MPRI 2-12-1: Phong Nguyen **Fall 2024**

Lecture 1: Introduction to Lattices

1 Background

We consider $\mathbb{R}^n$ with its usual topology of an Euclidean vector space. We will use bold letters to denote vectors, usually in row notation. The Euclidean inner product of two vectors $\mathbf{x} = (x_i)_{i=1}^n$ and $\mathbf{y} = (y_i)_{i=1}^n$ is denoted by:

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i y_i.$$

The corresponding Euclidean norm is denoted by:

$$\|\mathbf{x}\| = \sqrt{x_1^2 + \cdots + x_n^2}.$$

Denote by $B(\mathbf{x}, r)$ the open ball of radius r centered at $\mathbf{x}$:

$$B(\mathbf{x}, r) = \{\mathbf{y} \in \mathbb{R}^n : \|\mathbf{x} - \mathbf{y}\| < r\}.$$

A subset D of $\mathbb{R}^n$ is called *discrete* when it has no limit point, that is: for all $x \in D$, there exists $\rho > 0$ such that $B(x, \rho) \cap D = \{x\}$. As an example, $\mathbb{Z}^n$ is discrete (because $\rho = 1/2$ works), while $\mathbb{Q}^n$ and $\mathbb{R}^n$ are not. The set $\{1/n : n \in \mathbb{N}^*\}$ is discrete, but the set $\{0\} \cup \{1/n : n \in \mathbb{N}^*\}$ is not. Any subset of a discrete set is discrete.

For any ring R, we denote by $\mathcal{M}_{n,m}(R)$ (resp. $\mathcal{M}_n(R)$) the set of $n \times m$ (resp. $n \times n$) matrices with coefficients in R. $GL_n(R)$ denotes the group of invertible matrices in the ring $\mathcal{M}_n(R)$.

For any subset S of $\mathbb{R}^n$, we define the linear span of S, denoted by $\mathrm{span}(S)$, as the minimal vector subspace (of $\mathbb{R}^n$) containing S. And we denote by $S^\perp$ the subspace orthogonal to $\mathrm{span}(S)$:

$$S^\perp = \{\mathbf{y} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y} \rangle = 0 \text{ for all } \mathbf{x} \in S\}.$$

Let $\mathbf{b}_1, \ldots, \mathbf{b}_m$ be in $\mathbb{R}^n$. The vectors $\mathbf{b}_i$'s are said to be *linearly dependent* if there exist $x_1, \ldots, x_m \in \mathbb{R}$ which are not all zero and such that:

$$\sum_{i=1}^{m} x_i \mathbf{b}_i = 0.$$

Otherwise, they are said to be *linearly independent*.

The Gram determinant of $\mathbf{b}_1, \ldots, \mathbf{b}_m \in \mathbb{R}^n$, denoted by $\Delta(\mathbf{b}_1, \ldots, \mathbf{b}_m)$, is by definition the determinant of the Gram matrix $(\langle \mathbf{b}_i, \mathbf{b}_j \rangle)_{1 \leq i,j \leq m}$. This real number $\Delta(\mathbf{b}_1, \ldots, \mathbf{b}_m)$ is always ≥ 0, and it turns out to be zero if and only if the $\mathbf{b}_i$'s are linearly dependent. The Gram determinant is invariant by any permutation of the m vectors, and by any integral linear transformation of determinant ± 1 such as adding to one of the vectors a linear combination of the others. The Gram determinant has a very useful geometric interpretation: when the $\mathbf{b}_i$'s are linearly independent, $\sqrt{\Delta(\mathbf{b}_1, \ldots, \mathbf{b}_m)}$ is the m-dimensional volume of the parallelepiped spanned by the $\mathbf{b}_i$'s.

2 Lattices

We call *lattice* of $\mathbb{R}^n$ any discrete subgroup of $(\mathbb{R}^n, +)$; that is any subgroup of $(\mathbb{R}^n, +)$ which has the discreteness property. We remark that a group is discrete if and only if 0 is not a limit point:

Lemma 2.1 *Let L be a subgroup of $(\mathbb{R}^n, +)$. Then L is discrete if and only if there exists $\rho > 0$ such that $L \cap B(0, \rho) = \{0\}$.*

Proof. By definition, we only need to prove the converse. Let L be a subgroup of $(\mathbb{R}^n, +)$ such that $L \cap B(0, \rho) = \{0\}$. We claim that for all $\mathbf{x} \in L$, $L \cap B(\mathbf{x}, \rho) = \{\mathbf{x}\}$. Let $\mathbf{x} \in L$ and $\mathbf{y} \in L \cap B(\mathbf{x}, \rho)$. Because L is a group, we have $\mathbf{y} - \mathbf{x} \in L$. But we also have $\|\mathbf{y} - \mathbf{x}\| < \rho$ because $\mathbf{y} \in B(\mathbf{x}, \rho)$. Therefore $\mathbf{y} - \mathbf{x} \in L \cap B(0, \rho) = \{0\}$, so $\mathbf{y} = \mathbf{x}$. This shows that L is discrete. □

Thus, a lattice is any non-empty set $L \subseteq \mathbb{R}^n$ stable by subtraction (in other words: for all $\mathbf{x}$ and $\mathbf{y}$ in L, $\mathbf{x} - \mathbf{y}$ belongs to L), and such that $L \cap B(0, \rho) = \{0\}$ for some $\rho > 0$.

With this definition, the first examples of lattices which come to mind are the zero lattice $\{0\}$ and the *lattice of integers* $\mathbb{Z}^n$. Our definition implies that any subgroup of a lattice is a lattice, and therefore, any subgroup of $(\mathbb{Z}^n, +)$ is a lattice. Such lattices are called *integral lattices*. As an example, consider two integers a and $b \in \mathbb{Z}$: the set $a\mathbb{Z} + b\mathbb{Z}$ of all integral linear combinations of a and b is a subgroup of $\mathbb{Z}$, and therefore a lattice; it is actually the set $\gcd(a, b)\mathbb{Z}$ of all multiples of the gcd of a and b. For another example, consider n integers $a_1, \ldots, a_n$, together with a modulus M. Then the set of all $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ such that $\sum_{i=1}^n a_i x_i \equiv 0 \pmod{M}$ is a lattice in $\mathbb{Z}^n$ because it is clearly a subgroup of $\mathbb{Z}^n$.

