LECTURE 1:
Lattice Theory

H. Xiao NOVEMBER 2012

1.1 Lattice

Geometrically, a lattice can be defined as the set of intersection point of an infinite, regular, but not necessarily orthogonal n-dimensional grid. For example, the set of integer vectors $\mathbb{Z}^n$ is a lattice. In theoretical computer science, lattices are usually represented by a generating basis.

Definition 1.1 (Lattice) *Given m linearly independent vectors $b_1, b_2, \ldots, b_m \in \mathbb{R}^n$, the lattice generated by them is defined as $L(b_1, b_2, \ldots, b_m) = \{\sum x_i b_i | x_i \in \mathbb{Z}\}$. We refer to $b_1, b_2, \ldots, b_m$ as a basis of the lattice. We say that the rank of the lattice is m and its dimension is n. If $m = n$, the lattice is called a full-rank lattice. A lattice is usually denoted by Λ.*

Alternative Definition of Lattices

Definition 1.2 (Lattice) *A lattice is a discrete additive subgroup of $\mathbb{R}^n$ generated by all the integer combinations of some basis.*

Notice the similarity between the definition of a lattice and the definition of vector space generated by $b_1, b_2, \ldots, b_n$.

$$\text{span}\{b_1, b_2, \ldots, b_m\} = \{\sum_{i=1}^{m} x_i b_i | x_i \in \mathbb{R}\}$$

One difference is that in a vector space you can combine the basis vectors with arbitrary real coefficients, while in a lattice only integer coefficients are allowed, resulting in a discrete set of points.

Another difference between lattices and vector spaces is that vector spaces always admit an orthogonal basis. This is not true for lattices.

Given a lattice Λ, there are infinitely many different choices of lattice basis. Let B be a nonsingular matrix with one basis of Λ as the columns of it. One can obtain another basis C by a unimodular transformation(multiplying the basis vectors by a square matrix with integer entries and determinant plus or minus one.), then $|\det B| = |\det C|$. So this number is independent of the choice of the basis, and is called the *determinant* of Λ, denoted by $\det \Lambda$. It is equal to the volume of the parallelepiped $\{x_1 b_1 + \cdots + x_n b_n | 0 \leq x_i < 1 \text{ for } i = 1, \ldots, n\}$

Vector space

Definition 1.3 (Fundamental Parallelepiped) *Given m linearly independent vectors $b_1, b_2, \ldots, b_m \in \mathbb{R}^n$, their fundamental parallelepiped is defined as*

$$\{\sum_{i=1}^{m} x_i b_i | x_i \in \mathbb{R}, 0 \leq x_i < 1\}$$

vol= $|\det B|$

Theorem 1.4 (Hadamard inequality) $\det \Lambda \leq \|b_1\| \|b_2\| \cdots \|b_m\|$, *where $\|\cdot\|$ denotes Euclidean norm ($\|x\| = \sqrt{x^T x}$).*

1.2 Gram-Schmidt

Projection

1.3 LLL lattice basis reduction algorithm

Motivation

1.4 Applications

References

[CW87] D. Coppersmith and S. Winograd, "Matrix multiplication via arithmetic progressions," *Proceedings of the 19th ACM Symposium on Theory of Computing*, 1987, pp. 1–6.