum such that the "partial sums" of its components are precisely its convex subspaces.

Example 2.19. The convex filtration of $\mathbb{Q}^{\underline{n}}$ is the set

$$\left\{ \bigoplus_{l=1}^{k} \mathbb{Q}e_l : k \in \underline{n}_0 \right\},$$

ordered by inclusion, where $\{e_1, \ldots, e_n\}$ denotes the canonical basis of $\mathbb{Q}^{\underline{n}}$. This can easily be checked from the definitions. Also note that the basis inducing the sequence above is not unique if $n > 0$.

Example 2.20. Let $\zeta \in \mathbb{R} \setminus \mathbb{Q}$ and $V = \mathbb{Q} \cdot 1 + \mathbb{Q} \cdot \zeta \subset \mathbb{R}$ viewed as an ordered two-dimensional rational subspace. I claim that $\mathcal{C}(V) = \{\{0\}, V\}$. In fact, let $U \neq V$ be a convex subspace. Then there exists positive rational numbers r, s such that for all $n \in \mathbb{Z}_{\geqslant 0}$ and all $u \in U$ we have $n|u| < r + s\zeta \in \mathbb{R}$. Since $\mathbb{R}$ is Archimedean this forces $U = \{0\}$ as claimed. Since the set of convex subspaces of $\mathbb{Q}^{\underline{2}}$ is $\{\{0\}, \mathbb{Q}(1,0), \mathbb{Q}^2\}$, this shows that the order on V is not anti-lexicographic, i.e., there does not exist an order isomorphism between $\mathbb{Q}^{\underline{2}}$ and V.

Proposition 2.21. *Let U be a convex subspace of an ordered F-vector space V. Denote the equivalence class of $v \in V$ in V/U by $\overline{v}$ and define on V/U the*

relation $\overline{v_1} \leqslant \overline{v_2}$ *if either* $\overline{v}_1 = \overline{v}_2$*, or* $\overline{v}_1 \neq \overline{v}_2$ *and* $v_1 \leqslant v_2$*. Then* $(V/U, \leqslant)$ *is an ordered vector space.*

Let $U \oplus V/U$ *be the anti-lexicographic sum of* U *and* V/U *and* $s : V/U \to V$ *be a linear section of the projection* $V \to V/U$*. Then the map* $U \oplus V/U \to V$ *given by*

$$(u, \overline{v}) \mapsto u + s(\overline{v})$$

is an isomorphism of ordered vector spaces.

Proof. To show that the relation $\leqslant$ on V/U is well-defined it suffices to show that if $v_1 \leqslant v_2$ with $\overline{v}_1 \neq \overline{v}_2$ then $v_1 + u \leqslant v_2$ for all $u \in U$. In fact, since $v_2 - v_1 \notin U$ is positive, the convexity of U immediately implies that for any $u \in U$ we have $|u| < v_2 - v_1$ from which the claim follows.

That this binary relation is an order and that V/U is an ordered F-vector space with this order follows immediately from the properties of the order $\leqslant$ on V.

The only remaining assertion to prove is that the map $(u, \overline{v}) \mapsto u + s(\overline{v})$ is an isomorphism of ordered vector spaces. By general results from linear algebra this map is an isomorphism of vector spaces so it suffices to show that if $0 \leqslant (u, \overline{v})$ in $U \oplus V/U$ then $0 \leqslant u + s(\overline{v})$ in V. In case $\overline{v} = 0$ then from $s(\overline{v}) = 0$ we obtain $0 \leqslant u$ as desired. If $0 < \overline{v}$ then we have $0 < v$ in V and $s(\overline{v}) = v + u'$ for some $u' \in U$. Thus, by what was proven in the first paragraph, we have $0 - u - u' < v$, i.e., $0 < u + (v + u') = u + s(\overline{v})$ as was to be shown. □

Corollary 2.22. *Let* V *be an ordered vector space of finite dimension. Then there is a canonical isomorphism of ordered vector spaces*

$$V \simeq \bigoplus_{U \in \mathcal{C}^*(V)} U/U'$$

where U' *denotes the predecessor of* U *in* $\mathcal{C}(V)$ *.*

Proof. We proceed by induction on the dimension of V. The case $V = \{0\}$ is trivial. For $V \neq \{0\}$, let V' denote the predecessor of V in $\mathcal{C}(V)$. By induction, we have a canonical isomorphism of ordered vector spaces

$$V' \simeq \bigoplus_{U \in \mathcal{C}^*(V')} U/U'.$$

Combining this with the order isomorphism $V \simeq V' \oplus V/V'$ obtained from the previous proposition applied to V' we get

$$V \simeq \left(\bigoplus_{U \in \mathcal{C}^*(V')} U/U' \right) \oplus V/V' = \bigoplus_{U \in \mathcal{C}^*(V)} U/U'$$

as an anti-lexicographic sum. □

2.3 Real ordered vector spaces

We now prove the main result of this chapter. It is a particular case of a result in [6], which we give here for completeness. We first prove the following lemma. Recall definition (2.16) where we introduced the several relations on elements of an ordered vector space.

Lemma 2.23. *Let V be an ordered vector space over $\mathbb{R}$. Let $u, v \in V$ with v positive and $u \preccurlyeq v$. Then there exists a unique $\gamma \in \mathbb{R}$ such that $u - \gamma v \ll v$.*

Proof. Since $u \preccurlyeq v$ there exists $\nu \in \mathbb{R}$ positive, such that $|u| < \nu v$. Thus, the sets $A = \{\lambda \in \mathbb{R} : \lambda v \leqslant u\}$ and $B = \{\mu \in \mathbb{R} : u < \mu v\}$ are non-empty. Further, for all $\lambda \in A$ and all $\mu \in B$ we have

$$\lambda v \leqslant u < \mu v \implies (\lambda - \mu)v < 0 \implies \lambda < \mu.$$

Thus, A is bounded above, B is bounded below and $A \cap B = \varnothing$. We have $\mathbb{R} = A \cup B$ since $\leqslant$ is total and thus $\sup A = \inf B$. Denoting this number by γ we have, by construction,

$$(\gamma - \epsilon)v < u < (\gamma + \epsilon)v$$

for all $\epsilon > 0$. Equivalently, we have $|u - \gamma v| < \epsilon v$ for all $\epsilon > 0$. By lemma (2.18) we have $\mathcal{C}(u - \gamma v) \subset \mathcal{C}(v)$ and $\mathcal{C}(v) \neq \mathcal{C}(u - \gamma v)$. Thus, we conclude that $u - \gamma v \ll v$. □

Remark 2.24. The above lemma implies that for a *real* ordered vector space V, it is impossible to have a situation like in example (2.20) where there was no convex subspace of V of codimension 1.

Theorem 2.25. *Let V be a finite-dimensional ordered real vector space. Then V admits an anti-lexicographic basis.*

Proof. By proposition (2.22) it suffices to show that the convex filtration of V has $(\dim V) + 1$ elements. If $V = \{0\}$ there is nothing to prove and by induction on the dimension of V, it is enough to show that V admits a convex subspace of codimension one.

Let $U = \max\{\mathcal{C}(v) : v \in V\} \subset V$. This element of $\mathcal{C}(V)$ exists since V is finite-dimensional. If $U \neq V$ then there exists $v \in V \setminus U$ and we have $v \in \mathcal{C}(v) \subset U \subset V$ which is a contradiction. Thus $U = V$ and it follows that $V = \mathcal{C}(v)$ for some $v \in V$, which we can choose such that $v > 0$.

Since $\mathcal{C}(V)$ is finite and $\#\mathcal{C}(V) > 1$, the space V has a predecessor in $\mathcal{C}(V)$, which we denote by W. We claim that W has codimension 1 in V. Let $u \in V$. Since $V = \mathcal{C}(v)$ we have $u \preccurlyeq v$. By the lemma above, there exists a unique $\gamma \in \mathbb{R}$ such that $u - \gamma v \ll v$. Thus $u - \gamma v \in W$ and $V/W \simeq \mathbb{R}v$. □

2.4 Symmetric powers

As before let F be an ordered field. In the last section of this chapter we will study the symmetric powers of an F-vector space in the context of ordered algebraic structures.

Definition 2.26. Let V be an F-vector space, let $r \in \mathbb{Z}_{>0}$, and let $\mathrm{Sym}(r)$ denote the symmetric group on $\underline{r} = \{1, \dots, r\}$. Let $V^{\otimes r}$ denote the *r-fold tensor product* of V. The r-th *symmetric power* of V, denoted by $S^r(V)$, is the quotient of $V^{\otimes r}$ by the subspace spanned by the *commutation relations*:

$$\big\{v_1 \otimes \cdots \otimes v_r - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(r)} : v_1, \dots, v_r \in V,\ \sigma \in \mathrm{Sym}(r)\big\}.$$

The class of a generator $v_1 \otimes \cdots \otimes v_r$ is denoted by $v_1 \dots v_r$. We define $V^{\otimes 0} = F$.

The graded ring

$$S(V) = \bigoplus_{r \in \mathbb{Z}_{\geqslant 0}} S^r(V)$$

is the *symmetric algebra* of V. ♢

As a ring, $S(V)$ is the quotient of the *tensor algebra* $T(V)$ of V by the ideal $I = \bigoplus_{r \in \mathbb{Z}_{\geqslant 0}} I_r$ where I_r is the ideal generated by the commutation relations on $V^{\otimes r}$. Note that if $W \subset V$ is a subspace then for all $r \in \mathbb{Z}_{\geqslant 0}$ we have $S^r(W) \subset S^r(V)$. We refer the reader to [7, Chapter XVI, §8] for further details.

Notation. Let $\{v_i\}_{i \in \underline{n}}$ be a basis of an F-vector space V and $r \in \mathbb{Z}_{\geqslant 0}$. There is a canonical basis of $S^r(V)$ induced by this basis of V. Namely, let

$$P(r) = \{(p_1, \dots, p_n) \in (\underline{r}_0)^n : p_1 + \cdots + p_n = r\} \tag{2.27}$$

and for each $p = (p_1, \dots, p_n) \in P(r)$ let $v^p = v_1^{p_1} \dots v_n^{p_n} \in S^r(V)$. Then the map $P(r) \to S^r(V)$ given by $p \mapsto v^p$ is the aforementioned basis of $S^r(V)$. This follows from [7, Chapter XVI, Proposition 8.1] for example. Note that $r = 0$ is consistent. We have $P(0) = \{0 = (0, \dots, 0)\}$ and defining $v_k^0 = 1 \in F$ for any k we obtain $v^0 = 1 \in F$ as the induced basis of $S^0(V) = F$. An element of $S^r(V)$ can be uniquely written as $\sum_{p \in P} \lambda_p v^p$ with $\lambda_p \in F$. Furthermore, looking at $\{v_i\}_{i \in \underline{n}}$ as an *ordered* basis we see that $P(r)$ is ordered as a subset of the ordered set $(\underline{r}_0)^n$ (the latter is the $\underline{n}$-fold anti-lexicographic product of $\underline{r}_0$ as described in the review section of the introduction).

Proposition 2.28. *Let V be an F-vector space and V_1, V_2 be subspaces such that $V = V_1 \oplus V_2$. Let $\{v_i\}_{i \in \underline{k}}$ and $\{u_j\}_{j \in \underline{l}}$ be bases for V_1 and V_2 respectively. Let $r \in \mathbb{Z}_{\geqslant 0}$. Then for all $s, t \in \mathbb{Z}_{\geqslant 0}$ such that $s + t = r$, the map $S^s(V_1) \times S^t(V_2) \to S^r(V)$ given on basis vectors by $(v^p, u^q) \mapsto v^p u^q$ where $p \in P(s)$ and*

$q \in P(t)$ induces an injective linear map $S^s(V_1) \otimes S^t(V_2) \to S^r(V)$. Identifying the domain of this map with its image we have a direct sum decomposition

$$S^r(V) = \bigoplus_{s+t=r} S^s(V_1) \otimes S^t(V_2).$$

Proof. See [7, Chapter XVI, Proposition 8.2]. □

We will use the above proposition to define an order on $S^r(V)$ in such a way that if V is an ordered vector space and $\{v_i\}_{i \in \underline{n}}$ is an anti-lexicographic basis of V then the map $P(r) \to S^r(V)$ given by $p \mapsto v^p$ is an anti-lexicographic basis of $S^r(V)$. Later on we will prove that the resulting order depends only on the order of V; in particular, it is independent of the choice of the anti-lexicographic basis $\{v_i\}_{i \in \underline{n}}$ of V.

So fix $r \in \mathbb{Z}_{\geqslant 0}$ and an anti-lexicographic basis $\{v_k\}_{k \in \underline{n}}$ of V (note that this implies that all v_k are positive). Denote $\mathbb{R}v_k$ by V_k. So, $V_1 \oplus \cdots \oplus V_n$ is a decomposition of V in an anti-lexicographic sum of one-dimensional subspaces. Then the proposition above gives

$$S^r(V) \simeq \bigoplus_{p \in P(r)} S^{p_1}(V_1) \otimes \cdots \otimes S^{p_n}(V_n). \tag{2.29}$$

From the given basis $\{v_k\}$ of V_k we obtain a basis $\{v_k^{p_k}\}$ of $S^{p_k}(V_k)$. Since $v_k > 0$, from the two possible orders of $S^{p_k}(V_k)$ (see lemma (2.9)) we choose the one for which $v_k^{p_k}$ is positive for compatibility. The aforementioned lemma implies that this choice is independent of the choice of the basis v_k of V_k so long as $v_k > 0$. A basis for $S^{p_1}(V_1) \otimes \cdots \otimes S^{p_n}(V_n)$ is now $\{v_1^{p_1} \dots v_n^{p_n}\}$ and the order on this space is the unique one where this basis is positive.

By (2.29) we can order $S^r(V)$ as the anti-lexicographic sum of the one-dimensional ordered vector spaces appearing on the right hand side.

Finally, we order the symmetric algebra as the anti-lexicographic sum of the $S^r(V)$ for $r \in \mathbb{Z}_{\geqslant 0}$. This resulting order on $S^r(V)$ is anti-lexicographic. Let $P_0(r) = \{0\} \coprod P(r)$ be the ordered disjoint union of $\{0\}$ and $P(r)$, which amounts to saying that we introduce 0 as the minimum of $P_0(r)$. The convex filtration of $S^r(V)$ is $\{S_p^r(V)\}_{p \in P_0(r)}$ where we set $S_0^r(V) = \{0\}$ and, for $p \neq 0$,

$$S_p^r(V) = \bigoplus_{q \in P(r), q \leqslant p} S^{q_1}(V_1) \otimes \cdots \otimes S^{q_n}(V_n). \tag{2.30}$$

Furthermore, the choice of the order on $P(r)$ is such that, identifying V with $S^1(V)$, the order resulting from the above construction is the same as the order on V. These observations hint that the order on $S^r(V)$ is *independent* of the choice of the decomposition $V_1 \oplus \cdots \oplus V_n$ of V (and thus, of the anti-lexicographic basis $\{v_1, \dots, v_n\}$ inducing it). We prove this in the following lemma but we first introduce the following definition.

Definition 2.31. Let V be a finite-dimensional, anti-lexicographically ordered, F-vector space and $\{v_k\}_{k\in\underline{n}}$ an anti-lexicographic basis of V. We define the functions $\deg : S(V)\backslash\{0\} \to \mathbb{Z}_{\geqslant 0}$ and $\mathrm{lt} : S(V) \to S(V)$ and $\mathrm{lc} : S(V) \to F$ called respectively, the *degree*, *leading term* and *leading coefficient* functions, as follows.

(i) We define $\mathrm{lt}(0) = 0$ and $\mathrm{lc}(0) = 0$.

(ii) Let $s \in S^r(V)$, $s \neq 0$, for some $r \in \mathbb{Z}_{\geqslant 0}$. We define $\deg(s) = r$. Write $s = \sum_{p\in P(r)} \lambda_p v^p$ where $\{v_p : p \in P(r)\}$ is the anti-lexicographic basis of $S^r(V)$ as in (2.27) and let $q = \max\{p \in P(r) : \lambda_p \neq 0\}$. We define $\mathrm{lt}(s) = \lambda_q v^q$ and $\mathrm{lc}(s) = \lambda_q$.

(iii) Let $s \in S(V)$, $s \neq 0$. Write $s = \sum_{r\in\mathbb{Z}_{\geqslant 0}} s_r$ where $s_r \in S^r(V)$, and let $d = \max\{r \in \mathbb{Z}_{\geqslant 0} : s_r \neq 0\}$. We define $\deg(s) = d$ and $\mathrm{lt}(s) = \mathrm{lt}(s_d)$ and $\mathrm{lc}(s) = \mathrm{lc}(s_d)$. $\diamondsuit$

Remark 2.32. (a) Note that $\mathrm{lt}(s)$ and $\mathrm{lc}(s)$ depend on the anti-lexicographic basis $\{v_1, \dots, v_n\}$ of V chosen. Even so, we avoid expressing this in the notation since whenever we use these functions the basis in use will be clear from the context.

(b) It is straight-forward to see that both functions are multiplicative, i.e., $\mathrm{lt}(st) = \mathrm{lt}(s)\mathrm{lt}(t)$ for any $s, t \in S(V)$ (and the same holds for lc).

(c) For any $s \in S(V)$ we have $\mathcal{C}(s) = \mathcal{C}(\mathrm{lt}(s))$, i.e., the convex space generated by s is the same as the one generated by its leading term. In fact, we have the following slightly stronger statements. For all $s \in S(V)$ we have $s \simeq \mathrm{lt}(s)$. For all s, $t \in S(V)$ we have $s \simeq t$ if and only if $\mathrm{lt}(s) = \mathrm{lt}(t)$.

We now give the promised lemma.

Lemma 2.33. *Let $S^r(V)$ be ordered via the construction above with respect to a fixed anti-lexicographic basis $\{v_1, \dots, v_n\}$ of V. Let $u_1, \dots, u_r, w_1, \dots, w_r \in V$ with $u_k \preccurlyeq w_k$ for all $k \in \underline{r}$. Then $u_1 \dots u_r \preccurlyeq w_1 \dots w_r$ in $S^r(V)$. Furthermore, if all w_k are non-zero and for at least one $k \in \underline{r}$ we have $u_k \ll w_k$ then $u_1 \dots u_r \ll w_1 \dots w_r$ in $S^r(V)$.*

Proof. Both statements of the lemma are trivially true if any of the u_k's or any of the w_l's are zero. We thus assume all of them to be non-zero.

Writing u_k and w_k in terms of the anti-lexicographic basis we obtain

$$u_k = \sum_{l\in\underline{n}} \alpha_{k,l} v_l, \quad w_k = \sum_{l\in\underline{n}} \beta_{k,l} v_l, \quad k \in \underline{r}$$

with $\alpha_{k,l}, \beta_{k,l} \in F$. Let $f : \underline{r} \to \underline{n}$ be given by

$$k \mapsto f(k) = \max\{l : \alpha_{k,l} \neq 0\}$$

and let $g : \underline{r} \to \underline{n}$ be the corresponding function for the w_k's. From this it follows that

$$\mathrm{lt}(u_k) = \alpha_{k,f(k)} v_{f(k)}, \quad \mathrm{lt}(w_k) = \beta_{k,g(k)} v_{g(k)}.$$

Since lt is multiplicative, we have

$$\mathrm{lt}\left(\prod_{k\in\underline{r}} u_k\right) = \prod_{k\in\underline{r}} \mathrm{lt}(u_k) = \prod_{k\in\underline{r}} \alpha_{k,f(k)} v_{f(k)}$$

with a corresponding equation for $\mathrm{lt}(w_1 \dots w_r)$.

Let $q \in P(r)$ such that $\mathrm{lt}(u_1 \dots u_r) \in S^r_q(V)$ and $p \in P(r)$ such that $\mathrm{lt}(w_1 \dots w_r) \in S^r_p(V)$ (these elements of $P(r)$ exist and are unique by the way we defined the function lt). The condition that $u_k \preccurlyeq w_k$ means that for all k we have $f(k) \leqslant g(k)$ for all k and this implies that $q \leqslant p$ in the order we defined for $P(r)$, i.e., the order induced by $(\underline{r}_0)^n$. By equation (2.30) we have

$$\mathrm{lt}(u_1 \dots u_r) \preccurlyeq \mathrm{lt}(w_1 \dots w_r)$$

and the third item in the remark above implies that $u_1 \dots u_r \preccurlyeq w_1 \dots w_r$. If for $k \in \underline{r}$ we have $u_k \ll w_k$ then for this k we obtain $f(k) < g(k)$ and, hence, $q < p$ in $P(r)$. The same reasoning as before then gives $\mathrm{lt}(u_1 \dots u_r) \ll \mathrm{lt}(w_1 \dots w_r)$ and then $u_1 \dots u_r \ll w_1 \dots w_r$. □

Corollary 2.34. *The order on $S^r(V)$ above does not depend on the choice of the anti-lexicographic basis $\{v_1, \dots, v_n\}$ of V chosen for the construction above.*

Proof. Let $\{v_k\}_{k\in\underline{n}}$ and $\{w_k\}_{k\in\underline{n}}$ be two anti-lexicographic bases for V. Let $S^r(V)$ be ordered using the basis $\{v_k, \}_{k\in\underline{n}}$. We have $v_k \sim w_k$ for all $k \in \underline{n}$. By applying lemma (2.33) using $\{v_k\}$ as the fixed anti-lexicographic basis, we immediately get, for all $p \in P(r)$, that $v_1^{p_1} \dots v_n^{p_n} \sim w_1^{p_1} \dots w_n^{p_n}$. Thus, $\{w_1^{p_1} \dots w_n^{p_n}\}_{p\in P(r)}$ is also an anti-lexicographic basis for $S^r(V)$. The corollary is proven. □

Proposition 2.35. *Let V be a finite-dimensional, anti-lexicographically ordered, F-vector space. Then the symmetric algebra $S(V)$ is an ordered ring.*

Proof. Axiom (i) of the definition is clear as $S(V)$ is an ordered F-vector space. Writing $V = V_1 \oplus \dots \oplus V_n$ as the anti-lexicographic sum of one-dimensional subspaces, to prove (ii) it suffices to show that the product maps

$$S^p(V_k) \times S^q(V_l) \to S^p(V_k) \otimes S^q(V_l) \subset S^{p+q}(V)$$

for all admissible p, q, k and l have the property that the product of positive elements is positive. Such a product is given by

$$(\lambda v_k^p, \mu v_l^q) \mapsto \lambda\mu v_k^p v_l^q$$

with $\lambda, \mu \in F$ positive and v_k, v_l a positive basis of V_k, V_l respectively. Since $\lambda\mu v_k^p v_l^q$ is positive the proof is complete. $\square$

Example 2.36. Let $\mathbb{R}^3$ be anti-lexicographically ordered and $\{e_1, e_2, e_3\}$ its canonical basis. This is an anti-lexicographic basis. The symmetric algebra $S(\mathbb{R}^3)$ can be identified with the polynomial algebra $\mathbb{R}[e_1, e_2, e_3]$. For every $d \in \mathbb{Z}_{\geqslant 0}$, the subspace $S^d(\mathbb{R}^3)$ is identified with the set of homogeneous polynomials in e_1, e_2 and e_3 of degree d. For $d = 2$, for example, an anti-lexicographic basis for $S^2(\mathbb{R}^3)$ is given by

$$\{e_1^2,\ e_1 \cdot e_2,\ e_2^2,\ e_1 \cdot e_3,\ e_2 \cdot e_3,\ e_3^2\}$$

in this order.

CHAPTER 3

Layered Euclidean spaces

In this chapter we develop the theory of *layered Euclidean spaces*. Put simply, these are real inner-product spaces where the inner-product takes values in an ordered real vector space. In close analogy to the classical case where lattices are discrete subgroups of Euclidean spaces, layered Euclidean spaces are the ambient spaces into which *layered lattices*, the subject to be discussed in our next chapter, can be embedded.

We start in a more general setting, where the field is not necessarily the field of real numbers and then move to this particular case where we can prove an analogue of the decomposition theorem of Hilbert spaces. This theorem implies the existence of Gram-Schmidt bases, which will be important later on.

In this chapter, F denotes an ordered field.

3.1 Layered forms

Definition 3.1. Let D and V be F-vector spaces with V ordered. Let

$$B : D \times D \to V$$

be a bilinear symmetric function. Such a function is called a *V-valued form*. We say B is *positive-semidefinite* if for all $x \in D$ we have $B(x, x) \geqslant 0$ and say B is *positive-definite* if for all non-zero $x \in D$ we have $B(x, x) > 0$. The set

$$\operatorname{rad} B = \{y \in D : \forall x \in D, B(x, y) = 0\}$$

is called the *radical* of B. Given an ordered basis $\{b_i\}_{i\in I}$ of D, the *Gram matrix* of B with respect to this basis is the V-valued matrix $\mathbf{B} = (B(b_i, b_j))_{i,j\in I}$.

We say B is *layered* if for all $x, y \in D$ we have $B(x, y) \preccurlyeq B(y, y)$, i.e., the convex subspace generated by $B(x, y)$ is contained in the convex subspace generated by $B(y, y)$ (see definition (2.16)). ♢

Proposition 3.2. *Let D and V be F-vector spaces with V ordered. Let $B : D \times D \to V$ be a form on D. Then* $\operatorname{rad} B$ *is a subspace and B factors through* $D/\operatorname{rad} B \times D/\operatorname{rad} B$. *Moreover, if B is positive-semidefinite and layered then* $\operatorname{rad} B = \{y \in D : B(y, y) = 0\}$ *and the induced form on* $D/\operatorname{rad} B$ *is a positive-definite layered form.*

Proof. That $\operatorname{rad} B$ is a subspace follows from the bilinearity of B. By definition, B is zero on $D \times \operatorname{rad} B$ and by symmetry also on $\operatorname{rad} B \times D$, hence, it factors through $D/\operatorname{rad} B \times D/\operatorname{rad} B$.

