LECTURE 5:
Integer lattices

Polyhedral Theory April 2013

Before we proceed to the study of integer polyhedra, we need study an important ingredient: integer lattices. Sometimes it is called geometry of numbers.

5.1 Lattices

5.1.1 Definition

A subset Λ of $\mathbb{R}^n$ is called an (additive) group if

(i) $0 \in \Lambda$;

(ii) if x, $y \in \Lambda$, then $x + y \in \Lambda$ and $-x \in \Lambda$.

The group is said to be generated by $B = [b_1, \ldots, b_k] \in \mathbb{R}^{n \times k}$ is

$$\Lambda = \{\sum_{i=1}^{k} \lambda_i b_i \mid \lambda_1, \ldots, \lambda_k \in \mathbb{Z}\} = \{Bx \mid x \in \mathbb{Z}^n\},$$

and denoted by $\Lambda(B)$. The group is called a ***lattice*** if $b_1, \ldots, b_k$ are linearly independent. B is called a ***basis*** of $\Lambda(B)$. In particular, $\mathbb{Z}^n$ is the special lattice generated by standard unit vectors, i.e., $\mathbb{Z}^n = \Lambda(e_1, \ldots, e_n)$.

5.1.2 Multiple bases

The interesting thing is that $\mathbb{Z}^n$ can also be generated by vectors $e_1 + e_2, e_3, \ldots, e_n$ (since the sum $\lambda_1 e_1 + \lambda_2 e_2$, where $\lambda_1, \lambda_2 \in \mathbb{Z}$, can be written as $\lambda_1(e_1 + e_2) + (\lambda_2 - \lambda_2)e_2$, and the coefficients remain integral; for the converse, we rewrite $\lambda_1(e_1 + e_2) + \lambda_2 e_2$ as $\lambda_1 e_1 + (\lambda_1 + \lambda_2)e_2$). Thus the basis of a lattice is not unique. Furthermore, it turns out that all the bases of a given lattice are unimodular equivalent.

5.2 Unimodular matrices

A nonsingular integral matrix U is ***unimodular*** if $\det(U) = \pm 1$.

Following are some useful facts about unimodular matrices.

Proposition 5.1 *Let U be a unimodular matrix. Then*

(a) the inverse U^{-1} is also unimodular;

(b) x is an integral vector if and only if Ux is an integral vector.

Proof. Since U is integral, all cofactors of U are integers. It follows that all entries of U^{-1} are also integers, as $|\det(U)| = 1$. Finally, $UU^{-1} = I$ implies $\det(U)\det(U^{-1}) = 1$, hence $|\det(U^{-1})| = 1$. This proves part (a). It is obvious that if x is an integral vector, then Ux is also an integral vector. The converse follows from part (a), since $x = U^{-1}(Ux)$. □

Now we are ready to establish the connection between different bases of the same lattice.

Theorem 5.2 *Let B and B' be nonsingular matrices. Then columns of B and those of B' generate the same lattice, i.e., $\Lambda(B) = \Lambda(B')$ if and only if $B' = BU$ for some unimodular matrix U (i.e., $B^{-1}B'$ is unimodular).*

Proof. cf Schrijver corollary 4.3a or Intger points in polyhedra, Shmonin, Lemma 2. □

(REMOVE THE FOLLOWING AS IN THE THEOREM ABOVE, WE ASUME THAT THE MATRIX IS UNIMODULAR, WHICH MEANS THAT ITS A SQUARE MATRIX. SO THE GROUP GENERATED BY B MUST BE A LATTICE! BUT WE ACTUALLY HAVE A MORE COMMON THEOREM CF. "LATTICES AND HERMITE NORMAL FORM" BY GENNADY SHMONIN. Be cautious that in the follow theorem, we condier general form matrices of full row rank, where do not claim that the set $\Lambda(B)$ is a lattice - $\Lambda(B)$ is just the group generated by the columns of B, where the vectors are not necessarily linearly independent.)

5.3 Hermit normal form

The following operations on a matrix are called ***elementary column operations***:

(1) exchanging two columns;

(2) multiplying a column by -1;

(3) adding an integral multiply of one column to another column.

By elementary linear algebra, it is easy to see that each elementary column operation can be achieved by multiplying a unimodular matrix from right(is actually a particular unimodular transformation). (From elementary linear algebra, it's trivial. But here we still explain it in details.) Now we explicitly specify appropriate unimodular matrices for each of the elementary column operations. ...

We say a matrix B of full row rank is in ***Hermite normal form*** if it has the form $B = [H\ 0]$, where H is a nonsingular, lower triangular, nonnegative matrix, in which each row has a unique maximum entry, which is located on the main diagonal of H.

Since the elementary column operations are actually unimodular transformations of a matrix, the group generated by the columns of the matrix is invariant under these operations; in other words, if we had transformed the matrix into a matrix in Hermite normal form, we also proved that this group can be generated by linearly independent vectors, and therefore, is a lattice. So we have the following theorem.

Theorem 5.3 (Existence of HNF) *Each rational matrix of full row rank can be brought into Hermite normal form by a series of elementary column operation.*

Proof. □

Due to unimodularity of elementary column operations, we can derive the following corollary.

Corollary 5.4 *Let B be a rational matrix of full row rank. Then there is a unimodular matrix U such that the matrix BU is in Hermite normal form.*

The corollary above implies that *every rational lattice has a basis in Hermite normal form.* In the following theorem, we shall see that any rational matrix of full row rank has a unique Hermite normal form.

Theorem 5.5 (Uniqueness of HNF) *Let B be a rational matrix of full row rank. Then B has a unique Hermite normal form $[H\ 0]$.*

Proof. cf thm 1 in ”Hermite normal form: Computation and applications” by Gennady Shmonin. □

5.4 Linear Diophantine equations

Linear Diophantine equations are...

Hermite normal form turns out to be very useful for solving systems of linear Diophantine equations.

Let A be a mtrix and b a vector, and consider the problem of finding an integral vector x satisfying system $Ax = b$. In fact, we may assume that A has full row rank; otherwise, we may remove redundant equations from the system. Yet, we assume all input data to be rational. We can find a unimodular matrix U such that $[H|0] = AU$ is a matrix in Hermite normal form. Now we can apply a standard trick to transform a system of linear equations into a more suitable from: $Ax = b$ is equivalent to $(AU)(U^{-1}x) = b$, and therefore, $[H|0]z = b$, where $Z = U^{-1}x$ is integral if and only if x is integral. We can observe that the components corresponding to zeros in Hermite normal form may take arbitrary values, while feasibility of the system $[H|0]z = b$, and therefore, of $Ax = b$, depends only on whether the vector $H^{-1}b$ is integral. Now we can derive the following condition for a system of linear Diophantine equations to have a solution.

Theorem 5.6 (Integer analogue of Farkas' Lemma) *Let A be a rational matrix and let b be a rational column vector. Then the system $Ax = b$ has an integral solution x, if and only if $y^T b$ is an integer for each rational row vector y for which $y^T A$ is integral.*

5.5 Polynomial algorithm for Hermite normal form

5.6 Algorithm for linear Diophantine equations

References

[CW87] Gennady Shmonin, “Lattices and Hermite normal form” and “Hermite normal form: Computation and applications”, *Integer Points in Polyhedra.*