We give a few basic properties of lattices:

Proposition 2.2 *Let L be a lattice in $\mathbb{R}^n$.*

1. *There exists $\rho > 0$ such that for all $\mathbf{x} \in L$:*
$$L \cap B(\mathbf{x}, \rho) = \{\mathbf{x}\}.$$
2. *L is closed.*
3. *For all bounded subsets S of $\mathbb{R}^n$, $L \cap S$ is finite.*
4. *L is countable.*

Proof. Property 1 follows from Lemma 2.1. It follows that any convergent sequence of L is stationary, which proves property 2. If S is a bounded subset, it must be included in some closed ball B. The set $L \cap B$ is closed and bounded, thus compact. Suppose *ad absurdum* that $L \cap S$ is infinite: there is an injective sequence $(x_i)_i$ in $L \cap S$. By compacity, we may extract a convergent injective sequence $(y_i)_i$ in $L \cap S$, which contradicts property 1. This proves property 3. Since $\mathbb{R}^n$ is the union of all $B(0, r)$ for $r \in \mathbb{N}$, we obtain property 4. □

Notice that a set which satisfies either property 1 or 3 is necessarily discrete, but an arbitrary discrete subset of $\mathbb{R}^n$ does not necessarily satisfy property 1 nor 3. It is the group structure of lattices which allows such additional properties.

2.1 The rank

We define the *dimension* or *rank* of a lattice L, denoted by $\mathrm{rank}(L)$, as the dimension d of its linear span denoted by $\mathrm{span}(L)$. The rank is the maximal number of linearly independent lattice vectors. If $\mathrm{rank}(L) \geq 1$, Prop. 2.2 allows to define the first minimum $\lambda_1(L)$ of L as the shortest non-zero norm of a lattice vector:
$$\lambda_1(L) = \min_{\mathbf{x} \in L, \mathbf{x} \neq 0} \|\mathbf{x}\|.$$

It is useful to know what rank-one lattices look like:

Lemma 2.3 *Let L be a rank-one lattice in $\mathbb{R}^n$. There exists a non-zero $\mathbf{v} \in L$ such that $L = \mathbb{Z}\mathbf{v}$.*

Proof. There exists $\mathbf{v} \in L$ such that $\|\mathbf{v}\| = \lambda_1(L)$. We have $\mathbb{Z}\mathbf{v} \subseteq L$ because L is a group. Reciprocally, let $\mathbf{w} \in L$. Because $\mathrm{span}(L) = \mathrm{span}(\mathbf{v})$, there exists $\mu \in \mathbb{R}$ such that $\mathbf{w} = \mu\mathbf{v}$. Then $\mathbf{w} - \lfloor\mu\rceil\mathbf{v} \in L$ because L is a group, where $\lfloor\mu\rceil$ denotes an integer closest to μ. And $\|\mathbf{w} - \lfloor\mu\rceil\mathbf{v}\| = \|(\mu - \lfloor\mu\rceil)\mathbf{v}\| \leq$

$\frac{1}{2}\|\mathbf{v}\|$. Since $\|\mathbf{v}\| = \lambda_1(L)$, this implies that $\mu = \lfloor \mu \rceil$, so $\mu \in \mathbb{Z}$. This proves $L \subseteq \mathbb{Z}\mathbf{v}$, and therefore the equality. □

The projection of a lattice may not be discrete, but any set of linearly independent lattice vectors induces by projection a lattice of lower rank, as follows:

Theorem 2.4 *Let L be a d-rank lattice in $\mathbb{R}^n$. Let $\mathbf{v}_1, \ldots, \mathbf{v}_k \in L$ be linearly independent: $1 \leq k \leq d$. Let π be the orthogonal projection over $\mathrm{span}(\mathbf{v}_1, \ldots, \mathbf{v}_k)^\perp$. Then $\pi(L)$ is a lattice of rank $d - k$.*

Proof. Since $\pi(L)$ is a subgroup of $\mathbb{R}^n$, it suffices to prove that 0 is not a limit point. Suppose *ad absurdum* that there exists an injective sequence $(\pi(\mathbf{x}_i))_i$ converging to 0, where $\mathbf{x}_i \in L$. By definition of the projection, we have:

$$\|\mathbf{x}_i\|^2 = \|\pi(\mathbf{x}_i)\|^2 + \|\mathbf{x}_i - \pi(\mathbf{x}_i)\|^2.$$

Here, the left term $\|\pi(\mathbf{x}_i)\|^2$ is bounded because it converges to zero. And we note that the right term $\|\mathbf{x}_i - \pi(\mathbf{x}_i)\|^2$ can always be made $\leq (\sum_{j=1}^n \|\mathbf{v}_j\|)^2$. Indeed, $\mathbf{x}_i - \pi(\mathbf{x}_i) \in \mathrm{span}(\mathbf{v}_1, \ldots, \mathbf{v}_k)$, so there exist real numbers $t_1, \ldots, t_k$ such that:

$$\mathbf{x}_i - \pi(\mathbf{x}_i) = \sum_{j=1}^{k} t_j \mathbf{v}_j.$$

By subtracting $\sum_{j=1}^n \lfloor t_j \rfloor \mathbf{v}_j$ to $\mathbf{x}_i$, we make the $\mathbf{t}_j$'s belong to $[0, 1]$, so that $\|\mathbf{x}_i - \pi(\mathbf{x}_i)\| \leq \sum_{j=1}^n \|\mathbf{v}_j\|$, without changing $\pi(\mathbf{x}_i)$ nor the fact that $\mathbf{x}_i \in L$. Thus, the sequence $(\mathbf{x}_i)_i$ of lattice vectors can be made bounded, so it cannot be injective by Prop. 2.2, which contradicts the injectivity of $(\pi(\mathbf{x}_i))_i$.