Clearly $\operatorname{rad} B \subset \{y \in D : B(y, y) = 0\}$ holds. To prove the other inclusion, let $x, y \in D$ with $B(y, y) = 0$. Since B is layered, we have $B(x, y) \in \mathcal{C}(B(y, y))$ but since $\mathcal{C}(B(y, y)) = \mathcal{C}(0) = \{0\}$ we conclude that $B(x, y) = 0$.

Finally, the induced map on $D/\operatorname{rad} B$ is clearly bilinear, symmetric, positive-semidefinite and layered. It remains to show that it is positive-definite but this follows from the inclusion $\{y \in D : B(y, y) = 0\} \subset \operatorname{rad} B$ just proven. □

Definition 3.3. Let D and V be F-vector spaces with V ordered and $B : D \times D \to V$ be a positive-semidefinite, layered form. Following definition (2.16), let $\mathcal{C}(V)$ be the convex filtration of V. For $U \in \mathcal{C}(V)$ the set

$$D_U = \{x \in D : B(x, x) \in U\}$$

is called the *U-th layer* of D. The set of all layers of D we denote by $\mathcal{L}(D)$.

Let $x \in D$. The set

$$\bigcap \{D_U \in \mathcal{L}(D) : x \in D_U\}$$

is the *layer* of x and we denote it by $\mathcal{L}(x)$. ♢

Remark 3.4. The following remarks are straight-forward to check.

(a) The set of layers of D is ordered by inclusion. With this order, the map $U \mapsto D_U$ is a morphism of ordered sets.

(b) By proposition (2.15), for any $x \in D$, the layer of x is $\mathcal{L}(x) = D_{\mathcal{C}(B(x,x))}$.

(c) The radical of B is the minimal layer of D.

The following theorem is the main result of this section and is a strengthening of proposition (3.2).

Theorem 3.5. *Let D and V be F-vector spaces with V ordered and $B : D \times D \to V$ be a positive-semidefinite, layered form. Let $\mathcal{C}(V)$ be the convex filtration of V and $\mathcal{L}(D)$ be the set of layers of D. Then the layers are subspaces and for all $U \in \mathcal{C}(V)$ the form B induces a positive-definite, layered form*

$$B_U : D/D_U \times D/D_U \to V/U.$$

Proof. Recall from proposition (2.21) that V/U is an ordered F-vector space. Let $U \in \mathcal{C}(V)$ and consider the map $B_U : D \times D \to V/U$ given by the composition of B with the projection $V \to V/U$. It is clear that this map is a positive-semidefinite, layered form. Applying proposition (3.2) to B_U immediately gives the result since $\operatorname{rad} B_U = D_U$. □

Definition 3.6. A *layered space* is a triple (D, V, B) where D and V are F-vector spaces with V ordered and $B : D \times D \to V$ is a positive-definite, layered form. In a layered space, the form B is called the *inner-product*. A *layered Euclidean space* is a layered space where D and V are finite-dimensional and $F = \mathbb{R}$. ♢

Definition 3.7. If B is the inner-product on a layered space (D, V, B) we denote by $q_B : D \to V$ the map given by $q_B(x) = B(x, x)$ and call it the *associated quadratic norm*. ♢

Example 3.8. (a) A Euclidean space is a layered Euclidean space.

(b) If (D, V, B) is a layered space and $D' \subset D$ is a subspace then, denoting by B' the restriction of B to $D' \times D'$, the triple (D', V, B') is a layered space.

(c) The quotient of a layered space by one of its layers is a layered space by the theorem above.

(d) Let $U \in C^*(V)$ and U' be the predecessor of U in $\mathcal{C}(V)$. Combining (b) and (c) we see that $(D_U/D_{U'}, U/U', \langle\cdot,\cdot\rangle)$ is a layered Euclidean space with $\dim U/U' = 1$.

(e) $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space with $\dim V = 1$ and $v \in V, v > 0$. Then $(E, \langle\cdot,\cdot\rangle)$ is a Euclidean space under the identification $V \simeq \mathbb{R}$ given by $v \mapsto 1$. Any other choice of positive basis for V corresponds to a uniform scaling of the lengths of vectors of $(E, \langle\cdot,\cdot\rangle)$. In particular, by (d) above, and for any $U \in \mathcal{C}^*(V)$, we may identify $(E_U/E_{U'}, U/U', \langle\cdot,\cdot\rangle)$ with a classical Euclidean space (as in (d), we let U' be the predecessor of U in $\mathcal{C}(V)$).

We recall the definition of a flag of a vector space D given in the review section of the introduction. This will be used below.

Definition 3.9. Let (D, V, B) be a layered space. Let $I \to D$ be an ordered basis of D and $\mathcal{F}(I \to D)$ be its induced flag. The basis $I \to D$ is a *layered basis* of D if $\mathcal{L}(D) \subset \mathcal{F}(I \to D)$. ♢

Remark 3.10. (a) The inclusion $\mathcal{L}(D) \subset \mathcal{F}$ implies that each layer of D is *generated* by a subset of the image of the basis $I \to D$. Note that this automatically implies that the inclusion map $\mathcal{L}(D) \to \mathcal{F}(I \to D)$ is a morphism of ordered sets. Intuitively, this means that the basis vectors "come in the right order", meaning, first vectors generating the first non-trivial layer, then the second, and so forth. As such, a layered basis induces in a canonical way, for each $U \in \mathcal{C}^*(V)$, an ordered basis of the layered space $(D_U/D_{U'}, U/U', \langle\cdot,\cdot\rangle)$ where $U' \in \mathcal{C}^(V)$ is the predecessor of U.

(b) If two bases of a layered Euclidean space generate the same flag, then one is layered if and only if the other is.

The following result gives a criterion for identifying a layered form B in terms of its Gram matrix with respect to certain bases. Although it can be stated in a slightly more general form, for simplicity, and since we are mostly interested in this special case, we restrict ourselves to anti-lexicographically ordered vector spaces. We need the following definition.

Definition 3.11. Let $m \in \mathbb{Z}_{\geqslant 0}$. An m-by-m symmetric matrix $\mathbf{M}$ with coefficients in F is said to be *positive-(semi)definite* if the form it induces on F^m by the rule

$$(x, y) \mapsto x^T \mathbf{M} y$$

is positive-(semi)definite. ♢

Theorem 3.12. *Let D and V be finite-dimensional F-vector spaces with V anti-lexicographically ordered (see definition* (2.12)*) and convex filtration $\mathcal{C}(V)$. Denote by $\mathcal{C}^*(V)$ the subset $\mathcal{C}(V) \setminus \{\{0\}\}$. Let $\{v_W\}_{W \in \mathcal{C}^*(V)}$ be an anti-lexicographic basis of V.*

Let $B : D \times D \to V$ be a V-valued form on D and $\{D_U : U \in \mathcal{C}(V)\}$ be a family of subspaces of D such that $D_{U'} \subset D_U$ whenever $U' \leqslant U$ and with $D_{\{0\}} = \{0\}$ and $D_V = D$. Let $\{I_U \subset D_U : U \in \mathcal{C}(V)\}$ be a family of ordered subsets such that for any $U \in \mathcal{C}(V)$, the coproduct $\coprod_{U' \leqslant U} I_{U'} \to D_U$ is an ordered basis of D_U.

For each pair $(U, U') \in \mathcal{C}^*(V) \times \mathcal{C}^*(V)$ let $\mathbf{B}_{U,U'}$ be the V-valued matrix

$$\mathbf{B}_{U,U'} = (B(x, y))_{x \in I_U, y \in I_{U'}}$$

and for each $W \in \mathcal{C}^*(V)$ let $\mathbf{B}^W_{U,U'}$ be the F-valued matrices such that we have

$$\mathbf{B}_{U,U'} = \sum_{W \in \mathcal{C}^*(V)} \mathbf{B}^W_{U,U'} v_W. \tag{3.13}$$

Then the statement D is a layered space and for all $U \in \mathcal{C}(V)$ its U-th layer equals D_U is equivalent to the following two conditions.

(a) *For all* $U, U', W \in \mathcal{C}^*(V)$, *with* $\min\{U, U'\} < W$ *we have* $\mathbf{B}^W_{U,U'} = 0$.

(b) *For all* $W \in \mathcal{C}^*(V)$ *the matrix* $\mathbf{B}^W_{W,W}$ *is positive-definite.*

Before giving the proof we remind the reader that for an ordered finite set S and $s \in S$, we denote the *predecessor* of s by $s-1$, whenever it exists (see the review and notation section of the introduction).

Proof of theorem 3.12. Suppose (a) and (b) hold. Let $U, U' \in \mathcal{C}^*(V)$ and $x \in I_U, y \in I_{U'}$. By definition $B(x,y)$ is an entry of $\mathbf{B}_{U,U'}$ and from equation (3.13) and (a) we see that $B(x,y) \in \min\{U, U'\}$ for all such pairs x, y. Since $\mathcal{C}(B(y,y)) = U'$, the layered property $B(x,y) \preccurlyeq B(y,y)$ holds for these pairs of vectors. By the linearity of B in the second argument and (b) we see that for all $y \in \operatorname{span} I'_U$ we have $B(y,y) \in U'$ and positive. The linearity of B in the first argument now implies that $B(x,y) \preccurlyeq B(y,y)$ for all $x \in \operatorname{span} I_U$ and $y \in \operatorname{span} I_{U'}$.

Let $U_0, U'_0 \in \mathcal{C}^*(V)$ and $x \in D_{U_0} \setminus D_{U_0-1}$ then we have $x = \sum_{U \leqslant U_0} x_U$ with $x_U \in \operatorname{span} I_U$. Let $y \in D_{U'_0} \setminus D_{U'_0}$ and similarly write $y = \sum_{U' \leqslant U'_0} y_{U'}$ with $y_{U'} \in \operatorname{span} I_{U'}$. From what we saw, for any $U \leqslant U_0$ and any $U' \leqslant U'_0$, we have $B(x_U, y_{U'}) \preccurlyeq B(y_{U'}, y_{U'}) \preccurlyeq B(y_{U'_0}, y_{U'_0})$. Since $B(x,y)$ is a sum of terms of the form $B(x_U, y_{U'})$ we conclude that for all $x \in D_{U_0} \setminus D_{U_0-1}$ and $y \in D_{U'_0} \setminus D_{U'_0-1}$ we have $B(x,y) \preccurlyeq B(y_{U'_0}, y_{U'_0})$. Since the convex subspace generated by the latter is U'_0 this proves that B is layered. From this and the bilinearity of B it is straight-forward to check that $B(x,x) \simeq B(x_{U_0}, x_{U_0})$ and since the latter is positive, by what we already shown, we conclude that B is positive-definite. Hence, D is a layered space. It remains to show that for any $U \in \mathcal{C}(V)$, the U-th layer of D equals D_U. We already have $D_{\{0\}} = \{0\}$ as required. For any $U \in \mathcal{C}^*(V)$, from (a) and the fact that $\coprod_{U' \leqslant U} I_{U'} \to D_U$ is a basis of D_U, we see that D_U is contained in the U-th layer of D. To prove the other inclusion let $x \in D$ be in the U-th layer. Since $D = D_V$ we can write $x = \sum_{U' \in C^*(V)} x_{U'}$ where $x_{U'} \in \operatorname{span} I_{U'}$. Since x is in the U-th layer we have $B(x,x) \in U$. The right-hand side then gives

$$\sum_{U', U''} B(x_{U'}, x_{U''}) \in U$$

and now (a) and (b) imply that $x'_U = 0$ for $U' > U$ thus $x \in D_U$.

The other implication is trivial to prove. For $U, U', W \in \mathcal{C}^*(V)$, an entry of $\mathbf{B}^W_{U,U'}$ is the v_W-component of $B(x,y)$ for $x \in I_U$ and $y \in I_{U'}$. The layered property of B immediately gives (a). This together with the fact that B is positive-definite gives (b). □

Remark 3.14. Under the notation of the above theorem, we note the following.

(a) If D is a layered space then for any $U \in \mathcal{C}(V)$ the ordered basis $\coprod_{U' \leqslant U} I_{U'} \to D_U$ of D_U is *layered*.

(b) By theorem (2.25), any finite-dimensional ordered real vector space is anti-lexicographically ordered so in the case we are most concerned with, namely when $F = \mathbb{R}$, we may drop this assumption from the theorem.

(c) The V-valued matrix

$$\mathbf{B} = (\mathbf{B}_{U,U'})_{U,U' \in \mathcal{C}^*(V)}$$

obtained as in the theorem above is none other than the Gram matrix of the form B written in a block-wise manner. This makes it easy to see if B is layered positive-definite.

(d) To elaborate on the former observation, define the F-valued matrices

$$\mathbf{B}^W = \left(\mathbf{B}^W_{U,U'}\right)_{U,U' \in \mathcal{C}^*(V)}.$$

Then the theorem states that B is layered and positive-definite if and only if these matrices have the following block shape:

$$\mathbf{B}^W = \left(\begin{array}{c|c|c} 0 & 0 & 0 \\ \hline 0 & \mathbf{B}^W_{W,W} & * \\ \hline 0 & * & * \end{array}\right) \begin{array}{l} \\ W\text{-th row} \\ \\ \end{array}$$

where $*$ stands for an arbitrary matrix of the appropriate dimension and with $\mathbf{B}^W_{W,W}$ positive-definite.

Example 3.15. Let $E = \mathbb{R}^3$, $V = \mathbb{R}^2$ and $B(x, y)$ given by $(x^T\mathbf{B}^1 y, x^T\mathbf{B}^2 y)$ where $\mathbf{B}^1 = \operatorname{diag}(1, 1, -1)$, $\mathbf{B}^2 = \operatorname{diag}(0, 1, 1)$ and $\operatorname{diag}(a, \ldots, z)$ denotes the square diagonal matrix with diagonal entries $a, \ldots, z$.

Denote the canonical basis of E by $\{e_1, e_2, e_3\}$ and the canonical basis of V by $\{v_1, v_2\}$. Then $\mathcal{C}(V) = \{V_0 = \{0\}, V_1 = \mathbb{R}v_1, V_2 = V\}$ in this order. Setting $I_{\{0\}} = \varnothing, I_{V_1} = \{e_1\}, I_{V_2} = \{e_2, e_3\}$ ordered as they are written and setting $D_k = \operatorname{span} I_k$ for $k \in \{0, 1, 2\}$, we are under the hypotheses of the theorem

and we obtain

$$\mathbf{B}^1 = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ 0 & 0 & -1 \end{array}\right), \quad \mathbf{B}^2 = \left(\begin{array}{c|cc} 0 & 0 & 0 \\ \hline 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right) \begin{array}{l} V_1\text{-th row} \\ \\ V_2\text{-th row.} \end{array}$$

So we see that (E, V, B) is a layered Euclidean space.

Notation. When dealing with a layered Euclidean space, following the standard notation used in the classical case, we will denote the inner-product by $\langle \cdot, \cdot \rangle$.

3.2 Orthogonality

In this section, we generalize the concept of orthogonality to layered Euclidean spaces. This generalization is straight-forward to define and one gets the feeling that it is "the right one", as many results are clear analogues of classical ones. Nonetheless, there are differences, for example, layered orthogonality is not a symmetric relation. We will show this after the following definition. On the other hand, the main result of this section points to the similarities of these two concepts: given any subspace of a layered Euclidean space, there exists an orthogonal complement to this subspace, i.e., a complement consisting of vectors orthogonal to that subspace. In the case of classical Euclidean spaces this result is a particular instance of the decomposition theorem for Hilbert spaces and it leads to the existence of orthogonal bases. The same is true in the present case, as we will see in Chapter 5.

We recall the reader of definition (2.16) where we introduced various relations on an ordered F-vector space.

Definition 3.16. Let (D, V, B) be a layered space. Given $x, y \in D$ we say x is *orthogonal* to y and write $x \perp y$ if $y = 0$ or both $y \neq 0$ and $\langle x, y \rangle \ll \langle y, y \rangle$. For subsets X, Y of D we say X is orthogonal to Y and write $X \perp Y$ if for all $x \in X$ and all $y \in Y$ we have $x \perp y$. Given a set X, the set

$$\{y \in E : \forall x \in X, y \perp x\}$$

we denote by $X^\perp$. $\diamondsuit$

Remark 3.17. (a) Note that in a classical Euclidean space we have $V = \mathbb{R}$ whose convex filtration is $\{(0), \mathbb{R}\}$ (in this order). Since $\langle y, y \rangle > 0$ if $y \neq 0$ we see that our definition amounts to the classical $\langle x, y \rangle = 0$ as a condition for x to be orthogonal to y.

(b) Also note that if for two elements $x, y \in D$ we have $\mathcal{L}(x) = \mathcal{L}(y)$ then $x \perp y$ if and only if $y \perp x$. This is not true in general as the following example illustrates.

(c) Orthogonality is not, in general, a *symmetric* relation. That this is the case can be seen from the definition once we realize that if $\langle x, x\rangle$ and $\langle y, y\rangle$, being elements of V, do not generate the same convex subspace, then orthogonality depends on the convex space generated by $\langle x, y\rangle$. The fact that $\langle \cdot, \cdot\rangle$ is layered only ensures that this space is *contained* in the minimum of the convex subspaces generated by the norm of x and of y.

Example 3.18. The following example shows that the relation $\perp$ defined above is not, in general, symmetric in x and y. Let $E = \mathbb{R}^2$ and $V = \mathbb{R}^{\underline{2}}$ and $\{u, v\}$ be the canonical basis of V (it is an anti-lexicographic basis of V). Define the form B via $(x, y) \mapsto (x^T\mathbf{B}^1 y)u + (x^T\mathbf{B}^2 y)v$ where

$$\mathbf{B}^1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \mathbf{B}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Let $I_{\{0\}} = \varnothing, I_{\mathbb{R}u} = \{e_1\}$ and $I_V = \{e_2\}$ where $\{e_1, e_2\}$ is the canonical basis of E. By theorem (3.12), the triple (E, V, B) is a layered Euclidean space. It is straightforward to see that $e_1 \perp e_2$ but $e_2 \not\perp e_1$.

Definition 3.19. Let (D, V, B) be a layered space. An ordered basis $\{b_i\}_{i\in I}$ of D is called an *orthogonal basis* if whenever $i, j \in I$ with $i < j$ we have $b_j \perp b_i$. $\diamondsuit$

Proposition 3.20. *Let $X, X_1, X_2 \subset D$ be subsets of a layered space. Then we have the following.*

(a) *$X^\perp$ is a subspace of D.*

(b) *If $0 \in X$ then $X^\perp \cap X = \{0\}$.*

(c) *$(X_1 \cup X_2)^\perp = X_1^\perp \cap X_2^\perp$.*

Proof.

(a) First note that $0 \in X^\perp$. If $X \subset \{0\}$ then $X^\perp = E$ and we are done. Now let $y_1, y_2 \in X^\perp$, $x \in X$ with $x \neq 0$ and $\alpha \in \mathbb{R}$. We have

$$\langle \alpha y_1 + y_2, x\rangle = \alpha\langle y_1, x\rangle + \langle y_2, x\rangle.$$

Since the convex subspace generated by the latter is strictly contained in the convex subspace generated by $\langle x, x\rangle$, this shows that $\alpha y_1 + y_2 \perp x$. Since this holds for any $x \in X$ we have $\alpha y_1 + y_2 \in X^\perp$ and $X^\perp$ is a subspace.

(b) Clearly $0 \in X^\perp \cap X$. If $x \in X^\perp \cap X$ with $x \neq 0$ then $x \perp x$, i.e., we have $\langle x, x\rangle \ll \langle x, x\rangle$ which is an impossibility.

(c) Obvious. □

From now on we specialize to the case of layered Euclidean spaces. Nonetheless we remark that all the results of this chapter still apply to the more general case of arbitrary layered spaces.

The next result of this chapter establishes the existence of orthogonal complements, i.e., given a subspace D of a layered Euclidean space the subspace $D^\perp$ is a complement for D in E. In chapter 4 we will use this theorem when developing a *Gram-Schmidt procedure* for E, a concrete way of finding orthogonal bases of E.

Theorem 3.21. *Let E be a layered Euclidean space and D be a subspace of E. For each $U \in \mathcal{C}(V)$ set $D_U = D \cap E_U$ and if $U \neq \{0\}$ denote by U' the predecessor of U in $\mathcal{C}(V)$. Then the following holds.*

(a) *The map $\phi : E \to \bigoplus_{U \in \mathcal{C}^*(V)} \mathrm{Hom}\,(D_U/D_{U'}, U/U')$ given by*

$$y \mapsto (x + D_{U'} \mapsto \langle x, y\rangle + U')_{U \in \mathcal{C}^*(V)}$$

is well-defined and linear.

(b) *The kernel of ϕ is $D^\perp$.*

(c) *The restriction $\phi|_D$ is an isomorphism of vector spaces.*

(d) *The natural map $D \oplus D^\perp \to E$ is an isomorphism of vector spaces.*

Proof. Since $\langle \cdot, \cdot \rangle$ is layered, for each $U \in \mathcal{C}^*(V)$ and for all $y \in E$, we have $\langle D_{U'}, y\rangle \subset U'$. Also, for any $x \in D_U$, we have $\langle x, y\rangle \in U$. Thus the map $D_U/D_{U'} \to U/U'$ given by

$$x + D_{U'} \mapsto \langle x, y\rangle + U'$$

is well-defined. It follows that the map ϕ is well-defined. That ϕ is linear is clear so we have proven (a).

Let $y \in E$. Then we have $y \in \ker \phi$ if and only if for all

$$(x_U + D_{U'})_{U \in \mathcal{C}^*(V)} \in \bigoplus_{U \in \mathcal{C}^*(V)} D_U/D_{U'}$$

and all $U \in C^*(V)$ we have $\langle x_U, y\rangle \in U'$. This holds if and only if for all $U \in \mathcal{C}^*(V)$ we have

$$\forall x \in D_U : \langle x, y\rangle \in U'.$$

This, in turn, is equivalent to the condition that for all $x \in D$ one has $y \perp x$, that is, to $y \in D^\perp$. We have established that $\ker \phi = D^\perp$ proving (b).

It now follows that

$$\ker \phi|_D = (\ker \phi) \cap D = D^\perp \cap D = \{0\}$$

so $\phi|_D$ is injective. Further, we have

$$\dim\left(\bigoplus_{U\in\mathcal{C}^*(V)} \operatorname{Hom}(D_U/D_{U'}, U/U')\right) = \dim D$$

so $\phi|_D$ is surjective and we obtain (c).

Finally, item (d) follows since $\dim D^\perp = \dim\ker\phi = \dim E - \dim D$. □

For the following theorem we recall, from section (1.2), that an ordered basis $\{b_i\}_{i\in\underline{m}}$ of a vector space E induces a flag $F_0 \subsetneqq \cdots \subsetneqq F_m$ of E via the formula $F_i = \operatorname{span}\{b_j : j \leqslant i\}$.

Theorem 3.22. *Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space with $\dim E = m$. Let $\{b_i\}_{i\in\underline{m}}$ be an ordered basis of E and $F_0 \subsetneqq \cdots \subsetneqq F_m$ be the flag of E induced by this basis. Then there exists a unique basis $\{b_i^*\}_{i\in\underline{m}}$ such that for all $i \in \underline{m}$ we have $b_i^* \in F_{i-1}^\perp$ and $b_i - b_i^* \in F_{i-1}$. Furthermore, this basis is orthogonal and induces the same flag $F_0 \subsetneqq \cdots \subsetneqq F_m$ of V.*

Proof. Let $i \in \underline{m}$. By theorem (3.21) we have that $E = F_{i-1}^\perp \oplus F_{i-1}$. Since $b_i \notin F_{i-1}$ there exists a unique non-zero $b_i^* \in F_{i-1}^\perp$ such that $b_i - b_i^* \in F_{i-1}$. From this we see that $b_i^* = b_i - (b_i - b_i^*) \in F_i$. Hence, for each $i \in \underline{m}$ we have $b_i^* \in F_i \setminus F_{i-1}$. It is now clear that the two bases induce the same flag of E, namely, $F_0 \subsetneqq \cdots \subsetneqq F_m$. Finally, since for any $i \in \underline{m}$ and any $j < i$ we have $b_j^* \in F_{i-1}$ it follows that $b_i^* \perp b_j^*$ so $\{b_i^*\}_{i\in\underline{m}}$ is an orthogonal basis of E. □

The bases whose existence are guaranteed by the theorem above will be further studied in chapter 5. For now, we use this theorem for the following result.

Corollary 3.23. *Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space. Then E has a* layered, orthogonal *basis. Let $I \to E$ be such a layered, orthogonal basis of E. Denote the image of $i \in I$ by $x_i \in E$. Then for any $i, j \in I, i \neq j$ we have $x_i \perp x_j$ and $x_j \perp x_i$.*

Proof. The existence of layered orthogonal bases follows from applying the theorem above to a layered basis, whose existence is trivial to prove (see remark (3.10 (b))).

Let $i, j \in I$ with $i < j$. If x_i, x_j are in the same layer, i.e., $\mathcal{L}(x_i) = \mathcal{L}(x_j)$, then orthogonality is symmetric for this pair of vectors (see remark (3.17)) so we have $x_i \perp x_j$ and $x_j \perp x_i$. If they are not in the same layer, the fact that $I \to E$ is layered implies that $\mathcal{L}(x_i) \subsetneqq \mathcal{L}(x_j)$. By the layered property of the inner-product we have $\langle x_i, x_j\rangle \preccurlyeq \langle x_i, x_i\rangle \ll \langle x_j, x_j\rangle$ and thus $x_i \perp x_j$. Since $I \to E$ is orthogonal we also have $x_j \perp x_i$. □

Another useful result is the following.

