LECTURE 6:
Integer polyhedra

Polyhedral Theory April 2013

6.1 Hilbert basis

The Hermite normal form $[B\ \mathbf{0}]$ of a rational matrix $A \in \mathbb{Q}^{m\times n}$ can be considered as a minimal generating set of the lattice $\Lambda(A)$ generated by A.

In this section, we are going to deal with the lattice points in a polyhedral cone. Is there any similar basis for the integer points in a polyhedral cone C generated by rational vectors $\{a_1, \ldots, a_n\}$? A finite set of vectors $\{a_1, \ldots, a_t\}$ is a ***Hilbert basis*** if each integral vector b in $\text{cone}\{a_1, \ldots, a_t\}$ is a non-negative integral combination of $a_1, \ldots, a_t$. Especially, we are interested in ***integral Hilbert bases***, which are Hilbert bases consisting of integral vectors only.

Theorem 6.1 *Each rational polyhedral cone C is generated by an integral Hilbert basis. Furthermore, if C is pointed, the minimal integral Hilbert basis is unique (minimal relative to set inclusion).*

Proof. Without loss of generality, let C be generated by integral vectors $a_1, \ldots, a_s$, i.e., $C = \text{cone}\{a_1, \ldots, a_s\}$. We claim that the finite set $H = \{h_1, \ldots, h_t\}$ of integral vectors contained in the zonotope

$$Z := \{x \in \mathbb{R}^n \mid x = \sum_{i=1}^{t} \lambda_i a_i, 0 \leqslant \lambda_i \leqslant 1 \text{ for } i = 1, \ldots, t\}$$

is a Hilbert basis. Following is an example with $n = 2$, $s = 2$ and $t = 8$.

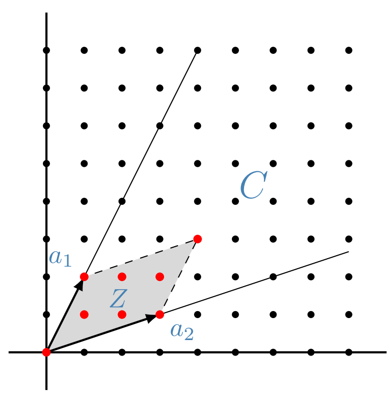

Figure 6.1: The cone C and the polytope Z

Clearly, H generates C, as $a_1, \ldots, a_s$ are contained in H. To see that vectors in H form a Hilbert basis, let $p \in C \cap \mathbb{Z}^n$. Then, we have

$$p = \sum_{i=1}^{s} \lambda_i a_i, \lambda_i \geqslant 0, i = 1, \ldots, t,$$

for some λ_i (not necessarily integer). Furthermore, we have

$$p - \sum_{i=1}^{s} \lfloor \lambda_i \rfloor a_i = \sum_{i=1}^{s} (\lambda_i - \lfloor \lambda_i \rfloor) a_i.$$

Then the RHS vector above occurs in H, as the LHS is integral, and the RHS belongs to Z. Since $a_1, \dots, a_s$ are also contained in H, it follows that (16) decompose p into a non-negative integral combination of H. So vectors in H form a Hilbert basis.

Next, suppose C is pointed.

□

6.2 Integer hulls and integer polyhedra

The ***integer hull*** P_I of P is defined by:

$$P_I := \text{conv}(P \cap \mathbb{Z}^n). \tag{6.1}$$

So the integer hull P_I of P is the convex hull of the integral vectors in P. A rational polyhedron P is an ***integer polyhedron*** if $P = P_I$. Clearly, for any rational polyhedral cone C, $C = C_I$, as C is generated by rational, and hence integral, vectors. Therefore, a rational polyhedral cone is always an integer polyhedron.

Theorem 6.2 *The integer hull P_I of a rational polyhedron P is a polyhedron. If $P_I \neq \emptyset$, then $rec(P) = rec(P_I)$.*

Proof. (1) If P is a polytope(thus bounded), then $|P \cap \mathbb{Z}^n|$ is finite, so P_I is a polytope.
(2) If P is a polyhedral cone, then $P = P_I$.
(3) Assume $P = Q + C$, where Q is polytope and C is the characteristic cone of P. Let C be generated by $a_1, \dots, a_s \in \mathbb{Z}^n$ and let Z be the polytope (parallelepiped, strictly speaking zonotope)

$$Z := \{\sum_{i=1}^{s} \lambda_i a_i \mid 0 \leqslant \lambda_i \leqslant 1 \text{ for } i = 1, \dots, s\}. \tag{6.2}$$

We show that

$$P_I = (Q + Z)_I + C, \tag{6.3}$$

which implies the theorem, as $Q + Z$ is a polytope, and hence $(Q + Z)_I$ is a polytope.