□

2.2 Lattice bases

Let $\mathbf{b}_1, \ldots, \mathbf{b}_m$ be arbitrary vectors in $\mathbb{R}^n$. Denote by $L(\mathbf{b}_1, \ldots, \mathbf{b}_m)$ the set of all integral linear combinations of the $\mathbf{b}_i$'s:

$$L(\mathbf{b}_1, \ldots, \mathbf{b}_m) = \left\{ \sum_{i=1}^{m} n_i \mathbf{b}_i : n_1, \ldots, n_m \in \mathbb{Z} \right\}$$

This set is a subgroup of $\mathbb{R}^n$, but it is not necessarily discrete. For instance, one can show that $L((1), (\sqrt{2}))$ is not discrete because $\sqrt{2} \notin \mathbb{Q}$. However, notice that if the $\mathbf{b}_i$'s are in $\mathbb{Q}^n$, then $L(\mathbf{b}_1, \ldots, \mathbf{b}_m)$ is discrete, and so is a lattice. When $L = L(\mathbf{b}_1, \ldots, \mathbf{b}_m)$ is a lattice, we say that L is spanned by the $\mathbf{b}_i$'s, and that the $\mathbf{b}_i$'s are *generators*. When the $\mathbf{b}_i$'s are further

linearly independent, we say that $(\mathbf{b}_1, \ldots, \mathbf{b}_m)$ is a *basis* of the lattice L, in which case each lattice vector decomposes itself uniquely as an integral linear combination of the $\mathbf{b}_i$'s.

Theorem 2.5 *Let $\mathbf{b_1}, \ldots, \mathbf{b}_d \in \mathbb{R}^n$ be linearly independent. Then the set $L(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ is a lattice of rank d.*

Proof. Let $L = L(\mathbf{b}_1, \ldots, \mathbf{b}_d)$. Since L is a subgroup of $\mathbb{R}^n$, it suffices to show that 0 is not a limit point of L. Suppose *ad absurdum* that 0 is a limit point: there is an injective sequence $(\mathbf{x}_m)_m$ converging to 0. Each $\mathbf{x}_m$ decomposes uniquely as $\mathbf{x}_m = \mathbf{y}_m B$, where B is the row matrix representing the $\mathbf{b}_i$'s, and $\mathbf{y}_m \in \mathbb{Z}^d$. By expressing $\mathbf{y}_m$ with respect to $\mathbf{x}_m$, one sees that $(\mathbf{y}_m)$ must converge to 0, which implies that $(\mathbf{y}_m)$ is stationary, which contradicts the injectivity of $(\mathbf{x}_m)$.

Since the $\mathbf{b}_i$'s are linearly independent, the rank is exactly d. □

Bases and sets of generators are useful to represent lattices, and to perform computations. One will typically represent a lattice on a computer by some lattice basis, which can itself be represented by a matrix with real coefficients. In practice, one will usually restrict to integral lattices, so that the underlying matrices are integral matrices.

Any lattice basis of L must have exactly d elements. There always exist d linearly independent lattice vectors, however such vectors do not necessarily form a basis, as opposed to the case of vectors spaces. But the following theorem shows that one can always derive a lattice basis from such vectors:

Theorem 2.6 *Let L be a d-rank lattice of $\mathbb{R}^n$. Let $\mathbf{c}_1, \ldots, \mathbf{c}_d$ be linearly independent vectors of L. There exists a lower triangular matrix $(u_{i,j}) \in \mathcal{M}_d(\mathbb{R})$ such that $|u_{i,i}| \leq 1$ and the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_d$ defined as $\mathbf{b}_i = \sum_{j=1}^{i} u_{i,j}\mathbf{c}_j$ form a basis of L.*

Proof. We present two proofs.

The first proof is due to Siegel. Let $1 \leq i \leq d$. Consider the following set:

$$S_i = \left\{ x_i \in]0,1] : \exists x_1, \ldots, x_{i-1} \in \mathbb{R} \text{ such that } \sum_{j=1}^{i} x_j \mathbf{c}_j \in L \right\}.$$

This set is actually finite because $x_i \in S_i$ implies that $x_i\mathbf{c}_i + \sum_{j=1}^{i-1}(x_j - \lfloor x_j \rfloor)\mathbf{c}_j$ belongs to $L \cap B(0, \sum_{j=1}^{i} \|\mathbf{c}_j\|)$ which is finite. And S_i is not empty since it contains 1, therefore it has a smallest element which is strictly

positive, and which we denote by $u_{i,i} \in]0, 1]$. By definition, there exist $u_{i,1}, \ldots, u_{i,i-1} \in \mathbb{R}$ such that $\mathbf{b}_i = \sum_{j=1}^{i} u_{i,j}\mathbf{c}_j \in L$.

It remains to prove that the $\mathbf{b}_i$'s form a basis. Since $u_{i,i} > 0$, the $\mathbf{b}_i$'s are linearly independent. Now, let $\mathbf{y} \in L$. Since the $\mathbf{b}_i$'s are linearly independent, there exist $y_1, \ldots, y_n \in \mathbb{R}$ such that $\mathbf{y} = \sum_{i=1}^{d} y_i\mathbf{b}_i$. Define $\mathbf{x} = \sum_{i=1}^{d} x_i\mathbf{b}_i$ where $x_i = y_i - \lfloor y_i \rfloor$. We have $\mathbf{x} \in L$ and $0 \leq x_i < 1$. Suppose *ad absurdum* that not all the y_i's are integral: let k be the largest index such that $y_k \notin \mathbb{Z}$. Then $x_k > 0$ and $x_i = 0$ if $i > k$. Thus:

$$\mathbf{x} = u_{k,k}x_k\mathbf{c}_k + \sum_{j=1}^{k-1} u_{k,j}x_k\mathbf{c}_j + \sum_{i=1}^{k-1} x_i \sum_{j=1}^{i} u_{i,j}\mathbf{c}_j.$$

Since $0 < x_k < 1$, $0 < u_{k,k}x_k < u_{k,k}$ which contradicts the fact that $u_{k,k}$ is the smallest element of S_k.