Proposition 3.24. *Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space and $\{x_i\}_{i\in I} \subset E$ an orthogonal basis. Then for all $U \in \mathcal{C}^*(V)$, denoting its predecessor in $\mathcal{C}(V)$ by U', we have*

$$\#\{x_i : x_i \in E_U \setminus E_{U'}\} = \dim E_U/E_{U'}.$$

Proof. By induction it suffices to prove the case $U = V$. Let $I_V = \{i : x_i \in E_V \setminus E_{V'}\}$. We clearly have

$$\#I_V \geqslant \dim E_V/E_{V'}$$

or else $\{x_i\}_{i\in I}$ would not generate E. To show the equality suppose we had

$$\#I_V > \dim E_V/E_{V'}.$$

Then there exists numbers $\lambda_i \in \mathbb{R}$, for $i \in I_V$, not all zero, such that

$$x = \sum_{i\in I_V} \lambda_i x_i \in E_{V'}.$$

If $i_0 \in I_V$ is any index with $\lambda_{i_0} \neq 0$ then the orthogonality conditions $x_{i_0} \perp x_i$, which hold for all $i \in I_V$ (see remark (3.17)), imply that

$$\lambda_{i_0}\langle x_{i_0}, x_{i_0}\rangle = \langle x, x_{i_0}\rangle - \sum_{i\neq i_0} \lambda_i\langle x_i, x_{i_0}\rangle \in V'$$

contradicting the fact that $x_{i_0} \in E_V \setminus E_{V'}$. □

The proposition above tells us that an orthogonal basis is, up to a permutation of its vectors, a layered basis. The following result will be used in chapter 5. It establishes an important property of those bases that, after some permutation, form a layered basis.

Proposition 3.25. *Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space and $D \subset E$ be a subspace. Let $c_1, \ldots, c_m \in D$ be a linearly independent set of vectors which, up to a permutation, form a layered basis of D. Then for any $x \in E$ we have that $x \in D^\perp$ if and only if $x \perp \{c_1, \ldots, c_m\}$.*

Proof. It is clear that if $x \in D^\perp$ then $x \perp \{c_1, \ldots, c_m\}$ holds. For the other implication, note that for every $U \in \mathcal{C}^*(V)$ a subset S_U of $\{c_1, \ldots, c_m\}$ forms a basis for $D_U = D \cap E_U$. Denote by U' the predecessor of U in $\mathcal{C}(V)$. Thus, the linear map $D_U/D_{U'} \to U/U'$ given by $y + D_{U'} \mapsto \langle x, y\rangle + U'$ is zero if and only if it is zero on S_U. This is the case since we are assuming that $x \perp \{c_1, \ldots, c_m\}$. It follows that x is an element in the kernel of the map ϕ of theorem (3.21). By item (b) of that theorem, we have $x \in D^\perp$. □

3.3 Exterior powers of layered Euclidean spaces

In the final section of this chapter we prove that exterior powers of a layered Euclidean space are layered Euclidean spaces. This result is important not only in what we will do later but also if one would like to extend this theory to manifolds, i.e., develop a generalized Riemannian geometry.

We briefly recall some definitions and results from chapter 2. Let V be an ordered real vector space of finite dimension $n \in \mathbb{Z}_{\geqslant 0}$. In (2.26) we introduced the symmetric algebra $S(V)$ of V and in proposition (2.35) we saw that it is an ordered graded ring with the order which, on each homogenous component $S^r(V), r \in \mathbb{Z}_{\geqslant 0}$, is characterized by the following property. If $\{v_i\}_{i \in \underline{n}}$ is an anti-lexicographic basis of V then the map $P(r) \to S^r(V)$ where

$$P(r) = \{p = (p_1, \dots, p_n) \in (\underline{r}_0)^n : p_1 + \cdots + p_n = r\},$$

given by $p \mapsto v^p = v_1^{p_1} \dots v_n^{p_n}$ is an anti-lexicographic basis of $S^r(V)$. The ring $S(V)$ is then ordered as the anti-lexicographic sum of the $S^r(V)$. Let $P_0(r) = \{0\} \coprod P(r)$ ordered as a coproduct, i.e., 0 is the minimum of $P_0(r)$. The convex filtration of $S^r(V)$ is given by $\mathcal{C}(S^r(V)) = \{S^r_p(V) : p \in P_0(r)\}$ where $S^r_0(V) = \{0\}$ and

$$S^r_p(V) = \bigoplus_{q \leqslant p} S^{q_1}(V_1) \otimes \cdots \otimes S^{q_n}(V_n)$$

for $p \neq 0$.

If F is a field and D is an F-vector space, we denote by $\bigwedge^r D$ the r-fold exterior power of D. We refer the reader to [7, Chapter XIX] for definitions and basic properties of the exterior power.

Theorem 3.26. *Let $(E, V, \langle \cdot, \cdot \rangle)$ be a layered Euclidean space and $r \in \mathbb{Z}_{\geqslant 0}$. Let $\bigwedge^r E$ be the r-fold exterior power of E and $S^r(V)$ the ordered r-th symmetric power of V. Define $\langle \cdot, \cdot \rangle : \bigwedge^r E \times \bigwedge^r E \to S^r(V)$ extending by bilinearity the formula*

$$\langle x_1 \wedge \cdots \wedge x_r, y_1 \wedge \cdots \wedge y_r \rangle = \det(\langle x_i, y_j \rangle)_{i,j=1,\dots,r}.$$

Then $(\bigwedge^r E, S^r(V), \langle \cdot, \cdot \rangle)$ is a layered Euclidean space.

Let $I \to E$ be a layered basis of E and

$$\bigwedge^r I = \{(i_1, \dots, i_r) \in I^r : i_1 < \cdots < i_r\} \tag{3.27}$$

with the order induced by the anti-lexicographic order on I^r. Denote by x_i the image of $i \in I$ in E. Then $\bigwedge^r I \to \bigwedge^r E$ given by

$$(i_1, \dots, i_r) \mapsto x_{i_1} \wedge \cdots \wedge x_{i_r} \tag{3.28}$$

is a layered basis of $\bigwedge^r E$.

Proof. The map $E^r \times E^r \to S^r(V)$ given by

$$(x, y) \mapsto \det(\langle x_s, y_t\rangle)_{s,t=1,\dots,r}$$

is multilinear and alternating in the x_s and in the y_t and so factors through $\bigwedge^r E \times \bigwedge^r E \to S^r(V)$. The resulting map is bilinear and symmetric and thus an $S^r(V)$-valued form.

Let $I \to E$ be a layered basis of E. By definition, if $\mathcal{F}$ is the flag induced by $I \to E$, we have $\mathcal{L}(E) \subset \mathcal{F}$ as ordered sets. Thus, every layer of E is generated by a subset of the image of $I \to E$. Denote by $x_i \in E$ the image of $i \in I$ in E. Then general results of multilinear algebra show that the map $\bigwedge^r I \to \bigwedge^r E$ given by (3.28) is an ordered basis of $\bigwedge^r E$.

The idea of the proof is to use theorem (3.12). We will introduce certain subspaces of $\bigwedge^r E$ indexed by $\mathcal{C}(S^r(V))$. To simplify notation we will use the natural bijection $p \mapsto S^r_p(V)$ between $P_0(r)$ and $\mathcal{C}(S^r_p(V))$ to use the former as the index set. Thus, for each $p \in P_0(r)$ let

$$D_p = \operatorname{span}\left\{x_i : i \in \textstyle\bigwedge^r I, \langle x_i, x_i\rangle \in S^r_p(V)\right\} \subset \textstyle\bigwedge^r E.$$

Clearly, we have $D_0 = \{0\}, D_{\max P_0} = D$ and whenever $q \leqslant p$, we have $D_q \subset D_p$ as required in theorem (3.12). Let $I_0 = \varnothing$ and, for $p \in P(r)$, let

$$I_p = \left\{i \in \textstyle\bigwedge^r I : \langle x_i, x_i\rangle \in S^r_p(V) \setminus S^r_{p-1}(V)\right\}. \tag{3.29}$$

With these definitions we see that for all $p \in P(r)$ the map $\coprod_{q\leqslant p} I_q \to D_p$ is an ordered basis of D_p, again, as required by theorem (3.12). Finally, let

$$\mathbf{B}_{p,p'} = (\langle x_i, x_j\rangle)_{i\in I_p, j\in I_{p'}}$$

and $\mathbf{B}^q_{p,p'}$ as in equation (3.13) for $p, p', q \in P(r)$.

The proof will be complete once we show that the *real* matrices $\mathbf{B}^q_{p,p'}$ satisfy (a) and (b) of theorem (3.12). For this, we assume that $I \to E$ is not only layered but also orthogonal. This can be done as the existence of such a basis is guaranteed by (3.23), and since the conclusion that $\bigwedge^r E$ is a layered Euclidean space does not depend on a choice of basis. We use the following lemma.

Lemma 3.30. *Let E be a layered Euclidean space with $\dim E = m$ and $\{x_i\}_{i\in\underline{m}}$ be an orthogonal basis of E. Let $\bigwedge^r \underline{m} = \{(i_1, \dots, i_r) \in \underline{m}^r : i_1 < \dots < i_r\}$ with the order induced by $\underline{m}^{\underline{r}}$. For each $i = (i_1, \dots, i_r) \in \bigwedge^r \underline{m}$ let $x_i = x_{i_1} \wedge \dots \wedge x_{i_r} \in \bigwedge^r E$. Then we have*

$$\langle x_i, x_i\rangle \simeq \prod_{s=1}^{r} \langle x_{i_s}, x_{i_s}\rangle.$$

Furthermore, if $j \in \bigwedge^r \underline{m}$ is such that $i < j$ then $\langle x_i, x_j\rangle \ll \langle x_i, x_i\rangle$ holds.

Proof. To prove the first statement we have to show that

$$\langle x_i, x_i\rangle - \prod_{s=1}^{r}\langle x_{i_s}, x_{i_s}\rangle \ll \prod_{s=1}^{r}\langle x_{i_s}, x_{i_s}\rangle.$$

From a well-known formula for the determinant, we can rewrite the difference on the left-hand side above as

$$\sum_{\sigma\in\mathrm{Sym}(r),\sigma\neq\mathrm{id}} \mathrm{sgn}\,(\sigma)\prod_{s=1}^{r}\langle x_{i_s}, x_{i_{\sigma(s)}}\rangle$$

where $\mathrm{Sym}(r)$ denotes the symmetric group on $\underline{r}$. Hence, it is enough to show that for each $\sigma \in \mathrm{Sym}, \sigma \neq \mathrm{id}$ we have

$$\prod_{s=1}^{r}\langle x_{i_s}, x_{i_{\sigma(s)}}\rangle \ll \prod_{s=1}^{r}\langle x_{i_s}, x_{i_s}\rangle. \tag{3.31}$$

By the layered property of the inner-product on E we have $\langle x_{i_s}, x_{i_{\sigma(s)}}\rangle \preccurlyeq \langle x_{i_s}, x_{i_s}\rangle$ for all s; and since the set $\{u \in \underline{r} : i_u < i_{\sigma(u)}\}$ is non-empty (here we use that $\sigma \neq \mathrm{id}$), for such an u we have $\langle x_{i_u}, x_{i_{\sigma(u)}}\rangle \ll \langle x_{i_u}, x_{i_u}\rangle$ by the orthogonality condition $x_{i_{\sigma(u)}} \perp x_{i_u}$. Hence, by lemma (2.33), the relation (3.31) indeed holds.

Now, to prove the second statement of this lemma, let $j \in \bigwedge^r \underline{m}$ with $i < j$. By the definition of the order on $\bigwedge^r \underline{m}$, the set $\{u : i_u < j_{\sigma(u)}\}$ is non-empty *for every* $\sigma \in \mathrm{Sym}(r)$ *including* $\sigma = \mathrm{id}$. By what we just proved it is enough to show that for all σ we have

$$\prod_{s=1}^{r}\langle x_{i_s}, x_{j_{\sigma(s)}}\rangle \ll \prod_{s=1}^{r}\langle x_{i_s}, x_{i_s}\rangle.$$

The rest of the proof is the same as in the first part. □

End of the proof of (3.26). We now prove (a) and (b) of theorem (3.12) for $\mathbf{B}^q_{p,p'}$. Let $p, p', q \in P(r)$ with $p < q$ and $i \in I_p, j \in I_{p'}$. By the lemma just proven we have

$$\langle x_i, x_j\rangle \ll \mathrm{lt}(\langle x_i, x_i\rangle) \in S^r_p(V)$$

by definition of I_p. This implies $\langle x_i, x_j\rangle \in S^r_p(V)$ and since $p < q$, in the expansion of $\langle x_i, x_j\rangle$ in the anti-lexicographic basis $\{v^p\}_{p\in P(r)}$, the q-th component is zero. This, in other words, is nothing other than the fact that the entry of $\mathbf{B}^q_{p,p'}$ given by $\langle x_i, x_j\rangle$ is zero. Hence, $\mathbf{B}^q_{p,p'} = 0$. The case where $p' < q$ follows from the symmetry of $\mathbf{B}^q_{p,p'}$, namely, $\mathbf{B}^q_{p,p'} = (\mathbf{B}^q_{p',p})^T = 0$ by the previous case. This proves (a).

To prove (b), we note that for any $q \in P(r)$ the diagonal entries of $\mathbf{B}^q_{q,q}$ are the q-th components of $\langle x_i, x_i \rangle$ for $i \in I_q$. Since, by definition of I_q, we have $\mathcal{C}(\langle x_i, x_i \rangle) = S^r_q(V)$, this q-th component is the *leading coefficient* of $\langle x_i, x_i \rangle$. This fact and the lemma above imply that the diagonal entries of $\mathbf{B}^q_{q,q}$ equal

$$\left\{ \mathrm{lc}\left(\prod_{s=1}^{r} \langle x_{i_s}, x_{i_s} \rangle \right) \right\}_{i \in I_q},$$

which are positive. To finish the proof we will show that the non-diagonal entries of $\mathbf{B}^q_{q,q}$ are zero (since a diagonal matrix with positive diagonal entries is positive-definite). A non-diagonal entry of $\mathbf{B}^q_{q,q}$ is the q-th component of $\langle x_i, x_j \rangle$ for $i, j \in I_q$ and $i \neq j$. By the lemma, $\langle x_i, x_j \rangle \ll \mathrm{lt}(\langle x_i, x_i \rangle) \in S^r_q(V)$. Hence we have $\mathcal{C}(\langle x_i, x_j \rangle) < S^r_q(V)$ and this component is zero as was to be shown.

We now know that $\bigwedge^r E$ is a layered Euclidean spaces with layers $\{D_p : p \in P_0(r)\}$. Returning to the case where $I \to E$ is a layered basis of E but not necessarily orthogonal, to finish the proof, we have to show that $\bigwedge^r I \to \bigwedge^r E$ is a layered basis of $\bigwedge^r E$. This was already shown: the flag induced by $\bigwedge^r I \to \bigwedge^r E$ contains $\mathcal{L}(\bigwedge^r E) = \{D_p : p \in P_0(r)\}$. □

Corollary 3.32. *Let $I \to E$ be a layered, orthogonal basis of a layered Euclidean space $(E, V, \langle \cdot, \cdot \rangle)$. Then for any $r \in \mathbb{Z}_{\geqslant 0}$ the basis $\bigwedge^r I \to \bigwedge^r E$ of $\bigwedge^r E$ described in the theorem above is layered and* orthogonal.

Proof. That $\bigwedge^r I \to \bigwedge^r E$ is layered is stated in the theorem. That this basis is orthogonal is, since we now know that $\bigwedge^r E$ is a layered Euclidean space, *exactly* the statement of lemma (3.30). □

CHAPTER 4

Layered lattices

In this chapter we introduce and study the concept of a *layered lattice*. A classical lattice is a discrete subgroup of a Euclidean space. This is equivalent to being a group generated by a linearly independent set of vectors of a Euclidean space. As we generalized Euclidean spaces and studied *layered* Euclidean spaces in the last chapter, here we will generalize lattices to layered lattices. These are subgroups of layered Euclidean spaces having a certain "layer" property that is equivalent to being generated by a subset of a *layered basis* (recall definition (3.9)).

We then give a more intrinsic definition of a layered lattice, which does not refer to any ambient space. Of course, we prove the equivalence of the two definitions.

4.1 Embedded layered lattices

We start by recalling a standard result about classical lattices.

Definition 4.1. Let E be a Euclidean space. An *embedded lattice* is a subgroup L of E that is discrete with respect to the induced topology. We say L is *full in* E if the $\mathbb{R}$-span of L equals E. $\diamondsuit$

Proposition 4.2. *A subgroup $L \subset E$ of a Euclidean space is an embedded lattice if and only if it is generated by a linearly independent set of elements of E.*

Proof. This is proven in [9, Proposition 3.3]. Alternatively, see theorem (1) and corollary (1) of [11, Chapter 2]. □

Remark 4.3. It is clear from the above proposition that a lattice is a finitely generated, torsion-free abelian group and, hence, a free group of finite rank.

For the following we remind the reader of definitions (3.6) of a layered Euclidean space and (3.9) of a layered basis.

Definition 4.4. Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space. An *embedded layered lattice* is a subgroup L of E generated by a subset (of the image) of a layered basis. We say that L is *full in* E if the $\mathbb{R}$-span of L equals E. ♢

As before, for an ordered vector space V we denote by $\mathcal{C}(V)$ the convex filtration of V (see definition (2.16)), and by $\mathcal{C}^*(V)$ the subset $\mathcal{C}(V) \setminus \{\{0\}\}$. We remind the reader that by remark (3.8 (e)), the quotient of two successive layers of a layered Euclidean space has the structure of a *classical* Euclidean space.

Proposition 4.5. *Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space and $L \subset E$ be a subgroup. For each $U \in \mathcal{C}(V)$ let E_U be the U-th layer of E and set $L_U = L \cap E_U$. Then L is an embedded layered lattice if and only if for each $U \in \mathcal{C}^*(V)$, denoting its predecessor in $\mathcal{C}(V)$ by U', the quotient $L_U/L_{U'} \subset E_U/E_{U'}$ is an embedded lattice in the Euclidean space $(E_U/E_{U'}, \langle\cdot,\cdot\rangle)$.*

Proof. Suppose L is an embedded layered lattice. Replacing E by the $\mathbb{R}$-span of L we may suppose L is full. Let thus $I \to L \subset E$ be a layered basis of E generating L. Let $U \in \mathcal{C}^*(V)$. By definition, there is a subset $I_U \subset I$ such that $I_U \to E_U$ is an ordered basis of E_U and similarly for the predecessor U' of U in $\mathcal{C}(V)$. We clearly have $I_{U'} \subset I_U$ and the map $I_U \setminus I_{U'} \to E_U \to E_U/E_{U'}$ is an ordered basis of $E_U/E_{U'}$. We saw in remark (3.8), that the latter is a Euclidean space.

From $L_U = L \cap E_U$ we have that the image of $I_U \setminus I_{U'}$ under this composition is contained in $L_U/L_{U'} \subset E_U/E_{U'}$ and generates this subgroup. By proposition (4.2) above $L_U/L_{U'} \subset E_U/E_{U'}$ is an embedded lattice.

Now suppose that for any $U \in \mathcal{C}^*(V)$ the subgroups $L_U/L_{U'} \subset E_U/E_{U'}$ are embedded lattices. Using proposition (4.2), for each such U let $I_U \subset L_U/L_{U'} \subset E_U/E_{U'}$ be an linearly independent set of elements of $E_U/E_{U'}$ generating $L_U/L_{U'}$. Let $I_U \to L_U/L_{U'}$ be the standard inclusion and take *any* lift $I_U \to L_U \subset E_U$ of this map to L_U. Now set $I = \coprod_{U \in \mathcal{C}^*(V)} I_U$, as coproduct of sets, anti-lexicographically ordered with respect to $\mathcal{C}^*(V)$ (see the review and notation section of the Introduction). It is immediate to verify that $I \to E$ is a layered basis of the $\mathbb{R}$-span of L, i.e., L is generated by a subset of a layered basis of E. □

4.2 Layered lattices

We start by recalling the definition of a classical lattice (see ([9, Section 4])).

Definition 4.6. A *lattice* is a pair (L, q) where L is a finitely generated abelian group and $q : L \to \mathbb{R}$ is a map satisfying the following three conditions.

(i) For all $x, y \in L$ we have

$$q(x + y) + q(x - y) = 2q(x) + 2q(y).$$

(ii) For all $x \neq 0$ in L we have $q(x) \neq 0$.

(iii) For any real number λ the set $\{x \in L : q(x) \leqslant \lambda\}$ is finite.

The map q is called the *quadratic norm* on L and (i) above is called the *parallelogram law.* ♢

We generalize this as follows.

Definition 4.7. A *layered lattice* is a triple (L, V, q) where L is a finitely generated abelian group, V is a finite-dimensional, ordered $\mathbb{R}$-vector space and $q : L \to V$ is a map satisfying the following three conditions.

(i) For all $x, y \in L$ we have

$$q(x + y) + q(x - y) = 2q(x) + 2q(y).$$

(ii) For all $x \neq 0$ in L we have $q(x) \neq 0$.

(iii) The set $q(L)$ is well-ordered as a subset of V.

The map q is called the *quadratic norm* on L and (i) above is called the *parallelogram law.* ♢

Remark 4.8. We will show below that a layered lattice (L, V, q) with V one-dimensional can be identified with a classical lattice, and that any two such identifications differ by a uniform scaling of the lattice points. Thus, a layered lattice is, in fact, a generalization of (4.6).

The following result is well-known in the theory of lattices. One of the main results of this chapter is its generalization to layered lattices.

Proposition 4.9. *Let (L, q) be a lattice. Then $\mathbb{R} \otimes_{\mathbb{Z}} L$ is a Euclidean space with inner-product $\langle \cdot, \cdot \rangle$ given on generators of the form $\alpha \otimes x$, with $\alpha \in \mathbb{R}$ and $x \in L$, by*

$$\langle \alpha \otimes x, \beta \otimes y \rangle = \alpha\beta \frac{q(x + y) - q(x - y)}{4}.$$

The injective homomorphism of groups $\iota : L \to E$ given by $x \mapsto 1 \otimes x$ is such that for all $x \in L$ one has $\langle \iota(x), \iota(x) \rangle = q(x)$ and makes $\iota(L)$ into an embedded lattice.

Proof. This is proven in [9, Proposition 4.1, pg. 74]. □

Remark 4.10. We note, and this will be important later on, that the proof of the above proposition remains valid if (iii) of definition (4.6) is replaced by the condition that $q(L) \subset \mathbb{R}$ is well-ordered. In the proof one only uses that $q(L \setminus \{0\})$ attains a minimum and that this minimum is positive.

Lemma 4.11. *Let (L, V, q) be a layered lattice. Then L is a free abelian group of finite rank. Furthermore the following holds.*

(a) *We have $q(0) = 0$.*

(b) *For all $x \in L$ and all $n \in \mathbb{Z}$ we have $q(nx) = n^2 q(x)$.*

(c) *For all $x \in L$ we have $q(x) \geqslant 0$, and $q(x) = 0$ if and only if $x = 0$.*

Proof. By first choosing $x, y = 0$, then $x = y$, and finally $x = 0$ in the parallelogram law we conclude, in turn, that $q(0) = 0$, that $q(2x) = 4q(x)$ and that $q(-y) = q(y)$. This establishes (a). An easy induction argument then shows that for any $n \in \mathbb{Z}$ and any $x \in L$ we have $q(nx) = n^2 q(x)$ establishing (b). Now suppose that for $x \in L$ we have $q(x) < 0$. Then for all $n \in \mathbb{Z}_{\geqslant 0}$ we obtain the inequalities $q(nx) = n^2 q(x) < q((n-1)x) < \cdots < q(x) < 0$ contradicting (iii) from the definition of q. Thus, $q(x) \geqslant 0$ for all $x \in L$. This together with (ii) from the definition of a layered lattice proves (c) and, in particular, that L is torsion-free. Since L is finitely generated we conclude that L is a free abelian group of finite rank. □

Lemma 4.12. *Let (L, V, q) be a layered lattice and define the map $\langle \cdot, \cdot \rangle : L \times L \to V$ by*

$$\langle x, y \rangle = \frac{q(x+y) - q(x-y)}{4}. \tag{4.13}$$

Then $\langle \cdot, \cdot \rangle$ is a $\mathbb{Z}$-bilinear, symmetric, positive-definite map on $L \times L$ such that for all $x, y \in L$ we have $\langle x, x \rangle = q(x)$ and $\langle x, y \rangle \preccurlyeq \langle y, y \rangle$.

Proof. Let $x, y, z \in L$. By (b) of the lemma (4.11) above we have $q(x-y) = q(y-x)$ and, hence, $\langle x, y \rangle = \langle y, x \rangle$, which shows that the map is symmetric. Using the parallelogram law we obtain the following equations:

$$\begin{aligned}
q(x+y+z) + q(x-y+z) &= 2q(x+z) + 2q(y) && \text{(I)}\\
q(x+y-z) + q(x-y-z) &= 2q(x-z) + 2q(y) && \text{(II)}\\
q(x+y+z) + q(x-y-z) &= 2q(x) + 2q(y+z) && \text{(III)}\\
q(x+y-z) + q(x-y+z) &= 2q(x) + 2q(y-z) && \text{(IV)}.
\end{aligned}$$

Taking the alternating sum (I)−(II)+(III)−(IV) we get

$$2q(x+y+x) - 2q(x+y-z) = 2q(x+z) - 2q(x-z) + 2q(y+z) - 2q(y-z),$$

which upon division by 8 amounts to the identity

$$\langle x+y,z\rangle = \langle x,z\rangle + \langle y,z\rangle$$

valid for all $x,y,z \in L$. Thus, $\langle\cdot,\cdot\rangle$ is bilinear over $\mathbb{Z}$.