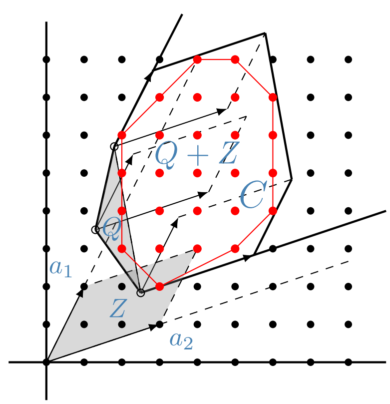

Figure 6.2: The structure of integer hull

To see $(Q + Z)_I + C \subseteq P_I$, observe

$$(Q + Z)_I + C \subseteq P_I + C = P_I + C_I \subseteq (P + C)_I = P_I. \tag{6.4}$$

The first inclusion comes from the fact that $Q + Z \subseteq P$. Since each integral vector in $Q + Z$ is also a integral vector in P, therefore $(Q + Z)_I \subseteq P_I$. As to the second inclusion, since the sum of any two integral vectors from P and C is still a integral vector in $P + C$, i.e., $(P \cap \mathbb{Z}^n) + (C \cap \mathbb{Z}^n) \subseteq (P + C) \cap \mathbb{Z}^n$, together with the property of Minkowski sum $P_I + C_I = \text{conv}\{P \cap \mathbb{Z}^n + C \cap \mathbb{Z}^n\}$, the second inclusion follows.

For the reverse inclusion, let $p \in P \cap \mathbb{Z}^n$. Then $p = q + c$ for some $q \in Q$ and $c \in C$. Note that $c = \sum_i \lambda_i a_i = \sum_i \lfloor \lambda_i \rfloor a_i + \sum_I (\lambda_i - \lfloor \lambda_i \rfloor) a_i$, where the first term is denoted by c' and the second by z. Clearly, $c' \in C \cap \mathbb{Z}^n$ and $z \in Z$. It follows that $p = (q+z) + c'$ and $q + z \in (Q+Z)_I$(as $q + z = p - c'$ and p and c' are integral). Since $c' \in C$, we have $p \in (Q+Z)_I + C$.

If $P_I \neq \emptyset$, then the characteristic cone of P_I is uniquely defined by the decomposition in (6.3). Hence, $\operatorname{rec}(P) = C = \operatorname{rec}(P_I)$. □

So in principle, an ILP is just a LP over the integer hull of a polyhedron.

Proposition 6.3 *Let P be a rational polyhedron. Then the following are equivalent.*

(1) $P = P_I$, *i.e.,* P *is the convex hull of the integral vectors in* P*,*

(2) each face of P *contains integral points,*

(3) each minimal face of P *contains integral points,*

(4) $\max\{c^T x \mid x \in P\}$ *is attained by a integral point, for each* $c \in \mathbb{R}^b$ *for which the maximum is finite.*

Proof. □

So in particular, if P is pointed, then $P = P_I$ if and only if each vertex of P is integral.

6.3 Unimodular transformations and integer polyhedra

Recall that affine images of polyhedra are polyhedra. Clearly the same is true for rational polyhedra and rational affine maps (i.e., affine maps $x \to Mx + t$ for a rational matrix $M \in \mathbb{Q}^{m \times n}$ and a rational vector $t \in \mathbb{Q}^n$). In the previous notes, we have sometimes used affine transformations to obtain a nice representation of polyhedra. For example, up to an affine map we can assume that a polyhedron is full-dimensional. Another example is the Gaussian elimination method. Implicitly, we perform affine transformation when we solve systems using Gaussian elimination. All row operations preserve the space spanned by the rows of the matrix, which ensures us that the solution we find in the affine space spanned by the matrix in row echelon form is also a point in the original space. Further, if we are given rational polyhedron $P \subseteq \mathbb{R}^n$, a linear functional $c \in \mathbb{R}^n$, and a rational affine map $\varphi : \mathbb{R}^n \to \mathbb{R}^n$, then the optimal solutions of $\max\{(\varphi^* c)^T x \mid x \in \varphi(P)\}$ are the affine images of the optimal solutions of $\max\{c^T x \mid x \in P\}$.

However, both properties does not hold anymore if we restrict to integer polyhedra and integral optimal solutions to integer linear programs. In general, the affine image of an integer polyhedron is not integral anymore (shift a segment with integral end points by some non-integral amount). The number of points in $P \cap \mathbb{Z}^n$ for a rational polyhedron P is not invariant under affine maps (Think e.g. of scaling a polyhedron. For any polytope P there is some $\varepsilon > 0$ such that $|P \cap \mathbb{Z}^n| \leqslant 1$.). Hence, finding an integral solution in an affine transform of a polyhedron does not tell us much about integral solutions in the original polyhedron. In the following we want to determine the set of transformations that preserve integrality and the information about integer points in a polyhedron, i.e. transformations that preserve the set $\mathbb{Z}^n$.Transformations defined by unimodular matrices turn out to satisfy all the requirement. Clearly, this is a subset of the affine transformations, so we can write such a map as $x \to Ux + t$ for some $U \in \mathbb{Q}^{n \times n}$ and $t \in \mathbb{Q}^n$. A translation by a vector t preserves $\mathbb{Z}^n$ if only if $t \in Z^n$. Hence, we have to characterize linear transformations U such that $U\mathbb{Z}^n = Z^n$. cf 8-4 in "Polyhedral Geometry and Linear Optimization"

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.