We now give a second proof. For all $1 \leq i \leq d$, let $E_i = \mathrm{span}(c_1, \ldots, c_i)$ and $L_i = E_i \cap L$. Clearly, each E_i is an i-dimensional subspace, and each L_i is a lattice of rank i. By Lemma 2.3, L_1 is of the form $L_1 = \mathbb{Z}\mathbf{b}_1$ where $\|\mathbf{b}_1\| \leq \|\mathbf{c}_1\|$. We claim that if $(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})$ is a basis of L_{i-1} for some $i \geq 2$, then there exists $\mathbf{b}_i \in L_i$ such that $\mathbf{b}_i \notin L_{i-1}$ and $(\mathbf{b}_1, \ldots, \mathbf{b}_i)$ is a basis of L_i. Consider the orthogonal projection π_i over $E_{i-1}^{\perp}$. By Th. 2.4, $\pi_i(L_i)$ is a rank-one lattice, so by Lemma 2.3 it is of the form $\mathbb{Z}\pi_i(\mathbf{b}_i)$ for some $\mathbf{b}_i \in L_i$. We must have $\mathbf{b}_i \notin L_{i-1}$, otherwise $\pi_i(\mathbf{b}_i) = 0$. It remains to prove that $(\mathbf{b}_1, \ldots, \mathbf{b}_i)$ is a basis of L_i. They are clearly linearly independent. Let $\mathbf{v} \in L_i$. Then there exists $x_i \in \mathbb{Z}$ such that $\pi_i(\mathbf{v}) = x_i\pi_i(\mathbf{b}_i)$. Therefore $\pi_i(\mathbf{v} - x_i\mathbf{b}_i) = 0$, so $\mathbf{v} - x_i\mathbf{b}_i \in E_{i-1}$. And by definition, $\mathbf{v} - x_i\mathbf{b}_i \in L$, so $\mathbf{v} - x_i\mathbf{b}_i \in L \cap E_{i-1} = L_{i-1}$. Thus, there exist $x_1, \ldots, x_{i-1} \in \mathbb{Z}$ such that:

$$\mathbf{v} - x_i\mathbf{b}_i = \sum_{j=1}^{i-1} x_j\mathbf{b}_j,$$

and therefore

$$\mathbf{v} = \sum_{j=1}^{i} x_j\mathbf{b}_j.$$

Hence, we proved that $(\mathbf{b}_1, \ldots, \mathbf{b}_i)$ is a basis of L_i. By iterating the process, starting with $\mathbf{b}_1$, we showed the existence of $\mathbf{b}_2, \ldots, \mathbf{b}_d$ such that $(\mathbf{b}_1, \ldots, \mathbf{b}_i)$ is a basis of L_i for all i. Because $\pi_i(L_i)$ is a rank-one lattice generated by $\mathbf{b}_i \in L_i$, we have $\|\pi_i(\mathbf{b}_i)\| \leq \|\pi_i(\mathbf{c}_i)\|$, which implies that $|u_{i,i}| \leq 1$. □

This gives the unconditional existence of lattice bases:

Corollary 2.7 *Any lattice of $\mathbb{R}^n$ has at least one basis.*

Proof. We could have applied the previous result. Instead, we are going to do a proof by induction on the rank of the lattice. Lemma 2.3 allows to initialize the induction. Let L be a d-rank lattice. Let $\mathbf{v} \in L$ be non-zero. The intersection $\mathrm{span}(\mathbf{v}) \cap L$ is a rank-one lattice, so is of the form $\mathbb{Z}\mathbf{b_1}$ by Lemma 2.3. Let π be the orthogonal projection over $\mathbf{v}^\perp$. By Th. 2.4, $\pi(L)$ is a lattice of rank $d-1$, so by induction, we may assume it has a basis $(\pi(\mathbf{b}_2), \ldots, \pi(\mathbf{b}_d))$.

We claim that $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ is a basis of L. Clearly, the $\mathbf{b}_i$'s are linearly independent. Let $\mathbf{u} \in L$. There exist $x_2, \ldots, x_d \in \mathbb{Z}$ such that:

$$\pi(\mathbf{u}) = \sum_{j=2}^{d} x_j \pi(\mathbf{b}_j).$$

Thus, $\mathbf{u} - \sum_{j=2}^{d} x_j \mathbf{b}_j \in \mathrm{span}(\mathbf{v}) \cap L = \mathbb{Z}\mathbf{b}_1$, so there is $x_1 \in \mathbb{Z}$ such that

$$\mathbf{u} - \sum_{j=2}^{d} x_j \mathbf{b}_j = x_1 \mathbf{b}_1.$$

This shows that $\mathbf{u}$ is an integral linear combination of the $\mathbf{b}_i$'s. □

Thus, even if sets of the form $L(\mathbf{b}_1, \ldots, \mathbf{b}_m)$ may or may not be lattices, all lattices can be written as $L(\mathbf{b}_1, \ldots, \mathbf{b}_m)$ for some linearly independent $\mathbf{b}_i$'s. Corollary 2.7 together with Theorem 2.5 give an alternative definition of a lattice: a non-empty subset L of $\mathbb{R}^n$ is a lattice if only if there exist linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_d$ in $\mathbb{R}^n$ such that:

$$L = L(\mathbf{b}_1, \ldots, \mathbf{b}_d).$$

This characterization suggests that lattices are discrete analogues of vector spaces.

Lattice bases are characterized by the following elementary result, whose proof is omitted:

Theorem 2.8 *Let $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ be a basis of a lattice L in $\mathbb{R}^n$. Let $\mathbf{c}_1, \ldots, \mathbf{c}_d$ be vectors of L: there exists a $d \times d$ integral matrix $U = (u_{i,j})_{1 \le i,j \le d} \in \mathcal{M}_d(\mathbb{Z})$ such that $\mathbf{c_i} = \sum_{j=1}^{d} u_{i,j} \mathbf{b}_j$ for all $1 \le i \le d$. Then $(\mathbf{c}_1, \ldots, \mathbf{c}_d)$ is a basis of L if and only if the matrix U has determinant ± 1.*

As a result, as soon as the lattice dimension is ≥ 2, there are infinitely many lattice bases.