Using the properties of q established in the previous lemma we have

$$\langle x,x\rangle = \frac{q(2x)-q(0)}{4} = \frac{4q(x)}{4} = q(x) \tag{4.14}$$

establishing the desired formula. Since by the same lemma for all $x \in L$ we have $q(x) \geqslant 0$ with $q(x)=0$ if and only if $x=0$, this formula also establishes that $\langle\cdot,\cdot\rangle$ is positive-definite.

It remains to show that for all $x,y \in L$ we have $\langle x,y\rangle \preccurlyeq \langle y,y\rangle$. Let $x,y \in L$ and $S = \{x+ny : n \in \mathbb{Z}\}$. Since $q(S) \subset q(L)$ and the latter is well-ordered, there exists $z = x+my \in S$ with $q(z) = \min q(S)$. Thus we have $q(z) \leqslant q(z \pm y)$ since $z \pm y \in S$. Using equation (4.14), the bilinearity of $\langle\cdot,\cdot\rangle$ and the fact that $q(z) \geqslant 0$ we obtain $\mp 2\langle z,y\rangle \leqslant \langle y,y\rangle$. Thus we have

$$|\langle z,y\rangle| \leqslant 1/2\langle y,y\rangle$$

and we conclude that $\langle z,y\rangle \preccurlyeq \langle y,y\rangle$. Since $z = x+my$ we also have $\langle x,y\rangle \preccurlyeq \langle y,y\rangle$, as was to be shown. □

Notation. From now on, whenever we have a layered lattice (L,V,q), we will freely use $\langle\cdot,\cdot\rangle$ to denote the associated bilinear symmetric map given by the above lemma.

We recall from the review section of the introduction that a subgroup K of a free group L is called a *pure* subgroup if the quotient L/K is free.

Lemma 4.15. *Let (L,V,q) be a layered lattice and $\langle\cdot,\cdot\rangle : L \times L \to V$ as in the previous lemma. For each $U \in \mathcal{C}(V)$ let $L_U = \{x \in L : q(x) \in U\}$. Then L_U is a* pure *subgroup of L. Define $q : L/L_U \to V/U$ by*

$$q(x+L_U) = q(x) + U. \tag{4.16}$$

Then $(L/L_U, V/U, q)$ is a layered lattice.

Proof. Let $U \in \mathcal{C}(V)$ and suppose $x,y \in L_U$. Then a straight-forward calculation gives

$$q(x+y) = q(x) + 2\langle x,y\rangle + q(y) \in U \tag{4.17}$$

since we have shown that $\langle x,y\rangle \preccurlyeq q(y) \in U$. Since $q(-y) = q(y) \in U$ we conclude that L_U is a subgroup of L. Now let $x+L_U \in L/L_U$ and suppose

there is $n \in \mathbb{Z}$ such that $n(x + L_U) = 0$ in L/L_U. This means that $nx \in L_U$. By lemma (4.11) we thus have $n^2 q(x) = q(nx) \in U$. From this we conclude that either $n = 0$ or $x \in L_U$. Hence, L/L_U is torsion-free and L_U is a pure subgroup of L.

The map $x + L_U \mapsto q(x) + U$ is well defined since if $x + L_U = y + L_U$ then

$$q(x + L_U) = q(x) + U = q(y + (x - y)) + U = q(y) + U$$

where the last equality can be seen by expanding $q(y+(x-y))$ like in equation (4.17) above. This map satisfies (i) and (ii) of the definition of a layered lattice. To see (iii) just note that, in general, if S is a well-ordered subset of an ordered vector space V and U is a convex subspace of V, then the image of S in V/U is well-ordered as well. This is an immediate consequence of the fact that the quotient map $V \to V/U$ is a morphism of ordered vector spaces. This concludes the proof. □

Definition 4.18. Let (L, V, q) be a layered lattice over an ordered field F. The subgroup $L_U = \{x \in L : q(x) \in U\}$ from the previous lemma is the *U-th layer* of L. The set $\mathcal{L}(L) = \{L_U : U \in \mathcal{C}(V)\}$ is called the *set of layers* of L.

For an element $x \in L$, the set

$$\mathcal{L}(x) = \bigcap \{L_U \in \mathcal{L}(L) : x \in L_U\}$$

is called the *layer* of x. ♢

Remark 4.19. As in remark (3.4), the set of layers is totally ordered by inclusion and, thus, a filtration of L. Note that the map $\mathcal{C}(V) \to \mathcal{L}(L)$ given by $U \mapsto L_U$ is a morphism of ordered sets. Also, we have $\mathcal{L}(x) = L_{\mathcal{C}(q(x))}$ where $\mathcal{C}(q(x))$ denotes the convex subspace generated by $q(x)$; see definition (2.16).

We come to the first of the main results of this chapter.

Theorem 4.20. *Let (L, V, q) be a layered lattice. Let $\langle \cdot, \cdot \rangle : \mathbb{R} \otimes_{\mathbb{Z}} L \times \mathbb{R} \otimes_{\mathbb{Z}} L \to V$ be the map given, on generators of the form $\alpha \otimes x, \beta \otimes y$ with $\alpha, \beta \in \mathbb{R}$ and $x, y \in L$, by*

$$\langle \alpha \otimes x, \beta \otimes y \rangle = \alpha\beta \langle x, y \rangle. \tag{4.21}$$

Then $(\mathbb{R} \otimes_{\mathbb{Z}} L, V, \langle \cdot, \cdot \rangle)$ is a layered Euclidean space. The injective map $\iota : L \hookrightarrow \mathbb{R} \otimes_{\mathbb{Z}} L$ given by $x \mapsto 1 \otimes x$ is such that for all $x \in L$ we have $\langle \iota(x), \iota(x) \rangle = q(x)$ and makes $\iota(L)$ into an embedded layered lattice.

Proof. In what follows we also will identify L with the subgroup $\iota(L)$ since ι is injective. The proof is done by induction on the dimension of V.

If $\dim V = 0$ then $L = E = \{0\}$ by the fact that $\langle \cdot, \cdot \rangle$ is positive-definite and we are done. If $\dim V = 1$, proposition (4.9) together with remark (4.10)

and an arbitrary chosen order isomorphism $V \simeq \mathbb{R}$, shows that E is a classical Euclidean space where L is an embedded classical lattice. By proposition (4.5), L is an *embedded layered lattice*.

Now suppose $n = \dim V > 1$ and let $V' \in \mathcal{C}(V)$ with $V' \neq \{0\}, V$. Let L' be the V'-th layer of L and $q_{V'}$ be the restriction of q to L'. By lemma (4.15), the triple $(L', V', q_{V'})$ is a layered lattice with $\dim V' < n$. By the induction hypothesis, $(\mathbb{R} \otimes_{\mathbb{Z}} L', V', \langle \cdot, \cdot \rangle_{V'})$ is a layered Euclidean space with $\langle \cdot, \cdot \rangle_{V'}$ given by equation (4.21) and $L' \subset \mathbb{R} \otimes_{\mathbb{Z}} L'$ is an embedded layered lattice. In what follows we let $E' = \mathbb{R} \otimes_{\mathbb{Z}} L'$.

Also by lemma (4.15), the triple $(L/L', V/V', q_{V/V'})$ is a layered lattice with $q_{V/V'}$ given by formula (4.16) and $\dim V/V' < n$. By the induction hypothesis this layered lattice is embedded in the layered Euclidean space $(\mathbb{R} \otimes_{\mathbb{Z}} L / \mathbb{R} \otimes_{\mathbb{Z}} L', V/V', \langle \cdot, \cdot \rangle_{V/V'})$ with $\langle \cdot, \cdot \rangle_{V/V'}$ again given by equation (4.21). Let $E = \mathbb{R} \otimes_{\mathbb{Z}} L$ and note that we can canonically identify $E/E' \cong \mathbb{R} \otimes_{\mathbb{Z}} L/L'$ by the flatness of $\mathbb{R}$.

I claim that $(E, V, \langle \cdot, \cdot \rangle)$ where $\langle \cdot, \cdot \rangle$ is given by formula (4.21) is a layered Euclidean space. Our first observation is that the following diagram is commutative. In the diagram, the horizontal arrows are the canonical maps (inclusions and projections) and the vertical arrows are the bilinear, symmetric, positive-definite, layered maps defined on L, L' and L/L' respectively given by lemma (4.12). Note that the morphisms on the second line are morphisms of *ordered* vector spaces.

$$\begin{tikzcd}
L' \times L' \arrow[r] \arrow[d] & L \times L \arrow[r] \arrow[d] & L/L' \times L/L' \arrow[d] \\
V' \arrow[r] & V \arrow[r] & V/V'
\end{tikzcd}$$

The commutativity of the left square is trivial. The commutativity of the right square follows from a simple computation: given $x, y \in L$ we have

$$\begin{aligned}
\langle x, y \rangle + V' &= (q(x+y) - q(x-y))/4 + V' \\
&= (q_{V/V'}(x+y+L') - q_{V/V'}(x-y+L'))/4 \\
&= \langle x + L', y + L' \rangle_{V/V'}.
\end{aligned}$$

Extending the map $\langle \cdot, \cdot \rangle$ on L to E by bilinearity we obtain the following diagram which again is commutative.

$$\begin{tikzcd} E' \times E' \arrow[r] \arrow[d] & E \times E \arrow[r] \arrow[d] & E/E' \times E/E' \arrow[d] \\ V' \arrow[r] & V \arrow[r] & V/V' \end{tikzcd} \tag{4.22}$$

In fact, the commutativity of the left square is again trivial to verify ($\langle \cdot, \cdot \rangle_{V'}$ is still the restriction of $\langle \cdot, \cdot \rangle$). To verify the commutativity of the right square we use the commutativity of the right square of the previous diagram together with the fact that $\langle \cdot, \cdot \rangle_{V/V'}$ on E/E' is obtained by extending $\langle \cdot, \cdot \rangle_{V/V'}$ on L/L' by bilinearity. The calculation is easy and we omit it.

Let $x \in E$. If $x \in E'$ then, by the induction hypothesis, $\langle \cdot, \cdot \rangle_{V'}$ is positive-definite and the above diagram shows that $\langle x, x \rangle \geqslant 0$ with equality if and only if $x = 0$. If $x \notin E'$ then since $\langle \cdot, \cdot \rangle_{V/V'}$ is positive-definite and $x + E'$ is non-zero we have $\langle x, x \rangle_{V/V'} > 0$ in V/V' which implies that $\langle x, x \rangle > 0$. Thus $\langle \cdot, \cdot \rangle$ is positive-definite.

Next we show that $\langle \cdot, \cdot \rangle$ is layered. To this end, note that the commutativity of diagram (4.22) holds *for every* $V' \in \mathcal{C}(V)$. In fact, although we fixed V' before, this choice was arbitrary. Furthermore, if we take either $V' = \{0\}$ or $V' = V$, the diagram collapses to a commutative square. Now, let $x, y \in E$ and take $E' = \mathcal{L}(y)$ and $V' = \mathcal{C}(\langle y, y \rangle)$. Then diagram (4.22) above gives

$$\langle x, y \rangle + V' = \langle x + E', y + E' \rangle_{V/V'} = \langle x + E', E' \rangle_{V/V'} = V'.$$

Hence, $\langle x, y \rangle \preccurlyeq \langle y, y \rangle$ and the proof that $\langle \cdot, \cdot \rangle$ is layered is complete.

Up to this point we have shown that $(E, V, \langle \cdot, \cdot \rangle)$ is a layered Euclidean space with $L \subset E$ and such that, for all $U \in \mathcal{C}^*(V)$ with predecessor U' in $\mathcal{C}(V)$, one has $L_U / L_{U'} \subset E_U / E_{U'}$ as an embedded (classical) lattice. By proposition (4.5), the subgroup $L \subset E$ is an embedded layered lattice. □

Corollary 4.23. *Let* (L, V, q) *be an* $\mathbb{R}$*-layered lattice with* $\dim V = 1$*. Then any order isomorphism* $V \to \mathbb{R}$ *makes* L *together with* $q : L \to V \simeq \mathbb{R}$ *into a (classical) lattice.*

Proof. By the previous theorem $(\mathbb{R} \otimes_{\mathbb{Z}} L, V, \langle \cdot, \cdot \rangle)$ is a layered Euclidean space into which L can be embedded. Since V is one-dimensional the result follows immediately from proposition (4.5). □

We recall definition (3.7) to the attention of the reader.

Remark 4.24. A classical lattice in a Euclidean space is a lattice in the sense of definition (4.6) when equipped with the associated quadratic norm map $q(x) = \langle x, x \rangle$. Axioms (i) and (ii) follow from the fact that the inner-product

is bilinear, symmetric and positive-definite. Axiom (iii) follows immediately from the discreteness of the embedded lattice.

The next theorem proves an analogue of the remark above. Namely, that an embedded layered lattice is a lattice in the sense of definition (4.7) when equipped with the associated quadratic norm. Recall that a set in a metric space is *bounded* if it is contained in some ball of finite radius. We first prove two lemmas.

Lemma 4.25. *Let $(E, \langle\cdot,\cdot\rangle)$ be a Euclidean space and $\phi \in \mathrm{Hom}\,(E, \mathbb{R})$ be a linear functional on E. Then for every $M \in \mathbb{R}$, the set $\{x \in E : \langle x, x\rangle + \phi(x) < M\}$ is bounded.*

Proof. As usual, we let q denote the quadratic norm associated to $\langle\cdot,\cdot\rangle$. It is enough to show that there exists $N \in \mathbb{R}$ positive, such that for all $x \in E$ with

$$q(x) + \phi(x) < M \tag{4.26}$$

we have $\sqrt{q(x)} \leqslant N$. Since ϕ linear and E is finite dimensional, ϕ is continuous and there exists $C > 0$ such that for all $x \in E$ we have $|\phi(x)| < C\sqrt{q(x)}$. Then, for $x \in E$ satisfying (4.26) we have

$$q(x) < M - \phi(x) < M + C\sqrt{q(x)}.$$

If $\sqrt{q(x)} \geqslant 1$ then the above inequality implies

$$\sqrt{q(x)} \leqslant \frac{M}{\sqrt{q(x)}} + C \leqslant |M| + C.$$

If, on the other hand, $\sqrt{q(x)} < 1$ then we obtain

$$\sqrt{q(x)} < \sqrt{|M| + C} < \max\{|M| + C, 1\}.$$

In either case, taking $N = \max\{|M| + C, 1\}$ establishes the result. □

Lemma 4.27. *Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space with $\dim V > 0$ and $L \subset E$ be an embedded layered lattice. Let $U \in \mathcal{C}(V)$ be the unique one-dimensional convex subspace of V, let E_U be the U-th layer of E and let $L_U = L \cap E_U$. Then for all $x \in L$, the function $f_x : E_U \to U$ given by*

$$f_x(y) = q(x + y) - q(x)$$

has the following property. The set $f_x(L_U) \subset U$ is well-ordered and for any non-empty subset $S \subset f_x(L_U)$ the set $f_x^{-1}(\min S) \cap L_U$ is finite.

Proof. Fix $x \in L$. First note that for all $y \in E_U$ we have

$$f_x(y) = q(x+y) - q(x) = q(y) + 2\langle x, y\rangle \in U$$

since the inner-product is layered. Thus f_x is well-defined.

Let $s \in S$ be arbitrary. Let $\phi : E_U \to \mathbb{R}$ be the map $\phi(y) = 2\langle x, y\rangle$. This is a linear functional on E_U and $(E_U, U, \langle\cdot,\cdot\rangle)$ is a classical Euclidean space, hence, by lemma (4.25), the set $Y = \{y \in E_U : f_x(y) \leqslant s\}$ is bounded. Since $L_U \subset E_U$ is an embedded (classical) lattice it is discrete and closed, hence, it intersects Y in a *finite*, non-empty, set. Going through every element of this set we conclude that S has a minimum and since we have $f_x^{-1}(\min S) \cap L_U \subset Y \cap L_U$ the former is finite. □

We come to the second main result of the chapter.

Theorem 4.28. *Let $L \subset E$ be an embedded layered lattice in the layered Euclidean space $(E, V, \langle\cdot,\cdot\rangle)$. Define $q : L \to V$ by $q(x) = \langle x, x\rangle$. Then (L, V, q) is an $\mathbb{R}$-layered lattice.*

Proof. It is easy to verify that the map q satisfies axioms (i) and (ii) from the definition (4.7) of a layered lattice. Let $S \subset q(L)$ with $S \neq \varnothing$. We will prove that $\min S$ exists and that the set $q^{-1}(\min S) \cap L$ is finite. We proceed by induction on the dimension of V. If $\dim V = 0$ then $q(L) = \{0\}$ and there is nothing to prove.

Now suppose V has dimension $n > 0$. Denote by U the unique one-dimensional convex subspace of V. Let E_U denote the U-th layer of E and $L_U = L \cap E_U$. We saw that $(E/E_U, V/U, \langle\cdot,\cdot\rangle_{V/U})$ is a layered Euclidean space and it is easy to check from the definition, that $L/L_U \subset E/E_U$ is an embedded layered lattice. Let $\overline{S}$ be the image of S under the projection $V \to V/U$ and note that $\overline{S} \subset q_{V/U}(L/L_U)$ where $q_{V/U}$ is the quadratic norm associated to the inner-product $\langle\cdot,\cdot\rangle_{V/U}$. By the induction hypothesis, $\overline{S}$ has a minimum $\min \overline{S}$ and the set $\overline{X} = q_{V/U}^{-1}(\min \overline{S}) \cap (L/L_U)$ is finite.

Fix a set $X \subset L \cap q^{-1}(S)$ of representatives for $\overline{X}$. Let $x \in X$. The translate $S - q(x) \subset V$ is non-empty since S is non-empty. Let $f_x : E_U \to U$ denote the function $y \mapsto q(x+y) - q(x)$. Since $q(x) \in S$ we see that $0 \in S - q(x)$ and, hence, that $f_x(L_U) \cap (S - q(x)) \neq \varnothing$ (note that $f_x(0) = 0$). By the previous lemma, the set $f_x(L_U) \cap (S - q(x))$ has a minimum and the set $Y_x = \big\{y \in L_U : f_x(y) = \min\big(f_x(L_U) \cap (S - q(x))\big)\big\}$ is finite. In particular, the set $\bigcup_{x \in X}(x + Y_x)$ is finite.

Let

$$m = \min_{x \in X}\big\{\min\big(f_x(L_U) \cap (S - q(x))\big) + q(x)\big\} \in V.$$

To finish the proof it suffices to show that $m = \min S$ and that if $z \in L$ is such that $q(z) = m$ then $z \in x + Y_x$ for some $x \in X$.

First note that $m \in S$ and that $m = f_{x'}(y') + q(x') = q(x' + y')$ for some $x' \in X$ and $y' \in L_U$. Thus m projects to $\min \overline{S}$ under $V \to V/U$. Let $s \in S$. We will show that $m \leqslant s$. Looking modulo U we have that $\min \overline{S} \leqslant s + U$ thus unless $s - m \in U$ we have $m < s$. So suppose $s - m \in U$. Let $w \in L$ be such that $q(w) = s$. Then $w \in \overline{X}$ and there is $x \in X$ such that $w - x \in L_U$. Then we have

$$f_x(w - x) = q(x + w - x) - q(x) = q(w) - q(x) \in S - q(x)$$

from which it follows that

$$f_x(w - x) \in f_x(L_U) \cap (S - q(x)).$$

Thus we have $m \leqslant f_x(w - x) + q(x) = q(w) = s$ by construction.

Now let $z \in L$ such that $q(z) = m \in S$. The argument of the last paragraph (with $s = m$) shows that $z \in \overline{X}$ and that there is $x \in X$ such that $z - x \in L_U$. Again, a straight-forward computation gives

$$f_x(z - x) = q(z) - q(x) = \min S - q(x) = \min(S - q(x)).$$

Thus, $z - x \in Y_x$, i.e., $z \in x + Y_x$. □

Remark 4.29. Proposition (4.2) says that a finitely generated subgroup of a Euclidean space is an embedded lattice if and only if it is generated by a linearly independent set. In the context of embedded layered lattices this is no longer the case. The following example illustrates that the group generated by an arbitrary set of linearly independent vectors of a layered Euclidean space does not need to be an embedded layered lattice.

Let $E = \mathbb{R}^2, V = \mathbb{R}^{\underline{2}}$ with the anti-lexicographic order and denote by $\{e_1, e_2\}$ the canonical basis of E. Let

$$\mathbf{B}^1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \mathbf{B}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

and define $\langle \cdot, \cdot \rangle$ on E by $(x, y) \mapsto (x^T \mathbf{B}^1 y, x^T \mathbf{B}^2 y)$ where $x, y \in E$. The vectors $b_1 = e_2$ and $b_2 = \sqrt{2}e_2 + e_1$ form a basis of E but their $\mathbb{Z}$-span is not a layered lattice since

$$q(mb_1 + nb_2) = (n^2, (m + n\sqrt{2})^2)$$

thus $\{q(mb_1 + nb_2) : n \neq 0\} \subset q(L)$ has no minimal element. One also sees that $L/L_1 = L \subset E/E_1$ is not a lattice since rank $L = 2$ while $\dim E/E_1 = 1$.

Despite the above counter-example, we have the following very useful result. It tells us that bases of layered Euclidean spaces which are *rational*, in a precise sense to be described below, generate layered lattices. We recall definition (3.1) where we introduced the Gram-matrix associated to a bilinear form.

Proposition 4.30. *Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space and let $n = \dim V$ and $m = \dim E$. Let $\{v_k\}_{k\in\underline{n}}$ be an anti-lexicographic basis of V and $\{b_i\}_{i\in\underline{m}}$ be a basis of E. Suppose that the Gram matrix of $\langle\cdot,\cdot\rangle$ with respect to $\{b_i\}_{i\in\underline{m}}$ has values in the rational subspace $\sum_{k\in\underline{n}} \mathbb{Q}\cdot v_k$ of V. Then the group generated by $\{b_i\}_{i\in\underline{m}}$ is a layered lattice.*

Proof. Let $\{v_k^*\}_{k\in\underline{n}}$ be the dual basis of $\{v_k\}_{k\in\underline{n}}$. This induces an order-isomorphism $V \simeq \mathbb{R}^{\underline{n}}$ given by $v \mapsto (v_k^*(v))_{k\in\underline{n}}$. Let L be the group generated by $\{b_i\}_{i\in\underline{m}}$.

Let $U' \in \mathcal{C}(V)$. Let $E_{U'}$ be the U'-th layer of E and $L_{U'} = E_{U'} \cap L$. This is a subgroup of L and the map

$$\langle\cdot,\cdot\rangle_{U'} : E/E_{U'} \times E/E_{U'} \to V/U' \simeq \textstyle\sum_{k>\dim U'} \mathbb{R}\cdot v_k$$

given by

$$(x + E_{U'}, y + E_{U'}) \mapsto \langle x, y\rangle + U' \mapsto \textstyle\sum_{k>\dim U'} v_k^*(\langle x, y\rangle)v_k$$

is well-defined since $\langle\cdot,\cdot\rangle$ is a layered form. I claim that $L/L_{U'} \subset E/E_{U'}$ is an embedded layered lattice. If $U' = V$ then $E/E_{U'}$ and $L/L_{U'}$ equal $\{0\}$ and we are done. Now suppose $U' \neq V$ and let $U \in \mathcal{C}(V)$ be the successor of U' in $\mathcal{C}(V)$. By induction, we assume that $L/L_U \subset E/E_U$ is an embedded layered lattice.

By (3.8), the pair $(E_U/E_{U'}, \langle\cdot,\cdot\rangle_{U'})$ with $\langle\cdot,\cdot\rangle_{U'}$ restricted to E_U is a (classical) Euclidean space once we identify $U/U' \simeq \mathbb{R}$ via the order-isomorphism $V \simeq \mathbb{R}^{\underline{n}}$ described above. So, by proposition (4.5), to show that $L/L_{U'} \subset E/E_{U'}$ is an embedded layered lattice is suffices to show that $L_U/L_{U'} \subset E_U/E_{U'}$ is an embedded *classical* lattice.

The hypothesis on the Gram-matrix with respect to $\{b_i\}_{i\in\underline{m}}$ implies that $\langle L/L_{U'}, L/L_{U'}\rangle \subset \sum_{k>\dim U'} \mathbb{Q}\cdot v_k \subset V$. In particular, the restriction of this map to $L_U/L_{U'} \times L_U/L_{U'}$ satisfies $\langle L_U/L_{U'}, L_U/L_{U'}\rangle \subset \mathbb{Q}\cdot v_k$ for $k = \dim U$. Since $L_U/L_{U'}$ is finitely generated, there exists $p \in \mathbb{Z}_{>0}$ such that, in fact, we have

$$\langle L_U/L_{U'}, L_U/L_{U'}\rangle \subset \frac{1}{p}\mathbb{Z}\cdot v_k.$$

In particular, there exist $\epsilon \in \mathbb{R}_{>0}$ and a ball $B \subset E_U/E_{U'}$ with center 0 and radius ϵ such that $(L_U/L_{U'}) \cap B = \{0\}$. Thus $L_U/L_{U'}$ is a discrete subset of $E_U/E_{U'}$ and $L_U/L_{U'} \subset E_U/E_{U'}$ is an embedded classical lattice. This completes the induction.

Up to this point we have shown that $L \subset E$ is an embedded layered lattice. By theorem (4.28), we conclude that (L, V, q) is a layered lattice with the quadratic norm induced by $\langle\cdot,\cdot\rangle$. $\square$

4.3 Exterior powers of layered lattices

In this short section we prove that exterior powers of layered lattices are layered lattices. In a classical lattice, given a positive real number λ, there are only a finite number of sublattices with discriminant smaller than λ. We will use the result of this section to establish an analogue of this statement for layered lattices.

Theorem 4.31. *Let (L, V, q) be an layered lattice. Let $r \in \mathbb{Z}_{\geqslant 0}$. Let $\langle \cdot, \cdot \rangle : L \times L \to S^r(V)$ be the $\mathbb{Z}$-bilinear map which is given on generators $x_1 \wedge \cdots \wedge x_r$, $y_1 \wedge \cdots \wedge y_r \in \bigwedge^r L$ by the formula*

$$\langle x_1 \wedge \cdots \wedge x_r, y_1 \wedge \cdots \wedge y_r \rangle = \det(\langle x_i, y_j \rangle)_{i,j \in \underline{r}}.$$

Then the triple $(\bigwedge^r L, S^r(V), q)$ where $q : \bigwedge^r L \to S^r(V)$ is given by $q(x) = \langle x, x \rangle$ is a layered lattice.

Proof. By theorem (4.20), the lattice L can be embedded in a layered Euclidean space $(E, V, \langle \cdot, \cdot \rangle)$ of dimension equal to the rank of L. Take a layered basis $I \to L \subset E$ of E that generates L as a group. In theorem (3.26), we saw that defining $\langle \cdot, \cdot \rangle : \bigwedge^r E \times \bigwedge^r E \to S^r(V)$ by bi-linearly extending the formula

$$\langle x_1 \wedge \cdots \wedge x_r, y_1 \wedge \cdots \wedge y_r \rangle = \det(\langle x_i, y_j \rangle)_{i,j \in \underline{r}}$$

makes the triple $(\bigwedge^r E, S^r(V), \langle \cdot, \cdot \rangle)$ into a layered Euclidean space. Furthermore, we saw that $I \to E$ induces in a canonical way a layered basis $\bigwedge^r I \to \bigwedge^r E$. The subgroup of $\bigwedge^r E$ generated by this basis equals $\bigwedge^r L$ and, hence, $\bigwedge^r L \subset \bigwedge^r E$ is an embedded layered lattice. By theorem (4.28), $\bigwedge^r L$ is a layered lattice. $\square$

4.4 The discriminant

In this section we prove that the set of "sizes" of sublattices of a layered lattice is well-ordered. The idea of "size" is captured by the concept of the *discriminant* of a lattice. Our definition will coincide with the definition of discriminants of classical lattices whenever we have a layered lattice (L, V, q) where $V \simeq \mathbb{R}$ as ordered vector spaces.

Proposition 4.32. *Let (L, V, q) be a layered lattice of rank $r \in \mathbb{Z}_{\geqslant 0}$ and $\{b_i\}_{i \in \underline{r}}$ be an ordered basis of L. Then the quantity*

$$D(L) = \det(\langle b_i, b_j \rangle)_{i,j \in \underline{r}} \in S^r(V)$$

does not depend the basis chosen to calculate it.

Proof. The result follows exactly as in the classical case. Let $S(V)$ denote the symmetric algebra of V. If $\{c_j\}_{j\in\underline{r}}$ is another ordered basis for L then there exists a matrix

$$(\alpha_{ij})_{i,j\in\underline{r}} \in \mathrm{GL}_r(\mathbb{Z}) \subset \mathrm{GL}_r(S(V))$$

satisfying $b_i = \sum_j \alpha_{ij} c_j$ and we have

$$\det(\langle b_i, b_j\rangle) = \det(\alpha_{ij})\det(\langle c_i, c_j\rangle)\det((\alpha_{ij})^T) = \det(\alpha_{ij})^2 \det(\langle c_i, c_j\rangle).$$

Since the determinant of (α_{ij}) equals ± 1 this equation proves the result. □

Definition 4.33. Let (L, V, q) be a layered lattice. The quantity $D(L)$ introduced above is called the *discriminant* of L.

Remark 4.34. If (L, V, q) is a layered lattice with V one-dimensional then any order isomorphism $V \simeq \mathbb{R}$ allow us view it as a classical lattice. In this case, this isomorphism induces an isomorphism $S^r(V) \simeq \mathbb{R}$. The discriminant of (L, V, q) as a layered lattice corresponds, via this chosen isomorphism, to the discriminant of (L, q) as a classical lattice. As the choice of another order isomorphism $V \simeq \mathbb{R}$ has the effect of scaling the classical lattice, the discriminant will be scaled by the corresponding r-th power.

The main result of this section is the following.

Theorem 4.35. *Let (L, V, q) be a layered lattice of rank $r \in \mathbb{Z}_{\geqslant 0}$. Then for all $s \in \mathbb{Z}_{\geqslant 0}$ with $0 \leqslant s \leqslant r$ the set*

$$\{D(K) : K \subset L \text{ a sublattice or rank } s\} \subset S^s(V)$$

is well-ordered.

Proof. The theorem is trivially true if $s = 0$. Suppose $s = 1$. Then all sublattices of L of rank s are of the form $K = \mathbb{Z}x$ for some $x \in L, x \neq 0$. Thus we have

$$\{D(K) : K \subset L \text{ a sublattice of rank } 1\ \} = q(L) \setminus \{0\},$$

which is well-ordered.

For $s > 1$, if $K = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_s \subset L$ is a sublattice of rank s, then $\bigwedge^s L$ is a layered lattice by theorem (4.31) and $\bigwedge^s K \subset \bigwedge^s L$ is a sublattice of rank 1. Then we have

$$D\left(\bigwedge^s K\right) = q(x_1 \wedge \cdots \wedge x_s) = D(K)$$

and by the case $s = 1$ above we conclude that the theorem holds for general s as well. □

CHAPTER 5

The layered Gram-Schmidt procedure

In this chapter we introduce the Gram-Schmidt procedure: a way of obtaining, from a given basis of a layered Euclidean space, an orthogonal basis of that space (see definition (3.19)). The procedure generalizes the usual Gram-Schmidt procedure for Euclidean spaces. At the end of the chapter we give two ways of computing those bases. These results will be used in chapter 6.

5.1 Associated Gram-Schmidt bases

We start by restating theorem (3.22) from chapter 3.

Theorem 5.1. *Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space with $\dim E = m$. Let $\{b_i\}_{i\in\underline{m}}$ be an ordered basis of E and $F_0 \subsetneqq \cdots \subsetneqq F_m$ be the flag of E induced by this basis. Then there exists a unique basis $\{b_i^*\}_{i\in\underline{m}}$ such that for all $i \in \underline{m}$ we have $b_i^* \in F_{i-1}^{\perp}$ and $b_i - b_i^* \in F_{i-1}$. Furthermore, this basis is orthogonal and induces the same flag $F_0 \subsetneqq \cdots \subsetneqq F_m$ of V.*

Definition 5.2. Let $I \to E$ be an ordered basis of a layered Euclidean space. The basis given by the theorem above is called the *Gram-Schmidt basis associated to $I \to E$* and we denote it by $(I \to E)^*$. $\diamondsuit$

Notation. As written above, if $I \to E$ is a basis of a layered Euclidean space E, its associated Gram-Schmidt is denoted by $(I \to E)^*$. If b_i is the image of $i \in I$ in E we will denote its corresponding Gram-Schmidt vector by b_i^*.

Remark 5.3. Note that by remark (3.10 (b)), the Gram-Schmidt basis associated to a layered basis is still layered. Thus, it is a layered, orthogonal basis. In particular, the conclusion of corollary (3.23) holds for those bases.

Before showing how to compute a Gram-Schmidt basis from a given basis we give the following definition, which introduces a handy notation. We remind the reader of definition (2.16).

Remark 5.4. Note that if $(E, V, \langle\cdot,\cdot\rangle)$ is layered Euclidean space, then the choice of an anti-lexicographic basis $\{v_k\}_{k\in\underline{n}}$ of V induce order-isomorphisms $U/U' \simeq \mathbb{R}$ for every $U \in \mathcal{C}^*(V)$ and its predecessor $U' \in \mathcal{C}(V)$. These isomorphisms are all characterized as the linear maps induced by $v_k \mapsto 1$ for each k.

We recall some notation from the review section of the introduction: for an ordered set S and $s \in S$, whenever it exists, we denote the *predecessor* of s by s'.

Definition 5.5. Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space with $n = \dim V$ and let $\{v_k\}_{k\in\underline{n}}$ be an anti-lexicographic basis of V. For each $x \in E\backslash\{0\}$ define the linear map $(\cdot, x) : E \to \mathbb{R}$ as the composition

$$E \to \mathcal{C}(q(x)) \to \mathcal{C}(q(x))/(\mathcal{C}(q(x))') \simeq \mathbb{R}$$

given by

$$y \mapsto \langle y, x\rangle \mapsto \langle y, x\rangle + (\mathcal{C}(q(x))') \mapsto (y, x)$$

and the order-isomorphism $\mathcal{C}(q(x))/\mathcal{C}(q(x) - 1) \simeq \mathbb{R}$ obtained as in remark (5.4). For $x = 0$ we define $(\cdot, x) : E \to V$ to be the zero map. $\diamondsuit$

Remark 5.6. Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space and fix an anti-lexicographic basis of V. We note the following properties of the linear map $(\cdot, x)$ defined above. All of these follow directly from the definition and are straight-forward to prove.

(a) Let $x, y \in E$. If x and y have the same layer then $(x, y) = (y, x)$ since, then, $\mathcal{C}(q(x)) = \mathcal{C}(q(y))$.

(b) For any $x \in E \setminus \{0\}$ we have $(x, x) = \mathrm{lc}(\langle x, x\rangle) > 0$ where $\mathrm{lc}(\cdot)$ is the leading coefficient function we defined in (2.31).

(c) Let $x, y \in E$. If $y \perp x$ then $(y, x) = 0$.

Proposition 5.7. *Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space with $\dim V = n$ and $\dim E = m$. Fix an anti-lexicographic basis $\{v_k\}_{k\in\underline{n}}$ of V and let $\{b_i\}_{i\in\underline{m}}$ be an ordered basis of E. Then the Gram-Schmidt basis associated to $\{b_i\}_{i\in\underline{m}}$ satisfies the equations*

$$b_i^* = b_i - \sum_{r<i} \lambda_{i,r} b_r^*, \quad i \in \underline{m} \tag{5.8}$$

with $\lambda_{i,1}, \dots, \lambda_{i,i-1} \in \mathbb{R}$ *determined as the unique solution of the linear system*

$$\sum_{r \leqslant j} \lambda_{i,r}(b_r^*, b_j^*) = (b_i, b_j^*), \quad j < i \tag{5.9}$$

and where $(\cdot, b_j^*)$ *is as in the previous definition.*

Proof. Let $\{F_i\}_{i \in \underline{m}}$ be the flag induced by $\{b_i\}_{i \in \underline{m}}$ and let $\{b_i^*\}_{i \in \underline{m}}$ be its associated Gram-Schmidt basis. Fix $i \in \underline{m}$. Since $b_i - b_i^* \in F_{i-1}$ we can write

$$b_i - b_i^* = \sum_{r<i} \lambda_{i,j} b_r^* \in F_{i-1}.$$

This is equation (5.8). It remains to show that the numbers $\lambda_{i,1}, \dots, \lambda_{i,i-1} \in \mathbb{R}$ form the unique solution to the linear system (5.9).

To this end we take the image of equation (5.8) under $(\cdot, b_j^*)$ for each $j < i$ to obtain the system

$$\sum_{r<i} \lambda_{i,r}(b_r^*, b_j^*) = (b_i, b_j^*) - (b_i^*, b_j^*), \quad j < i.$$

By orthogonality and remark (5.6 (c)), for all $r > j$ we have $(b_r^*, b_j^*) = 0$ and for all $i > j$ we have $(b_i^*, b_j^*) = 0$. We thus obtain the linear system (5.9); it has a unique solution since it is a triangular system with diagonal entries equal to $(b_j^*, b_j^*) > 0$ by (5.6 (b)). □

Remark 5.10. (a) Following the notation of the proposition above, for each $1 \leqslant i \leqslant m$ and $1 \leqslant j < m$ define

$$\alpha_{i,r} = \frac{(b_i, b_r^*)}{(b_r^*, b_r^*)}, \ r \in \underline{i-1} \qquad \beta_{j,r} = \frac{(b_r^*, b_j^*)}{(b_j^*, b_j^*)}, \ r \in \underline{j-1}$$

(so there is no $\alpha_{1,r}$ and no $\beta_{1,r}$). Then solving the triangular system (5.9) we obtain, for each $i \in \underline{m}$ and each $j < i$,

$$\lambda_{i,j} = \alpha_{i,j} - \sum_{r<j} \lambda_{i,r} \beta_{j,r}. \tag{5.11}$$

Note that whenever b_r^* and b_j^* have the same layer, by remark (5.6 (a),(c)), we have $\beta_{j,r} = 0$. In particular, in the classical case where V is one-dimensional, we obtain the usual Gram-Schmidt procedure.

(b) Since the Gram-Schmidt basis associated to a given basis does not change the induced flag, there exist constants $\{\nu_{i,j}\}_{1 \leqslant j < i \leqslant m}$ such that $b_i^* = b_i - \sum_{j<i} \nu_{i,j} b_j$. Since $b_i^* \in F_i^\perp$ the same steps of the proof above give us the system

$$\sum_{r<i} \nu_{i,r}(b_r, b_j) = (b_i, b_j), \quad j < i. \tag{5.12}$$

This system is not necessarily triangular, in fact, it might even be singular. Thus, it is possible that we are unable to calculate $\{\nu_{i,j}\}_{1\leqslant j<i\leqslant m}$ from it. We will show later on that by first applying a "layering" procedure to the $\{b_i\}_{i\in\underline{m}}$, we arrive at an intermediate basis for which the system above *is* invertible. The advantage of (5.12) lies in the fact that it is much easier to give good bounds for the arithmetical operations involved in solving it, compared to the system (5.9) of the last proposition. We will return to this point later.

Next, we give some formulae establishing the effects on the associated Gram-Schmidt basis and to the change of basis matrix, when the original basis is subjected to certain "elementary" transformations. We remind the reader of definition (2.16) where we introduced the relations $\ll$, $\sim$ and $\simeq$ on an ordered vector space and of definition (5.5) where we introduced the functional $(\cdot, x)$ for an element x of a layered Euclidean space.

Proposition 5.13. *Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space with $\dim V = n$ and $\dim E = m$. Let $\{b_i\}_{i\in\underline{m}}$ be an ordered basis of E, let $\{b_i^*\}_{i\in\underline{m}}$ be its associated Gram-Schmidt basis and $\{\lambda_{i,j}\}_{1\leqslant j<i\leqslant m}$ be the numbers such that $b_i = b_i^* + \sum_{j<i}\lambda_{i,j}b_j^*$ for all $i \in \underline{m}$ (see proposition (5.7)).*

Let furthermore k, $l \in \underline{m}$, $l < k$, and $\gamma \in \mathbb{R}$. Define the vectors $\{c_i\}_{i\in\underline{m}}$ by $c_i = b_i$ for $i \neq k$ and $c_k = b_k + \gamma b_l$. Then $\{c_i\}_{i\in\underline{m}}$ is a basis of E and its associated Gram-Schmidt basis equals $\{b_i^*\}_{i\in\underline{m}}$. The corresponding set of numbers $\{\mu_{i,j}\}_{1\leqslant j<i\leqslant m}$ obtained from (5.9) with the basis $\{c_i\}_{i\in\underline{m}}$ in place of $\{b_i\}_{i\in\underline{m}}$ are given by the equations

$$\begin{aligned}
&\mu_{i,j} = \lambda_{i,j}, && \text{if } i \neq k,\ 1 \leqslant j < i,\\
&\mu_{k,j} = \lambda_{k,j} + \gamma\lambda_{l,j}, && \text{if } j < l,\\
&\mu_{k,l} = \lambda_{k,l} + \gamma,\\
&\mu_{k,j} = \lambda_{k,j}, && \text{if } l < j < k.
\end{aligned}$$

Proof. It is clear that $\{c_i\}_{i\in\underline{m}}$ is a basis of E and that the flags induced by $\{b_i\}_{i\in\underline{m}}$ and $\{c_i\}_{i\in\underline{m}}$ are the same. Let $\{F_i\}_{i\in\underline{m}}$ be this flag. Note that for any $i \in \underline{m}$, we have

$$c_i - b_i^* = c_i - b_i + b_i - b_i^* \in F_{i-1}.$$

Since by definition we have that $c_i^* \in F_{i-1}^{\perp} \cap F_i$ is unique with the property that $c_i - c_i^* \in F_{i-1}$, we conclude that $c_i^* = b_i^*$. Using this fact we have that, for $i \neq k$,

$$c_i = b_i = b_i^* + \sum_{j<i}\lambda_{i,j}b_j^* = c_i^* + \sum_{j<i}\lambda_{i,j}c_j^*$$

which implies $\mu_{i,j} = \lambda_{i,j}$ for $i \neq k$ and $j < i$. Similar reasoning gives us

$$c_k = b_k + \gamma b_l = c_k^* + \sum_{j<l}(\lambda_{k,j} + \gamma\lambda_{l,j})c_j^* + (\lambda_{k,l} + \gamma)c_l^* + \sum_{l<j<k}\lambda_{k,j}c_j^*$$

which implies the remaining formulae. □

In figure (5.14) below we exemplify proposition (5.13) in a simple case.

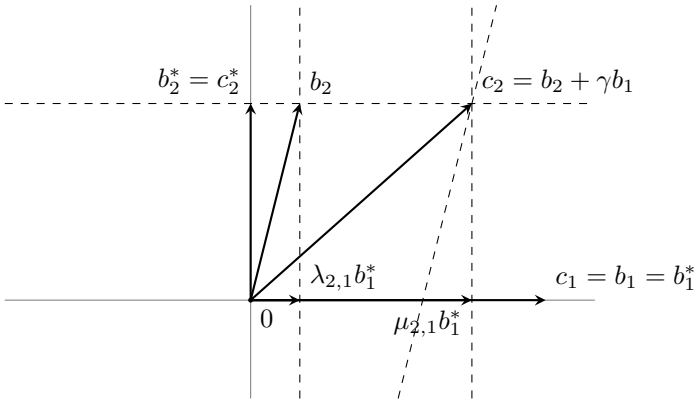

Figure 5.14: We have a basis $\{b_1, b_2\}$ of a two-dimensional layered Euclidean space and its associated Gram-Schmidt basis. The effect of adding a multiple γb_1 of the first basis vector to b_2 is reflected in the identity $\mu_{2,1} = \lambda_{2,1} + \gamma$.

Proposition 5.15. *Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space with $\dim V = n$ and $\dim E = m$. Let $\{b_i\}_{i\in\underline{m}}$ be an ordered basis of E, let $\{b_i^*\}_{i\in\underline{m}}$ be its associated Gram-Schmidt basis and $\{\lambda_{i,j}\}_{1\leqslant j<i\leqslant m}$ be the numbers such that $b_i = b_i^* + \sum_{j<i} \lambda_{i,j} b_j^*$ for all $i \in \underline{m}$ (see proposition (5.7)).*

Let furthermore $k \in \{2, \ldots, m\}$ and define the vectors $\{c_i\}_{i\in\underline{m}}$ by $c_i = b_i$ for $i \neq k$, $k-1$ and $c_{k-1} = b_k$ and $c_k = b_{k-1}$. Then $\{c_i\}_{i\in\underline{m}}$ is a basis of E. Denoting its associated Gram-Schmidt basis by $\{c_i^*\}_{i\in\underline{m}}$ and the corresponding set of numbers $\{\mu_{i,j}\}_{1\leqslant j<i\leqslant m}$ obtained from (5.9) with the basis $\{c_i\}_{i\in\underline{m}}$ in place of $\{b_i\}_{i\in\underline{m}}$, we have the following.

(a) *For all $1 \leqslant i < k-1$ we have $c_i^* = b_i^*$ and $\mu_{i,j} = \lambda_{i,j}$ for all $j < i$.*

(b) *We have $c_{k-1}^* = b_k^* + \lambda_{k,k-1} b_{k-1}^*$ and for $1 \leqslant j < k-1$ we have $\mu_{k-1,j} = \lambda_{k,j}$.*

(c) *We have $c_k^* = -\mu_{k,k-1} b_k^* + (1 - \mu_{k,k-1}\lambda_{k,k-1}) b_{k-1}^*$ where*

$$\begin{aligned}
\mu_{k,k-1} &= 0, && \text{if } q(b_{k-1}^*) \ll q(b_k^*),\\
\mu_{k,k-1} &= \lambda_{k,k-1} \tfrac{(b_{k-1}^*, b_{k-1}^*)}{(c_{k-1}^*, c_{k-1}^*)}, && \text{if } q(b_{k-1}^*) \sim q(b_k^*),\\
\mu_{k,k-1} &= \lambda_{k,k-1}^{-1}, && \text{if } q(b_k^*) \ll q(b_{k-1}^*) \text{ and } \lambda_{k,k-1} \neq 0,\\
\mu_{k,k-1} &= \tfrac{(b_{k-1}^*, b_k^*)}{(b_k^*, b_k^*)}, && \text{if } q(b_k^*) \ll q(b_{k-1}^*) \text{ and } \lambda_{k,k-1} = 0,
\end{aligned}$$

and for $1 \leqslant j < k-1$ *we have* $\mu_{k,j} = \lambda_{k-1,j}$.

(d) *For all* $k < i \leqslant m$ *we have* $c_i^* = b_i^*$ *and*

$$\begin{aligned}
&\mu_{i,j} = \lambda_{i,j}, \text{ for all } j < i \text{ with } j \neq k-1,\ k,\\
&\mu_{i,k-1} = \mu_{k,k-1}\lambda_{i,k-1} + (1 - \lambda_{k,k-1}\mu_{k,k-1})\lambda_{i,k},\\
&\mu_{i,k} = \lambda_{i,k-1} - \lambda_{k,k-1}\lambda_{i,k}.
\end{aligned}$$

Proof. Let $\{F_i\}_{i\in\underline{m}_0}$ and $\{G_i\}_{i\in\underline{m}_0}$ be the flags of E induced by the bases $\{b_i\}_{i\in\underline{m}}$ and $\{c_i\}_{i\in\underline{m}}$ respectively.

(a) This is trivial since $c_i = b_i$ for $1 \leqslant i < k-1$.

(b) Since $F_i = G_i$ for $i \neq k-1$, in particular for $i = k-2$, we have that $c_{k-1}^* \in G_{k-2}^\perp = F_{k-2}^\perp$ is the unique vector such that

$$b_k - c_{k-1}^* = c_{k-1} - c_{k-1}^* \in F_{k-2}.$$

Since $b_k^* + \lambda_{k,k-1}b_{k-1}^*$ fulfills these requirements we have

$$c_{k-1}^* = b_k^* + \lambda_{k,k-1}b_{k-1}^*. \tag{5.16}$$

Now, from (5.8) for $i = k$ and adding $\lambda_{k,k-1}b_{k-1}^*$ we obtain

$$b_k^* + \lambda_{k,k-1}b_{k-1}^* = b_k - \sum_{r<k-1} \lambda_{k,r}b_r^*.$$

Using (a) and (5.16) we obtain $c_{k-1}^* = c_{k-1} + \sum_{r<k-1} \lambda_{k,r}c_r^*$ from which we conclude that $\mu_{k-1,j} = \lambda_{k,j}$ for $1 \leqslant j < k-1$.

(c) By (b) applied to the bases $\{b_i\}_{i\in\underline{m}}$ and $\{c_i\}_{i\in\underline{m}}$ with their roles interchanged, we obtain

$$b_{k-1}^* = c_k^* + \mu_{k,k-1}c_{k-1}^* \tag{5.17}$$

and $\mu_{k,j} = \lambda_{k-1,j}$ for $j < k-1$. Substituting (5.16) in (5.17) we obtain the equation for c_k^* stated in the proposition. It remains to calculate $\mu_{k,k-1}$. Taking the image of both sides of equation (5.17) under the functional $(\cdot, c_{k-1}^*)$ we obtain

$$(c_k^*, c_{k-1}^*) + \mu_{k,k-1}(c_{k-1}^*, c_{k-1}^*) = (b_{k-1}^*, c_{k-1}^*).$$

Since $c_k^* \perp c_{k-1}^*$ we have $(c_k^*, c_{k-1}^*) = 0$, which gives

$$\mu_{k,k-1}(c_{k-1}^*, c_{k-1}^*) = (b_{k-1}^*, c_{k-1}^*). \tag{5.18}$$

If $q(b_{k-1}^*) \ll q(b_k^*)$, then (5.16) implies that $(\cdot, c_{k-1}^*) = (\cdot, b_k^*)$ and the right-hand side of equation (5.18) will equate to zero thus implying $\mu_{k,k-1} = 0$. Figure (5.19) below exemplifies this situation.

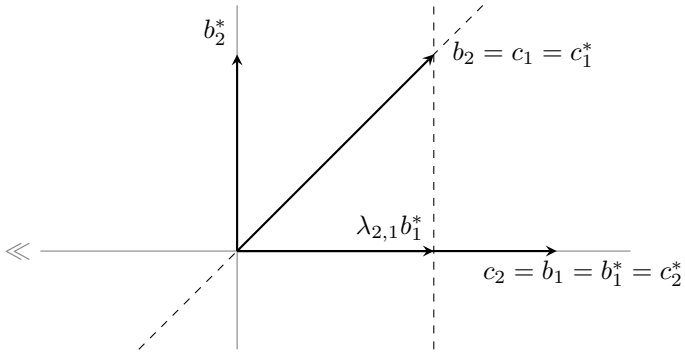

Figure 5.19: Here we represent the effect of swapping two basis vectors b_1 and b_2 with the property that $q(b_1^*) \ll q(b_2^*)$. The $\ll$ symbol beside the horizontal axis symbolizes the fact that this subspace is a lower layer. By (c) of proposition (5.15) we have $\mu_{2,1} = 0$ and $c_2^* = b_1^*$.