2.3 The covolume

Let $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$ and $(\mathbf{c}_1, \ldots, \mathbf{c}_d)$ be two bases of a lattice L in $\mathbb{R}^n$. By Theorem 2.8, there exists a $d \times d$ integral matrix $U = (u_{i,j})_{1 \leq i,j \leq d} \in \mathcal{M}_d(\mathbb{Z})$ of determinant ± 1 such that $\mathbf{c_i} = \sum_{j=1}^{d} u_{i,j}\mathbf{b}_j$ for all $1 \leq i \leq d$. It follows that the Gram determinant of those two bases are equal:

$$\Delta(\mathbf{b}_1, \ldots, \mathbf{b}_d) = \Delta(\mathbf{c}_1, \ldots, \mathbf{c}_d) > 0.$$

The *covolume* (or *determinant*) of the lattice L is defined as:

$$\mathrm{covol}(L) = \Delta(\mathbf{b}_1, \ldots, \mathbf{b}_d)^{1/2},$$

which is independent of the choice of lattice basis $(\mathbf{b}_1, \ldots, \mathbf{b}_d)$. For full-rank lattices, the covolume has the following elementary properties:

Lemma 2.9 *Let L be a full-rank lattice in $\mathbb{R}^n$. Then:*

1. *For any basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ of L, $\mathrm{covol}(L) = |\det(\mathbf{b}_1, \ldots, \mathbf{b}_n)|$.*
2. *For any $r > 0$, denote by $s_L(r)$ denote the number of $\mathbf{x} \in L$ such that $\|\mathbf{x}\| \leq r$. Let $v_n(r)$ be the volume of the ball of radius r in $\mathbb{R}^n$. Then:*

$$\lim_{r \to \infty} \frac{s_L(r)}{v_n(r)} = 1/\mathrm{covol}(L).$$

Proof. The first item follows from $\Delta(\mathbf{b}_1, \ldots, \mathbf{b}_d) = \det(BB^t) = (\det B)^2$ because B is square.

Let $B(r)$ be the (centered) open ball of radius r in $\mathbb{R}^n$. Let $\mathcal{P} = \{\sum_{i=1}^{n} x_i\mathbf{b}_i, -1/2 < x_i \leq 1/2\}$. Note that the sets $\mathbf{v} + \mathcal{P}$ form a partition of $\mathbb{R}^n$ as $\mathbf{v}$ runs over L, and each cell $\mathbf{v} + \mathcal{P}$ has measure $\mathrm{covol}(L)$. Let $\mathbf{v} \in B(r) \cap L$. Then:

$$\mathbf{v} + \mathcal{P} \subseteq B(r + \sum_{i=1}^{n} \|\mathbf{b}_i\|/2).$$

It follows that:

$$s_L(r)\mathrm{covol}(L) \leq \mathrm{vol}(B(r + \sum_{i=1}^{n} \|\mathbf{b}_i\|/2)) = v_n(r + \sum_{i=1}^{n} \|\mathbf{b}_i\|/2).$$

Hence:

$$s_L(r) \leq \frac{v_n(r + \sum_{i=1}^{n} \|\mathbf{b}_i\|/2)}{\mathrm{covol}(L)}.$$

On the other hand, if $r \geq \sum_{i=1}^{n} \|\mathbf{b}_i\|/2$:

$$B(r - \sum_{i=1}^{n} \|\mathbf{b}_i\|/2) \subseteq \cup_{\mathbf{v} \in B(r) \cap L} \mathbf{v} + \mathcal{P}.$$

Indeed, if $\mathbf{w} \in B(r - \sum_{i=1}^{n} \|\mathbf{b}_i\|/2)$ and $\mathbf{w} \in \mathbf{v} + \mathcal{P}$ then $\mathbf{v} \in \mathbf{w} - \mathcal{P}$ so $\|\mathbf{v}\| \leq r$. Thus:

$$s_L(r)\text{covol}(L) \geq \text{vol}(B(r - \sum_{i=1}^{n} \|\mathbf{b}_i\|/2)) = v_n(r - \sum_{i=1}^{n} \|\mathbf{b}_i\|/2).$$

We have therefore proved:

$$\frac{v_n(r - \sum_{i=1}^{n} \|\mathbf{b}_i\|/2)}{\text{covol}(L)} \leq s_L(r) \leq \frac{v_n(r + \sum_{i=1}^{n} \|\mathbf{b}_i\|/2)}{\text{covol}(L)},$$

and the result follows. □

The second statement of Lemma 2.9 says that, as the radius r grows to infinity, the number of lattice vectors inside the ball (centered at zero) of radius r is asymptotically equivalent to the ratio between the volume of the n-dimensional ball of radius r and the covolume of the lattice. This suggests the following heuristic, known as the Gaussian Heuristic: Let L be a full-rank lattice in $\mathbb{R}^n$, and C be a measurable subset of $\mathbb{R}^n$. The *Gaussian Heuristic* "predicts" that the number of points of $L \cap C$ is roughly $\text{vol}(C)/\text{covol}(L)$. We stress that this is only a heuristic: there are cases where the heuristic is proved to hold, but there are also cases where the heuristic is proved to be incorrect.

Given a lattice L, how does one compute the covolume of L? If an explicit basis of L is known, this amounts to computing a determinant: for instance, the volume of the hypercubic lattice $\mathbb{Z}^n$ is clearly equal to one. But if no explicit basis is known, there is sometimes another way, due to the following elementary result: if L_1 and L_2 are two lattices of $\mathbb{R}^n$ with the same dimension such that $L_1 \subseteq L_2$, then L_2/L_1 is a finite group of order denoted by $[L_2 : L_1]$ which satisfies

$$\text{covol}(L_1) = \text{covol}(L_2) \times [L_2 : L_1].$$

As an illustration, consider n integers $a_1, \ldots, a_n$, together with a modulus M. We have seen in Section 2 that the set L of all $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ such that $\sum_{i=1}^{n} a_i x_i \equiv 0 \pmod{M}$ is a lattice in $\mathbb{Z}^n$ because it is a subgroup of $\mathbb{Z}^n$. But there seems to be no trivial basis of L. However, note that $L \subseteq \mathbb{Z}^n$

and that the dimension of L is n because L contains all the vectors of the canonical basis of $\mathbb{R}^n$ multiplied by M. It follows that:

$$\text{covol}(L) = [\mathbb{Z}^n : L].$$

Furthermore, the definition of L clearly implies that:

$$[\mathbb{Z}^n : L] = M/\gcd(M, a_1, a_2, \ldots, a_n).$$

Hence:

$$\text{covol}(L) = \frac{M}{\gcd(M, a_1, a_2, \ldots, a_n)}.$$

2.4 Minkowski's successive minima and lattice reduction

A fundamental result of linear algebra states that any finite-dimensional vector space has a basis. We earlier established the analogue result for lattices: any lattice has a basis. In the same vein, a fundamental result of bilinear algebra states that any finite-dimensional Euclidean space has an orthonormal basis, that is, a basis consisting of unit vectors which are pairwise orthogonal. A natural question is to ask whether lattices also have orthonormal bases, or at least, orthogonal bases. Unfortunately, it is not difficult to see that even in dimension two, a lattice may not have an orthogonal basis. Informally, the goal of lattice reduction is to circumvent this problem: more precisely, the theory of lattice reduction shows that in any lattice, there is always a basis which is not that far from being orthogonal. Defining precisely what is meant exactly by not being far from being orthogonal is tricky, so for now, let us just say that such a basis should consist of reasonably short lattice vectors, which implies that geometrically, such vectors are not far from being orthogonal to each other.

In order to explain what is a reduced basis, we need to define what is meant by short lattice vectors. Let L be a lattice of dimension ≥ 1 in $\mathbb{R}^n$. There exists a non-zero vector $\mathbf{u} \in L$. Consider the closed hyperball B of radius $\|\mathbf{u}\|$, centered at zero. Then $L \cap B$ is finite and contains $\mathbf{u}$, so it must have a shortest non-zero vector. The Euclidean norm of that shortest non-zero vector is called the *first minimum* of L, and is denoted by $\lambda_1(L) > 0$ or $\|L\|$. By definition, any non-zero vector $\mathbf{v}$ of L satisfies: $\|\mathbf{v}\| \geq \lambda_1(L)$. And there exists $\mathbf{w} \in L$ such that $\|\mathbf{w}\| = \lambda_1(L)$: any such $\mathbf{w}$ is called a shortest vector of L, and it is not unique since $-\mathbf{w}$ would also be a shortest vector. The *kissing number* of L is the number of shortest vectors in L: it is upper bounded by some exponential function of the lattice dimension (see [2]).

If $\mathbf{w}$ is a shortest vector of L, then so is $-\mathbf{w}$. Thus, one must be careful when defining the *second-to-shortest* vector of a lattice. To circumvent this problem, Minkowski [6] defined the other minima as follows. For all $1 \leq i \leq \dim(L)$, the i-th *minimum* $\lambda_i(L)$ is defined as the minimum of $\max_{1\leq j\leq i} \|\mathbf{v}_j\|$ over all i linearly independent lattice vectors $\mathbf{v}_1, \ldots, \mathbf{v}_i \in L$. Clearly, the minima are increasing: $\lambda_1(L) \leq \lambda_2(L) \leq \cdots \leq \lambda_d(L)$. And it is possible to reach them simultaneously:

Lemma 2.10 *Let L be a d-rank lattice in $\mathbb{R}^n$. There exist linearly independent lattice vectors $\mathbf{v}_1, \ldots, \mathbf{v}_d$ such that $\|\mathbf{v}_i\| = \lambda_i(L)$ for all $1 \leq i \leq d$.*

Proof. Assume that for some $k < d$, $\mathbf{v}_1, \ldots, v_k \in L$ are linearly independent and such that : $\mathbf{v}_i = \lambda_i(L)$ for $1 \leq i \leq k$. Clearly, this holds for $k = 1$. Let E be the k-dimensional subspace spanned by$\mathbf{v}_1, \ldots, v_k$. Let $\mathbf{v}_{k+1} \in L$ such that $L \notin E$ and has minimal norm among such vectors. We claim that $\|\mathbf{v}_{k+1}\| = \lambda_{k+1}(L)$.

Since $\mathbf{v}_1, \ldots, v_{k+1}$ are linearly independent, we know that $\|\mathbf{v}_{k+1}\| \geq \lambda_{k+1}(L)$.

On the other hand, there exist linearly independent lattice vectors $\mathbf{w}_1, \ldots, \mathbf{w}_{k+1}$ inside the ball of radius $\lambda_{k+1}(L)$. Note that at least one $\mathbf{w}_j$ cannot belong to E, otherwise the rank of $\mathbf{w}_1, \ldots, \mathbf{w}_{k+1}$ would be $\leq k$. Therefore $\|\mathbf{v}_{k+1}\| \leq \|\mathbf{w}_{k+1}\| \leq \lambda_{k+1}(L)$.

So $\|\mathbf{v}_{k+1}\| = \lambda_{k+1}(L)$. We iterate until $k + 1 = d$. □

However, surprisingly, as soon as $\text{rank}(L) \geq 4$, such vectors do not necessarily form a lattice basis. The canonical example is the 4-rank lattice L defined as the set of all $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ such that $\sum_{i=1}^4 x_i$ is even. It is not difficult to see that $\dim(L) = 4$ and that all the minima of L are equal to $\sqrt{2}$. Furthermore, it can be checked that the following row vectors form a basis of L:

$$\begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

The basis proves in particular that $\text{covol}(L) = 2$. However, the following row vectors are linearly independent lattice vectors which also reach all the minima:

$$\begin{pmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

But they do not form a basis, since their determinant is equal to 4: another reason is that for all such vectors, the sum of the first two coordinates is even, and that property also holds for any integral linear combination of those vectors, but clearly not for all vectors of the lattice L. More precisely, the sublattice spanned by those four row vectors has index two in the lattice L.

Nevertheless, in the lattice L, there still exists at least one basis which reaches all the minima simultaneously, and we already gave one such basis. This also holds for any lattice of rank ≤ 4, but it is no longer true in dimension ≥ 5, as was first noticed by Korkine and Zolotarev in the 19th century, in the language of quadratic forms. More precisely, it can easily be checked that the lattice spanned by the rows of the following matrix

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

has no basis reaching all the minima (which are all equal to two).