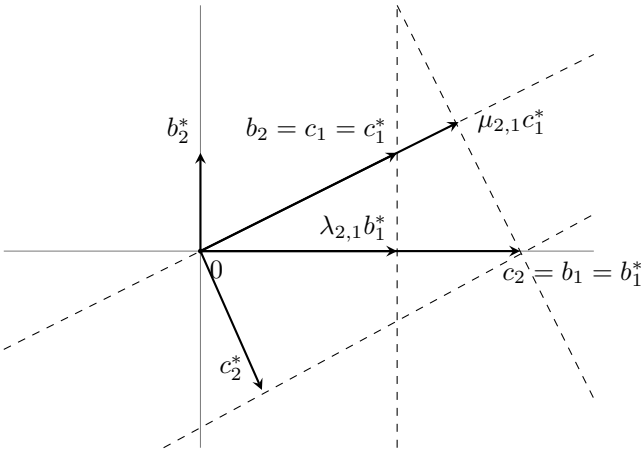

Figure 5.20: Swapping two basis vectors of the same layer has the effect described above on the associated Gram-Schmidt basis. It is analogous to the classical case. Item (c) of proposition (5.15) gives $\mu_{2,1} = \lambda_{2,1} \frac{(b_{k-1}^*, b_{k-1}^*)}{(c_{k-1}^*, c_{k-1}^*)}$.

Similar to equation (5.18), by symmetry we have

$$\lambda_{k,k-1}(b_{k-1}^*, b_{k-1}^*) = (c_{k-1}^*, b_{k-1}^*). \tag{5.21}$$

Now suppose $q(b^*_{k-1}) \sim q(b^*_k)$. Then b^*_{k-1} and b^*_k have the same layer, which has to be the layer of c^*_{k-1} as well (to see this compute $q(c^*_{k-1})$ using (5.16)). By remark (5.6), we have $(b^*_{k-1}, c^*_{k-1}) = (c^*_{k-1}, b^*_{k-1})$. Combining (5.18) with (5.21) we arrive at the desired expression for $\mu_{k,k-1}$. This situation is exemplified in figure (5.20) above.
Finally, suppose $q(b^*_k) \ll q(b^*_{k-1})$. Equation (5.16) implies

$$\begin{aligned} (\cdot, c^*_{k-1}) &= (\cdot, b^*_k), && \text{if } \lambda_{k,k-1} = 0, \\ (\cdot, c^*_{k-1}) &= \lambda_{k,k-1}(\cdot, b^*_{k-1}), && \text{if } \lambda_{k,k-1} \neq 0. \end{aligned}$$

In the first case, equations (5.18) and (5.16) give

$$\mu_{k,k-1} = \frac{(b^*_{k-1}, b^*_k)}{(b^*_k, b^*_k)}$$

as before, but now the numerator might be non-zero by the non-symmetry of the orthogonality relation (this is the case in figure (5.22) below). If $\lambda_{k,k-1} \neq 0$ we obtain

$$\mu_{k,k-1} = \frac{\lambda_{k,k-1}(b^*_{k-1}, b^*_{k-1})}{\lambda^2_{k,k-1}(b^*_{k-1}, b^*_{k-1})} = \lambda^{-1}_{k,k-1}$$

which is exemplified in figure (5.23).

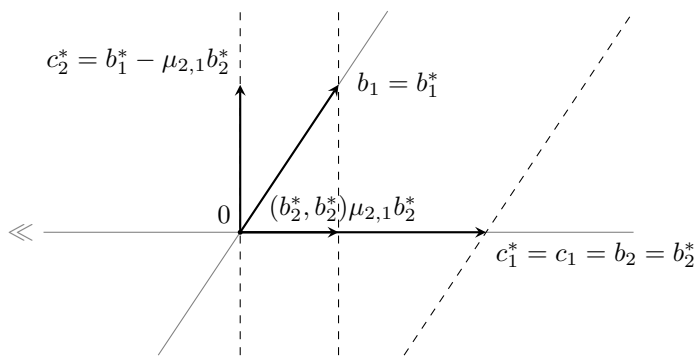

Figure 5.22: The effect of swapping basis vectors b_1, b_2 such that $q(b^*_2) \ll q(b^*_1)$ and $\lambda_{2,1} = 0$. Again, we draw the axes non-perpendicularly to illustrate the possibility that $b^*_1 \not\perp b^*_2$. The symbol $\ll$ beside the horizontal axis symbolizes the fact that that subspace is a lower layer. By (c) of proposition (5.15) we have $\mu_{2,1} = (b^*_1, b^*_2)/(b^*_2, b^*_2)$ and $c^*_2 = b^*_1 - \mu_{2,1}b^*_2$. Although in this two-dimensional case we have $b^*_2 = b_2$ this is not the case in general.

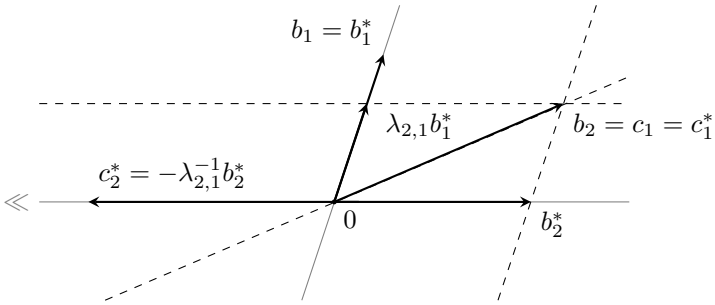

Figure 5.23: The effect of swapping basis vectors b_1, b_2 such that $q(b_2^*) \ll q(b_1^*)$ and $\lambda_{2,1} \neq 0$. We chose to draw the axes non-perpendicularly to illustrate the non-symmetry of the orthogonality relation, i.e., here we might have $b_1^* \not\perp b_2^*$. The symbol $\ll$ beside the horizontal axis symbolizes the fact that that subspace is a lower layer. By (c) of proposition (5.15) we have $\mu_{2,1} = \lambda_{2,1}^{-1}$ and $c_2^* = -\lambda_{2,1}^{-1} b_2^*$.

(d) For $i > k$, following the same argument as in (b) we have $F_{i-1} = G_{i-1}$, which together with $b_i = c_i$ immediately implies $c_i^* = b_i^*$. From this and equation (5.8) we obtain $\sum_{r<i} \mu_{i,r} c_r^* = \sum_{r<i} \lambda_{i,r} b_r^*$, which we can rearrange using that $c_r^* = b_r^*$ for $r \neq k, k-1$ to

$$\sum_{r \neq k-1,k} (\mu_{i,r} - \lambda_{i,r}) b_r^* = \sum_{r=k-1,k} (\lambda_{i,r} b_r^* - \mu_{i,r} c_r^*) \in \operatorname{span}\{b_{k-1}^*, b_k^*\}.$$

By the linear independence of the vectors $\{b_i^*\}_{i \in \underline{m}}$ we obtain $\mu_{i,r} = \lambda_{i,r}$ for $r \neq k, k-1$ and

$$\lambda_{i,k-1} b_{k-1}^* + \lambda_{i,k} b_k^* = \mu_{i,k-1} c_{k-1}^* + \mu_{i,k} c_k^*.$$

Now using the (b) and (c) to write b_{k-1}^* and b_k^* in terms of c_{k-1}^* and c_k^*, and substituting in the equation above we obtain, after comparing coefficients:

$$\begin{aligned} \mu_{i,k-1} &= \mu_{k,k-1} \lambda_{i,k-1} + (1 - \lambda_{k,k-1} \mu_{k,k-1}) \lambda_{i,k}, \\ \mu_{i,k} &= \lambda_{i,k-1} - \lambda_{k,k-1} \lambda_{i,k} \end{aligned}$$

which are the remaining equations stated in (d). □

5.2 Relation to the discriminant of lattices

In this short section we relate the discriminant (see definition (4.33)) of a lattice to the norms of the Gram-Schmidt vectors associated to any basis of

that lattice. Recall that in chapter 2, proposition (2.35), we showed that the symmetric algebra $S(V)$ of V is an ordered graded ring. We also remind the reader of definition (2.16) where we introduced the "infinitely close" relation $\simeq$ on an arbitrary ordered vector space.

Proposition 5.24. *Let $(E, V, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space with $\dim E = m$. Let $L \subset E$ be an embedded layered lattice of rank m and $\{b_i\}_{i\in\underline{m}}$ be an ordered basis of L. Then this is also a basis of E and, as such, its associated Gram-Schmidt basis satisfies*

$$D(L) \simeq \prod_{i\in\underline{m}} q(b_i^*) \in S^m(V). \tag{5.25}$$

Proof. We first establish that $\det(\langle b_i^*, b_j^*\rangle)_{i,j} = D(L)$. The proof of this fact is the same as in the classical case since it depends only on the abstract properties of the determinant and on the fact that the matrix $\mathbf{M}$ giving the change of basis $b_i^* \to b_i$ is lower triangular with diagonal entries equal to 1. This can be seen from the equations in (5.8).

Let $\mathbf{B}$ denote the Gram-matrix of L with respect to the given basis. We may view it as an element of $\mathrm{M}_m(S(V))$, the ring of $m \times m$ matrices over the symmetric algebra of V. Then we have

$$\det(\langle b_i^*, b_j^*\rangle)_{i,j} = \det(\mathbf{M}^T\mathbf{B}\mathbf{M}) = (\det \mathbf{M})^2 \det \mathbf{B} = \det \mathbf{B} = D(L)$$

since $\det \mathbf{M} = 1$. The left-hand side equals $\langle b^*, b^*\rangle$, where $b^* = b_1^* \wedge \cdots \wedge b_m^*$ and $\langle\cdot,\cdot\rangle : \bigwedge^m E \times \bigwedge^m E \to S^m(V)$ is the inner-product on the m-th exterior power of E (see theorem (3.26)). The result now follows from lemma (3.30). $\square$

5.3 A polynomial-time algorithm

In this section we describe an algorithm for calculating the associated Gram-Schmidt basis from a given basis of a layered Euclidean space in polynomial time, i.e., with the number of binary operations polynomially bounded by the length of the input. In (A.1) of the appendix we used proposition (5.7) to implement an algorithm that computes Gram-Schmidt bases, but we were not able to show that this would give rise to a polynomial-time algorithm. It is not hard to show that the procedure performs a number of *arithmetical operations* that is bounded by a polynomial in the dimension of the layered Euclidean space and its number of layers. Keeping control over the growth of the numbers involved in the calculations proved to be harder.

In a nutshell, the linear system (5.9) we solve in the "straight-forward" algorithm is *simpler* but *recursive* of depth equal to the the dimension of the space. The algorithm we now describe is of bounded depth but we calculate,

as an intermediate step, a basis for the space that, up to a permutation of the vectors, is a layered basis. This is done by solving a large number of linear systems. The solutions of these systems can be found with the number of binary operations bounded by a polynomial in the input.

Which of those two algorithms performs better is practice remains to be seen. It is the belief of the author that, with the clever use of the extended Euclidean algorithm to bound all numerators and denominators of the numbers involved, one can develop a polynomial-time version of the "straight-forward" algorithm.

We now refer the reader to the review section in complexity theory presented in the introduction. We will freely use the concepts introduced there.

Let $(\mathbb{R}^m, \mathbb{R}^{\underline{n}}, \langle\cdot,\cdot\rangle)$ be an m-dimensional layered Euclidean space with $m > 0$. Although the Gram-Schmidt procedure was formulated for layered Euclidean spaces (thus the vector spaces involved where *real* vector spaces), we assume those spaces are given by *rational data*, i.e., a rational Gram-matrix specifying the inner-products of the elements of the canonical basis of $\mathbb{Q}^m \subset \mathbb{R}^m$. Let $\mathbf{B}$ be this Gram-matrix of $\langle\cdot,\cdot\rangle$ (see definition (3.1)). This is an $\mathbb{Q}^{\underline{n}}$-valued matrix that can be decomposed in n *rational* matrices $\mathbf{B}^1, \ldots, \mathbf{B}^n \in \mathrm{M}_m(\mathbb{Q})$ with respect to the canonical basis of $\mathbb{Q}^{\underline{n}}$ (which is also an anti-lexicographic basis of this subspace of $\mathbb{R}^{\underline{n}}$). To be precise, let $\{e_i\}_{i\in\underline{m}}$ be the canonical basis of $\mathbb{Q}^m \subset \mathbb{R}^m$. Then the inner-product is determined by

$$\langle e_i, e_j\rangle = (\mathbf{B}^1_{i,j}, \ldots, \mathbf{B}^n_{i,j}) \in \mathbb{Q}^{\underline{n}}.$$

We are interested in computing the Gram-Schmidt basis associated to $\{e_i\}_{i\in\underline{m}}$ whose inner-products are specified as above.

Until the end of this section we denote the layered Euclidean space $\mathbb{R}^m$ by E and its layers by E_k, for $k \in \underline{n}_0$. We also denote the canonical basis of E by $\{e_i\}_{i\in\underline{m}}$ and the flag it induces by $\{F_i\}_{i\in\underline{m}_0}$; thus we have $F_i = \mathrm{span}\{e_j : j \leqslant i\}$.

Lemma 5.26. *Notation being as described above, for each $i \in \underline{m}$ let $k(i)$ be the minimal index k for which the intersection $(e_i + F_{i-1}) \cap E_k$ is non-empty and let c_i be a vector in this intersection. Then $\{c_i\}_{i\in\underline{m}}$ is a basis of E inducing the flag $\{F_i\}_{i\in\underline{m}_0}$. Furthermore, the matrix $(c_i, c_j)_{i,j\in\underline{m}} \in \mathrm{M}_m(\mathbb{R})$, where $(\cdot, x)$ is the functional of definition* (5.5)*, is non-singular.*

Proof. Since $E_n = E$ it is clear that, for each $i \in \underline{m}$, there exists a number $k(i) \in \underline{n}$ and a vector c_i as claimed in this lemma. Since $e_i \in F_i \setminus F_{i-1}$, we have $F_{i-1} \cap (e_i + F_{i-1}) = \varnothing$ and $e_i + F_{i-1} \subset F_i$. We conclude that $c_i \in (F_i \setminus F_{i-1}) \cap E_{k(i)}$. In particular, we have $F_i = \mathrm{span}\{c_j : j \leqslant i\}$. Thus, $\{c_i\}_{i\in\underline{m}}$ induces the same flag as $\{e_i\}_{i\in\underline{m}}$.

I claim that, for all $k \in \underline{n}_0$, we have

$$\mathrm{span}\{c_i : k(i) \leqslant k\} = E_k.$$

We clearly have the $\subset$ containment by construction, so to show equality we prove that their dimensions are equal. Let $k \in \underline{n}$. First, note that $F_0 \cap E_k \subset \cdots \subset F_m \cap E_k$ is a filtration of E_k with the property that each successive quotient has dimension at most one. Thus, *exactly* $\dim E_k$ of these inclusions are proper inclusions. Now, the set of indices i such that $(F_i \cap E_k) \subsetneqq (F_{i-1} \cap E_k)$ is equal to the set $\{i : (F_i \setminus F_{i-1}) \cap E_k \neq \varnothing\}$ and the latter is, of course, equal to

$$\#\{k(i) : k(i) \leqslant k\} = \dim(\operatorname{span}\{c_i : k(i) \leqslant k\}).$$

This proves the claim. It follows that, up to a permutation of the c_i, the ordered basis $\{c_i\}_{i \in \underline{m}}$ is layered.

We now show that the matrix $(c_i, c_j)_{i,j \in \underline{m}}$ is non-singular. This is the case if and only if its rows are linearly independent. Thus let $\lambda_1, \ldots, \lambda_m \in \mathbb{R}$ be such that for all $j \in \underline{m}$ we have $\sum_i \lambda_i (c_i, c_j) = 0$ (this is a linear combination of the rows resulting in the zero vector). To show that the matrix $(c_i, c_j)_{i,j \in \underline{m}}$ is non-singular it is enough to show that this implies $\lambda_i = 0$ for all i. Setting $x = \sum_i \lambda_i c_i \in E$ we see that, for all $j \in \underline{m}$, we have $(x, c_j) = 0$. Since we also have $\langle x, c_j \rangle \preccurlyeq \langle c_j, c_j \rangle$, this implies that $\langle x, c_j \rangle \ll \langle c_j, c_j \rangle$, i.e., $x \in \{c_1, \ldots, c_m\}^\perp$. We showed before that, up to a permutation of its vectors, the basis $\{c_i\}_{i \in \underline{m}}$ is layered, so by proposition (3.25) we have $x \in E^\perp = \{0\}$. This implies $\lambda_i = 0$ for all $i \in \underline{m}$. $\square$

Lemma 5.27. *There exists a polynomial-time algorithm that given a layered Euclidean space E, specified by matrices $\mathbf{B}^1, \ldots, \mathbf{B}^n \in \mathrm{M}_m(\mathbb{Q})$ as described above, computes a basis $\{c_i\}_{i \in \underline{m}}$ of E as in the previous lemma and with each $c_i \in \mathbb{Q}^m$.*

Proof. From the definition of the $\{c_i\}_{i \in \underline{m}}$, it is enough for us to compute, *at most*, mn intersections of affine subspaces of the form $e_i + F_{i-1}$ and layers E_k. More precisely, it is enough to decide if such an intersection is empty, and, if not, to calculate an element of it.

Fix $i \in \underline{m}$ and $k \in \underline{n}$. By theorem (3.5), the subspace E_k is the radical (see definition (3.1)) of the positive semi-definite layered form specified by

$$(x, y) \mapsto (0, \ldots, 0, x^T \mathbf{B}^{k+1} y, \ldots, x^T \mathbf{B}^n y) \in \mathbb{R}^{\underline{n}}.$$

Thus the condition that an element $x \in E$ is in the k-th layer holds if, and only if, for all $l > k$ and for all $y \in E$ we have $x^T \mathbf{B}^l y = 0$. This, in turn, is equivalent to the condition that

$$\forall l > k, \forall h \in \underline{m},\ x^T \mathbf{B}^l e_h = 0.$$

Let $x = e_i + \sum_{j<i} \alpha_j e_j \in e_i + F_{i-1}$ for unknown α_j. The equation above can now be written as

$$\forall l > k, \forall h \in \underline{m},\ \sum_{j<i} \alpha_j \mathbf{B}^l_{j,h} = -\mathbf{B}^l_{i,h}.$$

This is a *rational* linear system of dimensions, at most, $(n-k)(i-1)m < nm^2$ and whose entries are a subset of the entries of the matrices $\mathbf{B}^1, \ldots, \mathbf{B}^n$. Solving such systems can be done in polynomial time (this can be found, for example, in [13, Chapter 3, Theorem 3.3]). Thus, to decide if $(e_i + F_{i-1}) \cap E_k$ is non-empty and, if so, find an element c_i of this intersection is a problem solvable in polynomial time. Note that we have $c_i \in \mathbb{Q}^m$ since c_i is a solution of a rational linear system. $\square$

We come to the main result of this section: a polynomial-time layered Gram-Schmidt algorithm. Recall definition (1.9).

Theorem 5.28. *There exists a polynomial-time algorithm that, given $m \in \mathbb{Z}_{\geqslant 0}$ and matrices $\mathbf{B}^1, \ldots, \mathbf{B}^n \in \mathrm{M}_m(\mathbb{Q})$ specifying the inner-products of the canonical basis of an m-dimensional layered Euclidean space $(\mathbb{R}^m, \mathbb{R}^{\underline{n}}, \langle \cdot, \cdot \rangle)$, computes the Gram-Schmidt basis associated to the canonical basis of $\mathbb{R}^m$.*

Proof. Let $\{F_i\}_{i \in \underline{m}}$ be the flag induced by the canonical basis $\{e_i\}_{i \in \underline{m}}$ of $\mathbb{R}^m$. By lemmas (5.26) and (5.27), we can compute, in polynomial time, a basis $\{c_i\}_{i \in \underline{m}}$ inducing this same flag and with the property that the matrix $(c_i, c_j)_{i,j \in \underline{m}}$ is invertible and *rational*.

Let $i \in \underline{m}$ and let e_i^* be the Gram-Schmidt vector associated to e_i. Since $e_i^* \in e_i + F_{i-1}$ we can write $e_i^* = e_i + \sum_{j<i} \gamma_{i,j} c_j$. Taking the image of this equation under the functional $(\cdot, c_h)$ for each $h < i$ (see definition (5.5)) and using that $(e_i^*, c_h) = 0$ by orthogonality (recall that $e_i^* \in F_{i-1}^{\perp}$), we obtain

$$\sum_{j<i} \gamma_{i,j} (c_j, c_h) = -(e_i, c_h).$$

This is a rational linear system. By [13, Chapter 3, Theorem 3.3]), we can solve it in polynomial time to obtain e_i^*. $\square$

CHAPTER 6

Layered lattice basis reduction

6.1 LLL reduction

In this section we introduce the concept of LLL-reduced bases for layered lattices and investigate some of the properties of such bases. A procedure for computing reduced bases is given in the next section and a polynomial-time variant in the third and last section. We refer the reader to [8] for the definition and properties of *classical* LLL-reduced bases and to (3.6) and (4.4) to review the definitions of a layered Euclidean space and of an embedded layered lattice. We also recall definition (2.31) from chapter 2 where we defined the leading term function $\mathrm{lt} : S(V) \to S(V)$ for a fixed anti-lexicographic basis of an ordered real vector space V.

Definition 6.1. Let $L \subset E$ be a layered lattice of rank m embedded in a layered Euclidean space $(E, V, \langle\cdot,\cdot\rangle)$ of the same dimension. Let $\{b_i\}_{i\in\underline{m}}$ be an ordered basis of L and $\{b_i^*\}_{i\in\underline{m}}$ be its associated Gram-Schmidt basis. Let furthermore $c \in \mathbb{R}, c \geqslant 1$, and $\{\lambda_{i,j}\}_{1\leqslant j<i\leqslant m}$ be the set of real numbers such that $b_i = b_i^* + \sum_{j<i} \lambda_{i,j} b_j^*$. We refer the reader to (5.7) for details.

(i) The basis $\{b_i\}_{i\in\underline{m}}$ is called *size-reduced* if for all $i \in \underline{m}$ and all $j < i$ we have $|\lambda_{i,j}| \leqslant 1/2$.

(ii) The basis $\{b_i\}_{i\in\underline{m}}$ satisfies the *Lovász* condition for c if for all $i \in \underline{m}, i > 1$, we have $\mathrm{lt}(q(b_{i-1}^*)) \leqslant c \cdot \mathrm{lt}(q(b_i^*))$.

(iii) A basis satisfying (i) and (ii) above is called *c-reduced*. $\diamondsuit$

Remark 6.2. (a) Condition (ii) of the definition above does not depend on the choice of an anti-lexicographic basis for V used for defining the leading term function and it agrees with (ii) of definition (1.6) of the introduction.

(b) It is worth comparing the notion of reduced bases from [8, page 516, (1.4) and (1.5)] with our own. Under the assumption that for a layered lattice (L, V, q) we have an order isomorphism $V \simeq \mathbb{R}$, so that L can also be seen as a classical lattice, the following holds: if a basis of L is reduced in the sense of the original paper then it is c-reduced according to definition (6.1) for any $c \geqslant 2$. On the other hand, if a basis is 4/3-reduced according to our definition then it is reduced according to [8]. Our definition is, in fact, inspired by the weaker notion of "reducedness" given in [5].

The main result of this section establishes relations between bases satisfying some of the items of definition (6.1) and the corresponding properties of the induced bases in each layer. To be precise, we introduce the following definition. We recall remark (3.10 (a)).

Definition 6.3. Let P be a property of bases of (classical) Euclidean spaces and let $I \to E$ be a basis of a layered Euclidean space E. We say $I \to E$ has property P *layer-wise* if this basis is layered and for all $U \in \mathcal{C}^*(V)$ with predecessor U' in $\mathcal{C}(V)$, the basis of $E_U/E_{U'}$ induced by $I \to E$ has property P. $\diamondsuit$

Note that a basis of a layered lattice is also a basis of the layered Euclidean space it generates as an embedded layered lattice (see theorem (4.20)).

Theorem 6.4. *Let $c \in \mathbb{R}, c \geqslant 1$. Let $\{b_i\}_{i \in \underline{m}}$ be an ordered basis of a layered lattice L of rank m embedded in the layered Euclidean space $(E, V, \langle \cdot, \cdot \rangle)$ of dimension m. Then the following holds.*

(a) *The basis $\{b_i\}_{i \in \underline{m}}$ is layered if and only if its associated Gram-Schmidt basis is layered.*

(b) *The basis $\{b_i\}_{i \in \underline{m}}$ satisfies the Lovász condition for c if and only if it satisfies the Lovász condition for c layer-wise.*

(c) *If the basis $\{b_i\}_{i \in \underline{m}}$ is layered and size-reduced then it is size-reduced layer-wise.*

Proof. Let $\{b_i^*\}_{i \in \underline{m}}$ be the Gram-Schmidt basis associated to $\{b_i\}_{i \in \underline{m}}$.

Item (a) is trivial since a basis and its associated Gram-Schmidt basis induce the same flag (see remark (3.10)).

For (b), let $i \in \underline{m}$, $i > 1$, and let $U \in \mathcal{C}(V)$ be the predecessor of $\mathcal{C}(q(b_i^*))$. I claim that $\mathrm{lt}(q(b_{i-1}^*)) \leqslant c \cdot \mathrm{lt}(q(b_i^*))$ holds if and only if we have the inequality $q(b_{i-1}^*) + U \leqslant c \cdot q(b_i^*) + U$ in V/U. In fact, note that we have $\mathrm{lt}(q(b_i^*)) + U = q(b_i^*) + U$ in V/U. If $q(b_{i-1}^*) \notin U$ then $\mathcal{C}(q(b_{i-1}^*)) = \mathcal{C}(q(b_i^*))$ and we can apply

the same reasoning to conclude that $\mathrm{lt}(q(b_{i-1}^*)) + U = q(b_{i-1}^*) + U$ in V/U. The claim is then clear in this case. The case when $q(b_{i-1}^*) \in U$ is trivial as the equivalence reduces to $0 \leqslant c \cdot \mathrm{lt}(q(b_i^*)) + U$ if and only if $0 \leqslant c \cdot q(b_i^*) + U$. Thus the claim is proven.

Now assume that $\{b_i\}_{i \in \underline{m}}$ satisfies the Lovász condition for c and let $U \in \mathcal{C}(V)$. The hypothesis on $\{b_i\}_{i \in \underline{m}}$ implies, in particular, that for all $i \in \underline{m}$, $i > 1$, we have $\mathcal{L}(b_{i-1}^*) \subset \mathcal{L}(b_i^*)$. Furthermore, since Gram-Schmidt bases are orthogonal, by proposition (3.24), for exactly $\dim E_U$ of the elements of $\underline{m}$ the corresponding vector b_i^* satisfies $\mathcal{L}(b_i^*) = E_U$. It follows that

$$\mathrm{span}\{b_i^* : 1 \leqslant i \leqslant \dim E_U\} = E_U$$

and, thus, $E_U \in \mathcal{F}(\{b_i^*\}_{i \in \underline{m}})$. By remark (3.10 (b)), also $\{b_i\}_{i \in \underline{m}}$ is layered. Thus if $\{b_i\}_{i \in \underline{m}}$ satisfies the Lovász condition for c, then this basis is layered. Furthermore, for any $U \in \mathcal{C}^*(V)$ with predecessor U', the claim proven above implies that the basis of $L_U/L_{U'}$ induced by $\{b_i\}_{i \in \underline{m}}$ is c-reduced. Thus $\{b_i\}_{i \in \underline{m}}$ satisfies the Lovász condition for c layer-wise.

We now prove the converse. Let $i \in \underline{m}$, $i > 1$ and let U be the predecessor of $\mathcal{C}(q(b_i^*))$ in $\mathcal{C}(V)$. The hypothesis gives $q(b_{i-1}^*) + U \leqslant c \cdot q(b_i^*) + U$ in V/U which, by the claim proven above, lifts to $\mathrm{lt}(q(b_{i-1}^*)) \leqslant c \cdot \mathrm{lt}(q(b_i^*))$ in V.

Finally we show (c). Let $i \in \underline{m}$, $i > 1$ and let $\lambda_{i,1}, \ldots, \lambda_{i,i-1}$ be the real numbers such that $b_i = b_i^* + \sum_{j<i} \lambda_{i,j} b_j^*$. Let $U \in \mathcal{C}(V)$ be the predecessor of $\mathcal{C}(q(b_i))$ and E_U be the U-th layer of E. Then since $\{b_i\}_{i \in \underline{m}}$ is layered we have $E_U = \mathrm{span}\{b_j^* : j \leqslant \dim E_U\}$ and thus

$$b_i + E_U = b_i^* + \sum_{\dim E_U < j < i} \lambda_{i,j} b_j^* + E_U$$

in E/E_U. This is immediately seen to be equation (5.8) for the vector $b_i + E_U$ of E/E_U. By hypothesis we have $|\lambda_{i,j}| \leqslant 1/2$ for all $j < i$ thus giving the result. □

The next proposition describes a procedure that "size-reduces" a given basis. Together with the above theorem, is enables us to compute a c-reduced basis from a basis that is just layer-wise c-reduced.

Notation. In the proposition below, since we proceed in successive steps that change the given basis, we use the notation $a \leftarrow b$ to mean that we copy the value of b to a. This is *not* a mathematical equality as $a \leftarrow b$ followed by $b \leftarrow c$ does not imply $a = c$.

Proposition 6.5. *Let $\{b_i\}_{i \in \underline{m}}$ be a basis of an embedded layered lattice $L \subset E$. Let $\{b_i^*\}_{i \in \underline{m}}$ be its associated Gram-Schmidt basis and let $\{\lambda_{i,j}\}_{1 \leqslant j < i \leqslant m}$ be the sequence of numbers such that $b_i = b_i^* + \sum_{i<j} \lambda_{i,j} b_j^*$.*

Set $\mu_{i,j} \leftarrow \lambda_{i,j}$ for all $i \in \underline{m}$ and all $j < i$. For each $i \in \underline{m}$ perform the following substitution steps for each $j = i-1, i-2, \ldots, 1$ in sequence.

$$\begin{aligned} \mu &\leftarrow \lfloor \mu_{i,j} + 1/2 \rfloor \\ \mu_{i,j} &\leftarrow \mu_{i,j} - \mu, \\ \mu_{i,h} &\leftarrow \mu_{i,h} - \mu\lambda_{j,h}, \quad \text{for } h < j. \end{aligned}$$

Finally, after these steps, let $c_i = b_i^* + \sum_{j<i} \mu_{i,j} b_j^*$. Then the set of vectors $\{c_i\}_{i \in \underline{m}}$ so obtained is a size-reduced basis of L with the same associated Gram-Schmidt basis.

Proof. The main point of the proof is noticing that for each $i \in \underline{m}$ and $j < i$, by proposition (5.13) we are performing the updates to the numbers $\mu_{i,i-1}, \ldots, \mu_{i,1}$ corresponding to the substitution $b_i \leftarrow b_i - \mu b_j \in L$. By the same proposition, this does not change the associated Gram-Schmidt basis.

Each of the numbers $\mu_{i,h}$ will be updated exactly $i-h$ times and note that, from the *order* in which we are performing the substitutions, the last time $\mu_{i,h}$ will be updated corresponds exactly to the step where $j = h$. At this step we subtract $\mu = \lfloor \mu_{i,j} + 1/2 \rfloor$ from $\mu_{i,j}$. Hence, at the end of this step we have $|\mu_{i,j}| \leqslant 1/2$. It follows that the basis $\{c_i\}_{i \in \underline{m}}$ is size-reduced. □

Remark 6.6. Note that, in particular, if $\{b_i\}_{i \in \underline{m}}$ satisfies the Lovász condition for some $c \geqslant 1$ then the basis $\{c_i\}_{i \in \underline{m}}$ obtained from the above proposition will be a c-reduced basis of L.

Using the above theorem and remark (6.2) we establish a link between c-reduced bases of layered lattices and classical "LLL-reducedness" of the bases induced on the quotients of successive layers. This proves particularly useful as the following examples show. In fact, the shortcomings of the classical LLL algorithm alluded to in the introduction, has motivated us to generalize lattices and lattice basis reduction to better suit problems like (the ones found while) doing linear algebra over $\mathbb{Z}$. Below we show how to compute kernels and solving integral linear systems using layered lattice basis reduction and the above theorem. The second part of our work consists of showing that there is an algorithm, very much like the classical LLL algorithm, that computes a c-reduced basis given an arbitrary basis for a layered lattice. This will be the content of the next section.

Example 6.7. Let $f : \mathbb{Z}^n \to \mathbb{Z}^m$ be a homomorphism of abelian groups. We want to compute the kernel and image of f, i.e., bases for the free abelian groups $\ker f$ and $f(\mathbb{Z}^n)$. Let $L = \mathbb{Z}^n$ and $q : L \to \mathbb{R}^{\underline{2}}$ given by

$$q(x) = (||x||^2, ||f(x)||^2)$$

where $||\cdot||$ denotes the standard Euclidean norm on $\mathbb{Z}^n$ and $\mathbb{Z}^m$.

To see that (L, V, q) is a layered lattice, we notice that $L \subset \mathbb{R}^n$ and that q is the quadratic norm associated to an bilinear form $\langle \cdot, \cdot \rangle$ defined by (4.13) and (4.21). It is easy to see that $\langle \cdot, \cdot \rangle$ is positive-definite and layered, so $(\mathbb{R}^n, \mathbb{R}^{\underline{2}}, \langle \cdot, \cdot \rangle)$ is a layered Euclidean space. The Gram matrix associated to the canonical basis of $\mathbb{R}^n$ is rational so proposition (4.30) tells us that L is a layered lattice.

Back to our example, by theorem (6.4), a c-reduced basis of L will give us a c-reduced basis of the first layer of L, which is $\ker f$, and the images of the remaining vectors form a c-reduced basis of $f(\mathbb{Z}^n)$.

Example 6.8. As in the previous example, let $f : \mathbb{Z}^n \to \mathbb{Z}^m$ be an homomorphism of abelian groups. Let $b \in \mathbb{Z}^m$. We want to find all $x \in \mathbb{Z}^n$ such that $f(x) = b$. Let $L = \mathbb{Z}^n \times \mathbb{Z}$ and $q : L \to \mathbb{R}^{\underline{3}}$ given by

$$q(x, z) = (||x||^2, ||z||^2, ||f(x) - z \cdot b||^2)$$

where $||\cdot||$ denotes the usual Euclidean norm. Again, using proposition (4.30), one shows that L is a layered lattice. A c-reduced basis of L will encode all information we want. Namely, the basis for the first layer will be a c-reduced basis for $\ker f$. The second layer will equal the first one if the system has no *rational* solution and will have rank 1 otherwise. In the latter case, a basis for this second layer will be a pair (x, z) such that $f(x) = z \cdot b$. If $z = \pm 1$ we have a solution as wanted (after, possibly, taking $-(x, z)$ instead). By adding an arbitrary element of $\ker f$ we have *all* solutions. If $z \neq 1$ we know that there are *no* solutions to the original system, but we have computed the *minimal* (in absolute value) z such that there is a solution $\frac{1}{z}x \in \frac{1}{z}\mathbb{Z}$, i.e., a solution vector whose entries are rational numbers with the same denominator.

Example 6.9. Let $L \subset \mathbb{Z}^m$ be a subgroup of rank m. Let $\{e_i\}_{i \in \underline{m}}$ be the canonical basis of $\mathbb{Z}^m$ and $\{F_i\}_{i \in \underline{m}}$ be the flag induced by $\{e_i\}_{i \in \underline{m}}$. From a basis $\{b_i\}_{i \in \underline{m}}$ of L we obtain a matrix $(m_{i,j})_{i,j \in \underline{m}} \in \mathrm{M}_m(\mathbb{Z})$ whose rows give the coefficients of the vectors b_i when written in terms of the basis $\{e_i\}_{i \in \underline{m}}$. It is well-known that there exists a unique basis of L such that this matrix satisfies the following.

(a) For all $i \in \underline{m}$ one has $m_{i,i} > 0$.

(b) For all $i \in \underline{m}$ and $j < i$ one has $0 \leqslant m_{i,j} < m_{i,i}$.

(c) For all $i \in \underline{m}$ and $j > i$ one has $m_{i,j} = 0$.

This unique basis is called the *Hermite normal form of* L. We refer the reader to [3, §2.4] for details and a generalization to subgroups of $\mathbb{Z}^m$ of lower rank.

We will now show how to use layered lattices to find the Hermite normal form of L. Let $q : \mathbb{Z}^m \to \mathbb{R}^{\underline{m}}$ be the map given by $(x_i)_{i \in \underline{m}} \mapsto (||x_i||^2)_{i \in \underline{m}}$. As before, proposition (4.30) tells us that $(\mathbb{Z}^m, \mathbb{R}^{\underline{m}}, q)$ is a layered lattice. With this quadratic norm it is easy to see that the set of layers of $\mathbb{Z}^m$ is exactly

$\{F_i\}_{i\in\underline{m}}$. Furthermore, it is also clear that in this case $\{e_i\}_{i\in\underline{m}}$ is a orthogonal basis of $\mathbb{Z}^m$. As such, $\{e_i\}_{i\in\underline{m}}$ is its own associated Gram-Schmidt basis, i.e., $e_i^* = e_i$ for all $i \in \underline{m}$. Note that since $L \subset \mathbb{Z}^m$ is a subgroup, it is also a layered lattice.

Let $c > 1$ and suppose that $\{b_i\}_{i\in\underline{m}}$ is a c-reduced basis of L. By theorem (6.4 (b)), the basis $\{b_i\}_{i\in\underline{m}}$ is layered. Thus, we have $b_i \in F_i \setminus F_{i-1}$ for all $i \in \underline{m}$. This implies that the matrix $(m_{i,j})_{i,j\in\underline{m}}$ associated to this basis satisfies (c) above. We can arrange that (a) is also satisfied by, if necessary, taking the negative of some of the vectors of the basis. An easy induction argument then shows that for all $i \in \underline{m}$ we have $b_i^* = m_{i,i}e_i^* = m_{i,i}e_i$. The induction uses the equation

$$m_{i,i}e_i + \sum_{j<i} m_{i,j}e_j = b_i = b_i^* + \sum_{j<i} \lambda_{i,j}b_j^*,$$

which holds for all $i \in \underline{m}$, together with the observation we made previously that $\{e_i\}_{i\in\underline{m}}$ is layered and orthogonal. With little more work we also obtain $|m_{i,j}| = \lambda_{i,j}m_{j,j}$ for all $i \in \underline{m}$ and all $j < i$; since we have $|\lambda_{i,j}| \leqslant 1/2$, we obtain $|m_{i,j}| \leqslant m_{j,j}/2$. From these inequalities it is easy to find the Hermite normal form of L.

We refer the reader to [8] and [11] for the various useful properties of *classical* LLL-reduced bases.

6.2 The layered LLL algorithm

We now present a procedure for computing reduced bases of layered lattices. This will be done in a conceptual manner to highlight its resemblance with the classical LLL algorithm of [8]. In the appendix we give an implementation of this procedure in pseudo-code.

The input of this procedure consists of a real number $c > 4/3$, and a layered Euclidean space $(\mathbb{R}^m, \mathbb{R}^{\underline{n}}, \langle\cdot,\cdot\rangle)$. The layered Euclidean space is specified via a sequence of matrices $\mathbf{B}^1, \ldots, \mathbf{B}^n \in \mathrm{M}_m(\mathbb{R})$ such that, given $x, y \in \mathbb{R}^m$, we have

$$\langle x, y\rangle = (x^T\mathbf{B}^1y, \ldots, x^T\mathbf{B}^ny) \in \mathbb{R}^{\underline{n}}.$$

Note that these matrices are the components of the Gram-matrix of the inner-product with respect to the canonical basis of $\mathbb{R}^{\underline{n}}$ (which is also an anti-lexicographic basis). We assume that the group $\mathbb{Z}^m \subset \mathbb{R}^m$ is a layered lattice, which we denote by L. If $m < 2$ then any basis of L is automatically c-reduced so we assume from here on that $m \geqslant 2$.

The procedure consists of repeating iterations whose input is a basis $\{b_i\}_{i\in\underline{m}}$ of L and an index $k \in \underline{m}$, $k > 1$, such that $\{b_1, \ldots, b_{k-1}\}$ is a c-reduced basis for the layered lattice it generates. The initial iteration of the procedure has

$\{b_i\}_{i\in\underline{m}}$ equal to the canonical basis of $\mathbb{R}^m$ and $k = 2$ (note that b_1 is a c-reduced basis of the lattice it generates). At the end of each iteration we have a new index $l \in \underline{m+1}$ and a new basis $\{c_i\}_{i\in\underline{m}}$ of L such that $\{c_1, \dots, c_{l-1}\}$ is a c-reduced basis for the layered lattice it generates. Either $l = m+1$, in which case we terminate and output the basis $\{c_i\}_{i\in\underline{m}}$, or $l \in \underline{m}$, in which case we start a new iteration with input $\{c_i\}_{i\in\underline{m}}$ as basis and index $\max\{l, 2\}$.

We now describe an iteration in full detail. Let thus $\{b_i\}_{i\in\underline{m}}$ and $k \in \underline{m}$, $k > 1$ be given and let $\{b_i^*\}_{i\in\underline{m}}$ be the associated Gram-Schmidt basis. By assumption, $\{b_1, \dots, b_{k-1}\}$ is a c-reduced basis for the lattice it generates. The first part of the iteration is a *size reduction*. If $\lambda_{k,j} \in \mathbb{R}$ are the (unique) real numbers satisfying

$$b_k = b_k^* + \sum_{j<k} \lambda_{k,j} b_j^*,$$

we let λ be a nearest integer to $\lambda_{k,k-1}$ and let $b_k' = b_k - \lambda b_{k-1}$. We note that if $|\lambda_{k,k-1}| < 1/2$ then $\lambda = 0$ and we do nothing. We repeat the same procedure to $\lambda_{k,l}$ for $l = k-2, k-3, \dots, 1$ *in this order*. By proposition (6.5), we end the first part of the iteration with a vector b_k' such that $\{b_1, \dots, b_k'\}$ is a size-reduced basis of the lattice it generates *with the same* associated Gram-Schmidt basis. Thus, if $\mathrm{lt}(q(b_{k-1}^*)) \leqslant c \cdot \mathrm{lt}(q(b_k^*))$ then this basis is c-reduced. The final part of the iteration consists of testing this condition.

We set $c_i = b_i$ for $i \neq k, k-1$. If

$$\mathrm{lt}(q(b_{k-1}^*)) \leqslant c \cdot \mathrm{lt}(q(b_k^*)) \tag{6.10}$$

we also set $c_{k-1} = b_{k-1}$, $c_k = b_k'$ and select $l = k+1$ for the next iteration. If, on the other hand, we have

$$\mathrm{lt}(q(b_{k-1}^*)) > c \cdot \mathrm{lt}(q(b_k^*)) \tag{6.11}$$

then we set $c_{k-1} = b_k'$, $c_k = b_{k-1}$ and set $l = k-1$. This finishes the description of an iteration and, thus, of the whole algorithm.

Before we prove the next result, we remind the reader of the definition of a flag of a vector space (see the review section of the introduction), of the equivalence relation $\simeq$, defined on an ordered vector space, that we gave in (2.16) and of the discriminant of a layered lattice given in definition (4.33). We freely use the notation introduced in the present section.

Lemma 6.12. *In the notation above, the vectors $\{c_1, \dots, c_{l-1}\}$ form a c-reduced basis for the layered lattice they generate. Let $K_0 \subset \cdots \subset K_m$ be the flag of $\mathbb{R}^m$ induced by the basis $\{b_i\}_{i\in\underline{m}}$ and, similarly, $K_0' \subset \cdots \subset K_m'$ be the flag induced by the basis $\{c_i\}_{i\in\underline{m}}$. Then for all $i \neq k-1$ we have $K_i' = K_i$. If $l > k$ then we have $K_{k-1}' = K_{k-1}$ as well. If, on the other hand, we have $l \leqslant k$ then $D(K_{k-1}') < D(K_{k-1})$.*

Proof. The first statement of the lemma is clear. If we have an iteration for which $l > k$, then it is immediately clear that $K'_i = K_i$ for all $i \in \underline{m}_0$.

Now suppose that we have instead $l \leqslant k$. Then it is clear that $K'_i = K_i$ for all $i \neq k-1$. Let $\{b^*_i\}_{i\in\underline{m}}$ and $\{c^*_i\}_{i\in\underline{m}}$ be the Gram-Schmidt bases associated to $\{b_i\}_{i\in\underline{m}}$ and $\{c_i\}_{i\in\underline{m}}$ respectively. By proposition (5.15 (b)) and proposition (6.5), we have

$$c^*_{k-1} = b^*_k + \lambda_{k,k-1} b^*_{k-1}$$

with $|\lambda_{k,k-1}| \leqslant 1/2$. Thus we obtain

$$\langle c^*_{k-1}, c^*_{k-1}\rangle = \langle b^*_k, b^*_k\rangle + 2\lambda_{k,k-1}\langle b^*_{k-1}, b^*_k\rangle + \lambda^2_{k,k-1}\langle b^*_{k-1}, b^*_{k-1}\rangle.$$

Since $\langle b^*_{k-1}, b^*_k\rangle \ll \langle b^*_{k-1}, b^*_{k-1}\rangle$ by orthogonality, inequality (6.11) together with $c > 4/3$ gives

$$\langle c^*_{k-1}, c^*_{k-1}\rangle < \frac{3}{4}\langle b^*_{k-1}, b^*_{k-1}\rangle + \frac{1}{4}\langle b^*_{k-1}, b^*_{k-1}\rangle = \langle b^*_{k-1}, b^*_{k-1}\rangle.$$

By proposition (5.24) we have

$$D(K_{k-1}) \simeq \prod_{i\leqslant k-1} q(b^*_i) \simeq D(K_{k-2})q(b^*_{k-1})$$

where $D(\cdot)$ denotes the discriminant of a layered lattice. Similarly, we have $D(K'_{k-1}) \simeq D(K'_{k-2})q(c^*_{k-1})$. We noted before that $K'_{k-2} = K_{k-2}$, thus we conclude that $D(K'_{k-1}) < D(K_{k-1})$. □

Theorem 6.13. *The procedure described above terminates and the output is a c-reduced basis for the layered lattice $\mathbb{Z}^m \subset \mathbb{R}^m$.*

Proof. The procedure terminates if and only if $l = m+1$ is achieved at the end of an iteration. By the previous lemma, if this happens, the output of the algorithm will be a c-reduced basis for $\mathbb{Z}^m$.

Also from the previous lemma it follows that, for iterations where $l = k+1$, the quantities $D(K_i)$ remain unchanged for all $i \in \underline{m}_0$. Furthermore, for iterations where $l \leqslant k$ only $D(K_{k-1})$ is decreased, the rest remaining the same.

In theorem (4.35) we saw that the set $\{D(K) : K \subset L \text{ a sublattice of rank } k\}$ is well-ordered. It follows that iterations for which $l \leqslant k$, i.e., for which equation (6.11) holds, can occur only a finite number of times. After that, only iterations for which $l > k$ will occur. Eventually $l = m+1$ is attained and the procedure finishes. □

6.3 A polynomial-time reduction algorithm

In this section we fill an important gap: we were unable to prove that the layered LLL procedure of the last section is polynomial-time when given rational input.

We will give a polynomial-time algorithm that given a rational number $c > 4/3$ and a layered lattice specified as described below, computes a c-reduced basis of this lattice. This algorithm relies, mainly, on several applications of the standard LLL algorithm. In some of these applications, the LLL algorithm is used in the form of the kernel and image algorithm explained in [10, pg. 163], which we briefly described in the introduction and in (6.7). In this case, "weight" constants are used and, as we pointed out in the introduction, this was something we intended to avoid by developing the theory of layered lattices. This is a step forward to our goal since it implies the following. If it is possible to compute c-reduced bases of layered lattices with *two* layers in polynomial time and without the use of weight constants, then it is possible to compute c-reduced basis of *general* layered lattices also in polynomial time and without the use of weight constants.

We start by gathering some results on the theory of classical lattices that we will be using shortly. We remind the reader that a sublattice is called *pure* if the quotient of the lattice by this sublattice is free; a lattice embedded in a Euclidean space is called *full* if its rank equals the dimension of the Euclidean space.

Proposition 6.14. *Let $(E, \langle\cdot,\cdot\rangle)$ be a Euclidean space, $L \subset E$ be a lattice in E and $M \subset L$ be a sublattice of L. Then there is a unique pure sublattice $K \subset L$ of L such that $M \subset K$ and* $\operatorname{rank} M = \operatorname{rank} K$. *This lattice equals $(\mathbb{R} \cdot M) \cap L$.*

Proof. Let $F = \mathbb{R} \cdot M$ be the subspace generated by M. Since $L/(F \cap L) \subset E/F$ we see that $F \cap L$ is pure and dimension counting shows that $\operatorname{rank}(F \cap L) = \operatorname{rank} M$. We have to show uniqueness, so let $K \subset L$ be a sublattice with the properties stated above. Then, clearly, we have $K \subset F \cap L$ and they have the same rank. It follows that $(F \cap L)/K$ is a torsion subgroup of the free group L/K. Thus, we have $K = F \cap L$. □

Definition 6.15. The unique pure sublattice K of the proposition above is called the *purification* of M in L.

Definition 6.16. Let $L \subset E$ be a full lattice in a Euclidean space $(E, \langle\cdot,\cdot\rangle)$ and let $M \subset L$ be a sublattice. We define the following subsets of E:

$$\begin{aligned} L^{\dagger} &= \{x \in E : \langle L, x\rangle \subset \mathbb{Z}\} \\ M^{\perp} &= \{x \in E : \langle M, x\rangle = \{0\}\}. \end{aligned}$$

The set $L^\dagger$ is called the *dual* of L and $M^\perp$ is called the *orthogonal complement* of M in E. ♢

Proposition 6.17. *Let $(E, \langle\cdot,\cdot\rangle)$ be a Euclidean space, $L \subset E$ be a full lattice in E and $M \subset L$ be a sublattice of L of rank r. Then we have the following.*

(a) *The dual $L^\dagger$ is a full lattice in E and $L^{\dagger\dagger} = L$.*

(b) *$M^\perp$ is a subspace of E and we have $M^{\perp\perp} = \mathbb{R} \cdot M$.*

(c) *$L^\dagger \cap M^\perp$ is a pure sublattice of $L^\dagger$ and equals the kernel of the group homomorphism $L^\dagger \to \mathrm{Hom}\,(M, \mathbb{Z})$ given by $x \mapsto (m \mapsto \langle m, x\rangle)$.*

Proof. Items (a) and (b) are well known and we omit the proof. For (c), it is straight-forward to check that $L^\dagger \cap M^\perp$ is the kernel of the homomorphism $L^\dagger \to \mathrm{Hom}\,(M, \mathbb{Z})$ stated above and this implies that $L^\dagger / L^\dagger \cap M^\perp$ is torsion-free, i.e., $L^\dagger \cap M^\perp$ is pure. □

Definition 6.18. By a *kernel and image* algorithm we mean an algorithm that given an homomorphism $\mathbb{Z}^q \to \mathbb{Z}^p$ of free groups, specified by some integral matrix $\mathbf{F} \in \mathrm{M}_{p\times q}(\mathbb{Z})$, computes $r \in \mathbb{Z}_{\geqslant 0}$ and a basis of $\mathbb{Z}^q$ of which the first r vectors form a basis for the kernel of this homomorphism. ♢

Remark 6.19. The algorithm given in [10, pg. 163] is a polynomial-time kernel and image algorithm that uses the classical LLL algorithm as we briefly described in the introduction.