2.5 Hermite's constant and Minkowski's theorems

Now that successive minima have been defined, it is natural to ask how large those minima can be. Hermite [3] was the first to prove that the quantity $\lambda_1(L)/\mathrm{covol}(L)^{1/d}$ could be upper bounded over all d-rank lattices L. The supremum of $\lambda_1(L)^2/\mathrm{covol}(L)^{2/d}$ over all d-rank lattices L is denoted by γ_d, and called Hermite's constant of dimension d, because Hermite was the first to establish its existence in the language of quadratic forms. The use of quadratic forms explains why Hermite's constant refers to $\max_L \lambda_1(L)^2/\mathrm{covol}(L)^{2/d}$ and not to $\max_L \lambda_1(L)/\mathrm{covol}(L)^{1/d}$. Clearly, γ_d could also be defined as the supremum of $\lambda_1(L)^2$ over all d-rank lattices L of unit volume.

It is known that γ_d is reached, that is: for all $d \geq 1$, there is a d-rank lattice L such that $\gamma_d = \lambda_1(L)^2/\mathrm{covol}(L)^{2/d}$, and any such lattice is called *critical*. But finding the exact value of γ_d is a very difficult problem, which has been central in Minkowski's geometry of numbers. The exact value of γ_d is known only for $1 \leq d \leq 8$ and for $d = 24$ (see [1]): the values are summarized in the following table.

d	2	3	4	5	6	7	8	24
γ_d	$2/\sqrt{3}$	$2^{1/3}$	$\sqrt{2}$	$8^{1/5}$	$(64/3)^{1/6}$	$64^{1/7}$	2	4
Approximation	1.1547	1.2599	1.4142	1.5157	1.6654	1.8114	2	4

Furthermore, the list of all critical lattices (up to scaling and isometry) is known for each of those dimensions.

However, rather tight asymptotical bounds are known for Hermite's constant. More precisely, we have:

$$\frac{d}{2\pi e} + \frac{\log(\pi d)}{2\pi e} + o(1) \leq \gamma_d \leq \frac{1.744d}{2\pi e}(1 + o(1)).$$

For more information on the proof of those bounds: see [5, Chapter II] for the lower bound (which comes from the Minkowski-Hlawka theorem), and [2, Chapter 9] for the upper bound. Thus, γ_d is essentially linear in d. It is known that $\gamma_d^d \in \mathbb{Q}$ (because there is always an integral critical lattice), but it is unknown if γ_d is an increasing sequence.

Hermite's historical upper bound [3] on his constant was exponential in the dimension:

$$\gamma_d \leq (4/3)^{(d-1)/2}.$$

The first linear upper bound on Hermite's constant is due to Minkowski, who viewed it as a consequence of his Convex Body Theorem:

Theorem 2.11 (Minkowski's Convex Body Theorem) *Let L be a full-rank lattice of $\mathbb{R}^n$. Let C be a measurable subset of $\mathbb{R}^n$, convex, symmetric with respect to 0, and of measure $> 2^n \mathrm{covol}(L)$. Then C contains at least a non-zero point of L.*

This theorem is a direct application of the following elementary lemma (see [8]), which can be viewed as a generalization of the pigeon-hole principle:

Lemma 2.12 (Blichfeldt) *Let L be a full-rank lattice in $\mathbb{R}^n$, and F be a measurable subset of $\mathbb{R}^n$ with measure $> \mathrm{covol}(L)$. Then F contains at least two distinct vectors whose difference is in L.*

Indeed, we may consider $F = \frac{1}{2}C$, and the assumption in Theorem 2.11. implies that the measure of F is $> \mathrm{covol}(L)$. From Blichfeldt's lemma, it follows that there exist $\mathbf{x}$ and $\mathbf{y}$ in F such that $\mathbf{x} - \mathbf{y} \in L \setminus \{0\}$. But

$$\mathbf{x} - \mathbf{y} = \frac{1}{2}(2\mathbf{x} - 2\mathbf{y})$$

which belongs to C by convexity, and symmetry with respect to 0. Hence: $\mathbf{x} - \mathbf{y} \in C \cap (L \setminus \{0\})$, which completes the proof of Theorem 2.11.

One notices that the bound on the volumes in Theorem 2.11 is the best possible, by considering

$$C = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \ : |x_i| < 1 \right\},$$

where the $\mathbf{b}_i$'s form an arbitrary basis of the lattice. Indeed, in this case, the measure of C is exactly $2^n \mathrm{covol}(L)$, but by definition of C, no non-zero vector of L belongs to C.

In Theorem 2.11, the condition on the measure of C is a strict inequality, but it is not difficult to show that the strict inequality can be relaxed to an inequality $\geq 2^n \mathrm{covol}(L)$ if C is further assumed to be compact. By choosing for C a closed hyperball of sufficiently large radius (so that the volume inequality is satisfied), one obtains that any d-rank lattice L of $\mathbb{R}^n$ contains a non-zero $\mathbf{x}$ such that

$$\|\mathbf{x}\| \leq 2 \left(\frac{\mathrm{covol}(L)}{v_d} \right)^{\frac{1}{d}},$$

where v_d denotes the volume of the closed unitary hyperball of $\mathbb{R}^d$. This upper bound was historically obtained by Minkowski using a packing argument. Put a hyperball of radius $\lambda_1(L)/2$ at every lattice point: this is a packing. On the other hand, $\mathbb{R}^d$ is covered by the sets $\mathbf{v} + \mathcal{P}$ where $\mathcal{P}$ is a basis parallelepiped like in the proof of Lemma 2.9. It follows that the volume of the hyperball of radius $\lambda_1(L)/2$ must be less than that of $\mathcal{P}$, which is $\mathrm{covol}(L)$.

Using the well-known formula for $v_d = \pi^{d/2}/\Gamma(1+d/2)$ where Γ is Euler's gamma function, one can derive a linear bound on Hermite's constant, for instance:

$$\forall d,\ \gamma_d \leq 1 + \frac{d}{4}.$$

One can obtain an analogous result for the max-norm:

Theorem 2.13 *Let L be a d-rank lattice. Then there exists a non-zero $\mathbf{x}$ in L such that:*

$$\|\mathbf{x}\|_\infty \leq \mathrm{covol}(L)^{1/d}.$$

Notice that this bound is reached by $L = \mathbb{Z}^d$.