From now on and until the end of this section, we let $(\mathbb{R}^m, \mathbb{R}^{\underline{n}}, \langle\cdot,\cdot\rangle)$ be a layered Euclidean space; we let $\{V_k\}_{k\in\underline{n}}$ denote the convex filtration of $V = \mathbb{R}^{\underline{n}}$ and $\{E_k\}_{k\in\underline{n}_0}$ denote the layers of $E = \mathbb{R}^m$. We assume $L = \mathbb{Z}^m \subset E$ is an embedded layered lattice, and denote the layers of L by $\{L_k\}_{k\in\underline{n}_0}$. For each $k \in \underline{n}_0$ we denote by $m(k)$ the dimension of E_k, which is also the rank of L_k. Finally, we let $\{e_i\}_{i\in\underline{m}}$ be the canonical basis of $L \subset E$ and define matrices $\mathbf{B}^1, \ldots, \mathbf{B}^n \in \mathrm{M}_m(\mathbb{R})$ by the formula

$$\langle e_i, e_j\rangle = (\mathbf{B}^1_{i,j}, \ldots, \mathbf{B}^n_{i,j}).$$

We denote by q the quadratic norm associated to $\langle\cdot,\cdot\rangle$.

As in chapter 5, where we described a polynomial-time algorithm to compute Gram-Schmidt bases, for the purpose of defining and analyzing an algorithm, it is important that our input is *rational*. In the present case, this amounts to the extra assumption that the matrices $\mathbf{B}^k$ are rational, i.e., $\mathbf{B}^k \in \mathrm{M}_m(\mathbb{Q})$.

We now show that size-reducing a basis can be done in polynomial time. We recall definition (1.9) from the introduction.

Lemma 6.20. *There exists a polynomial-time algorithm that given a basis $\{b_i\}_{i\in\underline{m}}$ of $L = \mathbb{Z}^m$ specified in terms of its canonical basis, and matrices $\mathbf{B}^1, \ldots, \mathbf{B}^n \in \mathrm{M}_m(\mathbb{Q})$ as above, outputs a size-reduced basis of L with the same associated Gram-Schmidt basis.*

Proof. Let $\{b_i^*\}_{i\in\underline{m}}$ be Gram-Schmidt basis associated to the input basis and $\{\lambda_{i,j}\}_{1\leqslant j<i\leqslant m}$ be the rational numbers such that $b_i = b_i^* + \sum_{j<i}\lambda_{i,j}b_j^*$. By theorem (5.28) we can compute them in polynomial time with this input. Applying the substitution steps of proposition (6.5), we obtain the desired size-reduced basis. We will prove the lemma by giving a polynomial upper-bound for the number of bits necessary to represent the numbers $\mu_{i,j}$ appearing throughout the steps of that proposition, and a polynomial upper-bound for the number of arithmetical operations performed (both in terms of the input).

We start with the number of arithmetical operations. For each $i \in \underline{m}$, we perform $i-1$ steps and for each of those, 4 arithmetical operations are performed. The total number of arithmetical operations is therefore less than $4m^2$.

To bound the numbers involved, let $r_0 \in \mathbb{Z}_{\geqslant 0}$, $r > 1$, be an upper-bound for all the $|\lambda_{i,j}| \in \mathbb{Q}$ and $q_0 \in \mathbb{Z}_{\geqslant 0}$, $q > 1$, be an upper-bound for the absolute value of their denominators (note that their numerators are thus bounded, in absolute value, by r_0q_0). The number of bits sufficient to represent the $\lambda_{i,j}$ is then bounded by $\log_2 q_0 + \log_2(r_0q_0) = \log_2(r_0q_0^2)$. The bound we give below is in terms of m, $\log_2 r_0$ and $\log_2 q_0$.

Let $i \in \underline{m}$ and suppose we finished substitution step $j > 1$. Let $r \in \mathbb{Z}$, $r > 1$, be an upper-bound for the numbers $\mu_{i,j}$ at this point and $q \in \mathbb{Z}$, $q > 1$, an upper-bound for their denominators. After substitution step $j-1$ we have:

$$\begin{aligned} |\mu| &\leqslant r+1, \\ |\mu_{i,j}| &\leqslant r + |\mu| \leqslant 2(r+1), \\ |\mu_{i,h}| &\leqslant r + \mu r_0 \leqslant (r+1)(r_0+1). \end{aligned}$$

Thus, $r' = (r+1)(r_0+1)$ is an upper-bound for the $|\mu_{i,j}|$ after this substitution step. The denominators of these numbers are clearly bounded by $q' = qq_0$. By induction, we see that all the numbers $\mu_{i,j}$ appearing throughout the substitutions steps are bounded, in absolute value, by $(r_0+1)^i \leqslant (r_0+1)^m$. Similarly their denominators are bounded, in absolute value, by q_0^m. It follows that their *numerators* are bounded, in absolute value, by $q_0^m(r_0+1)^m$. The number of bits sufficient to represent all these numbers is thus bounded by

$$\log_2(q_0^m) + \log_2(q_0^m(r_0+1)^m) = m\log_2(q_0^2(r_0+1)).$$

The proof is complete since performing $4m^2$ arithmetical operations with numbers of this size can be done in polynomial time. We refer the reader to [13, §2.1]. □

We now describe an algorithm to compute reduced bases of layered lattices. The input of this algorithm is comprised of a parameter $c \in \mathbb{Q}$, $c > 4/3$, the rank m of $L = \mathbb{Z}^m$ and a sequence of rational matrices $\mathbf{B}^1, \ldots, \mathbf{B}^k \in \mathrm{M}_m(\mathbb{Q})$

specifying the inner-product in $E = \mathbb{R}^m$ in terms of the canonical basis of E. The algorithm is described in six steps enumerated as (a) through (f) below.

(a) The first step is to compute the Gram-Schmidt basis associated to the canonical basis $\{e_i\}_{i\in\underline{m}}$ of $L \subset E$, denoted by $\{e_i^*\}_{i\in\underline{m}}$, and the numbers $\{\lambda_{i,j}\}_{1\leqslant j<i\leqslant m}$ such that for all $i \in \underline{m}$ we have $e_i = e_i^* + \sum_{j<i} \lambda_{i,j} e_j^*$. We also let $d \in \mathbb{Z}_{>0}$ be a common multiple of the denominators of all the $\lambda_{i,j}$. Note that $de_i^* \in L$ holds for all $i \in \underline{m}$. This is done using the algorithm of theorem (5.28).

(b) Next, for each $k \in \underline{n}$ let

$$M_k = \sum_{e_i^* \in E_k} \mathbb{Z}\, de_i^* \subset L_k$$

and $\mathbf{F}_k$ be the matrix $((de_i^*)^T e_j)_{\{i:e_i^*\in E_k\},j\in\underline{m}}$. This matrix specifies the group homomorphism

$$f_k : L^\dagger \to (M_k, \mathbb{Z}) \simeq \mathbb{Z}^{m(k)}$$

given by $x \mapsto (z \mapsto z^T x)$. Using a kernel and image algorithm, compute a basis $\{d_i^k\}_{i\in\underline{m}}$ of $L^\dagger$ such that its first $r(k) = m - m(k)$ vectors form a basis for $\ker f_k$. Note that, by proposition (6.17), we have $\ker f_k = L^\dagger \cap M_k^\perp$.

(c) Next, for $k \in \underline{n}$, let $\mathbf{F}'_k$ be the matrix $((d_i^k)^T e_j)_{i\in\underline{r(k)},j\in\underline{m}}$ which specifies the group homomorphism

$$f'_k : L^{\dagger\dagger} \to \mathrm{Hom}\,(\ker f_k, \mathbb{Z}) \simeq \mathbb{Z}^{r(k)}$$

given by $x \mapsto (z \mapsto z^T x)$. Again using a kernel and image algorithm compute a basis $\{a_i^k\}_{i\in\underline{m}}$ of L whose first $m - r(k) = m(k)$ vectors form a basis for $\ker f'_k$. Again, by proposition (6.17), we have $\ker f'_k = L^{\dagger\dagger} \cap M_k^{\perp\perp} = L \cap (\mathbb{R}\cdot M_k) = L_k$.

(d) For each $k \in \underline{n}$, the homomorphism $L_k \to L \to \mathrm{Hom}\,(\ker f_{k-1}, \mathbb{Z})$ specified by the $m \times m(k)$ matrix whose j-th column is given by $\mathbf{F}'_{k-1} \cdot a_j^k$ has kernel L_{k-1}. Using a kernel and image algorithm, compute a basis for L_k such that the last $m(k) - m(k-1)$ vectors form a basis for a complement of this kernel. Note that $m(0) = 0$ as this equals the rank of L_0. Denote this basis by $\{a_i : m(k-1) < i \leqslant m(k)\}$.

(e) For each $k \in \underline{n}$ let N_k be the group generated by the vectors $\{a_i : m(k-1) < i \leqslant m(k)\}$ and define $q_k : N_k \to \mathbb{Q}$ by $x \mapsto x^T \mathbf{B}^k x$. Apply the classical LLL with "reducedness" parameter c to $\{a_i : m(k-1) < i \leqslant m(k)\}$. Denote the output by $\{b_i : m(k-1) < i \leqslant m(k)\}$.

(f) Size-reduce the sequence of vectors $\{b_i\}_{i\in\underline{m}}$ obtained from (e) using proposition (6.5). Output the sequence $\{c_i\}_{i\in\underline{m}}$ from that proposition.

This finishes the description of the algorithm. We come to the main theorem of this section. We remind the reader of definition (4.7).

Theorem 6.21. *For each $c > 4/3, c \in \mathbb{Q}$, there is a polynomial-time algorithm that given a layered lattice $(\mathbb{Z}^m, \mathbb{R}^{\underline{n}}, \mathbf{B}^1, \ldots, \mathbf{B}^k)$ of rank m, specified as above, computes a c-reduced basis of this lattice.*

Proof. The algorithm is the one described in steps (a) through (f) above. We start by showing the correctness of the algorithm. This also entails showing that whenever we call an algorithm to perform a computation we are giving *valid* input. For step (a), this is clear. In steps (b) and (c) note that $L^\dagger = L = L^{\dagger\dagger}$ and that $\ker f_k = M^\perp \cap L^\dagger$ by proposition (6.17). Thus we are computing a basis $\{b_i^k\}_{i \in \underline{m}}$ of L whose first $m(k)$ vectors form a basis of $M^{\perp\perp} \cap L^{\dagger\dagger} = (\mathbb{Q} \cdot M_k) \cap L = L_k$ for each $k \in \underline{n}$.

In step (d), note that the kernel of $L_k \to L \to \mathrm{Hom}\,(\ker f_{k-1}, \mathbb{Z})$ equals L_{k-1}. So using the family of bases from step (c), we compute a basis for L_k whose first vectors form a basis of L_{k-1}. At the end of step (d) we thus have a layered basis $\{a_i\}_{i \in \underline{m}}$ of L.

In (e), for each $k \in \underline{n}$, the group N_k generated by $\{a_i : m(k-1) < i \leqslant m(k)\}$ is a classical lattice when equipped with the quadratic map determined by $x \mapsto x^T \mathbf{B}^k x$. In fact, this pair is none other than the layered lattice $(L_k/L_{k-1}, V_k/V_{k-1}, q)$ with $q : L_k/L_{k-1} \to V_k/V_{k-1} \simeq \mathbb{R}$ of lemma (4.15) (recall that $\{V_k\}_{k \in \underline{n}}$ is the convex filtration of $\mathbb{R}^{\underline{n}}$). By corollary (4.23) this is a classical lattice. Applying the classical LLL algorithm with parameter c we compute a c-reduced basis for this lattice.

The output of step (e) is thus a layered basis of L *that satisfies the Lovász condition for c* (although it is not necessarily size-reduced). Thus the substitution steps from lemma (6.5) give a c-reduced basis for the (layered) lattice L. This finishes the proof of the correctness of the algorithm.

It remains to show that the algorithm is polynomial-time. Step (a) is done in polynomial time by theorem (5.28). In particular, finding $d \in \mathbb{Z}_{>0}$ that is a common multiple of the denominators of the $\mu_{i,j}$ can also be done in polynomial time. For each $k \in \underline{n}$, steps (b) and (c) are done in polynomial time since the kernel and image algorithm used is assumed to be polynomial-time. Since performing these steps for different $k, l \in \underline{n}$ can be done independently, we conclude that computing the family of bases $\{a_i^k\}_{i \in \underline{m}}$ is done in polynomial time. The input of step (d) is thus bounded by a polynomial in the input and it involves another application of a (polynomial-time) kernel and image algorithm. The same reasoning establishes that (e) is also done in polynomial time and, by lemma (6.20), step (f) too. $\square$

APPENDIX A

Two algorithms

In this short appendix we present two algorithms of our work in pseudocode. We start with an algorithm for the Gram-Schmidt procedure which can be derived from proposition (5.7).

input : A sequence of rational matrices $\{\mathbf{B}^1, \ldots, \mathbf{B}^n\} \in \mathrm{M}_m(\mathbb{Q})$ specifying the inner-product of the layered Euclidean space $(\mathbb{R}^m, \mathbb{R}^n, \langle\cdot,\cdot\rangle)$ with respect to the canonical basis.

output: The Gram-Schmidt basis $\{\mathbf{e}_i^*\}_{i=1}^m$ associated to the canonical basis $\{\mathbf{e}_i\}_{i\in\underline{m}}$ of $\mathbb{Q}^m$ viewed as a subspace of the layered Euclidean space and the numbers $\{\lambda_{i,j}\}_{1\leqslant j<i\leqslant m}, \lambda_{i,j} \in \mathbb{Q}$ given by equations (5.9) which specify the canonical basis in terms of its associated Gram-Schmidt basis.

```
for i = 1 to m do
    e*_i ← e_i;
    for j = 1 to i − 1 do
        /* Compute λ_{i,j} inductively.  */
        λ_{i,j} ← (e*_i^T · e'_j)/(e*_j^T · e'_j);
        /* Update e*_i.  */
        e*_i ← e*_i − λ_{i,j} · e*_j;
    end for
    /* Compute the o(i).  */
    o(i) ← n + 1;
    repeat
        o(i) ← o(i) − 1;
        e'_i ← B^{o(i)} · e*_i;
    until e*_i^T · e'_i ≠ 0;
end for
```

Algorithm A.1: Gram-Schmidt algorithm

We now give a quick description of the layered LLL algorithm. This is a simplified version based on the algorithm of section (6.2). We chose to describe the algorithm in this way for clarity. By $\mathrm{GS}(\{\mathbf{e}_i\}_{i=1}^m,\ k)$ we mean a call to a sub-procedure computing the first k vectors of the Gram-Schmidt basis associated to the basis $\{\mathbf{e}_i\}_{i=1}^m$ and the numbers $\lambda_{i,j}$, $1 \leqslant j < i \leqslant k$ expressing the vectors $\mathbf{e}_i$ in terms of its associated Gram-Schmidt basis.

input : A rational number $c > 4/3$ and an ordered sequence of *rational* matrices $\{\mathbf{B}^1, \ldots, \mathbf{B}^n\} \subset \mathrm{M}_m(\mathbb{Q})$ specifying the inner-product of the layered Euclidean space $(\mathbb{R}^m, \mathbb{R}^{\underline{n}}, \langle \cdot, \cdot \rangle)$ with the property that the group generated by the canonical basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ of $\mathbb{R}^m$ is a layered lattice.

output: A c-reduced basis $\{\mathbf{e}_i\}_{i=1}^m$ of the same layered lattice.

1 $k \leftarrow 2$;
2 $\{\mathbf{e}_i^*\}_{i=1}^k, \{\lambda_{i,j}\}_{1 \leqslant j < i \leqslant k} \leftarrow \mathrm{GS}(\{\mathbf{e}_i\}_{i=1}^m, k)$;
3 **for** $j = k-1$ **to** $j = 1$ **do**
4 **if** $|\lambda_{k,j}| > 1/2$ **then**
 `/* Size-reduce` $\lambda_{k,j}$`. [·] denotes the nearest integer function. */`
5 $\lambda \leftarrow [\lambda_{k,j}]$;
6 $\mathbf{e}_k \leftarrow \mathbf{e}_k - \lambda \cdot \mathbf{e}_j$;
7 $\{\mathbf{e}_i^*\}_{i=1}^k, \{\lambda_{i,j}\}_{1 \leqslant j < i \leqslant k} \leftarrow \mathrm{GS}(\{\mathbf{e}_i\}_{i=1}^m, k)$; `/* Update the Gram-Schmidt basis. */`
8 **end if**
9 **end for**
10 **if** $\mathrm{lt}(q(\mathbf{e}_{k-1}^*)) \leqslant c \cdot \mathrm{lt}(q(\mathbf{e}_k^*))$ **then**
 `/* To this point we have a` c`-reduced basis up to level` k`. */`
11 **if** $k < m$ **then**
12 $k \leftarrow k + 1$;
13 GOTO 2;
14 **end if**
15 EXIT;
16 **else**
17 $\mathbf{e} \leftarrow \mathbf{e}_k$, $\mathbf{e}_k \leftarrow \mathbf{e}_{k-1}$ and $\mathbf{e}_{k-1} \leftarrow \mathbf{e}$; `/* Swap` $\mathbf{e}_{k-1}, \mathbf{e}_k$ `*/`
18 **if** $k > 2$ **then**
19 $k \leftarrow k - 1$;
20 **end if**
21 GOTO 2;
22 **end if**

Algorithm A.2: Layered LLL algorithm

Samenvatting

Een rooster is een discrete ondergroep van een Euclidische ruimte. Elk rooster wordt voortgebracht door een stelsel lineair onafhankelijke vectoren. Zo een stelsel noemt men een basis voor het rooster. Dit proefschrift betreft het probleem om voor een gegeven rooster een goede basis te vinden. Algoritmisch gezien wordt een rooster gegeven door een basis, en het probleem kan dus geformuleerd worden als het vinden van een aantal transformaties dat de gegeven basis in een betere basis verandert. Men spreekt van een basisreductie-algoritme. Goede bases worden gereduceerde bases genoemd.

Basisreductie heeft een lange geschiedenis en het eerste algoritme, voor willekeurige roosters, dat in polynomiale tijd eindigt, is pas in 1982 beschreven in [8]. Dit algoritme is nu bekend als het LLL-algoritme. In dit proefschrift wordt de theorie van gelaagde roosters ontwikkeld en het basisreductie-probleem voor gelaagde roosters bestudeerd en opgelost. Een gelaagd rooster is een rooster waar de lengtes van vectoren verschillende ordes van grootte kunnen hebben. Dit concept vindt zijn oorsprong in situaties zoals de volgende.

Zij $f : \mathbb{Z}^n \to \mathbb{Z}^m$ een homomorfisme van vrije abelse groepen. Men wil een basis voor de kern van f bepalen. In [10] lost de auteur dit probleem op met behulp van roostertheorie. Hij introduceert het rooster $(\mathbb{Z}^n, q_M)$ waar de lengtefunctie $q_M : \mathbb{Z}^n \to \mathbb{R}$ gegeven is door

$$q_M(x) = ||x||^2 + M \cdot ||f(x)||^2$$

voor een groot positief getal M (met $||\cdot||$ noteren we de gebruikelijke Euclidische norm). Zij B_M de verzameling punten van $\mathbb{Z}^n$ met lengte kleiner dan M ten opzichte van de lengtefunctie q_M. Het is makkelijk in te zien dat B_M in $\ker f$ bevat is en dat, naarmate groter M gekozen wordt, er meer punten uit de

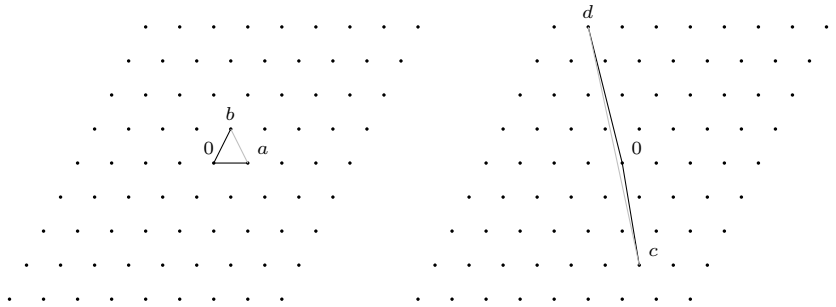

Figure 1.1: Twee bases voor hetzelfde rooster. Elk punt in het rooster wordt gerepresenteerd als $m \cdot a + n \cdot b$ of $p \cdot c + q \cdot d$ voor gehele getallen $m, n, p, q \in \mathbb{Z}$. De basis links is een "goede" basis omdat punten dicht bij 0 worden gerepresenteerd met kleine getallen m, n. De basis rechts, daarentegen, is een slechte basis; punten dicht bij 0 hebben grote getallen p, q nodig om beschreven te worden. Het verschil tussen beide is gerelateerd aan de vorm van de driehoeken in de figuur.

kern van f in B_M zullen liggen. Men kan bewijzen dat voor M groter dan een bepaalde grens, die afhankelijk is van f, het LLL-algoritme een basis van $\mathbb{Z}^n$ vindt zodanig dat de eerste $n - \text{rang } f$ vectoren de kern van f voortbrengen.

De theorie van gelaagde roosters beschrijft wat er gebeurt als we M "oneindig" laten worden. Dat wil zeggen, M is nu een symbool ∞ met de eigenschap dat voor alle positieve reële getallen λ en μ de ongelijkheid $\lambda < \mu \cdot \infty$ geldt. De nieuwe lengtefunctie $q_\infty : \mathbb{Z}^n \to \mathbb{R} \oplus \mathbb{R} \cdot \infty$ met

$$q_\infty(x) = ||x||^2 + ||f(x)||^2 \cdot \infty$$

neemt vectoren als waarden aan. Merk op dat de kern van f nu precies gelijk is aan B_∞, de verzameling vectoren van lengte kleiner dan ∞. Deze verzameling is dus een deelrooster van $\mathbb{Z}^n$ dat een orde van grootte ligt onder de rest van het rooster; het is een voorbeeld van wat we een *laag* van het gelaagde rooster noemen. In dit proefschrift definiëren we wat een gereduceerde basis van een gelaagd rooster is, en we laten zien dat zo'n basis in polynomiale tijd berekend kan worden.[1] We laten ook zien dat een gegeneraliseerde LLL-algoritme bestaat voor gelaagde roosters dat termineert, en dat gereduceerde bases kan vinden zonder gebruik te maken van "gewichten" zoals M hierboven. Dit is van praktisch belang, zoals het voorbeeld hierboven laat zien.

[1] Een gereduceerde basis is, in het bijzonder, gelaagd. Dat wil zeggen, alle lagen van het gelaagde rooster worden opgespannen door deelverzamelingen van deze basis.

Bibliography

[1] N. Bourbaki. *Algèbre*, volume 1 of *Éléments de mathématique*. Springer, 1981.

[2] J. Buchmann and A. Pethő. *Computation of independent units in number fields by Dirichlet's method*, volume 229 of *Lecture notes in computer science*. Springer, 1986.

[3] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate texts in mathematics*. Springer, 1993.

[4] I. Efrat. *Valuations, orderings and Milnor K-theory*, volume 124 of *Mathematical surveys and monographs*. AMS, 2006.

[5] E. Kaltofen. On the complexity of finding short vectors in integer lattices. In *Proceedings of EUROCAL '83*, pages 236–244. 1983.

[6] S. Koshi. Vector spaces with linear order. *Comment. Math. Special Issue*, 2:183–187, 1979.

[7] S. Lang. *Algebra*, volume 211 of *Graduate texts in mathematics*. Springer, 2002.

[8] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[9] H. W. Lenstra Jr. Flags and lattice basis reduction. In R. M. Miro-Roig C. Casacuberta, J. Verdera, and S. Xambo-Deschamps, editors, *3rd European congress on mathematics*, pages 37–52. Springer-Verlag, Barcelona, 2001.

[10] H. W. Lenstra Jr. Lattices. In J. P. Buhler and P. Stevenhagen, editors, *Surveys in algorithmic number theory*, pages 127–182. MSRI publications, 2009.

[11] P. Nguyen and B. Vallée, editors. *The LLL algorithm: survey and applications*. Information security and cryptography. Springer, 2009.

[12] M. Pohst. A modification of the LLL reduction algorithm. *J. Symbolic Comput.*, 4(1):123–127, 1987.

[13] A. Schrijver. *Theory of linear and integer programming*. Wiley interscience series in discrete mathematics and optimization. Wiley, 1998.

Curriculum Vitae

Personalia

Naam	Erwin Lavallière Torreão Dassen
Geboren	14 December 1979, te Campina Grande, Brazilië.

Opleidingen

2006 - 2010	Promovendus bij Prof. Dr. H. W. Lenstra Jr., Mathematisch Instituut, Universiteit Leiden.
2003 - 2005	Master of Science: Honors Magister in Algebra, Federal University of Santa Catarina, Brazil.
1999 - 2002	Bachelor degree in Mathematics and Scientific Computing, Federal University of Santa Catarina, Brazil.

Huidige werkgever

Centrum voor Wiskunde en Informatica (CWI), Amterdam.