Now that we know how to bound the first minimum, it is natural to ask if a similar bound can be obtained for the other minima. Unfortunately, one cannot hope to upper bound separately the other minima, because the successive minima could be unbalanced. For instance, consider the rectangular 2-rank lattice L spanned by the following row matrix:

$$\begin{pmatrix} \varepsilon & 0 \\ 0 & 1/\varepsilon \end{pmatrix},$$

where $\varepsilon > 0$ is small. The volume of L is one, and by definition of L, it is clear that $\lambda_1(L) = \varepsilon$ and $\lambda_2(L) = 1/\varepsilon$ if $\varepsilon \leq 1$. Here, $\lambda_2(L)$ can be arbitrarily

large compared to the lattice volume, while $\lambda_1(L)$ can be arbitrarily small compared to the upper bound given by Hermite's constant.

However, it is always possible to upper bound the geometric mean of the first consecutive minima, as summarized by the following theorem (for an elementary proof, see [8, 4]):

Theorem 2.14 (Minkowski's Second Theorem) *Let L be a d-rank lattice of $\mathbb{R}^n$. Then for any integer r such that $1 \leq r \leq d$:*

$$\left(\prod_{i=1}^{r} \lambda_i(L)\right)^{1/r} \leq \sqrt{\gamma_d}\mathrm{covol}(L)^{1/d}.$$

2.6 The covering radius

Let L be a d-rank lattice in $\mathbb{R}^n$. The covering radius $\mu(L)$ is defined as the maximal distance to the lattice:

$$\mu(L) = \sup_{\mathbf{t} \in \mathrm{span}(L)} \min_{\mathbf{v} \in L} \|\mathbf{t} - \mathbf{v}\|.$$

For instance, $\mu(\mathbb{Z}^n) = \sqrt{n/4} = \sqrt{n}/2$ which is much larger than $\lambda_1(L)/2 = 1/2$. The covering radius is the minimal radius of the ball $\mathcal{B}$ such that the balls $\mathbf{v} + \mathcal{B}$ cover $\mathrm{span}(L)$ when $\mathbf{v}$ runs over L. One has the following elementary bounds:

Theorem 2.15 *Let L be a d-rank lattice in $\mathbb{R}^n$. Then:*

$$\frac{\lambda_d(L)}{2} \leq \mu(L) \leq \frac{\sqrt{\sum_{i=1}^{d} \lambda_i^2(L)}}{2}.$$

2.7 Random Lattices

The upper bound on the first minimum derived from Hermite's constant is only tight for critical lattices, which are very special lattices. One might wonder what happens for more general lattices, say random lattices. But what is a random lattice? Surprisingly, from a mathematical point of view, there is a natural (albeit technically involved) notion of random lattice, which follows from a measure on full-rank lattices with determinant 1 introduced by Siegel [7] back in 1945. This measure is derived from Haar measures of classical groups. No formal definition of random lattices will be given here: the interested reader is referred to the theses [**?**, **?**]. Instead, we

list a few important properties of random lattices, to give more intuition. We saw in Section 2.5 that an n-rank lattice L satisfies:

$$\lambda_1(L) \leq \sqrt{\gamma_n}\text{covol}(L)^{1/n} \leq \sqrt{1+n/4}\text{covol}(L)^{1/n}. \quad (1)$$

As n grows to infinity, a random n-rank lattice L satisfies with overwhelming probability:

$$\lambda_1(L) \approx \sqrt{\frac{n}{2\pi e}}\text{covol}(L)^{1/n}.$$

This also holds for the few first minima, but in general we only know with overwhelming probability:

$$\lambda_i(L) = O(\sqrt{n})\text{covol}(L)^{1/n}.$$

In particular, the bound on the first minimum derived from Hermite's constant is not that far from being tight in the random case: the ratio between the two upper bounds is bounded independently of the dimension. Thus, even though it is easy to construct lattices for which the first minimum is arbitrarily small compared to Hermite's bound, such lattices are far from being random: the first minimum of random lattices is almost as large as the one of critical lattices.

As n grows to infinity, a random n-rank lattice L satisfies with overwhelming probability:

$$\mu(L) \approx \sqrt{\frac{n}{2\pi e}}\text{covol}(L)^{1/n}.$$

Theorem 2.6, together with the bounds on the minima, allow to prove that, asymptotically, in a random n-rank lattice L, there exists with overwhelming probability a lattice basis $(\mathbf{b}_1, \ldots, \mathbf{b}_n)$ such that:

$$\forall\ 1 \leq i \leq n, \|\mathbf{b}_i\| = O(n)\text{covol}(L)^{1/n}.$$

The previous properties are useful to distinguish specific lattices from random lattices. For instance, in cryptography, one often encounters lattices for which the first minimum is provably much smaller than Hermite's bound (1), so such lattices cannot be random, and they might have exceptional properties which can be exploited. And when a lattice is very far from being random, certain computational problems which are hard in the general case may become easy.

References

[1] H. Cohn and A. Kumar. The densest lattice in twenty-four dimensions. *Electron. Res. Announc. Amer. Math. Soc.*, 10:58–67 (electronic), 2004.

[2] J.H. Conway and N.J.A. Sloane. *Sphere Packings, Lattices and Groups.* Springer-Verlag, 1998. Third edition.

[3] C. Hermite. Extraits de lettres de M. Hermite à M. Jacobi sur différents objets de la théorie des nombres, deuxième lettre. *J. Reine Angew. Math.*, 40:279–290, 1850. Also available in the first volume of Hermite's complete works, published by Gauthier-Villars.

[4] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective.* Kluwer Academic Publishers, 2002.

[5] J. Milnor and D. Husemoller. *Symmetric Bilinear Forms.* Springer-Verlag, 1973.

[6] H. Minkowski. *Geometrie der Zahlen.* Teubner-Verlag, Leipzig, 1896.

[7] C. L. Siegel. A mean value theorem in geometry of numbers. *Annals of Mathematics*, 46(2):340–347, 1945.

[8] C. L. Siegel. *Lectures on the Geometry of Numbers.* Springer-Verlag, 1989.